Creating A Scalable Monitoring System That Everyone Will ❤️

@ThePracticalDev | @molly_struve | dev.to/molly_struve
Monitoring Mistakes

Overhauling the System

The Payoff
Monitoring Mistakes

Overhauling the System

The Payoff
I want to look away but I can't!
Monitoring Mistakes

Overhauling the System

The Payoff

@molly_struve
Monitoring Mistakes
Overhauling the System
The Payoff
@molly_struve
Monitoring Mistakes

Overhauling the System

The Payoff
Monitoring Mistakes

Overhauling the System

The Payoff

@molly_struve
Monitoring Mistakes

Overhauling the System

The Payoff

@molly_struve
Monitoring Mistakes
Overhauling the System
The Payoff

@molly_struve
Monitoring Mistakes

Overhauling the System

Waiting for your crush to text you back like

@molly_struve
Incredibly Inconsistent
Inconsistent Alerts

Reported data

Required no action

Monitoring Mistakes

Overhauling the System

The Payoff
Inconsistent Alerts

- Reported data
- Required no action

Immediate action required
Manual Monitoring
Manual Monitoring
### Processes

<table>
<thead>
<tr>
<th>Name</th>
<th>Started</th>
<th>Threads</th>
<th>Busy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712</td>
<td>less than a minute ago</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

Queues: analytics

### Jobs

<table>
<thead>
<tr>
<th>Process</th>
<th>TID</th>
<th>JID</th>
<th>Queue</th>
<th>Job</th>
<th>Arguments</th>
<th>Started</th>
</tr>
</thead>
<tbody>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712</td>
<td>wwRe3qsOK</td>
<td>e9434a825987d929c4ded8e7</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712</td>
<td>sivAZNh9S</td>
<td>a9243f80f9202fcd1b6525c</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712</td>
<td>CV33PB0YT</td>
<td>d0aa5777f8d24ada509abf57</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712</td>
<td>u3YO9amQw</td>
<td>3fb4f8c734dce7d9942284db5</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712</td>
<td>2t0JChEiE</td>
<td>538becf3319cac6ddf9ee08a</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
</tbody>
</table>
### Processes

<table>
<thead>
<tr>
<th>Name</th>
<th>Started</th>
<th>Threads</th>
<th>Busy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712</td>
<td>less than a minute ago</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Queues: analytics</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Jobs

<table>
<thead>
<tr>
<th>Process</th>
<th>TID</th>
<th>JID</th>
<th>Queue</th>
<th>Job</th>
<th>Arguments</th>
<th>Started</th>
</tr>
</thead>
<tbody>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712:XrkljcUcQIB8</td>
<td>wwRe3qsOK</td>
<td>e9434a825987d929c4ded8e7</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712:XrkljcUcQIB8</td>
<td>sivAZNh9S</td>
<td>a9243f80ff9202fc1b6525c</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712:XrkljcUcQIB8</td>
<td>CV33PB0YT</td>
<td>d0aa57778f2d4a509abf57</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712:XrkljcUcQIB8</td>
<td>u3YO9amQw</td>
<td>3fb4f8c734dc7d9942284d5</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712:XrkljcUcQIB8</td>
<td>2tr0JCheE</td>
<td>538befc3319cac6ddf9ee08a</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
</tbody>
</table>

---

**Monitoring Mistakes**

**Overhauling the System**

**The Payoff**
make on-call devs miserable
Monitoring Mistakes

Overhauling the System

The Payoff

WHAT IS GOING ON??
DON'T

Monitoring Mistakes

Overhauling the System

The Payoff

@molly_struve
Monitoring Mistakes
Overhauling the System
The Payoff
@molly_struve
Coverage doesn’t matter if you have no idea what is going on!
Monitoring Mistakes

Overhauling the System

The Payoff
Monitoring Must Haves

1. Consolidate Monitoring To a Single Place

Monitoring Mistakes  Overhauling the System  The Payoff

@molly_struve
Monitoring Mistakes
Overhauling the System
The Payoff
Monitoring Mistakes

Overhauling the System

The Payoff

@molly_struve
Monitoring Mistakes

Overhauling the System

The Payoff

@molly_struve
Monitoring Mistakes

Overhauling the System

The Payoff

@molly_struve
Monitoring Mistakes
Overhauling the System
The Payoff

- Honeybadger
- aws
- StatusCake
- fluentd
- circleci

@molly_struve
Monitoring Must Haves

1. Consolidate Monitoring To a Single Place
2. Make ALL Alerts Actionable

Monitoring Mistakes Overhauling the System The Payoff

@molly_struve
Monitoring Mistakes

Overhauling the System

The Payoff

Action
<table>
<thead>
<tr>
<th>Action Required</th>
<th>No action Needed</th>
</tr>
</thead>
</table>

