

Reliability from the ground up ...

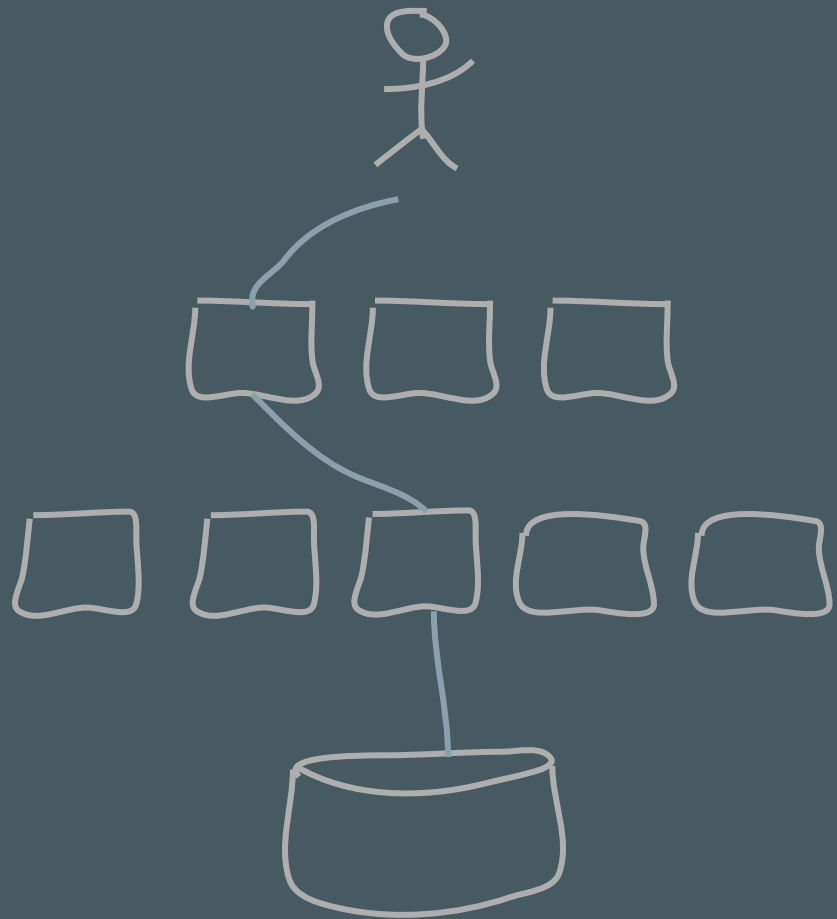
Designing for 5 9s

What do we mean when we talk about reliability?

Reliability, n. - the quality of being trustworthy or of performing consistently well.

Resilience, n. - the capacity to recover quickly from difficulties; toughness, the ability of a substance or object to spring back into shape.

Reliability is a property of the
system
not the sum of its parts



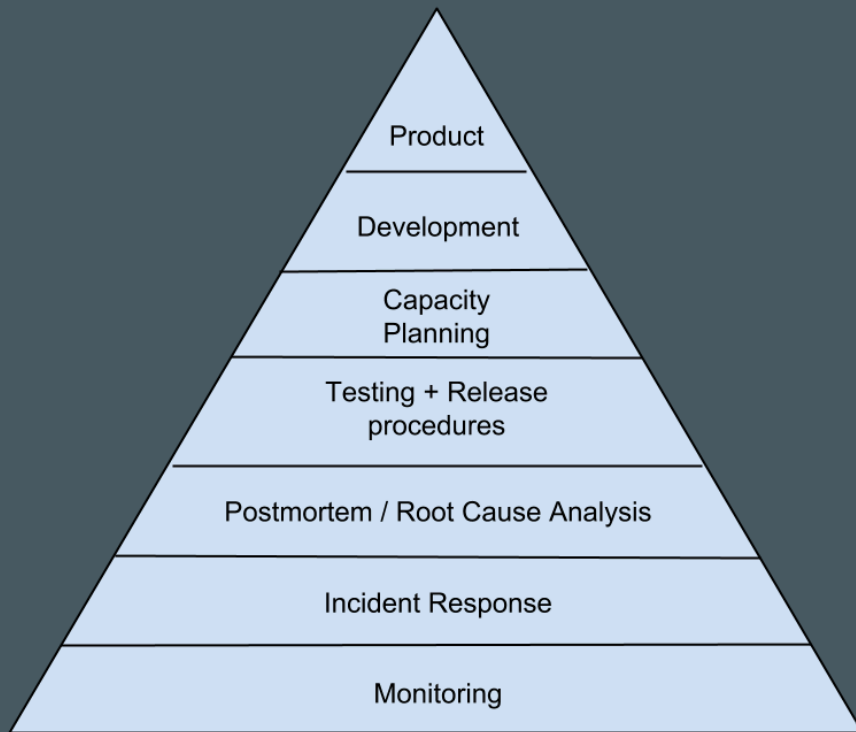


How much reliability do you need?

