

# Gestion des journaux - 2ème partie: utilisation de Tenshi

## Gestion & Supervision des Réseaux

### 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.

### Exercices

D'abord assurez vous que vos routeurs sont configurés pour envoyer les logs (journaux) à votre serveur - ceci doit avoir été fait au cours de l'exercice précédent.

#### Mettre à jour la configuration de syslog-ng

Si vous ne l'avez pas encore fait, loggez vous sur votre machine virtuelle et devenez l'utilisateur root:

```
$ sudo -s  
#
```

Configurer syslog-ng pour qu'il réception et sauvegarde les journaux de tout routeur dans un seul fichier, pour faciliter l'inspection et l'analyse:

Éditer `/etc/syslog-ng/conf.d/10-network.conf`,

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

... et ajouter ceci avant la dernière accolade fermante ( }; ):

```
file("/var/log/network/everything", owner(root) group(root) perm(0644));
```

Au final, le contenu de ce fichier doit ressembler à:

```
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"));  
  
    file("/var/log/network/everything", owner(root) group(root) perm(0644));  
};
```

Ceci activera la collecte de TOUT messages syslog qui correspond à la catégorie (facility) local0 et le stockage dans un seul fichier, afin que nous puissions lancer un script de supervision sur ces messages.

Assurez-vous d'avoir sauvé le fichier et quittez l'éditeur.

Redémarrez syslog-ng afin qu'il charge la nouvelle configuration

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

## Rotation des journaux

Créez un script qui effectuera la remise à zéro du fichier des journaux afin qu'il ne devienne pas trop gros (copier & coller).

```
# editor /etc/logrotate.d/everything
```

Ajouter ce qui suit dans le fichier

```
/var/log/network/everything {
    daily
    copytruncate
    rotate 1
    postrotate
        /etc/init.d/tenshi restart
    endscript
}
```

Puis sauvez le fichier et quitter l'éditeur.

## Installation de tenshi

```
# apt-get install tenshi
```

## Configuration de tenshi

Configuration de Tenshi pour que celui-ci vous envoie des alarmes par mail quand le routeur est reconfiguré (copier & coller):

```
# editor /etc/tenshi/includes-available/network
```

Ajouter ce qui suit dans le fichier

```
set logfile /var/log/network/everything
set queue network_alarms tenshi@localhost sysadm@localhost [*/1 * * * *] Log check

group_host 10.10
network_alarms SYS-5-CONFIG_I
network_alarms PRIV_AUTH_PASS
network_alarms LINK
group_end
```

Puis sauvez le fichier et quitter l'éditeur.

Créer un lien symbolique pour que le fichier de configuration de Tenshi soit chargé (copier & coller):

```
# ln -s /etc/tenshi/includes-available/network /etc/tenshi/includes-active
```

Enfin, redémarrer Tenshi:

```
# service tenshi restart
```

## Tester Tenshi

Loggez vous sur votre routeur, et effectuez des commandes “config” diverses (Exemples ci-dessous):

```
$ ssh cisco@rtrX          [où "X" est le numéro de votre routeur]
rtrX> enable
Password: <password>
rtrX# config terminal
rtrX(config)# int FastEthernet0/0
rtrX(config-if)# description Description Change for FastEthernet0/0 for Tenshi
rtrX(config-if)# ctrl-z
rtrX# write memory
```

Ne vous déconnectez pas immédiatement - comme dans les exercices syslog-ng précédemment, effectuez un shutdown / no shutdown de l’interface loopback:

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

attendre quelques secondes

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

Finir et sauvez la config (“write mem”):

```
rtrX(config-if)# CTRL-z          (équivalent à 'exit' 2 fois)
rtrX# write memory
rtr1# exit
```

Vérifiez que vous recevez des mails de la part de Tenshi pour l’utilisateur sysadm. Une méthode de vérification rapide est de regarder dans le répertoire du mail:

```
$ ls -l /var/mail
```

- Note: Tenshi inspecte /var/log/network/everything une fois par minute, donc vous devrez attendre jusqu’à une minute pour que le mail arrive jusqu’à l’utilisateur sysadm.

Assurez vous que vous vous êtes loggés en tant que sysadm (et pas root). Soit vous ouvrez une nouvelle session avec ssh sur votre machine virtuelle, soit vous quittez l’utilisateur root (exit).

Ensuite, faire:

```
$ mutt
```

Utilisez les flèches pour sélectionner un message envoyé par “tenshi@localhost”, puis appuyer sur ENTER pour le lire, et q pour revenir à l’index, et q à nouveau pour quitter mutt.

Si les mails n’arrivent pas, vérifier alors les choses suivantes:

- Les journaux arrivent-ils dans le fichier `/var/log/network/everything` ?

```
$ tail /var/log/network/everything
```

- Ces messages de logs montrent-ils bien un nom de machine tel que ‘rtr5’, voire une adresse IP comme 10.10.5.254 ? Souvenez-vous, tenshi est configuré de telle façon qu’il ne regarde que les noms de machine commençant pas ‘rtr’ ou bien les IP commençant par ‘10.10’ (ceci dépend de la façon dont vous avez configuré tenshi)
- Vérifiez la configuration tenshi. Redémarrer tenshi si vous la modifiez.
- Si vous êtes coincé quand même, demander à un instructeur de vous aider.

### **Faculcatif: Ajouter une nouvelle règle à Tenshi**

Voyez si vous arrivez à ajouter une nouvelle règle à Tenshi pour qu’un email soit envoyé si un individu essaye de faire “enable” sur votre routeur, avec un mauvais mot de passe.

Indices:

- “PRIV\_AUTH\_FAIL” est la chaîne que Cisco IOS utilise dans les messages dans ce cas.
- Pour tester votre nouvelle règle, connectez vous à votre routeur, tapez “enable” suivi d’un mot de passe incorrect.