Log Management Part 2: Using Tenshi

Network Management & Monitoring

Contents

1 Notes

- Commands preceded with "$" imply that you should execute the command as a general user - not as root.
- Commands preceded with "#" imply that you should be working as root.
- Commands with more specific command lines (e.g. "RTR-GW>" or "mysql>") imply that you are executing commands on remote equipment, or within another program.

2 Exercises

First make sure that your routers are configured to send logs to your PC (this should have been done in the previous exercise).

2.1 Update rsyslog configuration

Configure rsyslog to save all router logs in one file for monitoring purposes. Edit `/etc/rsyslog.d/30-routerlogs.conf`, find the line

```
local5.*    -?RouterLogs
```

... and add the following new line immediately after this:

```
local5.*    /var/log/network/everything
```

(but before the line which says '& ~'). So what you should end up with is:

```
# editor /etc/rsyslog.d/30-routerlogs.conf

$template   RouterLogs,"/var/log/network/%$YEAR%/%$MONTH%/%$DAY%/%HOSTNAME%-%$HOUR%.log"
local5.*    -?RouterLogs
local5.*    /var/log/network/everything
& ~
```

This will enable logging of ALL messages matching the local5 facility to a single file, so that we can run a monitoring script on the messages.

Now restart rsyslog:

```
# service rsyslog restart
```

2.2 Log rotation

Create a daily automated script to truncate the log file so it doesn't grow too big:

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

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

(Then save and exit)

2.3 Install tenshi

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

2.4 Configure tenshi

Configure Tenshi to send you alarms when the routers are configured

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

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

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

(Then save and exit)

Create a symlink so that Tenshi loads your new file:

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

Finally restart Tenshi:

```
# service tenshi restart
```

2.5 Testing

Log in to your router, and run some "config" commands (example below):

```
$ ssh cisco@rtrX        [where "X" is your router number]
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
rtrX# exit
```

Just as in the previous exercise, attempt to shutdown / no shutdown a loopback interface

Verify that you are receiving emails to the sysadm user from Tenshi. A quick check is to look in the mail directory:

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

Make sure you are logged in as sysadm (not root), then do:

```
$ mutt
```

Scroll `up/down` to select a message, hit `Enter` to view it, and `q` to quit.

If mails are not arriving, then check the following:

- Are logs arriving in the file `/var/log/network/everything`?

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

- Do these logs show a hostname like 'rtr5'? Remember that the way we have configured tenshi, it only looks at hostnames matching the pattern 'rtr'
- Check your tenshi configuration file. Restart tenshi if you change it.