Network Management & Monitoring

Log management, part II : Using Tenshi

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.

Exercises
---

1. Make sure that your routers are configured to send logs to your PC

2. Configure rsyslog to save all router logs in one file for monitoring purposes:

        # editor /etc/rsyslog.d/99-routerlogs.conf

        - Find the line

        local5.*   -?RouterLogs

        ... and add a new line below:

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

        # editor /etc/logrotate.d/everything

        - In the file add the following:

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

7. Check if Tenshi is already installed in your PC. If not, you can install it with:

        # apt-get install tenshi

8. 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 * * * *] Tenshi
Network Alarms

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

9. Create a symlink so that Tenshi loads your new file:

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

10. Restart Tenshi:

```
        # service tenshi restart
```

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

```
        # telnet 10.10.X.254            [where "X" is your router number]
        rtrX.ws.nsrc.org> enable
        Password: <password>
        rtrX.ws.nsrc.org# config terminal
        rtrX.ws.nsrc.org(config)# int FastEthernet0/0
        rtrX.ws.nsrc.org(config-if)# description Description Change for FastEthernet0/0
for Tenshi
        rtrX.ws.nsrc.org(config-if)# ctrl-z
        rtrX.ws.nsrc.org# write memory
        rtrX.ws.nsrc.org# exit

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

12. Verify that you are receiving emails to the sysadmin user from Tenshi

```
        $ su - sysadmn
        $ mutt -f /var/mail/sysadm
```