Infosys® | CONSULTING

VIEW POINT

WHEN A TINY DNS MISSTEP STOPPED THE INTERNET: WHY ARCHITECTS & CONSULTANTS MUST THINK BIGGER?

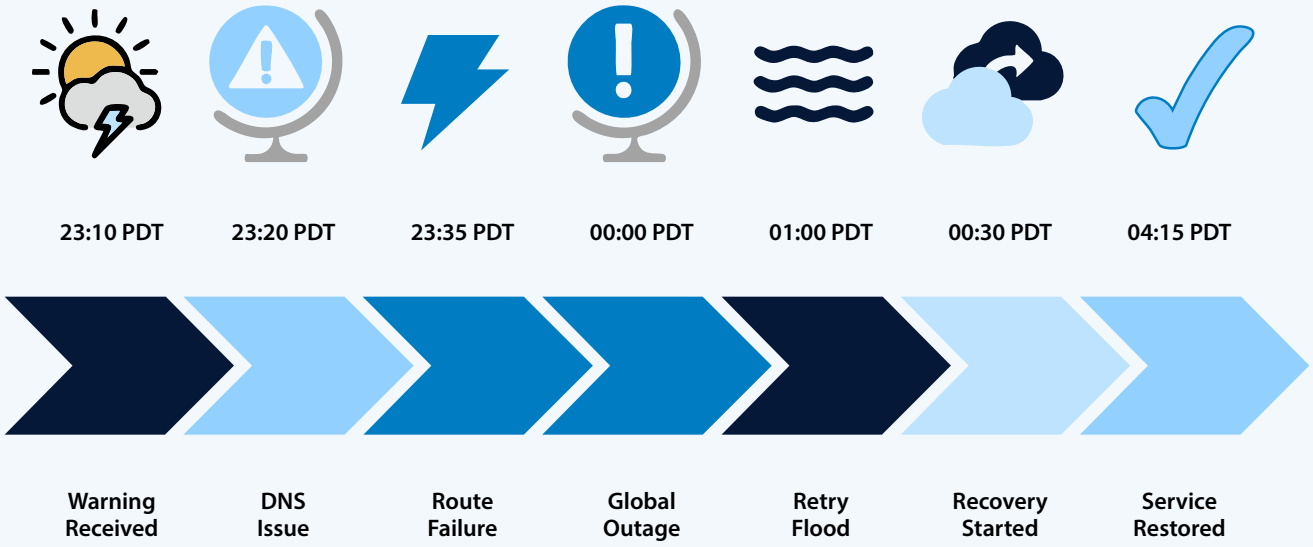
Introduction

It was the Diwali holiday and my daughter looked up at me, frustrated: "Papa, all my Roblox games are down none of them work." I smirked, finally, her games were gone, which I'd secretly welcomed for the break but then it struck me: the games are probably running on AWS. Could this be a real outage? I logged into the AWS Console, flicked open the Service Health Dashboard, and the alarms were already flashing. Within minutes I knew, one tiny glitch in DNS had brought half of the internet to a halt.

