Modern frameworks for modern alerting

Daniel Maher @phrawzty
Ara Pulido @arapulido

Datadog is a monitoring and analytics platform that helps companies improve observability of their infrastructure and applications

Daniel Maher, Developer Relations

dan.maher@datadoghq.com
@phrawzty

Ara Pulido, Technical Evangelist

ara.pulido@datadoghq.com
@arapulido

Endpoint foobar is unavailable

Logs

Logs

Infrastructure metrics

Logs

Infrastructure metrics

Work metrics

Logs

RUM data

Infrastructure metrics

Work metrics

Logs

RUM data

Infrastructure metrics

Resource metrics

Work metrics

Logs

RUM data

Infrastructure metrics

Resource metrics

Traces

Work metrics

Logs

RUM data

Infrastructure metrics

Resource metrics

Events in our app

Traces

Work metrics

Logs

RUM data

Infrastructure metrics

Resource metrics

Events in our app

Traces

Work metrics

AI/ML aggregated data

Logs

RUM data

Browser/UI tests

Infrastructure metrics

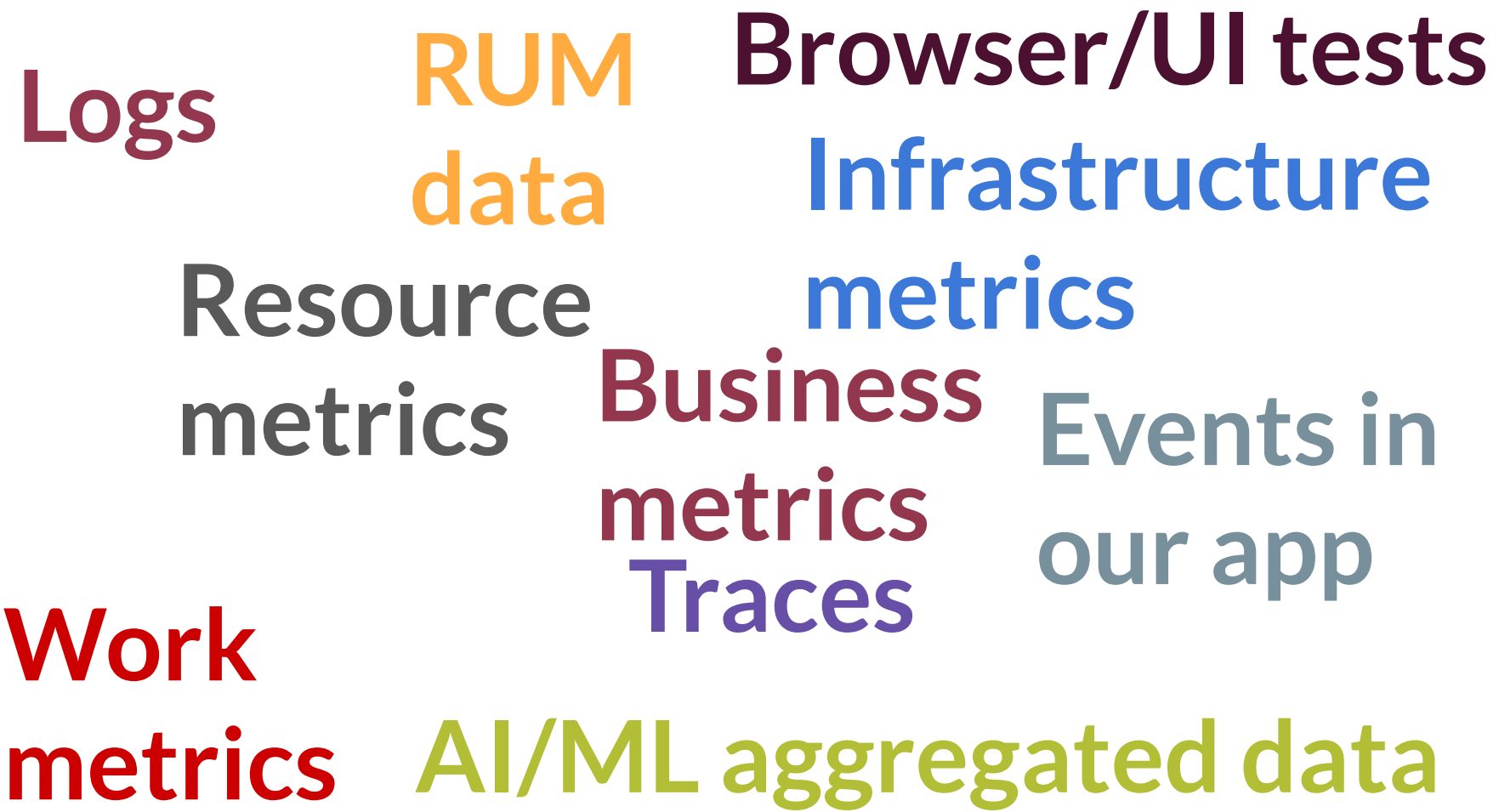
Resource metrics

Events in our app

Traces

Work metrics

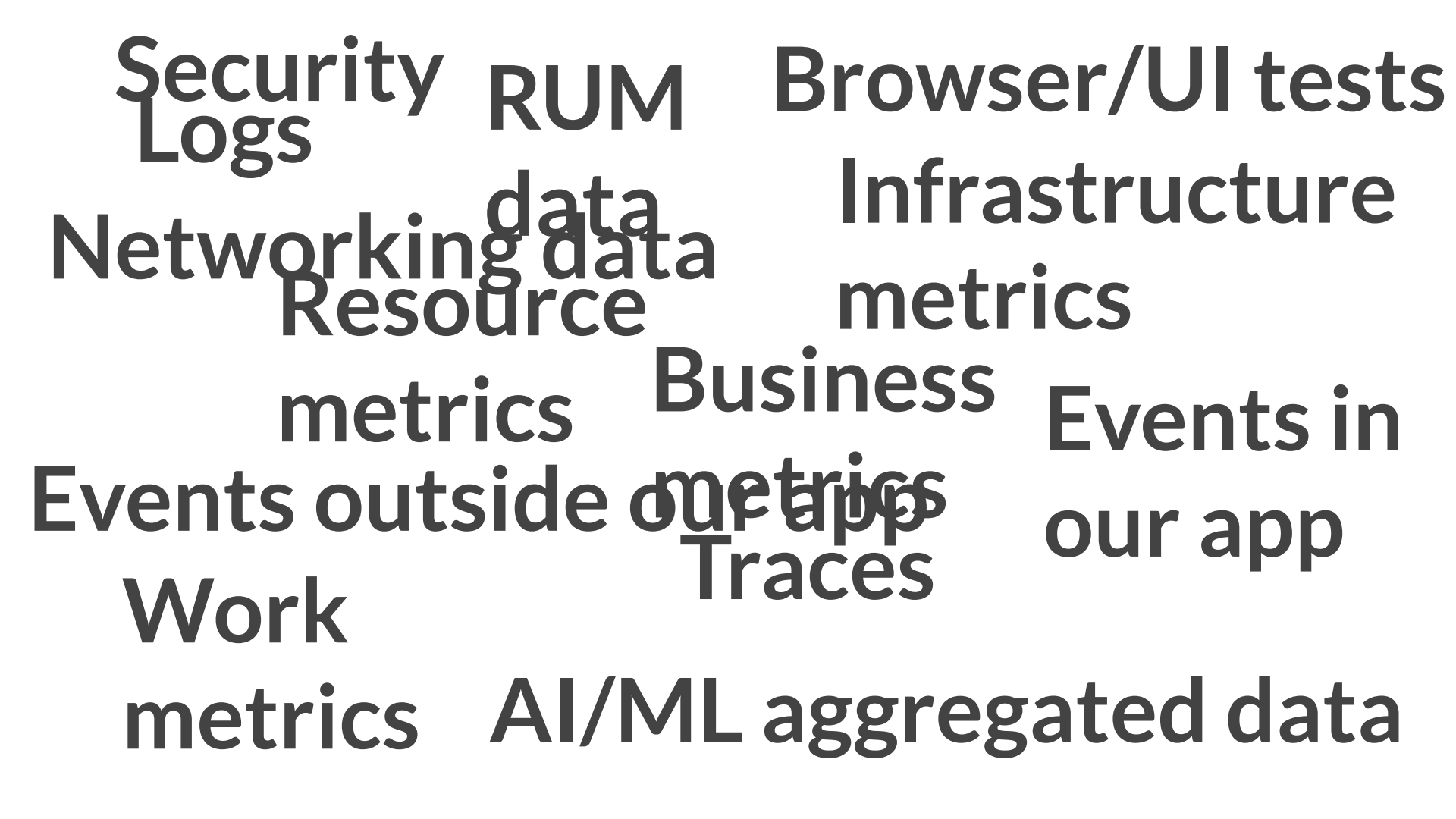
AI/ML aggregated data


Logs
RUM data
Browser/UI tests
Infrastructure metrics
Resource metrics
Business metrics
Events in our app
Traces
Work metrics
AI/ML aggregated data

Logs
RUM data
Browser/UI tests
Infrastructure metrics
Resource metrics
Business metrics
Events in our app
Events outside our app
Traces
Work metrics
AI/ML aggregated data

Logs
RUM data
Browser/UI tests
Networking data
Infrastructure metrics
Resource metrics
Business metrics
Events in our app
Events outside our app
Traces
Work metrics
AI/ML aggregated data

Security Logs
RUM data
Browser/UI tests
Networking data
Infrastructure metrics
Resource metrics
Business metrics
Events in our app
Events outside our app
Traces
Work metrics
AI/ML aggregated data


Security Logs
RUM data
Browser/UI tests
Networking data
Infrastructure metrics
Resource metrics
Business metrics
Events in our app
Events outside our apps
Traces
Work metrics
AI/ML aggregated data

FOUR
Security
Logs
RUM
Browser/UI tests
data
Infrastructure
Networking data
Resource
metrics
metrics
Business
metrics
Events in
our app
Events outside our apps
Traces
Work
metrics
AI/ML aggregated data

FOUR GOLDEN

Security
Logs
RUM
Browser/UI tests
data
Infrastructure
Networking data
Resource
metrics
Business
metrics
Events in
our app
Events outside our apps
metrics
Traces
Work
metrics
AI/ML aggregated data

Security
Logs
RUM
Browser/UI tests
data
Infrastructure
Networking data
Resource
metrics
metrics
Business
Events in
Events outside our apps
metrics
our app
Traces
Work
metrics
AI/ML aggregated data
FOUR
GOLDEN
SIGNALS

