

Firewall-Wizards: Re: [fw-wiz] (no subject)

Re: [fw-wiz] (no subject)

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-03/0112.html>

From: Devdas Bhagat (devdas_at_dvb.homelinux.org)

Date: 03/23/04

To: firewall-wizards@honor.icsalabs.com

Date: Tue, 23 Mar 2004 19:59:04 +0530

On 23/03/04 08:42 +0000, Hilal Hussein wrote:

>

> *Dear List,*

>

> *i have cisco pix firewall that is sending it log data to a cisco syslog*

> *server (windowsxp workstation).*

Why not use a Linux/Unix syslog box?

> *it is working fine with me since it is a service, so i will be sure that it*

> *is running whenever the server is up and running.*

>

> *But i have two questions concerning this syslog:*

> *1 – the log files are too big since everyfile contains the whole day logs,*

> *and since the file size is about 400 + Mb, i am not able to open it. kindly,*

> *is there any third party utility which i can use to manage (open, check,*

> *filter,) the log files of the cisco syslog?*

400 MB of data is not all that much for a dedicated Syslog server to handle.

Repeat after me, Perl is your friend.

(If not Perl, choose your flavour of scripting language).

Devdas Bhagat

firewall-wizards mailing list

firewall-wizards@honor.icsalabs.com

<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>