First Five Minutes on a System

What to do and why

Guidelines and Ideas
No hard rules…
Started writing at 4:21pm Jan 21

Please feel free to POLITELY comment

** means a real life example with names removed for reasons

Server vs Desktop vs Router vs Device vs Other

- Server might have lots of services
- Desktop might have overly tweaked configs
- Router might be out of logging space
- Device might have corrupt storage medium

Different actions depending on scope. There is not generic item that will instantly report what issues might exist. Understand the environment and business need for the device. More than one issue could be present and distract you from seeing the whole picture.

** Raspberry PI - Over logging and partition full, SD card is over “write limit”.

Motivation

We all get escalations… Maybe it is a family computer, maybe it is a production service. For whatever reason we want to fix the issue and often don’t have time or resources to toss more hardware at the problem. Using Linux we can do a great deal of validation that is non-destructive. Some Operating Systems have very cumbersome tools that make troubleshooting an issue. Example might be a corrupt registry on a Microsoft Windows OS.

** 20 years of accounting is on here and this is the only backup….

The real world

You will never be asked to look at something configured well. The desktops or servers that we are asked to review are often barely standing or insecure. If you want to enable an architecture that requires no trouble shooting we shall have another talk.

Great systems are a lot of work. http://sts.ono.at/blog/2012/02/01/a-systems-policy/

** It must be a hacker our systems are perfect.

What to do first after smelling for smoke?

Regardless of what is broken there are some simple things to check.

- df
- date
- dmesg

** I think it is the cat-warmer2000 service that is causing all the trouble, oh, wait out of disk space.

df (-h means human readable)

What mounts are mounted?

Are any full?

Are any surprisingly empty?

Are any missing?

Any storage space left to work with?

```
lathama@lappy7:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1       113G   11G   96G  11% /
udev             10M     0   10M   0% /dev
tmpfs           1.6G   18M  1.5G   2% /run
tmpfs           3.8G  124M  3.7G   4% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           3.8G     0  3.8G   0% /sys/fs/cgroup
tmpfs           769M  8.0K  769M   1% /run/user/1000
```

df Part 2

If unsure, compare to mount

Does it look sane?

** mount causes a kernel crash, run, just run….

```
lathama@lappy7:~$ mount

sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)

proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)

udev on /dev type devtmpfs (rw,relatime,size=10240k,nr_inodes=981721,mode=755)

devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)

tmpfs on /run type tmpfs (rw,nosuid,relatime,size=1574484k,mode=755)

/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)

<snip>
```

date

Having an incorrect date is a huge issue. This could make things fail like DHCP, NFS, Web Browsing, TLS/SSL and many many more.

```
lathama@lappy7:~$ date

Thu Jan 21 16:33:40 CST 2016

lathama@lappy7:~$ ntpq -p

     remote           refid      st t when poll reach   delay   offset  jitter

==============================================================================

 bisesa.kakaopor 74.117.214.2     2 u    1   64    1   58.894   -0.407   0.537

 resolver2.level 10.67.8.18       3 u    -   64    1   36.579   -2.468   0.078

 ntp.newfxlabs.c 128.9.176.30     2 u    4   64    0    0.000    0.000   0.000
```

** We set it to that date to avoid the license fee

dmesg or kernel ring buffer

An in memory log that survives in memory in the case that the system logging functions are not working, started or other.

Output Way to noisey to paste here…. Everyone read the manual page as new features to this old tool make it much better

** The HDD is fine, that kernel error is a mistake

Solid ground, now we can get to work

- uptime
  - You want to see 0 - 60 days, anything else is just scary
  - Updates happen, or they should
- free -h
  - RAM NOM NOM NOM << Cookie Monsters cousin Data Dragon
- top
  - Load average is not a percentage - can be 4000.00
  - swap usage shown
- cd /
  - Look for cores and maybe /var/cores on some systems

** Our 1000 days of uptime means we know what we are doing (system does not survive a reboot)

Logs are your friends

Do a “ls -lha /var/log” and see if there are recent logs, and validate they are current with “date”. If the file descriptors are not up to today there is a larger issue.

** Custom log configure to implement magical unicorn fart features disabling all logs.

Validating Packages - First need of root or sudo!!!

Manual changes, security concerns or other, simple solution

apt-get install --reinstall $(dpkg --get-selections |grep -v deinstall)

or

yum reinstall $(yum list installed | awk '{print $1}')

** All our packages are up-to-date and we trust bob who repackages all the Distro packages to fix their stupid mistakes.

Tools to not use..

Some tools are not commonly installed on all systems. So it can be frustrating to rely on them. It is best to learn to use the lowest common denominator to troubleshoot systems with. Tools like **sar**, **mpstat**, **iostat**, and **pidstat** from Netflix' s article are not installed on my laptop for example.

** We use an inhouse developed validation tool written in COBOL and we paid a lot of money for it so use it...

Defense of the stupid user….

Who is accessing the system? Who has accessed the system recently? Who should not be accessing the system right now?

passwd, w, last, who, wall and many many more. Resetting all users passwords is ALWAYS an option and should never be ignored as an option (unless directory service).

** Live tracking a user who was fired deleting files on a system in the 90s

Wall

wall “System is going down for reboot in 2 minutes.”

^^^^^^^^

This will find the user 95% of the time… you will hear a WTF or grunt...

5 minutes has been up for a while...

You should have…

- Determined if the system is on fire.
- Documented problem
- Acknowledge that the system owner is not willing to do the right thing