Server Technology

Benjamin Brewster

Why You Need to Care

- Because someday you'll have to:
  - Recover from a business-ending, lawsuit-inducing virus
  - Set up hard drives in a redundant manner
  - Plan for interrupting notifications
  - Handle power outages, earthquakes, and floods

Essential Technologies

- Backups
- RAID
- UPS
- Notifications
- Logs
- Environmental concerns

Backups

- Practically speaking, no technology, no system, no policy, and no methodology is more important than having a backup that is:
  - Frequent
    - Must occur often enough to catch changes
  - Comprehensive
    - Has to cover everything
  - Accessible
    - The best backup in the world is useless if it takes too long to download or mail
  - Verifiable
    - It needs to report its success or failure loudly, and the backup needs to be tested
  - Secured
    - If the backup is used for any kind of work, it's not a backup
    - Needs to be stored off-site, away from bad guys, safe from the environment

Backups - a Case Study

BAD

WORSE

- A large tax prep firm client of mine once had a lower-level employee browse Facebook on a company computer...
- ...who clicked a bad link...
- ...and got a cryptographic ransomware (cryptoware) on her PC...
- ...which encrypted all named/lettered drives on her PC: C:, D:, etc...
- ... including the company network share, which was mapped as Z:

Backups - a Case Study - to the Rescue

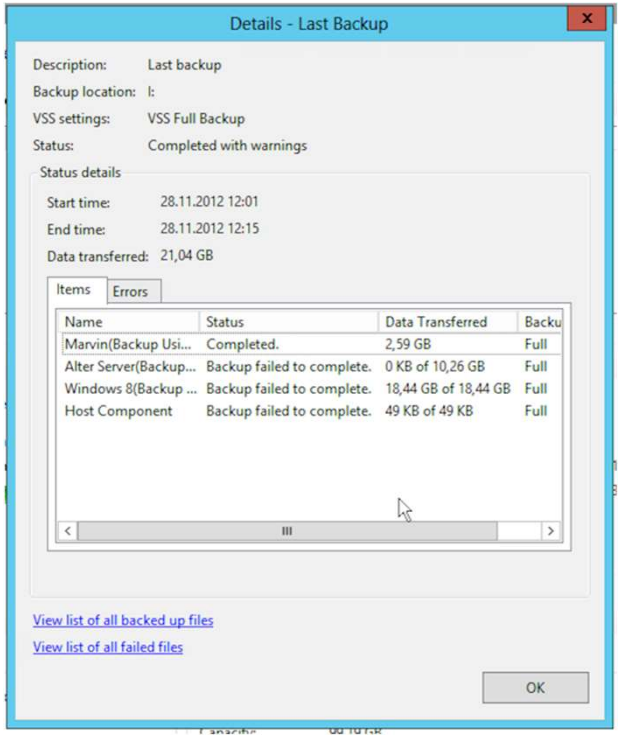
- The cryptography was not beatable, and the process ran as fast as it could on the server: we were able to observe its progress before we killed it

- The only reason our client is still in business today is because we had nightly backups of the company server, where all data was stored

- We sure as heck weren't going to pay some *jerk* ransom money
  - FYI, nearly all of the cryptoware authors remain uncaught

Windows Backup

- Windows Server has a great backup tool built in!
- Other backup tools include Acronis, Veeam, ShadowProtect, and a ton of others
- Windows PC has a built-in backup client called File History
  - Fundamental issue is: if a USB or network drive is connected to your PC, you could lose it too, to a virus, flood, power surge, etc.; thus, that's not a valid backup
- I have tested lots of them: Carbonite, Dropbox, iDrive, Shadow Protect PC, Google Drive, Box
  - My favorite is Dropbox



Backup System Classification

- Dropbox, Box, etc. are not actually backup clients, but they are close
  - They're file versioning and sharing systems: previous versions of files often are only available for a month, so you better hope you notice a virus before then!
- `git` is not a backup client, though it has similarities
  - It's a version control system
- *Long-term* storage is properly called an archive: these should be periodically transferred off-site

Linux, Mac Backup, and Images

- Linux backup is not built in, but there are lots of clients
- Old-school techniques include rsync that are still widely used
  - Easy to set up in a cron job:
  - `$ rsync -avzh /root/mycoolfiles /fileserver/mount/mycoolfiles5-5-2018`

- macOS uses Time Machine, a backup utility that keeps snapshots of your files and system state
  - Not designed to keep these as long-term, off-line archives

- Images are a way to restore the entire computer back to an earlier state, just like restoring to a particular snapshot in VirtualBox
  - Famous applications include Ghost, Acronis, ShadowProtect, and Paragon
  - Images are normally kept as differentials: one master image is taken, and then "deltas" are taken that only record what has changed

Why Spend Time Talking About Backups?