- Monitoring Mistakes
- Overhauling the System
- The Payoff
<table>
<thead>
<tr>
<th>Action Required</th>
<th>No action Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>#ops_alerts</td>
<td></td>
</tr>
<tr>
<td>#dev_alerts</td>
<td></td>
</tr>
<tr>
<td>Action Required</td>
<td>No action Needed</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>#ops_alerts</td>
<td>#ops_reporting</td>
</tr>
<tr>
<td>#dev_alerts</td>
<td>#dev_reporting</td>
</tr>
</tbody>
</table>

- Monitoring Mistakes
- Overhauling the System
- The Payoff

@molly_struve
Monitoring Must Haves

1. Consolidate Monitoring To a Single Place
2. Make ALL Alerts Actionable
3. Make Sure Alerts Are Mutable

Monitoring Mistakes

Overhauling the System

The Payoff

@molly_struve
Monitoring Must Haves

1. Consolidate Monitoring To a Single Place
2. Make ALL Alerts Actionable
3. Make Sure Alerts Are Mutable
I heard you, mother.

#WillAndGrace
Miss new alerts
Monitoring Mistakes

Overhauling the System

The Payoff

@molly_struve
Monitoring Mistakes

Overhauling the System

The Payoff

@molly_struve
Monitoring Must Haves

1. Consolidate Monitoring To a Single Place
2. Make ALL Alerts Actionable
3. Make Sure Alerts Are Mutable
4. Track Alert History

@molly_struve
Tracking Alert History
Tracking Alert History

48 MB

16 MB

Wed 22
12:00
Thu 23
12:00

Monitoring Mistakes  Overhauling the System  The Payoff

@molly_struve
Tracking Alert History

48 MB

16 MB

Monitors Mistakes  Overhauling the System  The Payoff

@molly_struve
Monitoring Must Haves

1. Consolidate Monitoring To a Single Place
2. Make ALL Alerts Actionable
3. Make Sure Alerts Are Mutable
4. Track Alert History
5. Remove ALL Manual Monitoring

Monitoring Mistakes → Overhauling the System → The Payoff

@molly_struve
Monitoring Mistakes
Overhauling the System
The Payoff

@molly_struve
Manual Monitoring

Scale
## Processes

<table>
<thead>
<tr>
<th>Name</th>
<th>Started</th>
<th>Threads</th>
<th>Busy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712</td>
<td>less than a minute ago</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td><strong>Queues:</strong> analytics</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Jobs

<table>
<thead>
<tr>
<th>Process</th>
<th>TID</th>
<th>JID</th>
<th>Queue</th>
<th>Job</th>
<th>Arguments</th>
<th>Started</th>
</tr>
</thead>
<tbody>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712:XrkjljcUcQIB8</td>
<td>wwRe3qsOK</td>
<td>e9434a825987d929c4ded8e7</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712:XrkjljcUcQIB8</td>
<td>sivAZNh9S</td>
<td>a9243f80ff920fcd1b6525c</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712:XrkjljcUcQIB8</td>
<td>CV33PB0YT</td>
<td>d0aa57778d24ada509abf57</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712:XrkjljcUcQIB8</td>
<td>u3YO9amQw</td>
<td>3fb4f8c734dc7d9942284db5</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
<tr>
<td>Youngs-MacBook-Pro.local:140735222771712:XrkjljcUcQIB8</td>
<td>2t0JCheE</td>
<td>538beef3319cacf6df9ee08a</td>
<td>analytics</td>
<td>Printer</td>
<td>&quot;damn&quot;</td>
<td>less than a minute ago</td>
</tr>
</tbody>
</table>
## Automatic Alerts

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Sidekiq Processes NOT running {{environment.name}}</td>
</tr>
<tr>
<td>OK</td>
<td>Sidekiq Queue {{sidekiq_queue.name}} Latency is greater than 6 hours in {{environment.name}}</td>
</tr>
<tr>
<td>OK</td>
<td>Sidekiq job duration is high</td>
</tr>
<tr>
<td>OK</td>
<td>Sidekiq periodic queue is backed up or not running on {{environment.name}}</td>
</tr>
</tbody>
</table>
Monitoring Must Haves

