

% Log Management Part 2: Using Tenshi

%

% Network Monitoring & Management

## # 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

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

### ## Update rsyslog configuration

If you have not already done so, log in to your virtual machine and become the root user:

```
~~~~~  
$ sudo bash
```

```
#  
~~~~~
```

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

Edit ``/etc/rsyslog.d/30-routerlogs.conf``,

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

... and find the line

```
~~~~~  
local0.*      -?RouterLogs  
~~~~~
```

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

```
~~~~~  
local0.*      /var/log/network/everything  
~~~~~
```

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

```
~~~~~  
$template RouterLogs,"/var/log/network/`${YEAR}/${MONTH}/${DAY}/${HOSTNAME}-${HOUR}.log"  
local0.*    -?RouterLogs  
local0.*    /var/log/network/everything  
& ~  
~~~~~
```

This will enable logging of ALL messages matching the local0 facility to a single file, so that we can run a monitoring script on the messages.

Be sure to save and exit from the file.

Now restart rsyslog so that it sees the new configuration:

```
~~~~~  
# service rsyslog restart  
~~~~~
```

```
## Log rotation
```

Create a daily automated script to truncate the log file so it doesn't grow too big (COPY and PASTE):

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

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

Then save and exit from the file.

```
## Install tenshi
```

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

```
## Configure tenshi
```

Configure Tenshi to send you alarms when the routers are configured (COPY and PASTE):

```
~~~~~  
# 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 from the file.

Create a symlink so that Tenshi loads your new file (COPY and PASTE):

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

Finally restart Tenshi:

```
# service tenshi restart
```

## Testing Tenshi

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
```

Don't exit from the router yet. Just as in the previous rsyslog exercises, attempt to shutdown / no shutdown loopback interface:

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

wait a few seconds

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

Then exit, and save the config ("write mem"):

```
rtrX(config-if)# ctrl-z          (same as exit, exit twice)
rtrX# write memory
rtrX# exit
```

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). Either open a new session to your virtual machine, or exit from the root user (exit). Then do:

```
$ mutt
```

~~~~~

Scroll `up/down` to select a message from "tenshi@localhost", then press  
`ENTER` to view it, and `q` to quit and 'q' again to quit mutt.

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.

\* If you are still stuck ask an instructor or a neighbor for help.

## Optional: Add a new Tenshi rule

See if you can figure out how to add a rule to Tenshi so that an email is  
sent if someone enters an incorrect enable password on your router.

Hints:

\* "PRIV\_AUTH\_FAIL" is the Cisco IOS log message in such cases.

\* To test your new rule log in to your router, type "enable" and then enter  
an incorrect enable password.

\* Note: Tenshi checks /var/log/network/everything once a minute, so you may  
have to wait up to a minute for the email to arrive to the sysadm user.