- To conclude this topic: your primary task is *business continuity*
- If you fail at this, you will have failed at your entire job

RAID

- **R**edundant **A**rray of **I**ndependent **D**isks combines multiple drives into one (or more) big ones for performance improvement or redundancy
- Difficult to simulate in a VM

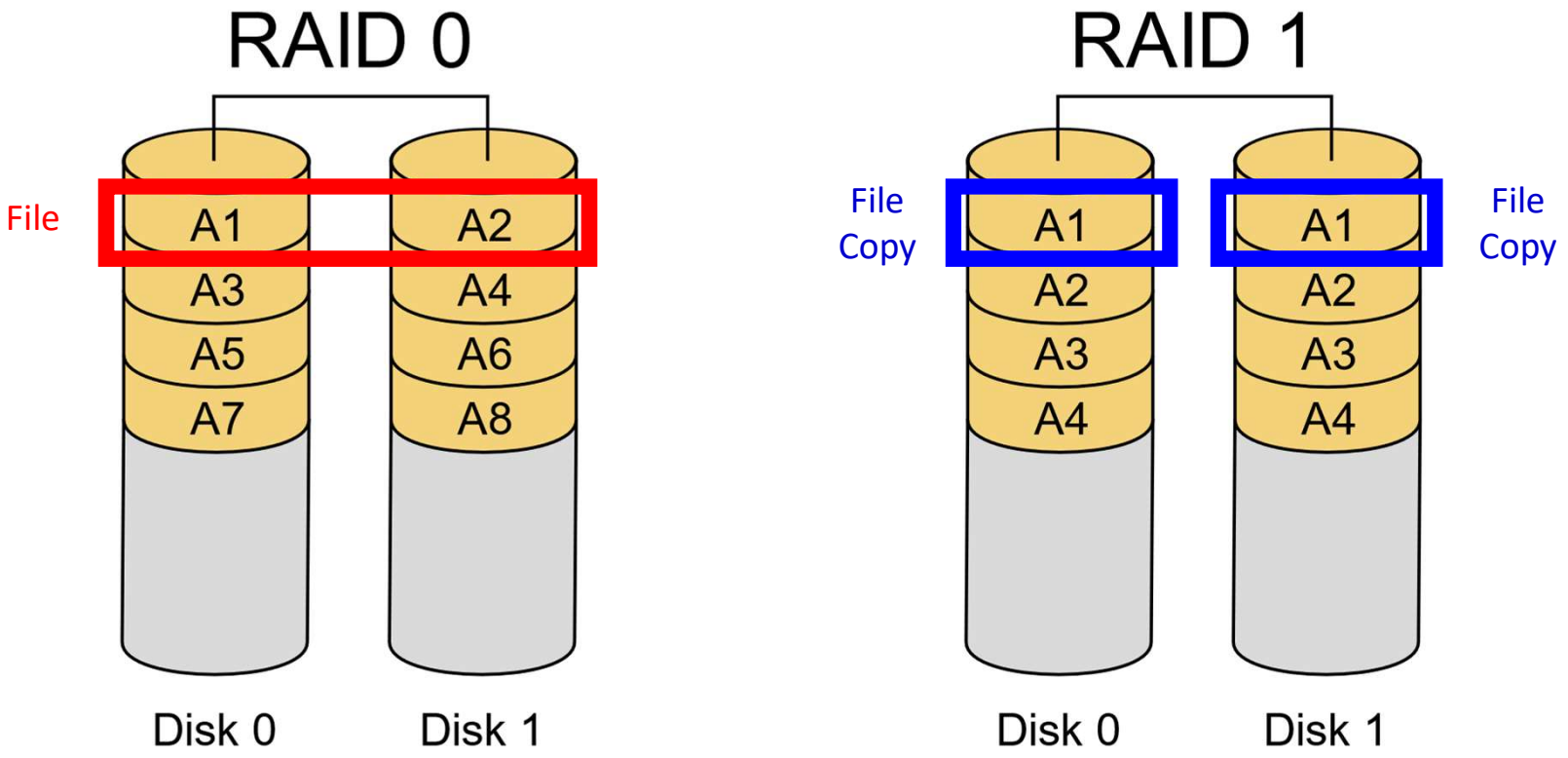
- Designed to provide fault tolerance with inexpensive disks