Alert

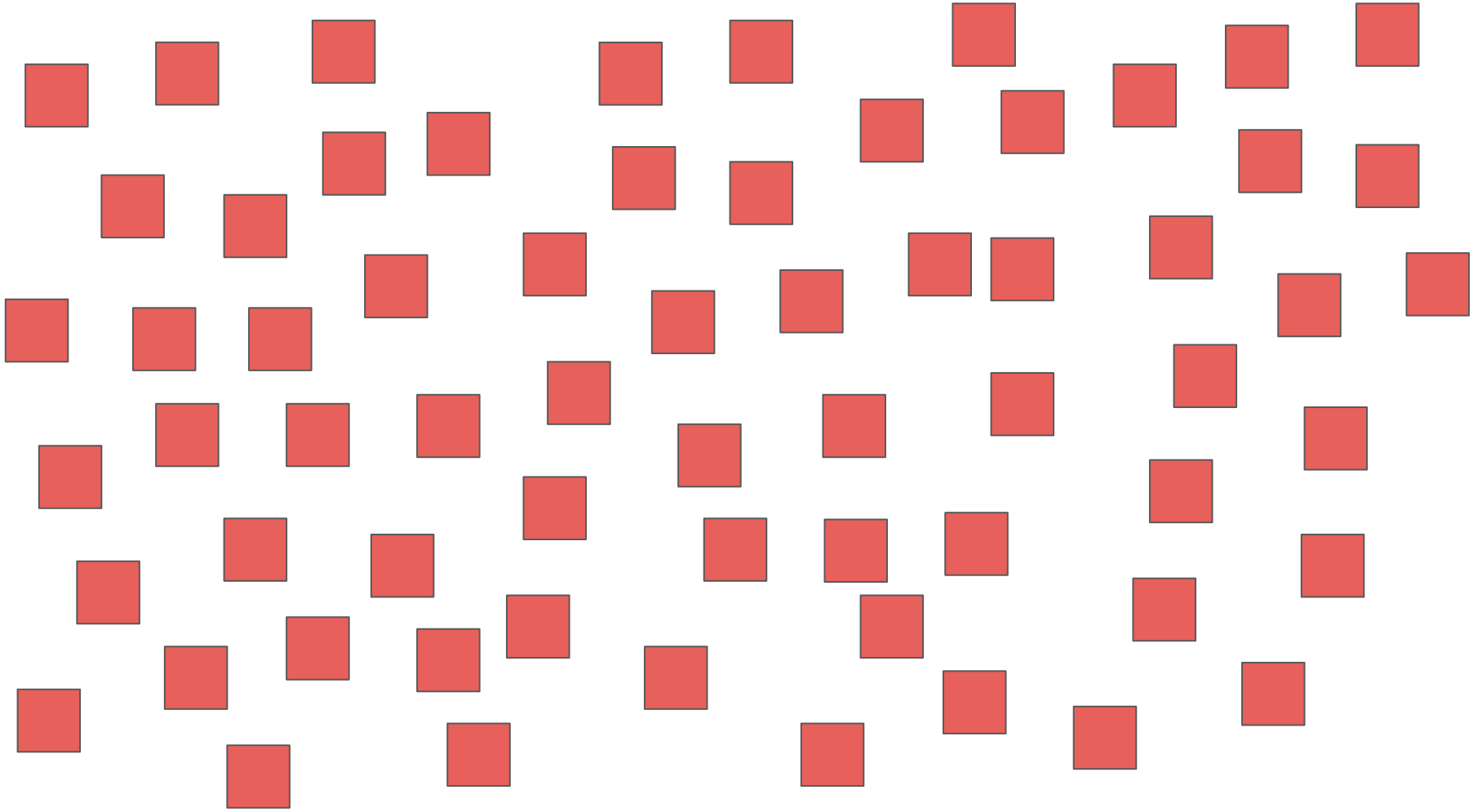
Fatigue

Information

Overload

Service **L**evel
Indicators
Objectives
Agreements

Alerts
Pages

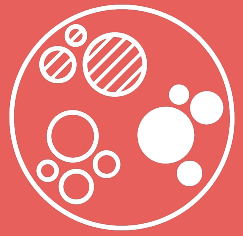


Symptoms vs. Causes

Symptom

18 % of queries are returning an error

Cause



