

Root Cause Analysis (RCA) Document

Incident: Major service outage in US-EAST-1 region northern Virginia
Source: AWS Public Updates, Reuters, Business Insider

Prepared by: Preeti

AWS Outage summary

On **October 20, 2025**, AWS experienced a major service disruption in the **US-EAST-1 (Northern Virginia)** region. The outage impacted multiple AWS services including DynamoDB, EC2, Lambda, and internal AWS APIs, leading to downtime for major global applications such as Snapchat, Fortnite, Ring.

The issue originated from **DNS resolution failures** for Dynamo DB endpoints, causing cascading dependency failures across services.

(**Note:** A cascading dependency failure means that when one main service fails, other services depending on it also stop working, causing a chain reaction.)

Impact Analysis

| Category | Details |
|-------------------|--|
| Start Time | 12:41 PM IST, October 20, 2025 |
| End Time | 3:30 AM IST, October 20, 2025 |
| Duration | 15 hours (with partial degradation) |
| Region Affected | US-EAST-1 (Northern Virginia) |
| Services Affected | DynamoDB, EC2, Lambda, API Gateway, Cloud Formation, S3, CloudWatch |
| External Impact | Global service disruptions for apps like Alexa, Snapchat, Ring, Venmo, Slack, Zoom |
| Business Impact | Users unable to authenticate, load apps, or access AWS-hosted web services |

Root Cause: Increased Error Rates and Latencies

There's a real technical issue going on here. It's disrupting DynamoDB and impacting 20 other services, which leads to "increased error rates and latencies."

Primary cause: A failure in DNS resolution of the DynamoDB API endpoint in the US-EAST-1 Region.

- The DNS error prevented many services from locating the correct IP addresses for the DynamoDB endpoint, which is a critical service. [Al Jazeera](#)
- Because many dependencies (AWS internal services and many customer-services) rely on DynamoDB or its endpoints in US-EAST-1, the failure cascaded across multiple services. [The Register+1](#)
- The problem appears to be internal (AWS infrastructure) rather than caused by an external cyberattack.

Action taken Immediately

Engineers were immediately engaged and are actively working on both mitigating the issues, and fully understanding the root cause, and they took step to resolve this.

- AWS Operations team quickly declared the incident after noticing high error rates.
- The team investigated and found the issue was caused by DNS lookup failures for the DynamoDB service.
- DNS settings were re-routed, and caches were refreshed to fix the problem.
- Services that depended on DynamoDB were gradually restored to normal.
- AWS shared regular updates on the Service Health Dashboard and @awscloud Twitter account to keep users informed.

Lessons Learned / Recommendations

- Continuous monitoring and quick escalation are critical to detect and resolve DNS-related issues faster.
- Dependency mapping between AWS services (like DynamoDB, API Gateway, and Lambda) helps understand impact scope early.
- Regular DNS health checks and cache validation should be part of proactive maintenance.
- Improved automated failover mechanisms can reduce downtime during similar incidents.
- Communication through the AWS Service Health Dashboard and status channels should continue promptly and transparently.
- Better documentation and post-incident drills help teams respond faster to similar outages in the future

Last updated

AWS said in an update at 6:35 a.m. ET that the DNS issue had been “fully mitigated” and that **AWS service operations were “succeeding normally.”**

“These issues can happen when systems become overloaded or a key part of the network goes down, and because so many websites and apps rely on AWS, the impact spreads quickly,” he added - Rob Jardin, chief digital officer at cybersecurity company NymVPN.

Conclusion

The AWS outage on October 20, 2025, happened because of a DNS lookup problem that affected the Dynamo DB service and other connected services. This caused interruptions for around 15 hours.

The AWS team quickly found the issue, fixed the DNS settings, and slowly restored all services. They also kept users updated through the AWS Service Health Dashboard and official channels.

In the future, AWS will work on better monitoring, stronger backup systems, and faster recovery plans to stop similar issues from happening again.

Reference Source of the context:

<https://www.cnn.com/2025/10/20/amazon-web-services-outage-takes-down-major-websites.html>

[AWS outage exposes Achilles heel: central control plane • The Register](#)