

CLOUD STRATEGY // THE ARCHITECT

Six Services Went Down. Google's Report Named Two Dozen.

What GCP's us-west1 outage revealed about failure domains

Service count isn't the failure domain.

6

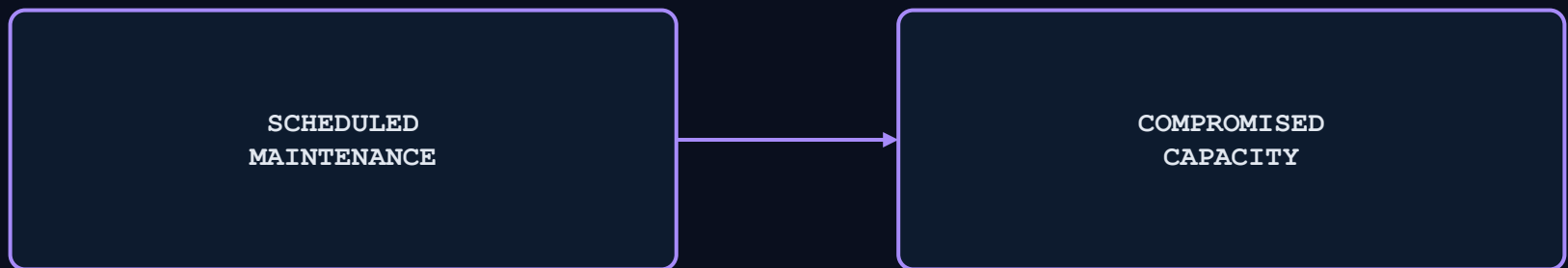
EARLY SIGNAL

20+

FINAL INCIDENT REPORT

Compute, storage, databases, messaging, build tooling, and identity — across both control-plane and data-plane operations.

It started with routine maintenance.



Planned fiber-optic work between data centers inside us-west1 unexpectedly reduced available inter-campus network capacity.

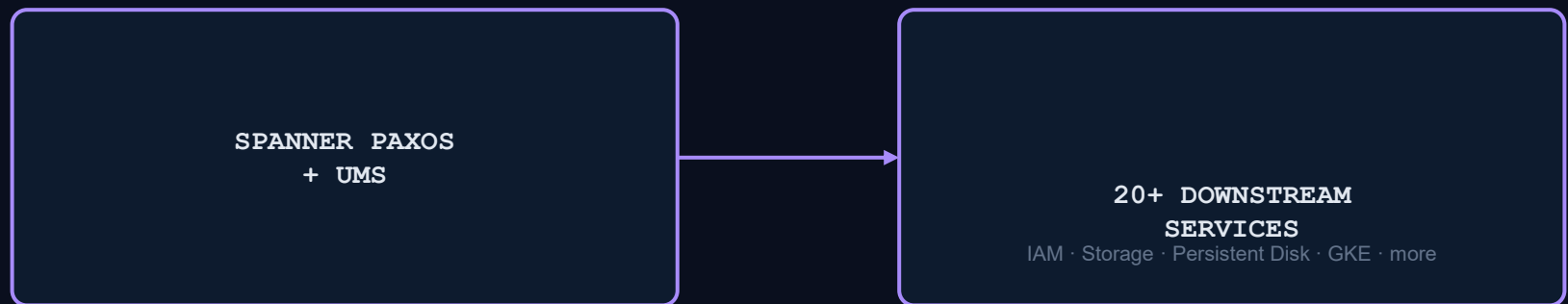
The mechanism built to catch this didn't.