- To the OS, these arrays appear as single disks (or multiple partitions), not as the component hard drives

Standard RAID Levels

- **RAID Level 0: Striping** - Each file is distributed across multiple disks. Throughput is multiplied by number of disks at the cost of 100% vulnerability by losing any one lost drive: if a drive drops, the whole array is lost.
- **RAID Level 1: Mirroring** - Each file is written to two drives, not just one. Reading is done from whichever drive responds fastest. Large reads can be streamed from multiple drives, approaching RAID 1 speeds, but still limited to fastest drive. Writing speed is limited to slowest drive, as all have to be updated. Works as long as any drive still functions.

Standard RAID Levels

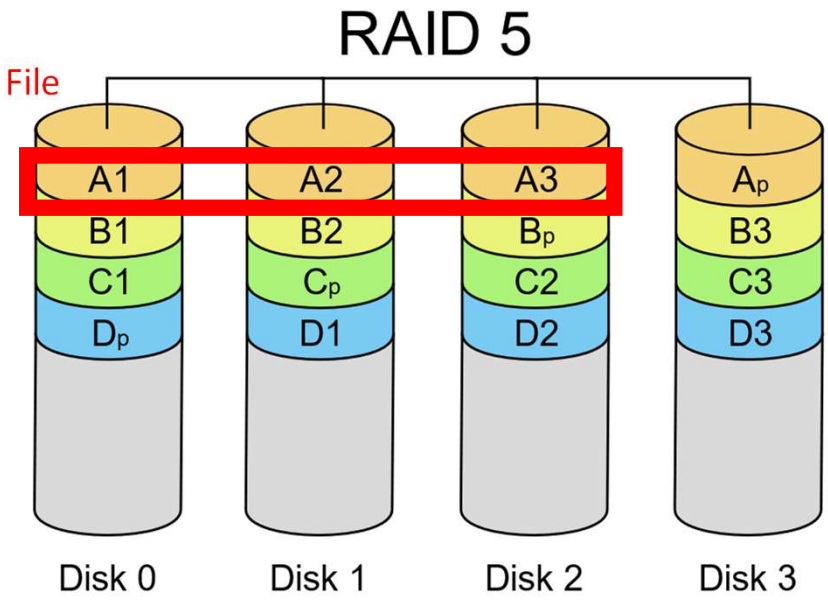


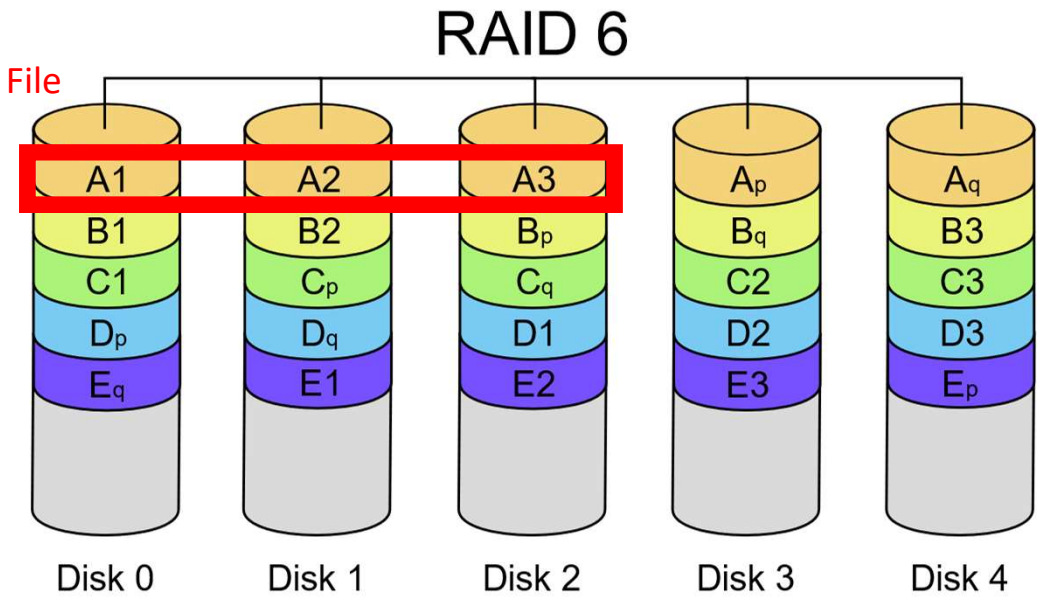
Standard RAID Levels