Optimizations



Baseline requirements
for uptime



Mikey Dickerson's hierarchy of reliability

Time per Year of Downtime

90% 36.5 days

99% 3.65 days

99.9% 8.76 hours

99.99% 52.56 minutes

99.999% 5.26 minutes

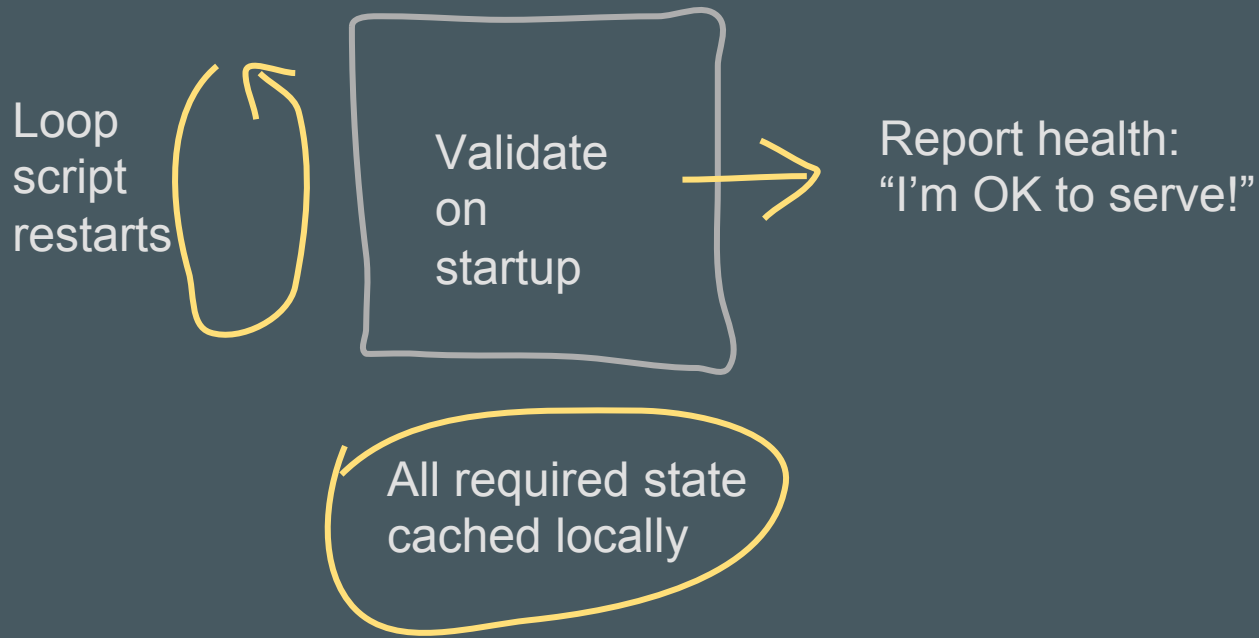
Principles for resilience

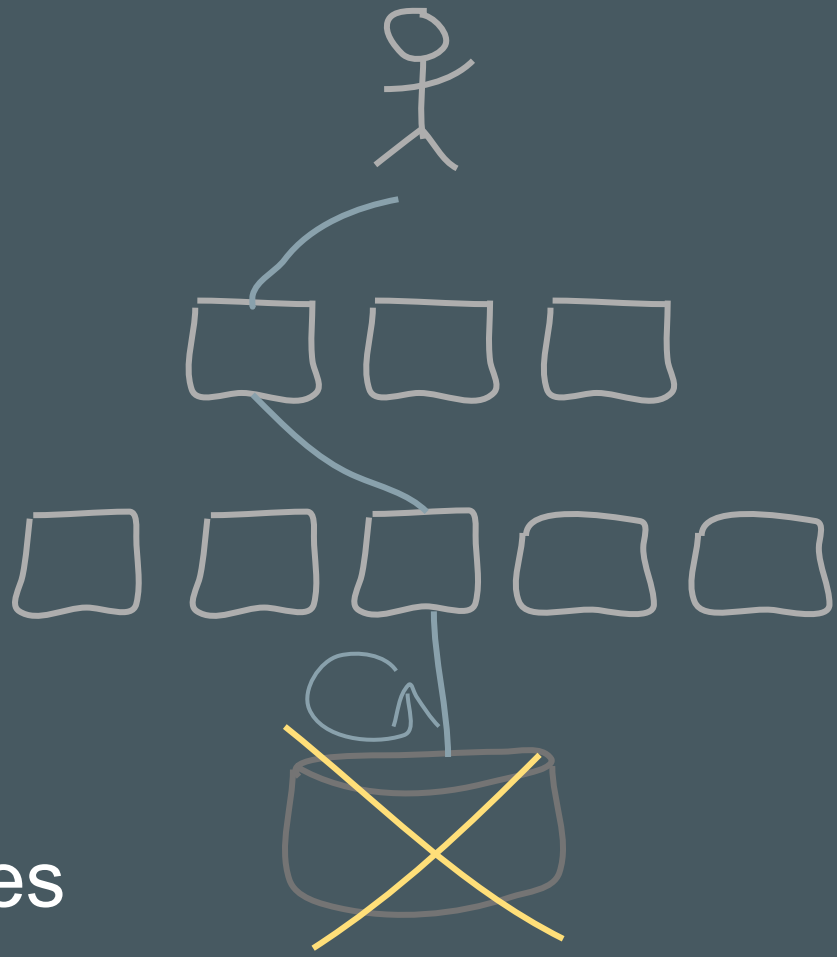
Rule #1:

Every node for itself

“Keep doing what you’re doing, unless it’s actively unsafe.”

Recovering from failure



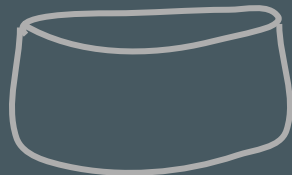


Failures of dependencies

Handling bad inputs



“I’d like a search result and a unicorn!”



“I’ve never heard of a unicorn :-(”



Rule #2:

Everything runs on more than one machine

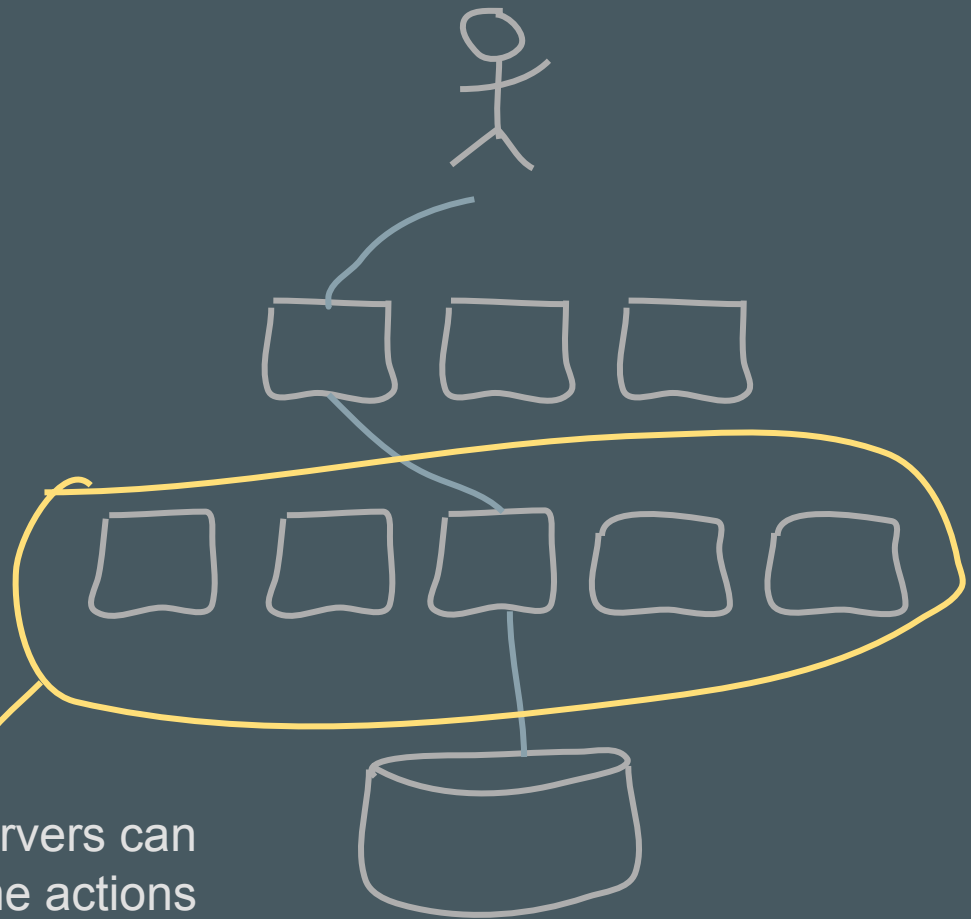
Serving components are stateless

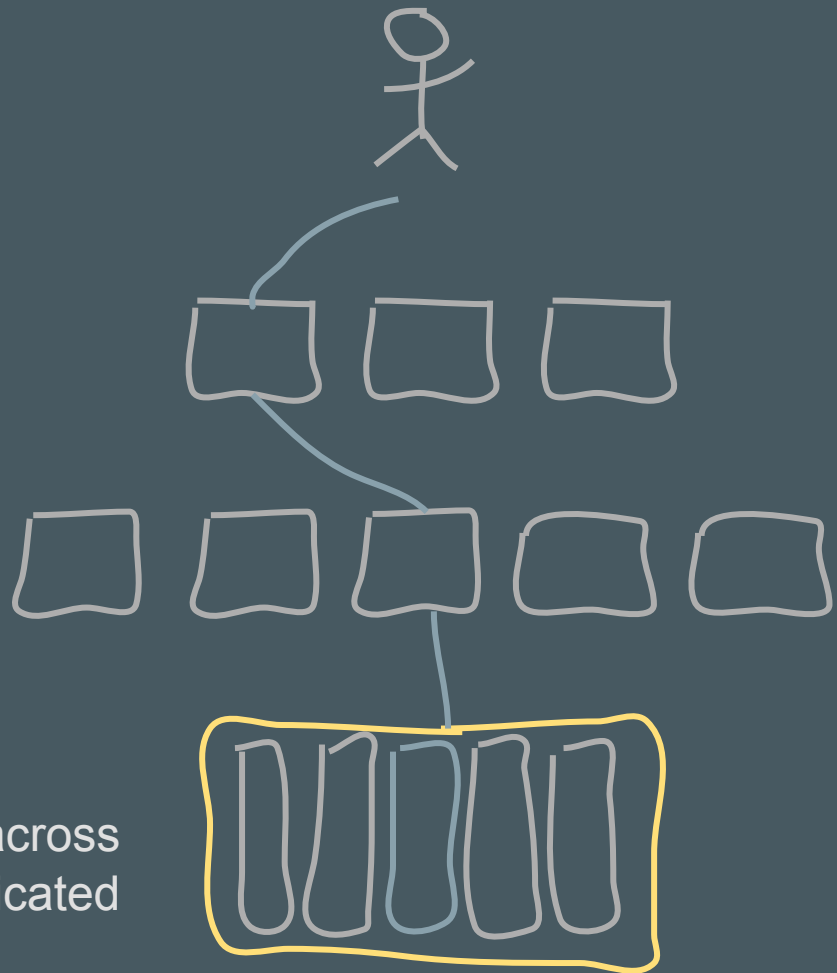
Idempotency and sharding

Data is split across machines and replicated

Idempotency

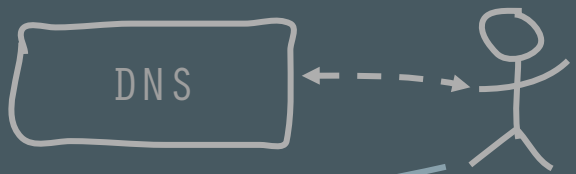
Any of these servers can perform the same actions