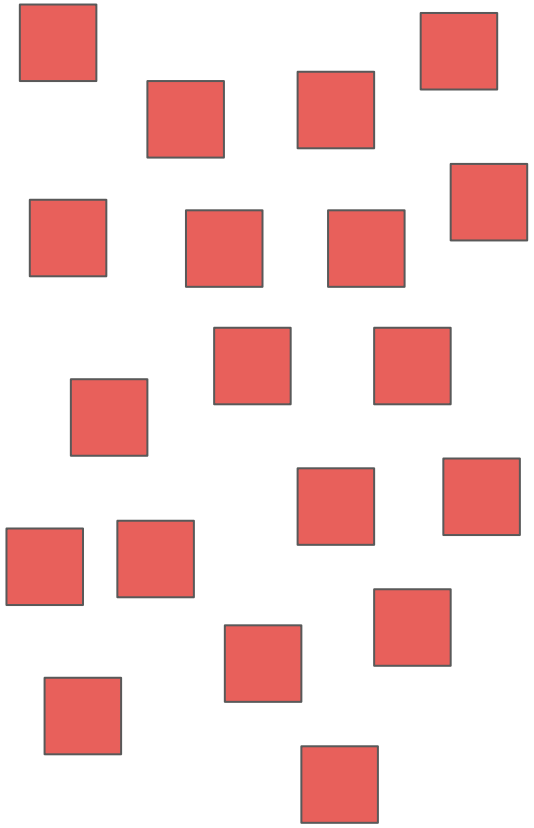
3 nodes of the cluster are down

It is so tempting to page on causes

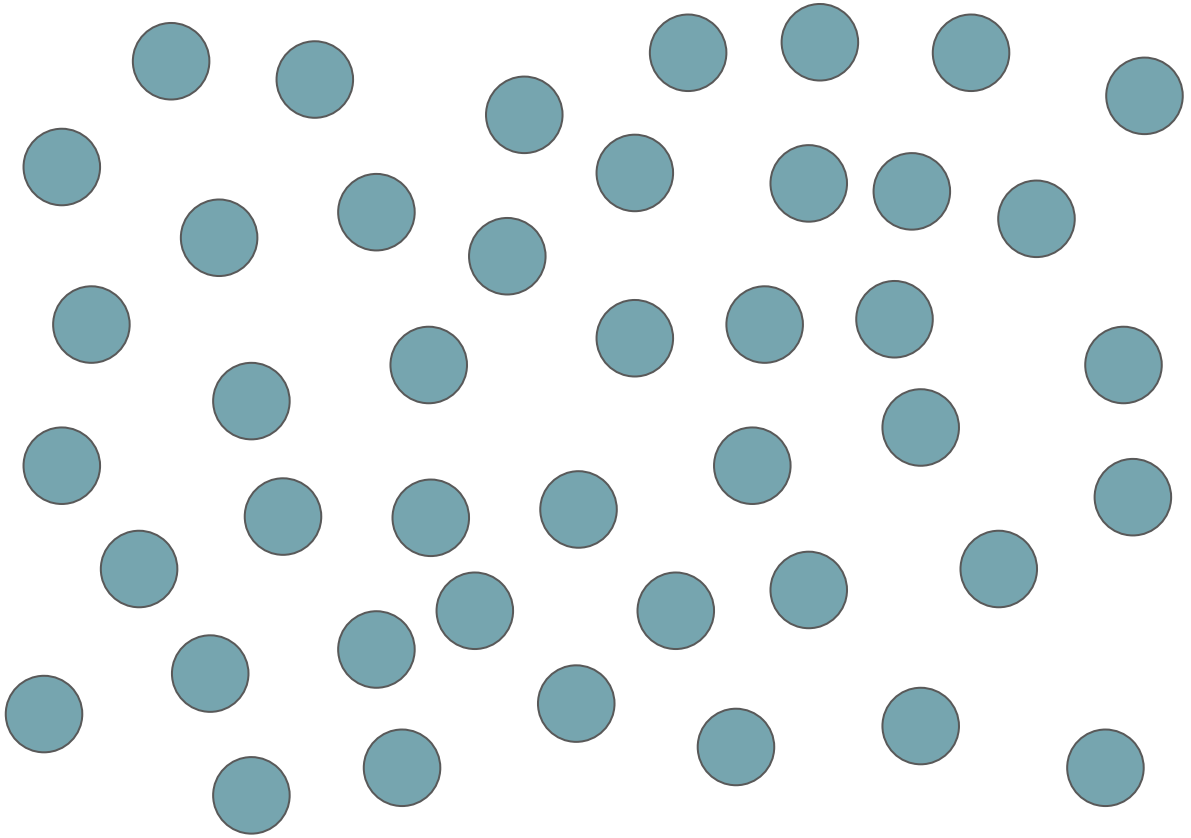
DON’T

SLAs are written based on symptoms

Symptoms

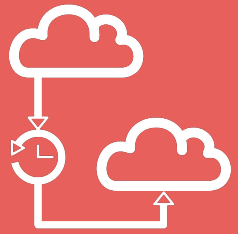


Causes

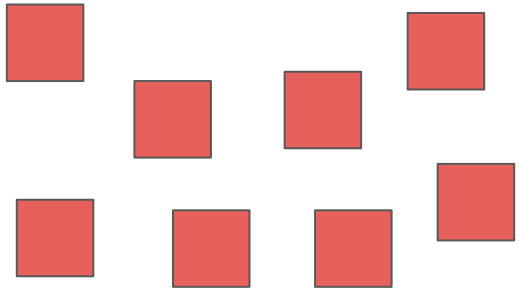


