AWS Outage: So What Happened?

From CRN: "**Amazon's Outage Root Cause, $581M Loss Potential And 'Apology:' 5 AWS Outage Takeaways"**

URL: https://www.crn.com/news/cloud/2025/amazon-s-outage-root-cause-581m-loss-potential-and-apology-5-aws-outage-takeaways?page=1

Published: October 27, 2025

Situation: A large portion of AWS was down for about 15 hours on Monday October 21st and brought down connectivity for businesses, VOIP phones, government systems, hospitals, and schools. It also affected people in their homes with malfunctioning IoT appliances such as "smart" mattresses and even cat litter boxes. Losses are estimated to be $581 million.

Task: As soon as they became aware of the problem, Amazon began searching for a root cause. Early on, they realized there was a DNS problem, but it took a deeper dive to locate the culprit. Two automatic systems had tried to update the same DNS database. The result was that it actually wiped the DNS entries needed by AWS' DynamoDB database, which was central to coordination of the distributed system.

Action: DNS services were restored, and DynamoDB was disabled until they could fix the automated processes and ensure the double-update issue wouldn't happen again. They also are working on a way to monitor the processes and stop them proactively if a conflict seems imminent. They also will examine how latency caused the processes to be delayed and create the conflict.

Result: The main lesson from this is that we all once again question the security and robustness of the cloud and its widely distributed, extremely complex infrastructure. Analysts recommend that users of cloud invest in resiliency by deploying on-premises backups and hybrid solutions.

Conclusion:

Zerowait's engineering team works with our customers to protect their organization's handling of critical and proprietary data, including their FileMaker databases. Our customers recognize that they must prioritize secure, on-premises storage to mitigate risks from external data stores and data transmissions. Zerowait's SimplStor-NVMe solutions offer a robust alternative, providing high-performance, encrypted storage arrays designed for on-premises environments.

Unlike off-premises Cloud solutions, Zerowait SimplStor ensures data remains under direct control, with features like end-to-end encryption and redundant failover. Zerowait's Solutions mitigate the risk of unencrypted data interception. The Zerowait approach enhances compliance with regulations like GDPR or HIPAA and provides reliable, cost-effective scalability while safeguarding sensitive information from leaks and providing low-latency access for mission-critical operations.

Zerowait Corporation
707 Kirkwood Hwy, Wilmington DE 19805
TEL: 302-996-9408