

Re: Better Syslog server

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2003-03/0024.html>

From: Jameel Akari (jakari@bithose.com)

Date: 03/17/03

Date: Mon, 17 Mar 2003 14:08:08 -0500 (EST)
From: Jameel Akari <jakari@bithose.com>
To: Matt Harris <mdh@unix.si.edu>

On Mon, 17 Mar 2003, Matt Harris wrote:

> *I've been looking a bit on google/sourceforge/etc to try and find a more
> configurable and extensible syslog server, to no avail. Does anyone*

There is syslog-ng, but IMO it's still lacking.

```
> # commands for syslog facility "XXX"
> Facility XXX {
> # Send message to stdin of a script which can send alerts, etc
> Severity emerg ACTION /usr/local/libexec/parse-emerg.sh
> # 192.168.47.9 - sample dhcp server
> Host "192.168.47.9" {
> # log stuff from the dhcp server to a separate file
> Severity warn FILE /var/adm/dhcp.log
> }
> # send other stuff to a default file
> Severity DEFAULT FILE /var/adm/xxx.log
> }
```

Looks like a good idea to me.

> *functionality I'd like - for example, piping out to a smart script,
> sending to different files based on host that sent the message, etc*

Logging to a [My|Postgre]SQL backend instead of or in addition to file would be very cool. Stick a PHP frontend on it and make pretty charts and graphs.

Doing things like "tail -f /var/adm/messages | someparserscript.pl" kinda works, but is... non-optimal?

```
--
#!/jameel/akari
sleep 4800;
make clean && make breakfast
```