Lecture 08: When disaster strikes and all else fails

Hands-on Unix system administration DeCal

2012-10-22

Projects

- groups of four people
- submit one form per group with proposed project ideas and SSH *public* keys
- we'll be provisioning VMs and sending out an announcement

Tools of the trade

What's up?

- `uptime`: how long continuously running, what's the load average
  - 1, 5, 15 min average number of processes waiting for CPU (or IO)
- `w`, `who`: who's logged in on machine
  - `write`: write to a logged-in user
  - `wall`: write to all logged-in users

What's hosing?

- `top`, `htop` (Linux), `ps` (`ps aux`, `ps elf`)
- similarly `iftop` for network **i**nter**f**ace bandwidth, `iotop` (Linux) for disk IO

What's in use?

"The *action* can't be completed. . . in use" (Windows)
"The *operation* can't be completed. . . in use" (Mac OS X)

- `lsof` for files
- `lsof -i` for network ports
- **see also**: `netstat -pant`, `fuser`

Too much traffic

- `netcat`: "pipe" over TCP/UDP
- `wireshark`, `tshark`, `tcpdump`: packet sniffer/analyzer
- `nmap`: network scanner

Too many files

- `du`, `df`: directory, filesystem disk space usage
- `scp` (**s**ecure **c**o**p**y): transfer files over SSH
- rsync (**r**emote **sync**): intelligently transfer files (often over SSH)
- `tar` (**t**ape **ar**chiver): combine files into a tarball

Low-level “files”

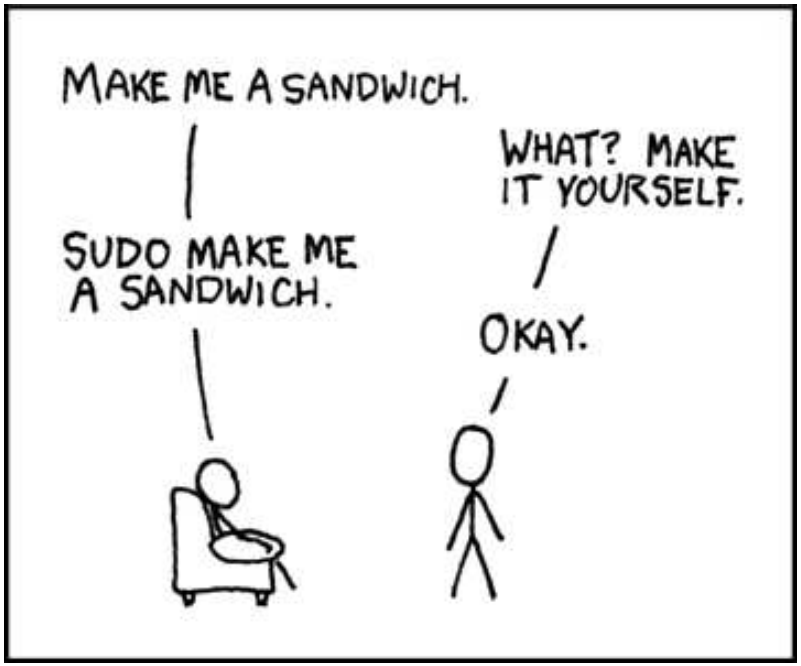
- `fdisk`, `parted` (Linux): edit partition table
- `fsck`: check filesystem for errors
- `dd`: copy block devices

Too many terminals

- `screen`, `tmux`
- "metaterminal"
  - ✦ access multiple terminal sessions inside a single terminal session
- other features: persistence (after logging off), session sharing (between users)

sudo

- `sudo`: **s**witch **u**ser **do** (usually used to give your command root powers)



via `xkcd.com`

Other tools

- `ldd` (shared library dependencies), `truss` or `strace` (trace system calls)
- `md5sum`: file checksum
- `watch`: execute command and repeatedly show output
- `seq`: print sequence of numbers

Disasters

Software meltdowns

- system load (`uptime` command) too damn high
- remote access (networking, firewall, SSH) broken

