

Re: Force newsyslog to rotate from custom script

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2004-05/0924.html>

From: Lowell Gilbert (freebsd-questions-local_at_be-well.ilk.org)

Date: 05/12/04

To: Barbish3@adelphia.net

Date: 12 May 2004 09:53:10 -0400

please.

top-post,

Don't

> -----Original Message-----

> From: lowell@be-well.ilk.org [<mailto:lowell@be-well.ilk.org>] On

> Behalf Of Lowell Gilbert

> Sent: Wednesday, May 12, 2004 8:54 AM

> To: Barbish3@adelphia.net

> Cc: freebsd-questions@FreeBSD.ORG

> Subject: Re: Force newsyslog to rotate from custom script

>

> "JJB" <Barbish3@adelphia.net> writes:

>

>> Problem description: My ipfilter log is rotated using

>> newsyslog.conf. The file is rotated on file size option. I have

>> custom script that reads the log and builds email containing list

>> of

>> abusive source IP address. This custom script is included in the

>> daily management report process. Problem is that on days that

>> there

>> is a lot of blocked traffic the log may rotate multiple times and

>> my

>> daily management report script only runs against the current

>> active

>> log.

>>

>> Is there some way to keep the log defined in newsyslog.conf

>> without

>> any rotate option and add something to my custom script to tell

>> newsyslog to rotate the log after the script has processed the

>> current active log file?

>>

>> I would recommend a slightly different approach. Either of a couple

>> of different approaches, in fact...

>>

>> One way to do this would be to use a separate config file for

freebsd-questions: Re: Force newsyslog to rotate from custom script

- > *newsyslog(8)* rather than */etc/newsyslog.conf*. Then you run
- > *newsyslog*
- > and use the *-f* option to have it use your special-purpose
- > configuration just for rotating this *ipfilter* log.
- >
- > The other way would be to do the rotation directly, in your script
- > which processes the file. It should only take three or four
- > commands
- > in the script. That would let you more or less eliminate any race
- > conditions that might leave data out of your logs.
- >
- > _____
- > *freebsd-questions@freebsd.org* mailing list
- > <http://lists.freebsd.org/mailman/listinfo/freebsd-questions>
- > To unsubscribe, send any mail to "*freebsd-questions-unsubscribe@freebsd.org*"
- >

"JJB" <Barbish3@adelphia.net> writes:

- > Thanks for your reply
- >
- > Both of your suggestions are good but have the same problem.
- >
- > When the *newsyslog* command is run the rotate space trigger in
- > *newsyslog.conf* may or may not be met.

If your script does the rotation itself, it will know whether and when the rotation occurred.

- > I need an return code or exit code from the *newsyslog* command to
- > check to tell if trigger was met and log really rotated.
- >
- > Does *newsyslog* issue such codes and how would I code an *csh* script
- > to check for it?

That's not available; *newsyslog* is intended for handling multiple files, which would make such an exit code indeterminate. You could get fairly close by running *newsyslog* in verbose mode and parsing out the result.

- > Trying to for see an DOS attack targeted at consuming all the log
- > disk space in */var*

If you just put */var/log* on its own filesystem, such an attack wouldn't hurt you much even if it managed to fill up the filesystem.

freebsd-questions@freebsd.org mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>
To unsubscribe, send any mail to "*freebsd-questions-unsubscribe@freebsd.org*"