

Re: What logs etc do I need to check frequently?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2003-12/2669.html>

From: Scott W (wegster_at_mindcore.net)

Date: 12/28/03

Date: Sun, 28 Dec 2003 13:09:23 -0500

To: Chuck Swiger <cswiger@mac.com>

Chuck Swiger wrote:

> Joachim Dagerot wrote:

>

>> As you with good memories know, I lost 3000 pictures of my first sons
>> first year this month. I did have a RAID-5 system with fresh disks,
>> however, shit happens and I have a feeling that this could have been
>> avoided if I read my log files better.

>

>

> I'm sorry that you lost data.

>

> While you may have been able to notice the problem with the RAID-5 array
> in time to do something, what you ought to do to avoid losing more data
> sometime in the future involves making good backups-- not poring over
> the system log files, not configuring RAID.

>

>> So basically,

>> a) I get a mail each time my a cron-event fires, this happens every 30
>> min so the mailbox are quite loaded, not very funny going through.

>

>

> If you can, change the cron task to not generate output unless there is
> a problem that you should know about. Failing that, append "> /dev/null
> 2>&1" to the line in your crontab, which will discard the output,
> meaning you won't get mail from cron.

>

>> a1) Is it possible to only get a mail with critical information, where
>> and what do I need to do to achieve this?

>

>

> My comments above should help you reduce the amount of junk mail you get
> from cron.

>

>> b1) Where will information about ongoing disk-problems appear? How can
>> I see that there is a flaky disk in a non-rebooted system?

>

freebsd-questions: Re: What logs etc do I need to check frequently?

>
> /var/log/messages. The system will complain quite noticeably in the face
> of hardware errors, and should log one or more lines for every bad
> sector it runs into.
>
> On the other hand, depending on the hard drive to fail gradually is
> risky: hard drives can fail catastrophically without giving significant
> warning. Some failure modes-- stiction in particular-- can sometimes be
> worked around on a temporary basis long enough to recover data without
> heroic measures (ie, paying a data recovery company a few grand).
>
> It's important to realize that while RAID modes which provide
> fault-tolerance do improve availability (ie, they can save your data if
> a drive goes), RAID is not a substitute for backups. In particular,
> RAID-5 or RAID-1 doesn't help a bit if someone deletes or overwrites a
> file....
>
>> In addition to the questions above, is there something else I need to
>> tune/install/setup/configure to get a very reliable system that
>> report critical data to me but where non-critical data is filtered
>> out?
>
>
> /etc/syslog.conf defines the configuration of system logging, and it is
> worth reviewing that to understand what is being logged and where.
>

Just to add my .02c here-- all of the above is excellent advice, and I think someone else already mentioned logcheck, which can be useful for other things as well (port scanning, Nimda attacks (which are STILL out there), and others)...I guess my only disagreement here is about RAID or disk vs tape backups. At this point, it's generally more inexpensive to buy a secondary disk, or even a RAID setup. than to go with tape. Tape itself isn't a guaranteed medium by any means...meaning there have been times I've gone to backup from tape to then find out it was a less than full backup or data was corrupted on the tape. I won't even get into tape drive issues where you write data on one unit and a different tape drive won't read the same tapes, other than to say it happens.

If you've got data that doesn't change often (ie like your pictures), and only grows, you've got a few options:

1. Set up a RAID-5 array. IMPORTANT-- designate at least one hot spare! If your main use is for backup, you can go with an older SCSI solution, but if so, I highly recommend using a RAID enclosure (with backplane, not a 'homemade' cabled setup-- older SCSI (scsi2, UW, etc) is pretty picky about cable length, and using an external cabled enclosure can cause read or write errors and other issues (dropping a drive offline). Fiber channel or older scsi hardware RAID solutions can be had on eBay for pennies on the dollar right now.. Note that I'm talking about hardware RAID here...software RAID is slower (generally), and IMHO just

Re: What logs etc do I need to check frequently?

freebsd-questions: Re: What logs etc do I need to check frequently?

not as reliable...yet.

You can use the setup as a 'live data logical drive,' and if you're overly paranoid, do a scheduled tar archive (or other means of backup, but with tar you can add the incrementals to your archive) to the drives, or to an alternate drive, as well.

2. Buy a secondary IDE disk, sized at least 2x the size of your data to allow for growth. Do NOT use this drive for anything other than backup, eg mount the drive as /backup and only use it for (cronned) data dumps.

You'll only be writing and reading to the drive occasionally, and as such, you should have a reasonably decent length of time the drive will work for, meaning it's likely to get replaced during upgrades years from now before the drive itself fails. Large IDE disks are getting insanely inexpensive...

DLT drives in the 15gb(uncompressed) range are < \$100, but as usual, become progressively more expensive as you go larger in size, with a 40gb running ~\$300-\$500+. Anything larger in tape backup you're going to pay through the teeth. (100gb = min \$1k on up) You can get a 100GB RAID array with enclosure/hardware RAID with a SCSI or Fiber Channel interface for ~200-\$500 (10-14 drives, set 2 hot spares if you'd like), and a scsi or HBA card for ~\$50. A fair number of businesses are also moving to 'disk backup' via SAN storage....

Anyways, just something else to think about- nothing against tape (ok, except they're slow and \$\$ by comparison)..

And yes, I practice what I preach - both my live and backup filesystems are on a 14 disk fiber channel array with 15k RPM FC Seagate Cheetahs in a EuroLogic enclosure...I've got a second one that in time may become backups only with more hot spares.

Scott

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"