Urgency

High



p99 latency > 100ms

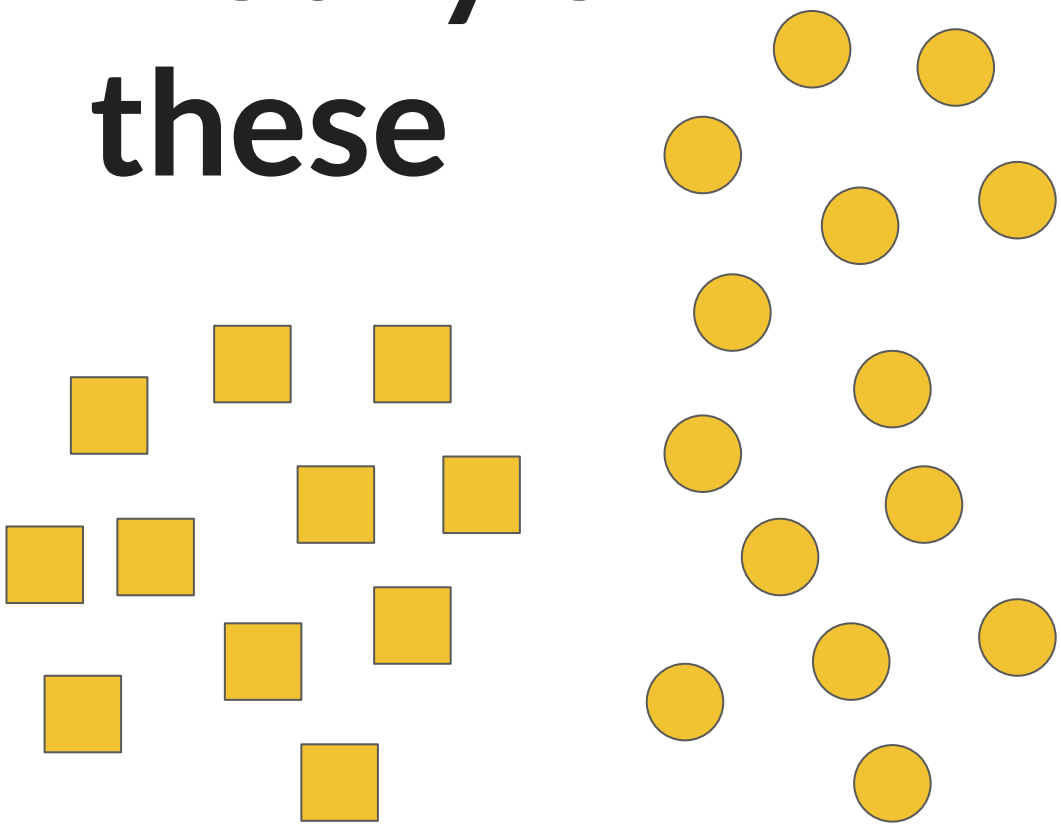


Only page on these
Related to your SLOs

Medium

1 node of the cluster is down

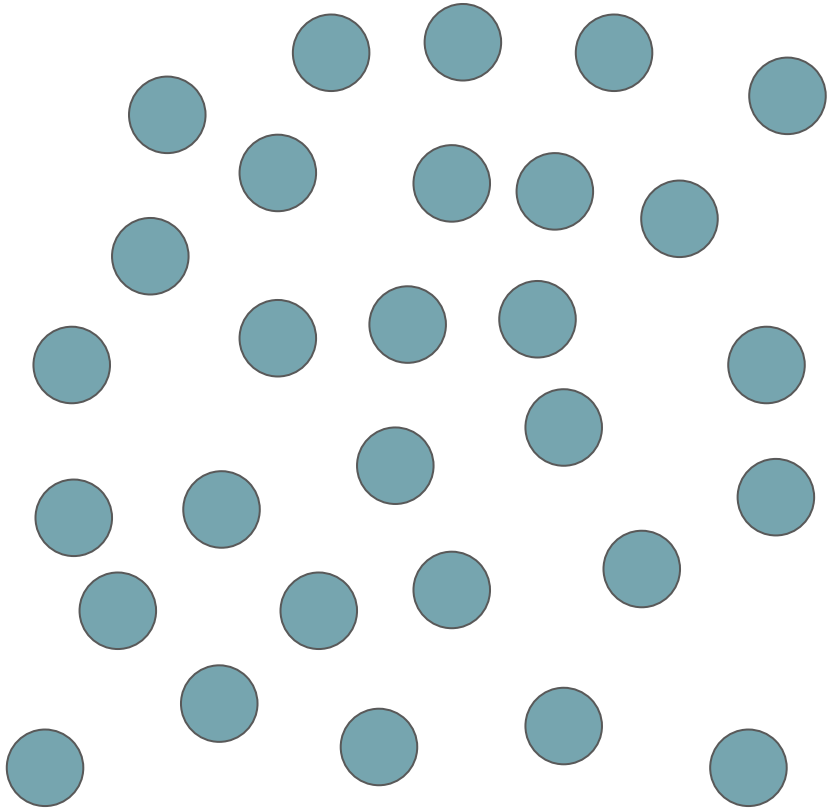
Notify on these



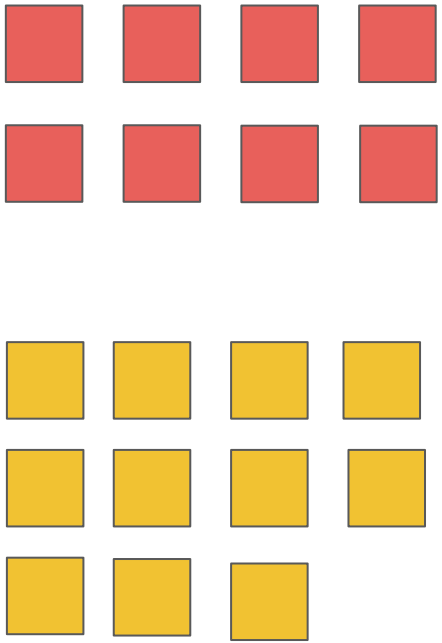
