

[HPADM] SUMMARY: syslog redirection

Source: <http://unix.derkeiler.com/Mailing-Lists/HP-UX-Admin/2006-01/msg00009.html>

- *From:* Timothy A Reed <treed21@xxxxxxx>
 - *Date:* Wed, 11 Jan 2006 08:13:56 -0700
-

Original question is at the bottom of this email. Thanks to:

Susan Pellerito
Mike Keighley
Bill Hassell
Martin Lodahl
David Lodge

All reminded me that since syslog communicates using UDP, if the central server is down, entries will be lost. And most suggested keeping the entries locally as well as sending to the central server so they will be available if needed.

Most complete answer was from David Lodge:
Yes.

Syslog sends over UDP on a "broadcast and forget" concept. If there's nobody to receive or the packet gets snarled up in the network traffic then the message is lost.

There are ways to mitigate these issues:

1. Use some form of HA clustering to ensure that there is always a log server available
2. Try and site the syslog server on the same subnet as your major production systems (so traffic doesn't have to route through the network core and minimises the risk of traffic loss)

If you're going ahead with this I would suggest having a look at syslogng as this allows a lot more filtering techniques than standard syslogd (e.g. load all syslogs directly into a database)

Thanks,
Tim Reed
Computer Scientist
Computer Sciences Corporation
treed21@xxxxxxx

[HPADM] SUMMARY: syslog redirection

Please note that this e-mail, including any attachments, contains information that is subject to United States laws and regulations. The use or further dissemination of these materials or information therein may be prohibited by United States law.

This is a PRIVATE message. If you are not the intended recipient, please delete without copying and kindly advise us by e-mail of the mistake in delivery. NOTE: Regardless of content, this e-mail shall not operate to bind CSC to any order or other contract unless pursuant to explicit written agreement or government initiative expressly permitting the use of e-mail for such purpose.

----- Forwarded by Timothy A Reed/GIS/CSC on 01/11/2006 08:04 AM -----

Timothy A Reed
/GIS/CSC To: hpux-admin@xxxxxxxxxxxxxx
cc:
01/10/2006 12:00 Subject: syslog redirection(Document link: Timothy A Reed)
PM

I'm being asked to route syslog messages to a central server. I know how to configure syslog.conf to do that. My question is: what happens if the central server is down or the network is unavailable? Will the message forwarding just be lost (on the central server) or will they queue up on the local server for later delivery? Will any additional messages be logged to the local server about the communication failure?

Thanks,
Tim

Thanks,
Tim Reed
Computer Scientist
Computer Sciences Corporation
treed21@xxxxxxx

Please note that this e-mail, including any attachments, contains information that is subject to United States laws and regulations. The use or further dissemination of these materials or information therein may be prohibited by United States law.

This is a PRIVATE message. If you are not the intended recipient, please delete without copying and kindly advise us by e-mail of the mistake in delivery. NOTE: Regardless of content, this e-mail shall not operate to bind CSC to any order or other contract unless pursuant to explicit written agreement or government initiative expressly permitting the use of e-mail for such purpose.

--
--> Please post QUESTIONS and SUMMARIES only!! <--
To subscribe/unsubscribe to this list, contact majordomo@xxxxxxxxxxxxxx
Name: hpux-admin@xxxxxxxxxxxxxx Owner: owner-hpux-admin@xxxxxxxxxxxxxx

Archives: ftp.dutchworks.nl:/pub/digests/hpux-admin (FTP, browse only)
<http://www.dutchworks.nl/htbin/hpsysadmin> (Web, browse & search)

- Prev by Date: [*\[HPADM\] syslog redirection*](#)
- Next by Date: [*\[HPADM\] SUMMARY RE: Glance showing 100% disk I/O utilization incorrectly*](#)
- Previous by thread: [*\[HPADM\] RE: Glance showing 100% disk I/O utilization incorrectly*](#)
- Next by thread: [*\[HPADM\] SUMMARY RE: Glance showing 100% disk I/O utilization incorrectly*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)