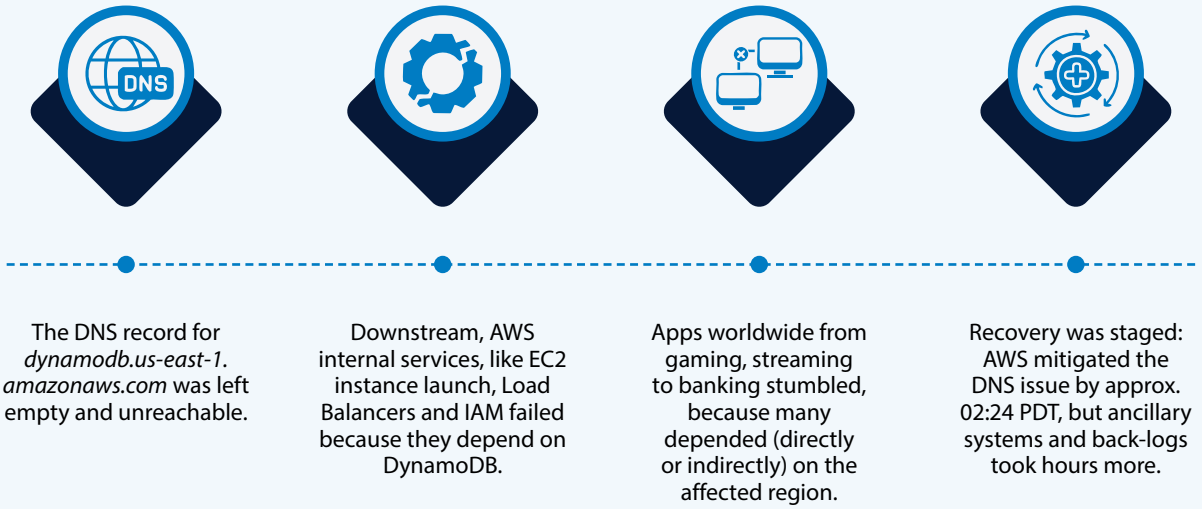
The big event in short

In the early hours of 20 October 2025, in the US-EAST-1 region, Amazon Web Services (AWS) experienced a major outage. DynamoDB's DNS automation suffered a race-condition that effectively deleted critical endpoint records.

Here is the timeline of events:



As a result:



In short: a "**small**" DNS mis-automation, in a critical region, cascaded into a major internet disruption.

And yes, it happened again on 28 October 2025 around 13:36 PDT, multiple AWS services were impacted in US-EAST-1 region due to increased Error Rates and Latencies. What about Microsoft Azure? Between 15:45 UTC on 29 October and 00:05 UTC on 30 October 2025, customers and Microsoft services leveraging Azure Front Door (AFD) may also have experienced latencies, timeouts, and errors. Affected Azure services include, but are not limited to: App Service, Azure Active Directory B2C, Azure Communication Services, and more.

External Document © 2025 Infosys Limited

Why this matters in Technology Transformation and Architecture

For organisations undergoing cloud transformation and application portfolio rationalisation, the lesson is stark: **resilience is built not just in code or infrastructure, but in the architecture of dependencies.**

Cloud-Engineer's View: Immediate actions & priorities

When your monitoring lights up, as the cloud engineer you:

Remain calm	Immediate action	Prioritise	Mitigate	Communicate	Recovery
Your team watches you. Clear head.	Immediately check the health dashboards, region status and logs to isolate: Is it my code, my region, or provider-side?	Are my critical services (authentication, payment, data store) down? Which can I fallback?	switch traffic (if you can) to alternate AZ/region; scale up fallback systems; disable non-critical launches to preserve capacity.	internal stakeholders first, then downstream teams, then customers (depending on SLA).	Once recovery begins, analyse logs, root-cause evidence, ensure you capture timing/ data for post-mortem and for design improvements.

The engineer's job is "keep the ship afloat" and ensure minimum business impact while documenting as you go. An engineer's go to services are (as mentioned below):

AWS Health Dashboard | **Amazon Event Bridge** | **Amazon CloudWatch** | **AWS Trusted Advisor** | **AWS Config** | **Amazon EC2** | **Amazon DynamoDB** | **Amazon S3** | **Application Logs**

Summary

Immediate Actions

- Check service health dashboards.
- Validate impact on running workloads.
- Redirect traffic via alternate regions if possible
- Communicate with DevOps and SRE teams.

Priorities

- Restore critical services.
- Monitor logs and alerts.
- Keep stakeholders informed.

Mindset

- Stay calm, follow incident playbooks.
- Focus on containment and recovery.

External Document © 2025 Infosys Limited

Cloud-Architect's View: What you do now & future actions

As the architect, your view goes broader:

Immediate action:
Immediately you verify whether your design assumed single-region dependencies (e.g., DynamoDB only in US-EAST-1 region) and whether there are critical single points of failure.

