Gestion et surveillance de réseau

July 23, 2014

% Utilisation de syslog-ng pour la gestion des journaux

Objectifs

- Apprendre utiliser syslog-ng pour gérer les journaux syslogs

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 "rtrX>" ou "mysql>") signifient que vous exécutez des commandes sur des équipements à distance, ou dans un autre programme.

Exercices

Veuillez identifier les participants qui utilisent le même routeur que vous, s'il y'en a. Constituez un groupe et faites ensemble l'exercice suivant. Il s'agit de désigner une personne pour se connecter au routeur de votre groupe, mais chacun d'entre vous participera à la configuration effective.

Configurez votre routeur virtuel afin qu'il envoie des messages

syslog à votre serveur :

Vos routeurs sont capables d'envoyer des messages syslog à de multiples destinations, ainsi un routeur peut envoyer des messages à 4 voire 5 destinations différentes. Nous devons donc configurer le routeur pour qu'il envoie des messages à chacun des PC de votre groupe.

Vous allez vous connecter en SSH au routeur de votre groupe et effectuer les opérations suivantes :

```
$ ssh cisco@10.10.X.254
rtrX> enable
rtrX# config terminal
```

Répétez la commande "logging 10.10.X.Y" pour chaque PC de votre groupe. En d'autres termes, si votre groupe est sur le routeur 6 et que vous utilisez les PC 21, 22, 23 et 24 vous répéterez la commande à quatre reprises avec l'IP de chaque machine (10.10.6.21, 10.10.6.22, et ainsi de suite).

```
rtrX(config)# logging 10.10.X.Y
...
rtrX(config)# logging facility local0
rtrX(config)# logging userinfo
rtrX(config)# exit
rtrX# write memory
```

Regardons le résumé de la configuration des journaux (logs) avec 'show logging'

```
rtrX# show logging
```

Déconnectez-vous du routeur (exit)

```
rtrX# exit
```

C'est fait. Le routeur devrait maintenant envoyer des paquets UDP SYSLOG à votre PC sur le port 514. Pour vérifier, ouvrez une session sur votre PC et effectuez l'opération suivante :

```
$ sudo -s
# apt-get install tcpdump   (ne vous inquiétez pas si il est déjà installé)
# tcpdump -s0 -nv -i eth0 port 514
```

Puis demandez à une personne de votre groupe de se connecter au routeur et d'entrer les commandes suivantes :

```
$ ssh cisco@10.10.X.254
rtrX> enable
rtrX# config terminal
rtrX(config)# exit
rtrX> exit
```

Des informations de TCPDUMP devraient s'afficher sur l'écran de votre PC. Celles-ci devraient ressembler à ce qui suit :

```
08:01:12.154604 IP (tos 0x0, ttl 255, id 11, offset 0, flags [none], proto UDP (17), length
    10.10.9.254.57429 > 10.10.9.36.514: SYSLOG, length: 110
    Facility local0 (16), Severity notice (5)
    Msg: 23: *Feb 19 08:01:10.855: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by cisc
08:01:15.519881 IP (tos 0x0, ttl 255, id 12, offset 0, flags [none], proto UDP (17), length
    10.10.9.254.57429 > 10.10.9.36.514: SYSLOG, length: 102
    Facility local0 (16), Severity notice (5)
    Msg: 24: *Feb 19 08:01:14.215: %SYS-5-CONFIG_I: Configured from console by cisco on vty(
```

Vous pouvez maintenant configurer le logiciel de journalisation sur votre PC afin qu'il reçoive ces informations et les enregistre dans un nouvel ensemble de fichiers :

2. Installez syslog-ng

Ces exercices s'effectuent en tant qu'utilisateur root. Si vous n'êtes pas un utilisateur root sur votre machine, vous pouvez le devenir en tapant :

```
$ sudo -s
# apt-get install syslog-ng
```

Éditez /etc/syslog-ng/syslog-ng.conf

Localisez les lignes

```
source s_src {
   system();
   internal();
};
```

et remplacez-les par :

```
source s_src {
   system();
   internal();
   udp();
};
```

Sauvez le fichier et quitter.

Maintant, créez une configuration pour nos logs d'équipement réseau:

```
# cd /etc/syslog-ng/conf.d/
# editor 10-network.conf
```

Dans ce fichier, copier et coller les lignes suivantes:

```
filter f_routers { facility(local0); };

log {
   source(s_src);
   filter(f_routers);
   destination(routers);
};

destination routers {
   file("/var/log/network/$YEAR/$MONTH/$DAY/$HOST-$YEAR-$MONTH-$DAY-$HOUR.log"
   owner(root) group(root) perm(0644) dir_perm(0755) create_dirs(yes)
   template("$YEAR $DATE $HOST $MSG\n"));
};
```

Sauvez le fichier et quitter.

Créez le répertoire /var/log/network/

```
# mkdir /var/log/network/
```

Redémarrez syslog-ng:

```
# service syslog-ng restart
```

Tester syslog

Pour s'assurer qu'il y ait des messages syslog, reconnectez vous au routeur et effectuez des commandes "config", puis déconnectez vous, c'est à dire:

```
# ssh cisco@10.10.X.254
rtrX> enable
rtrX# config terminal
rtrX(config)# exit
rtrX> exit
```

Veillez à vous déconnecter du routeur. Si un trop grand nombre de personnes se connectent et oublient de se déconnecter, d'autres ne pourront pas accéder au routeur.

Sur votre PC, regardez si des messages commencent à apparaître sous

/var/log/network/2013/. . . /

```
$ cd /var/log/network
$ ls
$ cd 2013
$ ls
... ceci vous montrera le contenu du répertoire pour le mois en cours
... faites 'cd' et le nom de ce répertoire
$ ls
... recommencer au niveau suivant (le jour du mois)
$ ls
```

En cas de problème

Si aucun fichier n'apparait sous le répertoire /var/log/network, alors une autre commande à essyer pendant qu'on est loggé sur le routeur, en mode configuration, est de faire un shutdown / no shutdown sur une interface Loopback (locale), par eemple:

```
$ ssh cisco@rtrX

rtrX> enable
rtrX# conf t
```

```
rtrX(config)# interface Loopback 999
rtrX(config-if)# shutdown
```

Attendre quelques secondes

```
rtrX(config-if)# no shutdown
```

Puis quitter, et sauver la configuration (“write mem”):

```
rtrX(config-if)# exit
rtrX(config)# exit
rtrX# write memory
rtr1# exit
```

Vèrifiez les logs sous ‘/var/log/network’

```
# cd /var/log/network
# ls
```

. . . suivre la hiérarchie des répertoires.

Toujours pas de logs ?

Essayez la commande suivante pour envoyer un message de log en local:

```
# logger -p local0.info 'Hello World!'
```

Si aucun fichier n’a été créé sous ‘/var/log/network’, alors vérifier la configuration pour des fautes de frappe. Ne pas oublier de redémarrer le service syslog-ng à chaque fois que vous changez la configuration.

Quelles autres commandes pouvez vous employer sur le routeur (ATTENTION!) qui provoqueront l’envoi de messages syslog ? Vous pouvez essayer de vous loger sur le router et taper un mot de passe incorrect pour “enable”

Assurez-vous de faire un “ls” dans le répertoire de vos logs pour voir si des logs ont été créés à un moment ou un autre.