

Re: Aggregating logs from numerous FreeBSD machines

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-01/0038.html>

From: Chuck Swiger (cswiger_at_mac.com)

Date: 01/13/05

Date: Thu, 13 Jan 2005 13:43:40 -0500
To: Mark Johnston <mjohnston@skyweb.ca>

Mark Johnston wrote:

- > *If I had to imagine an ideal system, it would be a central server that*
- > *securely collects syslog messages from all my servers, indexes them by server*
- > *and severity, and gives a reasonable management interface. Given expressions*
- > *based on facility, severity, log message, and the like, it could throw away*
- > *useless messages, or page me for critical ones. This would tie into*
- > *AIDE/Samhain/Tripwire (haven't picked one yet) and maybe even different*
- > *flavors of IDS. It could even warn me when processes run away with the CPU*
- > *or RAM, or disks get too full.*

Consider Big Brother from www.bb4.com. It monitors processes, ports, disk space, load average, looks for interesting stuff in the system logfile, and has a central web-based dashboard with historical logs.

[Slightly off-topic for freebsd-security, moving to -questions.]

--

-Chuck

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"