- **RAID Level 5: Block striping, distributed parity** - A block of data is distributed across multiple disks, but an extra parity drive is added. If any disk drops, it can be rebuilt by calculating the missing drive's contents from the others.
  - Array rebuild thus requires reading all data from all drives: if they're all from the same manufacturer, another could fail at about the same time!

- **RAID Level 6: Block striping, double distributed parity** - The same as RAID 5, but there are two parity drives, meaning that two can drop and the array can still be rebuilt (and function).

Standard RAID Levels



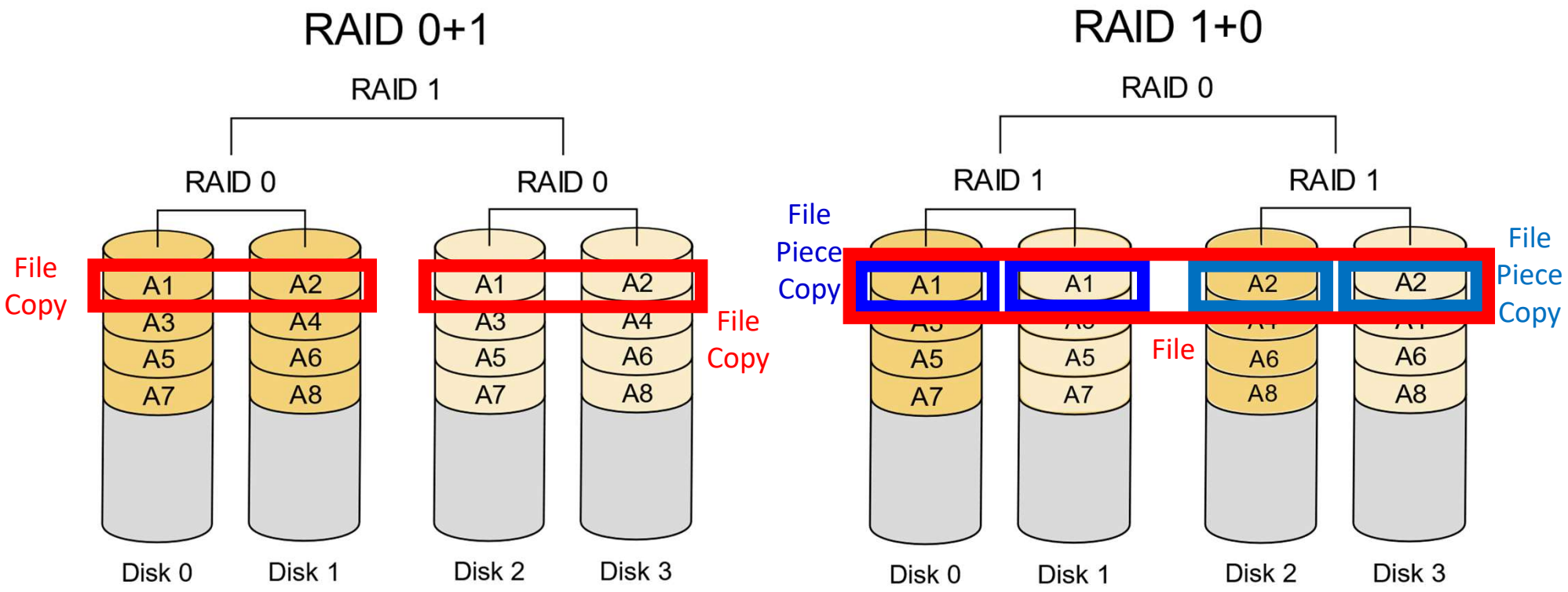


Nested RAID Levels

- **RAID 0+1** - Creates a stripe (out of two disks), and then mirrors the entire stripe onto two other disks. If one drive drops, that stripe is gone, but the other still functions. To rebuild, all data in the functioning stripe must be reread, causing the same problems and slowdown as RAID 5.