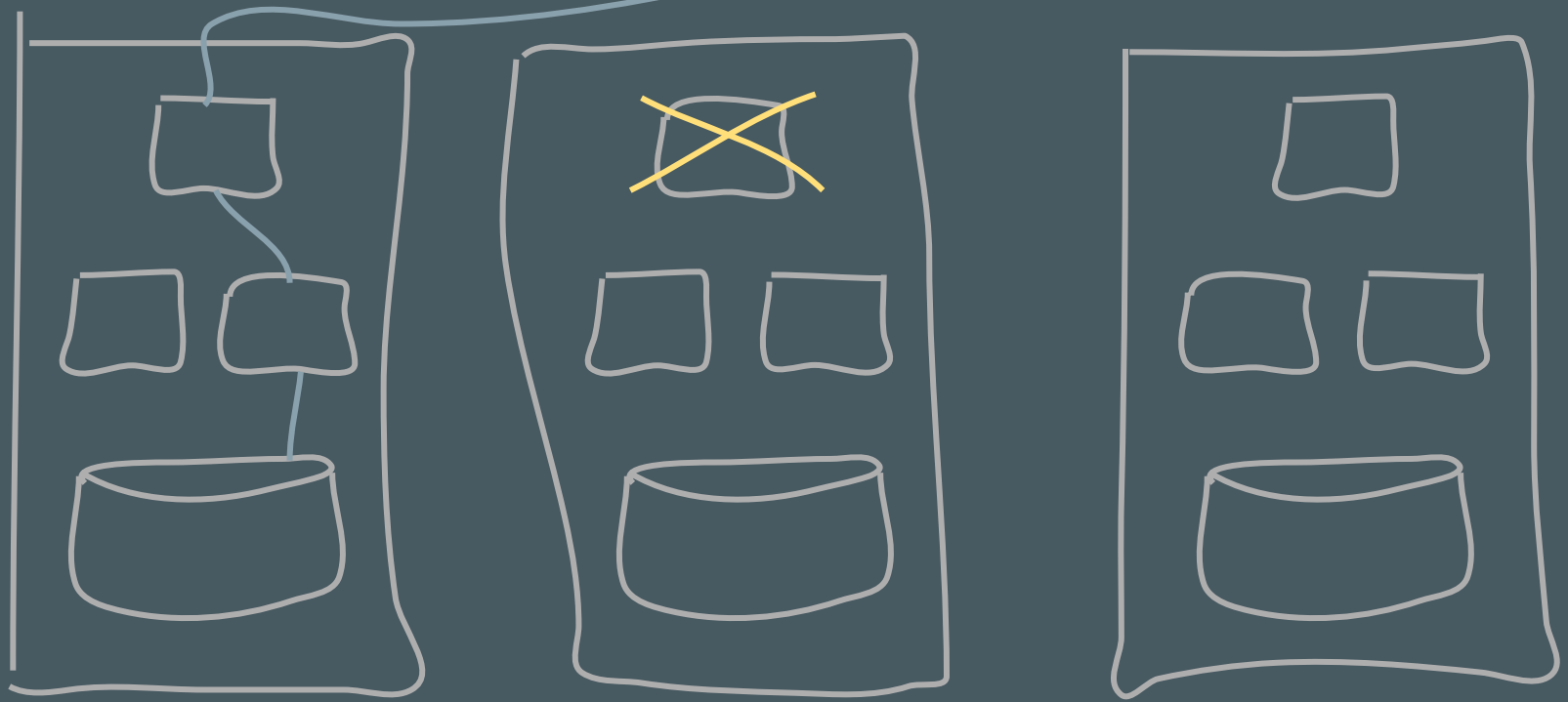


Sharding

Data is split across machines and replicated

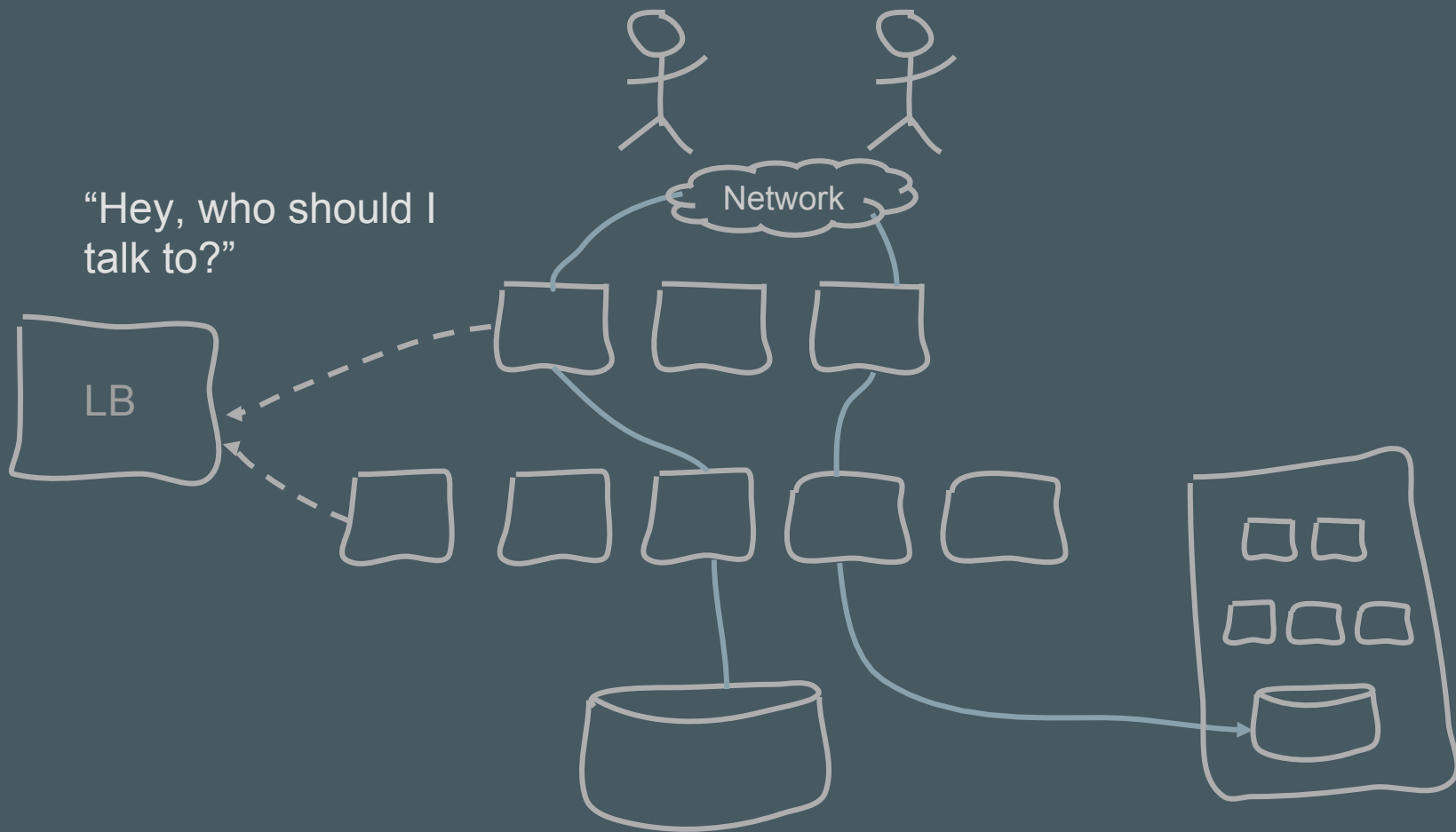


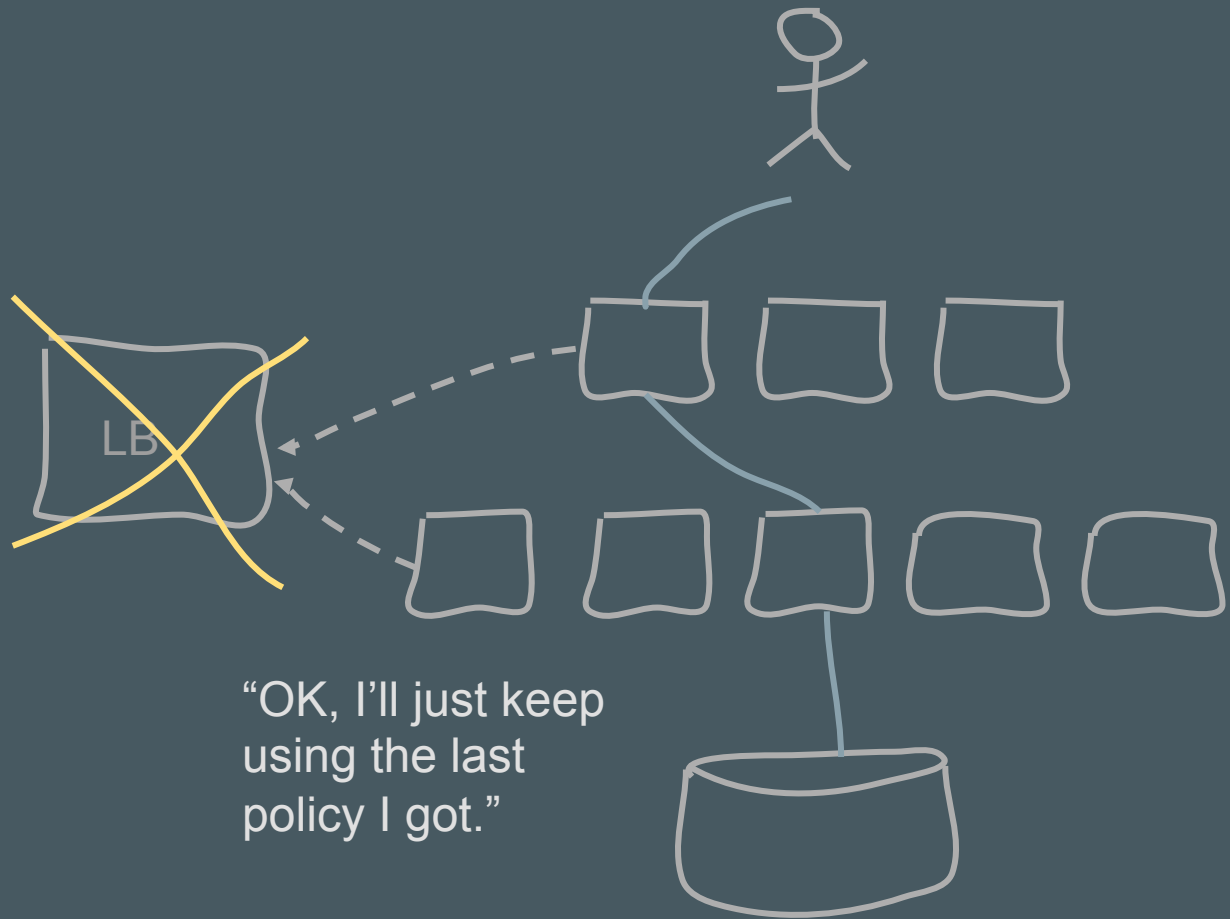
