

When Disaster Strikes

Hands-On UNIX System Administration DeCal

Week 12 — 11 April 2011

Administrivia

- Today is the last lecture!
(Next week: show up and hack/get help on final projects. You'll present them the following Monday, on **25 April**.)
- Three groups are doing IP-over-DNS. If you're one of them, think of something clever or unique for your project demo!

Be prepared!

- **Murphy's Law:** "Anything that can go wrong, will go wrong."
- Expect problems, and plan accordingly. Set up your systems to be disaster-proof, and make your life easier if Stuff Happens.

Software meltdowns

- Your system load is 500 and the SSH server can't get enough cycles to let you log in.
- You broke {networking, the firewall, SSH}.
- ... Now what?

Serial console

- UNIX systems *spawn* TTYs on VGA out. They can be configured to spawn TTYs on serial console too (NB: plain-text only; also need to configure GRUB).
- A **serial console server** aggregates multiple machines' serial consoles — like your virtual servers, different machines are accessible on different ports.

Remote power mgmt

- If you're running a serious operation, you'll have Uninterruptible Power Supplies powering your servers. There are also professional-grade power strips.
- These can be set up (via serial console) for remote power management — you can **remotely power cycle** a crashed server. BIOS also allows for remote power-{on,off}.

Lights-Out Mgmt

- **Out-of-band management systems**, like LOM cards, are more reliable than serial console connections.
- Some LOM systems (e.g., Dell DRAC) allow you to connect local media to a remote server and view its display locally. You can **install an OS remotely** — even Windows!

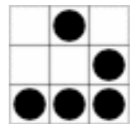
Hardware meltdowns

- Rackmounted servers allow for quick and easy access to hardware, so you can swap out a failed drive, CPU, RAM, very quickly.
- Make sure you have backups! (Test them!)
- For high availability, you need failover servers — if NFS goes down, every other NFS-dependent server will hang.

Hardware meltdowns

- Software like OpenNMS can monitor all your servers and perform some action when one fails.
- `irc.OCF/#outages` — alarmbot
- Start up a backup VM listening on the same IP address, or tell an already-running backup server to take over

Crackers

- http://www.catb.org/~esr/faqs/hacker-howto.html#what_is — crackers aren't hackers, despite the popular media. 
- If you have important media on your servers, make sure you have **offline/offsite backups** (tape media, rsync.net).
- If you're hacked, your data cannot be trusted and you have to start fresh.

Crackers

- An **intrusion detection system** may tip you off if you're hacked. The `/usr/bin/ssh` binary changing is a very good sign a cracker is on your system.
- Software like **SELinux** helps keep your systems secure (though it likely won't keep the FBI out — it was invented at the NSA).
- Watch out for holes (WordPress, phpBB...).

Security thru obscurity

The OCF used to have an intrusion detection system — a script that monitored essential system files' integrity — called “logrotate,” so crackers wouldn't realize what it was.

Staffers stopped reading documentation when building servers, didn't install logrotate because they thought it unimportant ... and now the original script is lost.