- **RAID 1+0 (aka 10) -** Data is first striped into two pieces, and then each piece is separately mirrored onto other drives. If a drive goes down, data can be read from any drive in the mirrored set to fulfill the stripe. Rebuilding requires copying just one drive.

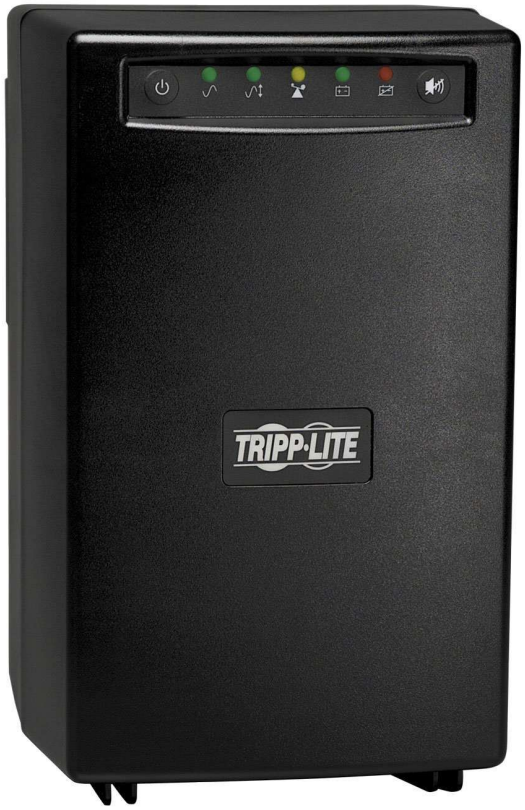
Nested RAID Levels



Uninterruptible Power Supplies

- In the vein of business continuity, let's examine UPS devices

- Keep a consistent power level, no matter what the mains voltage does, with various features such as:
  - Battery-backed
  - Pure sine wave
  - Consistent voltage
  - Alerting and reporting features
  - Can shutdown the server they're attached to (via network or USB cable) when the battery capacity is nearly exhausted



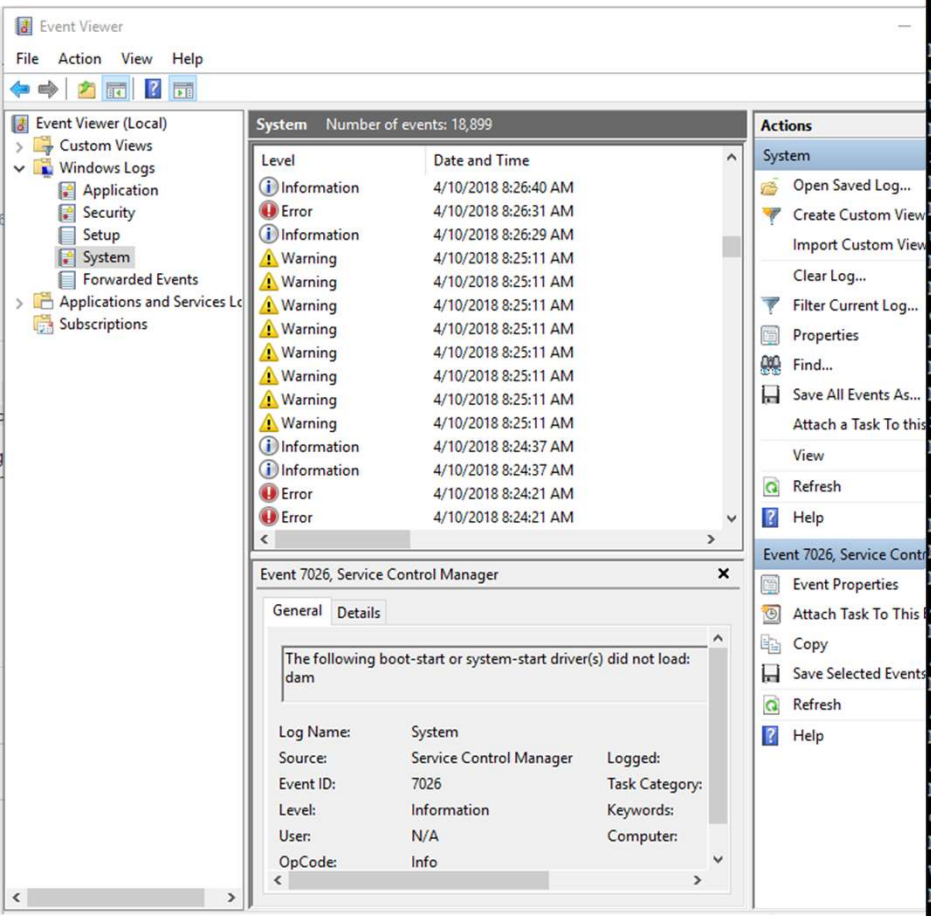
Tripp Lite SMART1500 :: Can provide almost one kilowatt @ 120VAC for ten minutes