Low

Database I/O is slower than usual

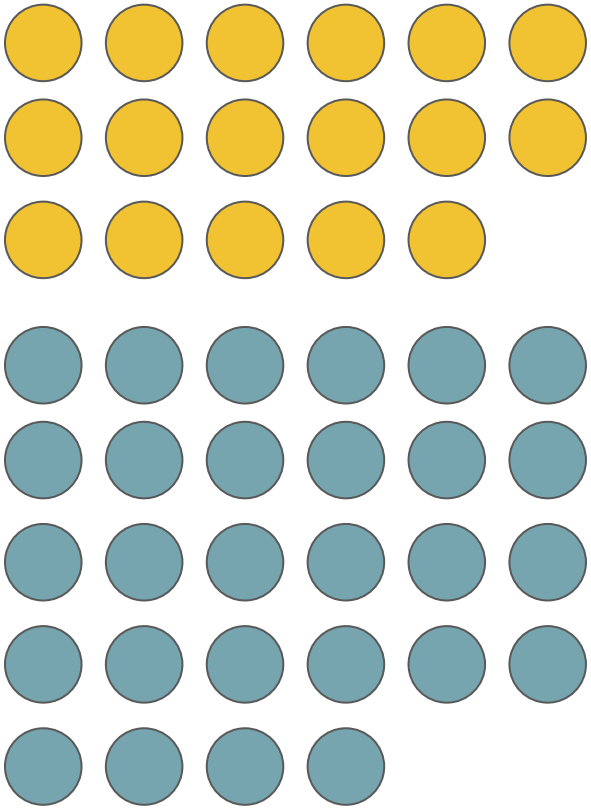
Log these



Symptoms



Causes

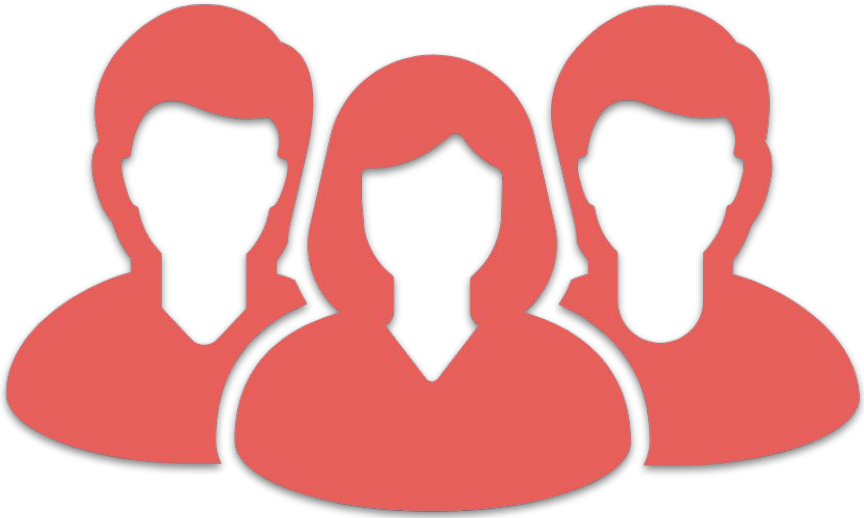


Error Budget

Urgency; but make it (error) budget

SLOs & SLAs

Alert or Page?

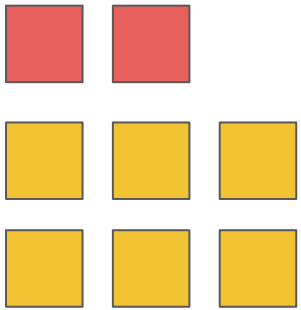