1. Consolidate Monitoring To a Single Place
2. Make ALL Alerts Actionable
3. Make Sure Alerts Are Mutable
4. Track Alert History
5. Remove ALL Manual Monitoring
Monitoring Mistakes

Overhauling the System

The Payoff
Monitoring Mistakes → Overhauling the System → The Payoff
On boarding is a breeze
3 On-boarding steps:

1. Monitoring Mistakes
2. Overhauling the System
3. The Payoff
3 On-boarding steps:

1. Show them the monitoring setup
2. Overhauling the System
3. The Payoff
3 On-boarding steps:

1. Show them the monitoring setup
2. If an alert goes off you have to address it
3. [Remaining on-boarding steps]

Monitoring Mistakes  Overhauling the System  The Payoff

@molly_struve
3 On-boarding steps:

1. Show them the monitoring setup
2. If an alert goes off you have to address it
3. How to mute a triggered alert
On boarding is a breeze
Happier on-call developers
All alerts must be actionable
I have several questions
No more noise
Alerts must be mutable
Alerts must be mutable
Diagnosing alerts is faster and easier
Tracking Alert History

- Monitoring Mistakes
- Overhauling the System
- The Payoff
Triggered #3727: High Priority Job Queue Backed Up
Today?
Today?  Going on longer?

Monitoring Mistakes  Overhauling the System  The Payoff
Triggered **#3727**: High Priority Job Queue Backed Up

**Today?**  
**Going on longer?**
Triggered #3727: High Priority Job Queue Backed Up

Alert History
Developers began helping to improve our monitoring system
All alerts must be actionable
30-40 Alerts
>90 Alerts
Basic Alerts
Basic Alerts

More Granular Alerts

Monitoring Mistakes  Overhauling the System  The Payoff

@molly_struve
Developers ❤ monitoring system
Monitoring Must Have Benefits

1. Monitoring Mistakes
2. Overhauling the System
3. The Payoff
On boarding is a breeze.
Monitoring Must Have Benefits

1. On boarding is a breeze.
2. On-call developers are a lot happier
Monitoring Must Have Benefits

1. On boarding is a breeze.
2. On-call developers are a lot happier.
3. Diagnosing alerts is faster and easier.

@molly_struve
Monitoring Must Have Benefits

1. On boarding is a breeze.
2. On-call developers are a lot happier
3. Diagnosing alerts is faster and easier
4. Developers helping to improve your monitoring systems
Monitoring Must Haves

1. Consolidate Monitoring To a Single Place
2. Make ALL Alerts Actionable
3. Make Sure Alerts Are Mutable
4. Track Alert History
5. Remove ALL Manual Monitoring
Questions?
Rate today’s session

Session page on conference website

Cyberconflict: A new era of war, sabotage, and fear

9:55am-10:10am Wednesday, March 27, 2019
Location: Ballroom

We’re living in a new era of constant sabotage, misinformation, and fear, in which everyone is a target, and you’re often the collateral damage in a growing conflict among states. From crippling infrastructure to sowing discord and doubt, cyber is now the weapon of choice for democracies, dictators, and terrorists.

David Sanger explains how the rise of cyberweapons has transformed geopolitics like nothing since the invention of the atomic bomb. Moving from the White House Situation Room to the dens of Chinese, Russian, North Korean, and Iranian hackers to the boardrooms of Silicon Valley, David reveals a world coming face-to-face with the perils of technological revolution—a conflict that the United States helped start when it began using cyberweapons against Iranian nuclear plants and North Korean missile launches. But now we find ourselves in a conflict we’re uncertain how to control, as our adversaries exploit vulnerabilities in our hyperconnected nation and we struggle to figure out how to deter these complex, short-of-war attacks.

David Sanger
The New York Times

David E. Sanger is the national security correspondent for the New York Times as well as a national security and political contributor for CNN and a frequent guest on CBS This Morning, Face the Nation, and many PBS shows.

O’Reilly Events App

Cyberconflict: A new era of war, sabotage, and fear

9:55 AM - 10:10 AM, Wed, Mar 27, 2019

Speakers

David Sanger
National Security Correspondent
The New York Times

Keynotes

David Sanger explains how the rise of cyberweapons has transformed geopolitics like nothing since the invention of the atomic bomb. From crippling infrastructure to sowing discord and doubt, cyber is now the weapon of choice for democracies, dictators, and terrorists.

SESSION EVALUATION