Notifications

- Speaking of notifications, we'll cover system monitoring and alerting in our last lecture
- Knowing that a server or network is down is a BIG DEAL
- I used a picture of a red Artisan KitchenAid mixer I own as the caller pic for the NOC when they would call, so that it would be bright red, and easy to see - I grew to loathe the call on sight, though I love the mixer

Log Files

- Some people say that IT is just crawling through log files
  - ...and they're quite right
- We examined the Event Viewer in a previous lab: everything happening on a Windows box that writes to the logs can be viewed here, in excruciating detail
- Logs can be pushed to a network or local server that runs a proprietary logging service, or to the industry standard **syslog** format
  - Logged message range in severity from "Emergency" to "Debug"




```
[1636][brewsteb@ben-CentOS:/var/log]$ sudo tail -20 secure
[sudo] password for brewsteb:
May 14 08:09:17 ben-CentOS unix_chkpwd[3332]: password check failed for user (brewsteb)
May 14 08:09:17 ben-CentOS gdm-password]: pam_unix(gdm-password:auth): authentication fail
ure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=brewsteb
May 14 08:09:17 ben-CentOS gdm-password]: gkr-pam: the password for the login keyring was
invalid.
May 14 08:11:07 localhost polkitd[811]: Loading rules from directory /etc/polkit-1/rules.d
May 14 08:11:07 localhost polkitd[811]: Loading rules from directory /usr/share/polkit-1/r
ules.d
May 14 08:11:07 localhost polkitd[811]: Finished loading, compiling and executing 8 rules
May 14 08:11:07 localhost polkitd[811]: Acquired the name org.freedesktop.PolicyKit1 on th
e system bus
May 14 08:11:17 localhost sshd[1193]: Server listening on 0.0.0.0 port 22.
May 14 08:11:17 localhost sshd[1193]: Server listening on :: port 22.
May 14 08:11:23 localhost gdm-autologin]: pam_unix(gdm-autologin:session): session opened
for user brewsteb by (uid=0)
May 14 08:11:29 localhost polkitd[811]: Registered Authentication Agent for unix-session:1
 (system bus name :1.33 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/Au
thenticationAgent, locale en_US.UTF-8)
May 15 07:52:43 localhost gdm-password]: gkr-pam: unlocked login keyring
May 15 16:28:44 localhost gdm-password]: gkr-pam: unlocked login keyring
May 15 16:30:34 localhost sudo: brewsteb : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=
/bin/tail -10 secure
May 15 16:31:20 localhost sudo: brewsteb : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=
/bin/tail -10 messages
May 15 16:31:40 localhost sudo: brewsteb : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=
/bin/tail -20 messages
May 15 16:31:56 localhost sudo: brewsteb : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=
/bin/tail -20 secure
May 15 16:36:16 localhost sshd[31400]: Accepted password for brewsteb from 10.214.154.77 p
ort 52433 ssh2
May 15 16:36:16 localhost sshd[31400]: pam_unix(sshd:session): session opened for user bre
wsteb by (uid=0)
May 15 16:36:34 localhost sudo: brewsteb : TTY=pts/1 ; PWD=/var/log ; USER=root ; COMMAND=
/bin/tail -20 secure
```

Environmental Concerns

- The environment is out to destroy everything you hold dear by:
  - Flooding (sometimes via frozen pipe explosion)
  - Power surges
  - Overheating
  - Dust clogging
  - Earthquakes
  - Vermin invasion