Multiple clusters
provide better redundancy



Rule #3:

Loosely coupled dependencies





“OK, I’ll just keep using the last policy I got.”

Rule #4:

Design for change

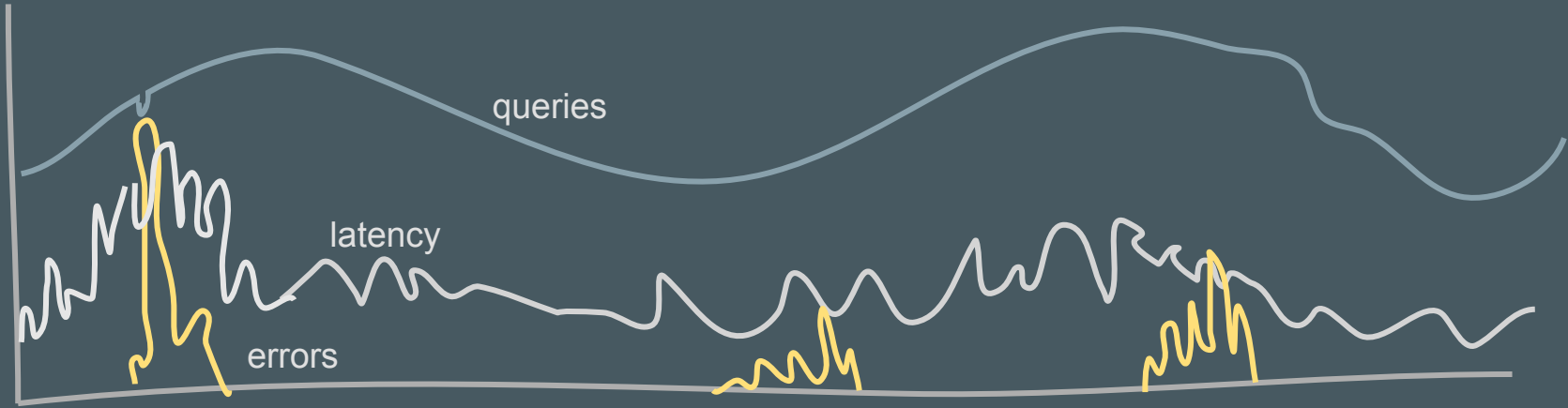
1. Use tools, not processes
2. Check in your configs
3. Canary all changes
4. Rollbacks should always be safe