Identify blast radius:
You check the application portfolio: which microservices, data stores, identity services are region-bound? Do we have cross-region/data-replicated architecture? Find out the overarching blast radius.

Collaborate:
You coordinate with engineering to route traffic away, enable fail-over regions, cut over to backups, mobilise DR runbooks.

In the medium/long term:
You perform architecture rationalisation. For example: move from monolithic region-centric design to distributed architecture; ensure each service has fallback in another region/another provider; review DNS, networking, automation pipelines (since this outage was in automation itself).

Strategy & direction:
You update the application portfolio strategy: retire or refactor systems that cannot tolerate regional failure; classify services by criticality and define their resilience target (RTO/RPO).

Finally:
You ensure that the contract with the cloud provider (SLAs) aligns with your risk tolerance, and you ask: what if the "region" fails? Do we own our data? Can we switch provider/region quickly?

An architect investigates the following services (as mentioned below):

- Well Architected Framework
- Multi Region Strategy
- Disaster Recovery Strategy
- Infra as Code
- Resilient Application Design
- Observability & Monitoring
- Chaos Engineering
- Development & Operations and Process Automation
- Identity & Security Resiliency

Summary

Immediate Actions

- Assess architectural dependencies on affected services.
- Review and activate DR plans and multi-region failover strategies of required.
- Review service mesh and observability tools.

Priorities

- Ensure business continuity.
- Identify single architectural points of failure.
- Engage with cloud provider for RCA.

Future Actions

- **Application Portfolio Rationalization (APR):** Identify apps tightly coupled to single-region services.
- **Redesign for Resilience:** Adopt multi-region, multi-cloud strategies.
- **Well-Architected:** Focus on reliability, performance and operational excellence.

External Document © 2025 Infosys Limited

Senior-Management View: Business continuity and strategic oversight

From the senior-management seat:

Immediate action

While immediate act would be to assemble a response team to maintain leadership visibility, reassure stakeholders, and preserve trust and clear communications. Engage with legal and compliance to evaluate SLA breaches, regulatory obligations, and customer commitments and maintain transparency.

Strategic direction

The incident underscores a critical truth that cloud services, while more reliable than traditional on-premises hosting, are not infallible. Senior leaders must adopt a **risk-adjusted view of technology**, treating cloud dependencies as they would any other key business dependency. This means asking:

- Are we overly reliant on a single cloud provider or a region?
- Can our services persist if one provider suffers a complete outage?
- Do we have geo-redundant and multi-cloud fallback strategies in place?

Future investment

Direct investment toward resilience initiatives that include multi-region and multi-cloud architectures. Demand proof of disaster recovery readiness, runbooks, ownership clarity, and tested failover mechanisms. Ensure architecture reviews explicitly address provider diversification and dependency risk.

Managing technology risk

Technology risk must be distributed, not concentrated. Clouds may be a sophisticated version of on-premises, but they are not invincible. Strategic oversight must evolve to a risk-adjusted view of technology, treat cloud architecture as a dynamic, risk-managed asset. One that is architected for business continuity, not just convenience.

Summary

Immediate Actions

- Assemble response team.
- Communicate with customers and partners.
- Assess financial and reputational impact.

Priorities

- Minimize business disruption.
- Ensure transparency and trust.
- Align IT response with business continuity plans.
- Strategic direction.

Future Actions

- Invest in **Multi Cloud Strategy & Governance.**
- Mandate **Cost Optimization** and **APR** to reduce technical debt.
- Build a **resilient cloud operating model** with clear accountability and escalation paths.
- Manage **Technology Risk**.

