



PROFESSIONAL SERVICES TECH NOTE #040

Syslog Forwarding

The Concept

System Log (syslog) Forwarding is a means for consolidating log files for multiple systems (NetApp storage or any other system) on a single server. These consolidated logs are then easier to monitor and provide custom alert notification. To enable syslog forwarding you must edit the `/etc/syslog.conf` file.

Example syslog.conf entry

```
# Log all kernel messages, and anything of level err or higher to the console.
*.err;kern.* /dev/console
# Also log console messages to a remote loghost system called adminhost.
*.err;kern.* @adminhost
```

Note: The NetApp syslog.conf file uses the same syntax as most Unix/Linux distributions so this example is applicable on other client systems.

What It Means To You

Systems logs contain a wealth of information but are ignored by a large majority of storage admins even though they are included in the weekly AutoSupport email. Log files take a lot of time to read and valid error messages and warnings are buried in hundreds of benign or false warning messages. Combining log files provides a better picture of overall health of entire infrastructure. Mining log files with tools like Swatch and Kiwi provide an extra layer of monitoring and reporting. These tools differ from SNMP monitoring because they are tuned to ignore routine messages and alert when something unexpected occurs. SNMP tools only look for expected events.

More Information

The Manual Pages for the syslog.conf file:

http://now.netapp.com/NOW/knowledge/docs/ontap/rel727/html/ontap/cmdref/man5/na_syslog.conf.5.htm

More information about the log monitoring and mining applications:

<http://partners.netapp.com/go/techontap/swatch-kiwi.html>

Brought to you by NetApp Americas Professional Services

Send comments, corrections & suggestion to Michael Cope at mcope@netapp.com
Tech Note archive: http://communities.netapp.com/community/products_and_solutions?view=documents