Reports of cloud system failures and discuss the causes of each incident

Name: Bingying Liang

ID: 48999397

CS7346 Cloud Computing

June 19 2023

Cloud system failures can occur due to various reasons, including human error, technical issues, and natural disasters. However, the exact cause of each incident can be hard to pin down, and a thorough investigation is often required to fully understand the contributing factors. In the following are some cloud system failures.

1. **Amazon Web Services(AWS) outage in 2020**: A major outage impacted AWS's Kinesis Data Streams, which are used to process large amounts of data in real-time. The outage affected many services that rely on it, such as Amazon's Ring doorbells, iRobot's Rooomba, and software created by Adobe and Roku. The cause was a capacity-related issue in the Kinesis service, with the addition of new capacity having triggered an issue that led to the outage.[5]
2. **Google Cloud outage in 2019**: Goolge's Cloud services, including YouTube, Gmail, and Google Drive, went down for several hours. The company said the outage was due to a configuration change that was intended for a small number of servers in a single region, but it was incorrectly applied to a larger number of servers across several neighboring regions. [2]
3. **Microsoft Azure outage in 2018**: Microsoft's Azure cloud service experienced a global outage due to a severe weather event. Lighting strikes near one of their data centers led to a power voltage increase that was detected by datacenter systems, which initiated an automatic shutdown. Many services that rely on Azure, including Office 365, were affected.[4]
4. **AWS S3 outage in 2017**: AWS's Simple Storage Service(S3) in the US-East-1 region had a major outage that affected many services. The cause was a debugging issue. And authorized S3 team member using an established playbook executed a command that was intended to remove a small number of servers for one of the S3 subsystems. However, the input to the command was entered incorrectly, leading to a larger set of servers to be removed than intended.[6]
5. **IBM Cloud outage in 2020**: IBM Cloud suffered a multi-zone, four-hour interruption of services on June 10, 2020 that affected IBM cloud customers in Washington, D.C., Dallas, London, Frankfurt, and Sydney. The outage impacted general cloud services, Kubernetes services, App connect, and Watson AI cloud services. An investigation revealed that a third party network provider flooded the IBM Cloud network with incorrect routing, which impacted IBM Cloud services and 80+ data centers. Another IBM cloud outage was reported on June 25, 2020, which lasted for three hours. IBM's cloud services went offline for over

three hours, afftecting several services and websites. IBM later revealed that the network outage was caused by a third-party BGP(Border Gateway Protocal) issue. BGP is responsible for routing traffic across the internet, and problems can cause significant outages.[1]

Outages and downtime are inevitable. But the end goal for IT decision makers should be to incorporate end-to-end network resilience to eliminate downtime, quickly discover where a problem occurred and remediate the issue. Speaking to Toolbox, Todd Rychecky, VP Sales, Americas at Opengear said, “It’s not if an outage is going to occur, but when it’s going to occur. It’s important to have a secure remote access solution implemented in your network, so you can react and remediate quickly. Be ready, be prepared, be smart.” The comman causes of cloud outages are data format bugs (a type of data whose format becomes incompatible with newer versions of the software), fault detection/handling bugs (componenet failures), and timing bugs.[3] Actually, ferwer hardware problems that lead to incidents.

Therefore, The cause of these incidents often involves a combination of factors that span human error, operational procedures, system behavior under failure conditions, and more. To prevent such failures, companies continuously invest in resilience measures, such as redundancy, backup and recovery strategies, error detection and correction methods, and staff training. There are some lessons from the outrage, and several ways to build fault-tolerance into public cloud infrastructure[7]:

1. Monitor on the edges of the network: Concentrate performance, throughput and security monitoring components that manage internet access or are cloud-facing. Part of this is ensuring you have a robust global domain name service (DNS), and perhaps even a backup DNS.
2. Monitor overall internet traffic patterns. Global internet traffic issues, security issues or outages can negatively affect access to your cloud services. One possibility is to use Opens a new window Oracle’s Internet Intelligence MapOpens a new window to watch for cable cuts, disasters, government-imposed internet shutdowns and other issues.
3. Consider a redundant or multi-cloud footprint. This includes both using redundant hardware and software at specific geographic locations and multiple physical cloud instances. You can configure a second cloud component with critical components as a backup location to which you can failover when the primary site fails. Alternatively, you can logically

cluster multiple separate locations and route traffic to each site depending upon network bandwidth, throughput or performance.

4. Implement and practice a disaster recovery plan Put plans in place to deal with expected outages, and test those plans. These should include natural disasters such as loss of local electrical power, failure of one or more hardware components and internet-related issues such as DDoS attacks. Document and communicate these plans, and test them frequently.

Be ready, be prepared, be smart.

References

[1] *5 Cloud Outages That Shook the World in 2020*. URL: https://www.spiceworks.com/tech/cloud/articles/5-cloud-outages-that-shook-the-world-in-2020/. (accessed:06.19.2023).

[2] *Google Cloud Networking Incident #19009*. URL: https://status.cloud.google.com/incident/cloud-networking/19009. (accessed: 06.19.2023).

[3] Haopeng Liu et al. "What Bugs Cause Production Cloud Incidents?" In: *Proceedings of the Workshop on Hot Topics in Operating Systems*. HotOS '19. Bertinoro, Italy: Association for Computing Machinery, 2019, pp. 155–162. ISBN: 9781450367271. DOI: 10.1145/3317550.3321438. URL: https://doi.org/10.1145/3317550.3321438.

[4] *Postmortem: VSTS 4 September 2018*. URL: https://devblogs.microsoft.com/devopsservice/p=17485. (accessed: 06.19.2023).

[5] *Summary of the Amazon Kinesis Event in the Northern Virginia (US-EAST-1) Region*. URL: https://aws.amazon.com/message/11201/. (accessed: 06.19.2023).

[6] *Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region*. URL: https://aws.amazon.com/message/41926/. (accessed:06.19.2023).

[7] *When Cloud Is Not Reliable: 4 Tips to Deal With Cloud Outages*. URL: https://www.spiceworks.com/tech/cloud/articles/when-cloud-is-not-reliable-tips-to-deal-with-cloud-outages/.