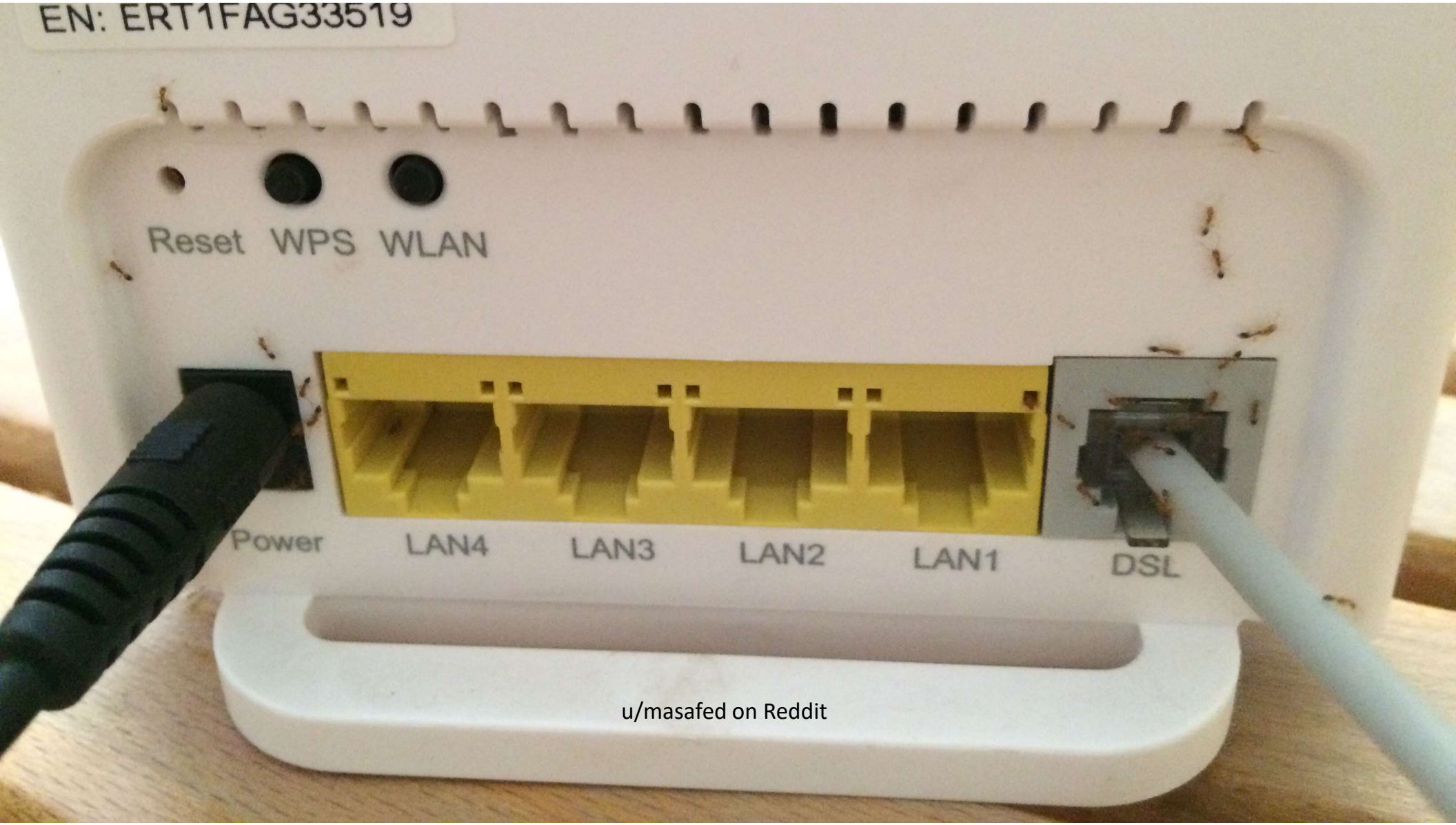
- There are sensors for all of this!