Hardware meltdowns

- failed hard drives
- failed fans, power supplies, CPU, RAM

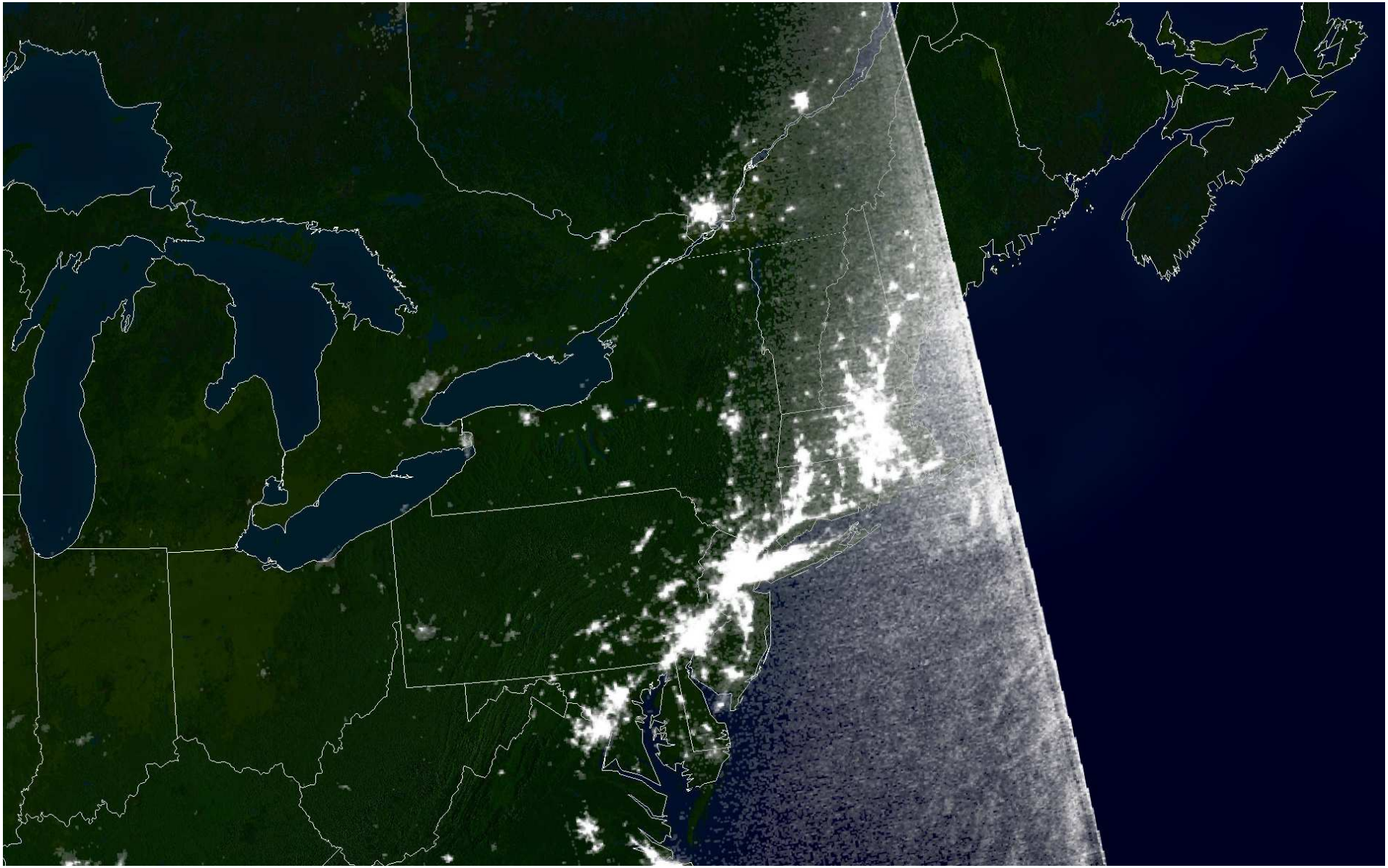
Criminals on the loose

- crackers will do Bad Things
- compromised accounts
- looks can be deceiving, uncertain what to trust

