Alerting Husbandry

Julien Goodwin
jgoodwin@studio442.com.au – @laptop006
Bad Alerts
Obsolete Alerts

- $THING is down!
  - Because we turned it down a year ago
- $THING has bug $FOO!
  - Really? The vendor fixed it three years ago and we upgraded.
Unactionable Alerts

- $THING is down!
- But it’s managed by another team, just thought you’d like to be woken up.
$SERVICE has failed SLA

So can I do anything about it?

Log for later reporting instead
Bad Thresholds

- $SERVER has a high load average of 4
- It has 32 cores, that’s no load
- $LUN is nearly full, only 100MB left
- It’s a 10T LUN, I have no time to respond
- It’s a 200MB LUN as /boot & a new kernel was installed
Hair trigger alerts

- $THING didn’t respond in 50ms
  - Once
  - It responded in 51ms
Non-Impacting Redundancy

- WEB_SERVER_4 is down
- But I have 8 servers, and only need 6 at full load
Spamming alerts

• $THING is down!
  • For the 28345972398th time
  • Even if it's important you've stopped caring
Nobody cares

- $TEST_SERVER has no backups
  - I want it that way
- Most of the earlier items end up in this bucket
Related Practices
E-mail alerts

- It’s not high priority enough to page, so I’ll email about it
- Within a few weeks the entire team will have a filter to mark read & delete
- Having a separate archived alert list may work well as a log
Undocumented Alerts

• $THING is broken!
  • So what am I supposed to do?
  • Document actions to take in a “playbook”
  • All oncallers should be able to follow
Alert Acceptance

• Have a review process for any new alerts or thresholds.
  • Require documentation, expected impact, test data, etc.
• Only oncallers should accept alerts.
Silencing

• If your alert system pages people you need a silence mechanism

• In practice this becomes a whole system

• Oncallers get very grumpy when woken up for other people’s planned work

• If relevant may include need to schedule silences for things like carrier outages
Production by Fiat

- $THING is now in production because I say so — $VP
- Good luck
A Plug

Contains great selections on alerting, postmortems, availability & more.