Proactive Approaches to Dealing with Configuration Errors

Tianyin Xu

YY Zhou (PI)

Misconfigurations are bad.

- **No need to motivate any more.**
  - Severe impact
    - Outage / unavailability (ask Google, Amazon, Azure, Facebook)
    - Security vulnerability (MBIA's massive data breach)
  - Prevalence
    - 27% of customer support issues in a major storage company
    - The dominant customer support tickets in Cloudera
    - The 2nd dominant cause of service disruption in a Google service

Existing approaches are reactive.

- **"Reactive" to failures**
  - The main focus is postmortem **diagnosis**.
    - Find the root causes according to failure symptoms
  - Less efficient, expensive.
  - Sad things already happened.

Be proactive in dealing w/ misconf.

- Defend systems *in the first place*!
  - **Expose misconfiguration vulnerabilities in the source code**
    - Developers can fix them before releasing the products.
  - **Design configuration to be simpler and less prone to errors**
    - Configuration can be user friendly.

What's next?

- Security-related misconfigurations
  - You probably never know until your nude pics are everywhere.
- Configuration in large-scale, distributed systems
  - where configuration is a big challenge
  - e.g., datacenters, networked systems
- Let's talk if you have config-related problems

Sorry, I only have 5 minutes... :-(

- Thanks!
- Comments and feedbacks?
- Collaboration?