FAILED
REROUTING

THE SAFETY MECHANISM THAT DIDN'T HOLD

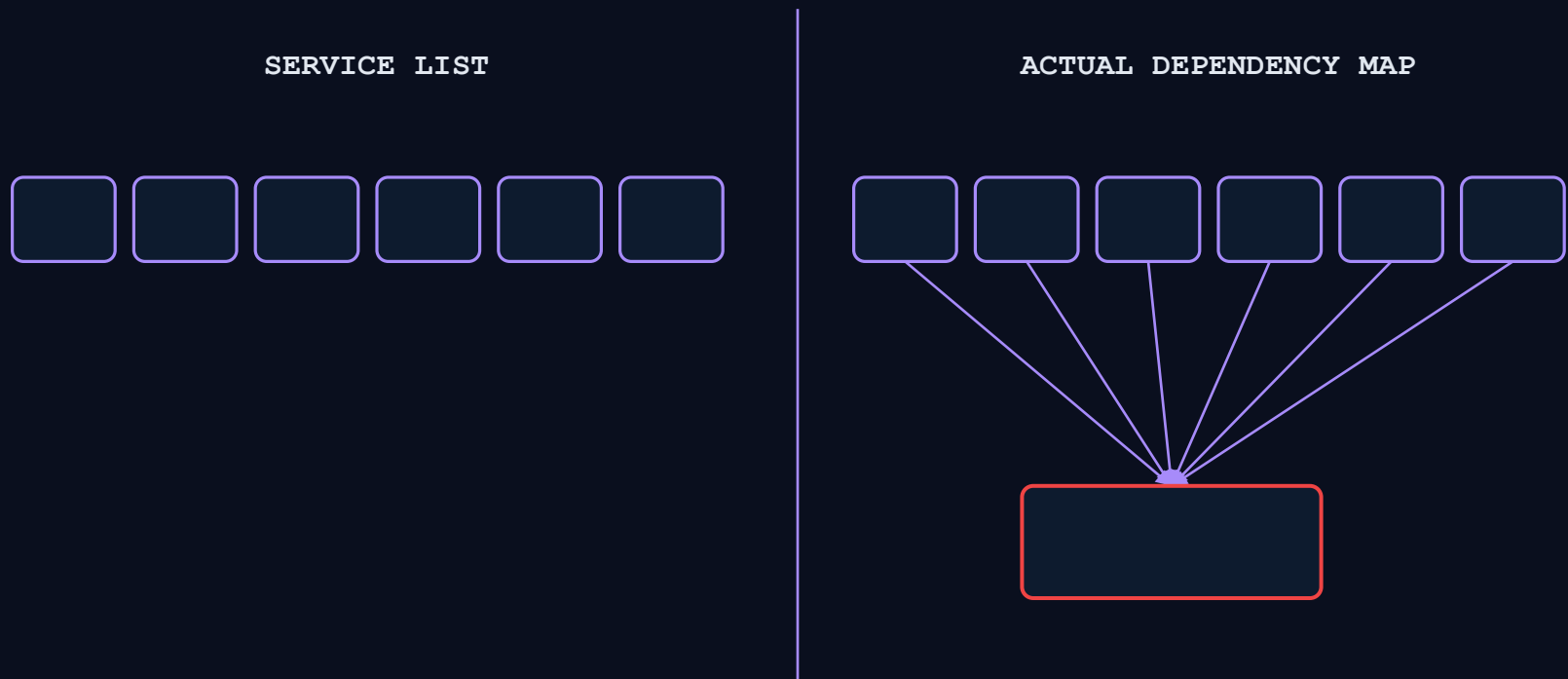
Automated rerouting failed to redistribute traffic to alternate capacity. Traffic volumes exceeded what remained, and the region began to congest.

One network condition reached two core systems.



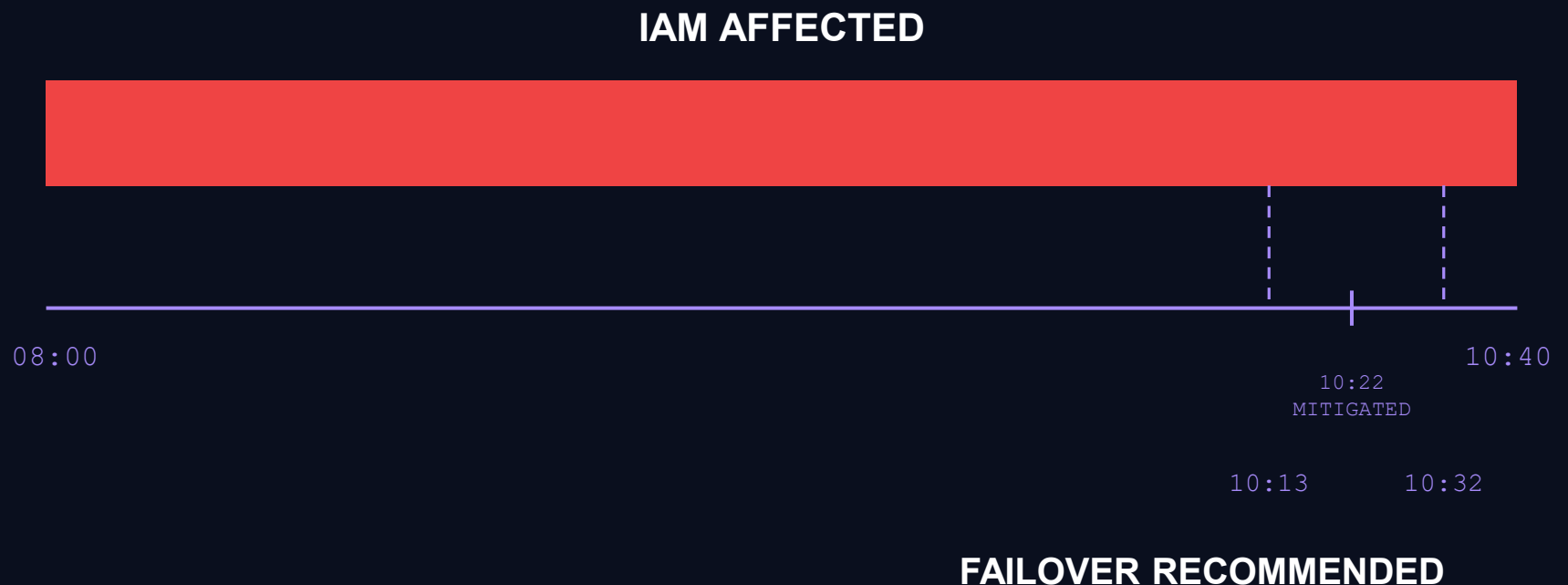
Latency in Paxos consensus and the Unified Metadata Server cascaded into timeouts and errors across products most customers think of as unrelated.

Your service list isn't your dependency map.



Selected services look independent. They share one thing underneath.

Google recommended failover. IAM was on the affected list.



Not proof failover was blocked — a documented tension between the escape path and a service inside the affected list.

Four questions before the next maintenance window.

- 01 What control plane authorizes recovery?
- 02 Where does that control plane fail geographically?
- 03 Can recovery run if the identity layer is impaired?
- 04 Which recovery actions have you actually tested?

`rack2cloud.com` | Follow The Architect for more