Escalation of problems

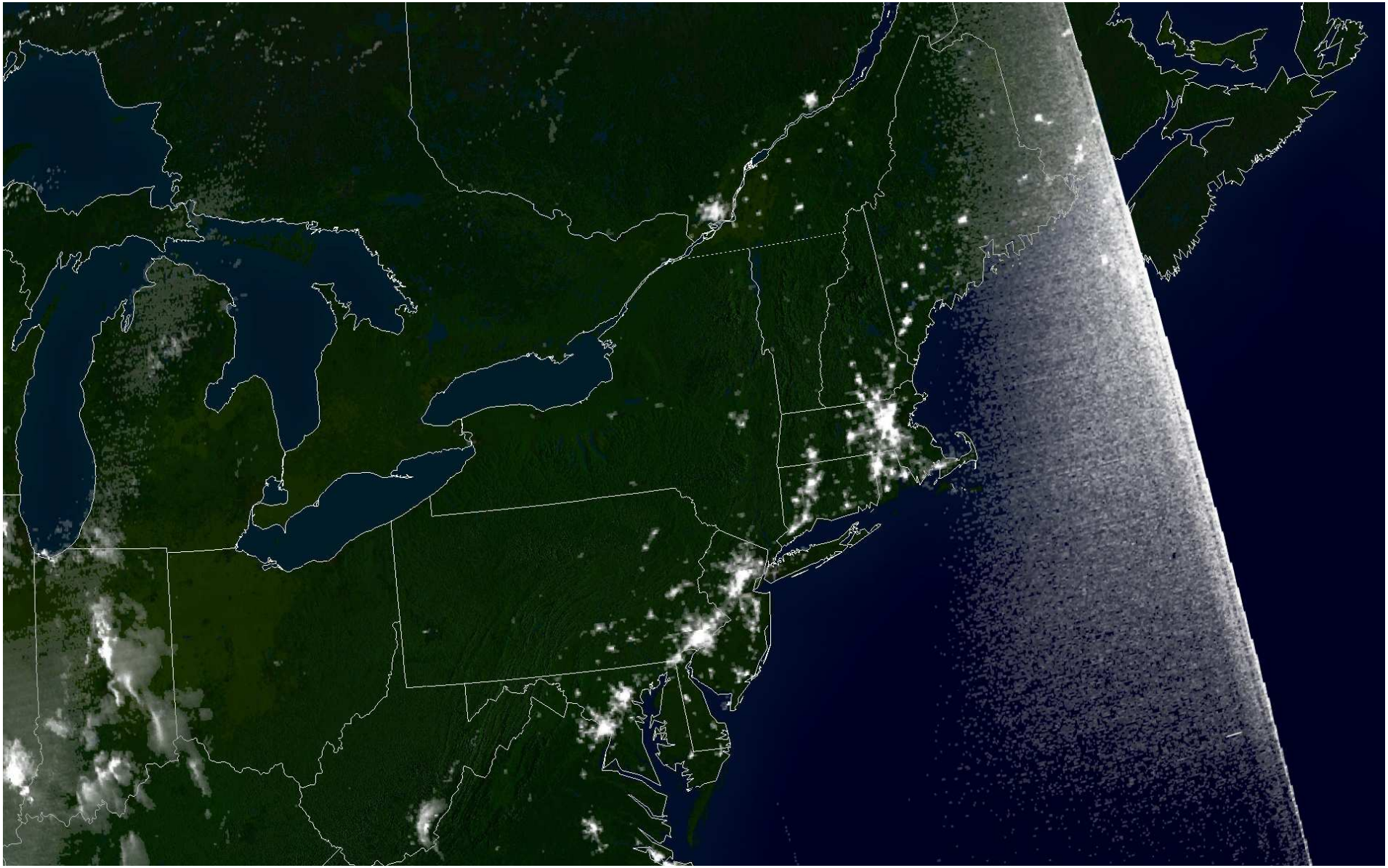
- we like to build systems on top of each other
- if one thing fails, it may break other things, causing other things to fail

2003 Northeast blackout



August 13, 2003, 9:21pm EDT (via en.wikipedia.org)

2003 Northeast blackout



August 14, 2003, 9:03pm EDT (via en.wikipedia.org)

Alleviating the pain

Be Prepared

- Boy Scout motto
- Murphy's Law: "Anything that can go wrong, will go wrong."
- s— happens

Power management

- Uninterruptible Power Supply (UPS)
- many UPSes can remotely power cycle servers

Out-of-band management

- separate hardware that can be remotely accessed
- independent from rest of hardware, dedicated NIC
- can access BIOS, power cycle, provide visual display
- e.g., IPMI, Dell DRAC, Sun LOM

Redundancy

- dual redundant power supplies typical
- RAID
- failover servers for high availability
- spare parts (hard drives!) for swapping

Monitoring

- many large scale operations (Google, Facebook) have many failed servers at any point in time, monitoring servers reroute traffic appropriately
- monitor syslog
- SNMP traps
- alarm notification by email, text message

Security

- subscribe to OS security announcements
- Intrusion Detection Software (e.g., snort, bro)
- be wary of lax permissions
- limit root access

Backups

- user data, system configuration
- ideally daily, weekly, monthly rotations
- RAID is not a backup
- e.g., `rsync`, `cron`, `rsnapshot`