External Document © 2025 Infosys Limited

Thought-leadership perspective: The transformation lever

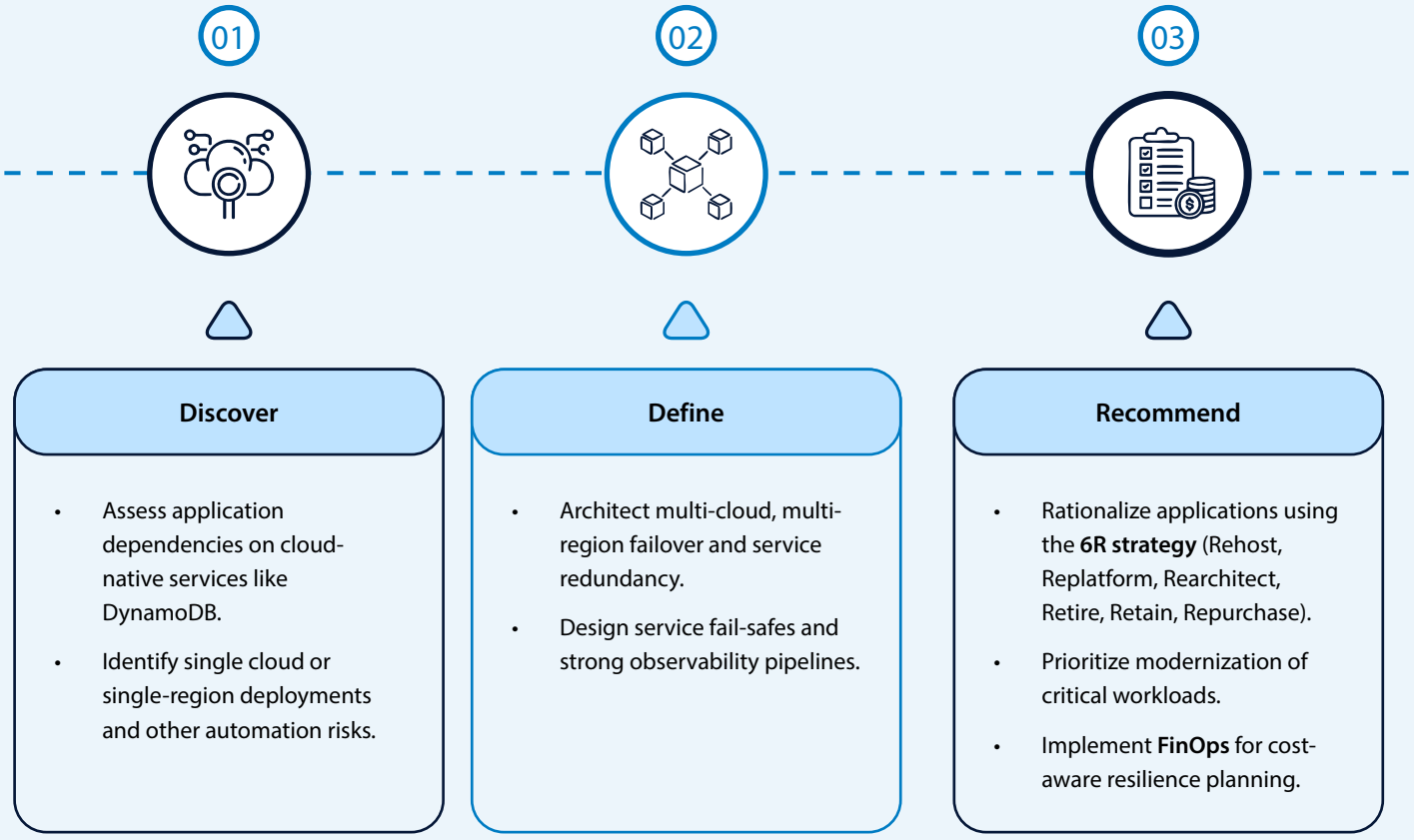
In this era of digital transformation, organisations are migrating, rationalising, modernising their application portfolios and reshaping architecture. But they often assume "cloud = always-on" and forget: **the cloud inherits new dependency chains**. Automation, DNS, routing, data-stores, they all become potential dominoes.

The recent AWS, Azure events make it clear even the largest cloud provider has a single regional failure due to DNS automation, yet the ripple across the internet was massive. This elevates the importance of architecture that explicitly **decouples** from single critical endpoints, **rationalises** the application portfolio to classify and isolate dependencies, and **validates** resilience via drills.

