

Re: Aggregating logs from numerous FreeBSD machines

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-01/0045.html>

From: Stanley Hopcroft (*Stanley.Hopcroft_at_IPAustralia.Gov.AU*)

Date: 01/14/05

Date: Fri, 14 Jan 2005 18:54:37 +1100

To: freebsd-security@freebsd.org

Dear Folks,

On Thu, Jan 13, 2005 at 04:39:11PM –0800, Ted Cabeen wrote:

> *Mark Johnston <mjohnston@skyweb.ca> writes:*

>

> > *Hi folks,*

> >

> > *My stack of trusty FreeBSD servers always seems to be growing, and it's
> > getting to the point where the daily and security output mail is too much to
> > make good use of. I'm looking for suggestions for log monitoring and
> > aggregation tools, especially from a monitoring–for–security perspective.*

> >

.. snip ..

>

> *syslog–ng is useful for separating incoming log entries by server,
> facility and priority. I'd start with that. You could then use
> something like logwatch or logcheck to mail you or trigger a nagios
> warning on strange log lines.*

>

a helpful way of looking at the problem may be

1 data collection/aggregation

log forwarding is the way to go (there is free code to forward events from MS event logs to syslog [these are Win binaries] for collecting all events.

Mr Cabeens suggestion of using the better classification of syslog–ng sounds very helpful on the host that is collecting the syslog'd events.

2 event correlation and or filtering.

FreeBSD–Security: Re: Aggregating logs from numerous FreeBSD machines

Programs like logsurfer and swatch can be used to react to stimuli in the event stream (ie the logs being tailed) and react by forking shell scripts, mailing, highlighting the message on a viewer etc.

The SourceForge project SEC can analyse multiple log files (the number is probably limited by the resources of your analysis/logging host) and do the above + process events (ie messages that occur with a particular time sequence eg within an interval of one another, or after a message ...)

SEC also does useful things such as compression (ie many stimuli one response).

Actively developed. Junk free mail list.

Mr John Rouillard gave a paper on SEC at the last LISA conference (Boston ?).

SEC like Swatch is a Perl application and the rules can use arbitrary in-line Perl code.

People use it for lots of things including real time Snort log analysis.

Lastlu, I am not sure if the name is a conscious pun, but SEC is absolutely completely unrelated to the Tivoli TEC product. If you appreciate, TECs capabilities you'll do more with SEC and have more fun (unless you happen to love Prolog and rules based processing).

Yours sincerely,

--

Stanley Hopcroft
IP Australia
Ph: (02) 6283 3189 Fax: (02) 6281 1353
PO Box 200 Woden ACT 2606
<http://www.ipaustralia.gov.au>

--

This message contains privileged and confidential information only for use by the intended recipient. If you are not the intended recipient of this message, you must not disseminate, copy or use it in any manner. If you have received this message in error, please advise the sender by reply e-mail. Please ensure all e-mail attachments are scanned for viruses prior to opening or using.

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"