Global state == global failure



Rule #5:

Observe the system, not the components



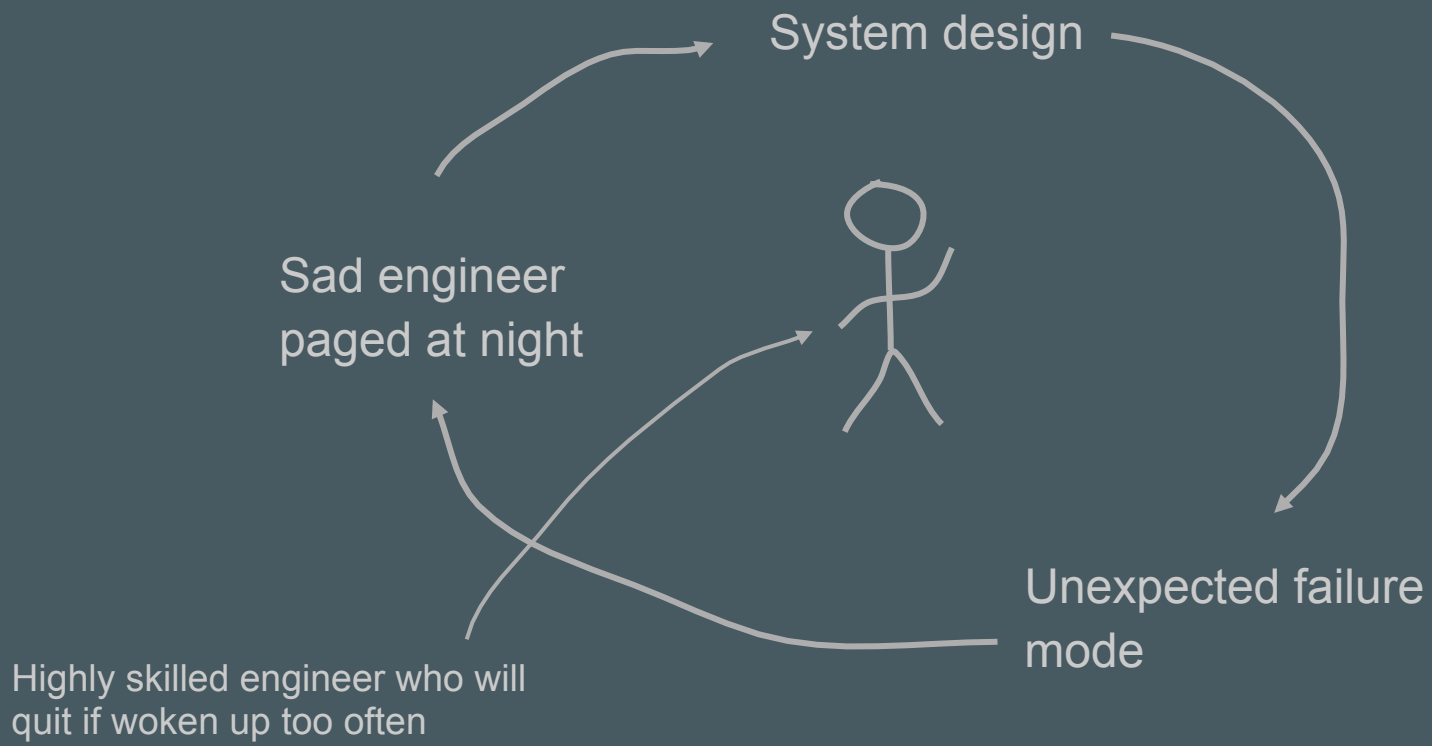
The only* dashboard you
need

Pick a few high level metrics that describe the overall behavior of the system. Make those perfect.

Everything else is background info.

The fifth nine is
people.

-Trisha Weir



Future proof

Supporting an ecosystem

- Healthy systems grow, which means more teams and systems
- Tooling and infrastructure scale better than people and processes

(Come to my talk later!)

The limits of control

grant me the serenity to accept the things I cannot change;
courage to change the things I can;
and **wisdom to know the difference**

Thank you.

Credits:

Susan J Fowler, Production Ready Microservices, O'Reilly, 2016

Mikey Dickerson, Hierarchy of Reliability

Trisha Weir et al, The Fifth Nine: Diverse Perspectives on Reliability, GHC 2015

astrid@gmail.com