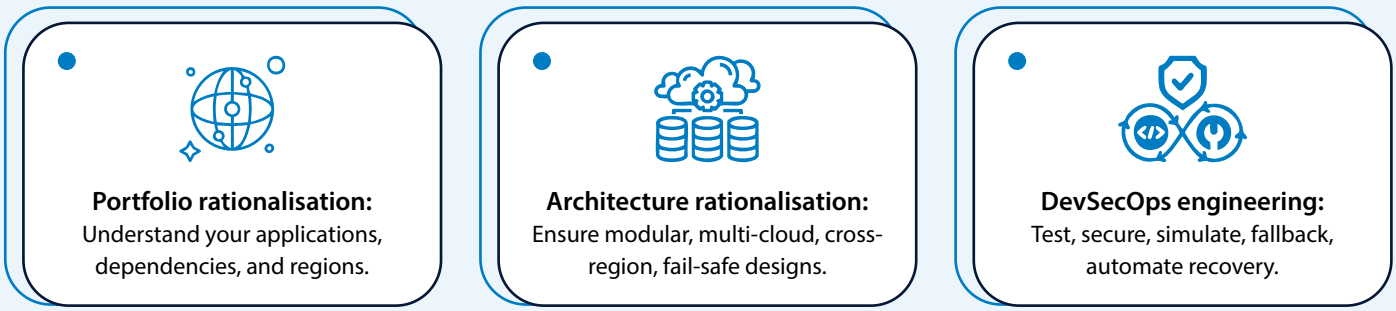
The Consultant's Lens: How Could This Be Prevented?

Architecture Advisory & Application Portfolio Rationalisation to the Rescue

Using the TT Cloud Offerings framework:



Transformation offering must thus anchor three elements:



When a DNS glitch brings half the internet down, it's no longer hypothetical: it's live proof your design must expect failure, not just infrastructure failure but service chain failure.

External Document © 2025 Infosys Limited

Conclusion & Next Steps

In short: A minute automation bug in DNS triggered a global outage. For our clients, the answer isn't just patching that bug, it's *rethinking architecture, managing technology risk and rationalising the application portfolio* to ensure your business doesn't collapse when your cloud service provider does.

Next steps for organisations:

- Map your current portfolio: region, provider, dependency.
- Identify: Critical services and their failure impact.
- Design: For multi-az (availability zone)/multi-region resiliency or multi-cloud fallback.
- Run failure simulations: DNS failure, region fail-over, provider outage.
- Embed this into your transformation roadmap: not as an after-thought, but as a strategic pillar.

If you'd like help building a tailored architecture and application portfolio rationalisation framework for your organisation, let's schedule a call.

External Document © 2025 Infosys Limited

Infosys® | CONSULTING

About the Author:

Chirantan Saha
Principal

Chirantan Saha is a Principal at Infosys Consulting based in Singapore; he is a veteran cloud engineer and architect turned consultant with 20+ years in enterprise architecture, cloud migration and infrastructure transformation. He specialises in helping organisations rationalise their applications, optimise cloud strategy and build resilient digital platform architecture, ensuring workloads deliver solutions that are not only resilient and scalable but also cost-efficient.

ABOUT INFOSYS CONSULTING:

Infosys Consulting is a next-generation consulting partner that bridges strategy and execution. With an AI-first mindset, deep industry knowledge, and the combined strengths of business and technology consulting, it helps enterprises turn bold vision into tangible outcomes, faster, smarter, and at scale.

Infosys Consulting is helping some of the world's most recognizable brands transform and innovate. Our consultants are industry experts that lead complex change agendas driven by disruptive technology. With offices in 20 countries and backed by the power of the global Infosys brand, our teams help the C-suite navigate today's digital landscape to win market share and create shareholder value for lasting competitive advantage.

CONNECT WITH US

LinkedIn YouTube