Environmental Concerns

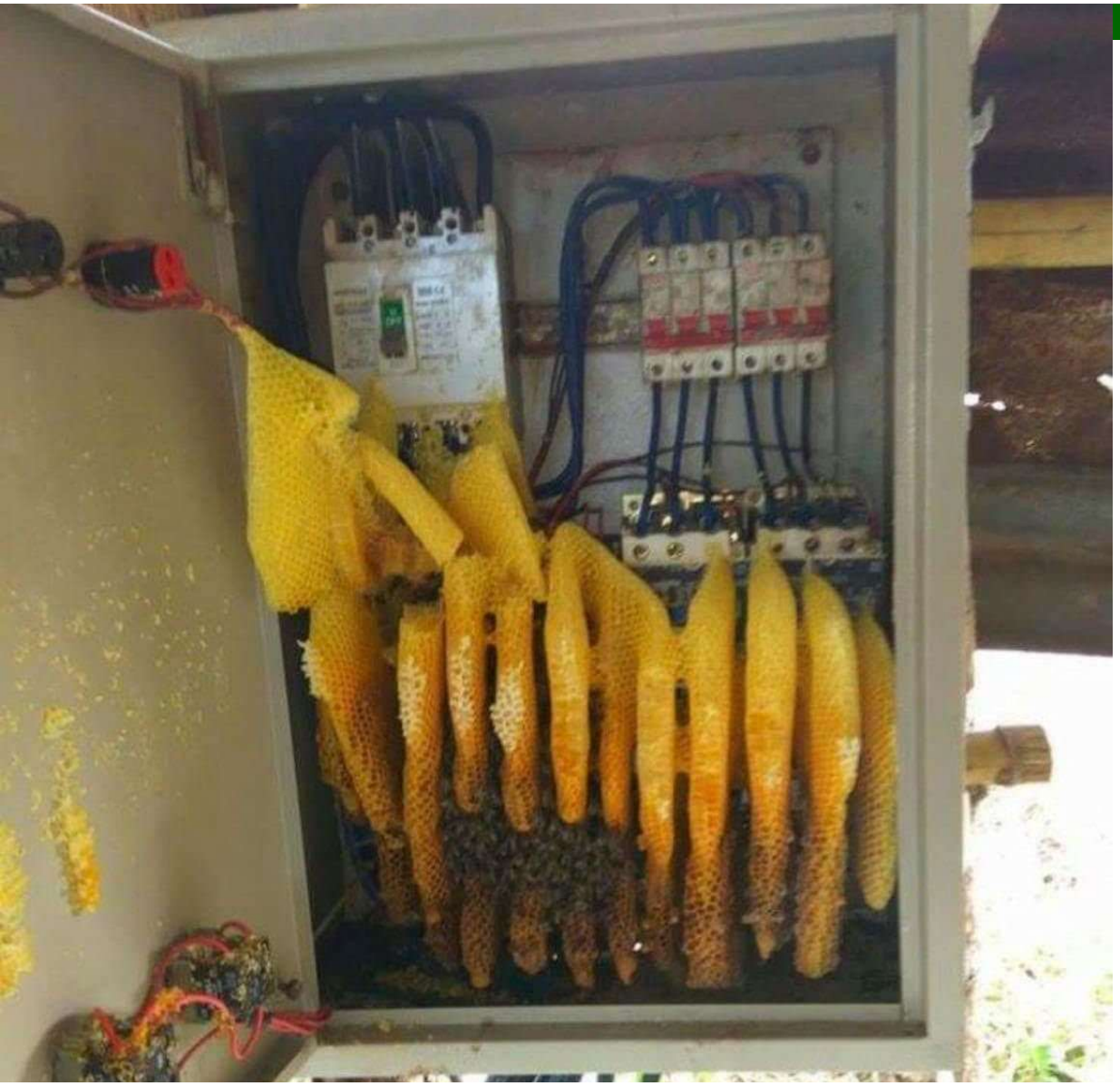
- This temperature, airflow, humidity, and dew point sensor plugs into this Watchdog 15-P climate monitor, and emails, texts, etc. when it reaches thresholds that you set

Environmental Concerns

- This is the OCTO-Base seismic isolation system by WorkSafe Technologies
- It's spec sheets tells the story: "Provides improved protection for larger seismic and blast events"



u/masafed on Reddit



- Peruse the r/techsupportgore subreddit for much more

- https://www.reddit.com/r/techsupportgore/

u/Eskaminagaga on Reddit

Conclusion

- Consumers always lie about what they did account, server, or network
- Sometimes bombs will hit your servers - your backups had better be secure
- Let the ants have the router (try Terro bait traps)
- Plan on having your hard drives fail in clusters, so keep spares on hand, and use drives from several manufacturers or batches; consider failover servers and backup devices, too!