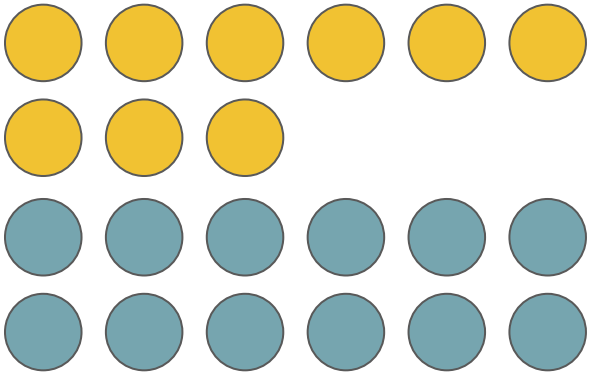
Availability vs. Accessibility

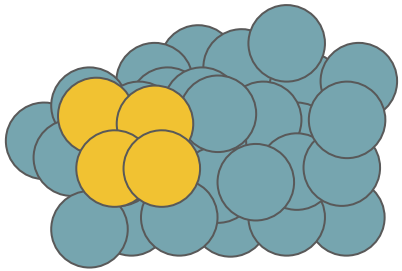
Organise data

by team

Team A







Information

Underload (?)

Thank you!

https://www.datadoghq.com

Daniel Maher @phrawzty
Ara Pulido @arapulido