EJSIT
European Journal of Science, Innovation and Technology
ISSN: 2786-4936
www.ejsit-journal.com
Volume 5 | Number 3 | 2025

How Cloud Service Reliability is Improved after Shifting from Reactive to Proactive Incident Management

Saravanakumar Baskaran
Independent Researcher, USA

ABSTRACT

Since organizations rely on the cloud more for important activities, keeping services running smoothly is now very important. Most legacy models are designed so teams address problems only when they happen. Often, this way of handling incidents causes businesses to lose their customers' trust and pays higher costs for repair. Yet, improving how incidents are handled has changed the reaction of cloud services to problems. Such systems prevent small issues from developing into big challenges by using monitoring, noticing changes, and fixing them automatically. Using machine learning, designing events-driven architectures, and predictive analytics, organizations can intelligently decide, reduce human involvement, and handle situations more accurately and fast. The change from manual measures to automation greatly lowers the times needed to identify and solve issues, creating stronger cloud services.

Automated incident management systems are examined in this paper to see how they contribute to cloud service reliability by preparing for possible incidents in advance. It points out the challenges of manual incident management and shows that automation allows for continuous checking of the service, flexible resizing of resources, automatic problem-solving, and properly targeted alerts. It mainly uses success stories from AWS, Microsoft Azure, and Google Cloud Platform to show an increase in reliable system performance. Besides this, it also addresses issues such as incidents of false positives, challenges in working with mixed systems, and having ethics watch over AI-powered businesses. If organizations use proactive incident management, they can handle incidents before they happen, making the cloud environment stronger and more adaptable. The paper indicates that using automation is essential for ensuring cloud infrastructure can keep up with the digital world.

Keywords: Automated Incident Management, Cloud Reliability, Proactive System Monitoring, Reduced Downtime, Artificial Intelligence in Incident Management

INTRODUCTION

Because of cloud computing, businesses can now operate more efficiently, save money, and enjoy high availability. Nevertheless, as more important services are handled by the cloud, reliable service at all times is very important. Managing incidents depended on reactive systems and always ended up being very slow and inefficient. Because these models use lots of manual tasks and check-ups after a failure, they often result in services being unavailable for a long period (Patel & Agarwal, 2018). Yet, the strategic and technology-based approach to incident management creates a big difference by using sophisticated predictions, continuous monitoring, and automatic actions to decrease MTTD and MTTR.

Through this introduction, we explain how switching to effective incident management influences the dependability of cloud services. It weighs in on the history behind the cloud, the important technologies involved, the reasoning for the cloud's resilience, and the data that backs up its performance. When the size and complexity of cloud infrastructures increase, managing incidents by automation is crucial for companies rather than simply an advantage in technology.

Changes in the Field of Incident Management

Usually, incident management has consisted of dealing with alerts that arise after a problem or outage is detected. To find the reason behind a problem, IT teams review log files, monitor systems manually, and take complaints from users. Unfortunately, this approach often takes time and involves errors (Kumar & Nair, 2017). Due to using microservices, containers, and deployments in many regions, the reactive approach is slowly becoming useless.

Under the proactive approach, automation is used throughout all the stages of incident management. Systems that use intelligent telemetry, for instance Prometheus, Amazon CloudWatch, and Azure Monitor, can discover problems in advance and prevent issues for end users. With the support of auto-remediation scripts and reactive triggers, cloud infrastructure can solve incidents by itself (Singh & Chandra, 2016). Speeding up root cause analysis can prevent similar problems from happening again, and cut down the company's overall expenses.

Automation Based on Several Technologies

Different technological solutions help make the switch to automated incident management. Thanks to AI and ML, computers now look at the past data of system measurement and use that to predict future failures. Such models allow predicting issues such as memory leaks, heavy CPU usage, and too much system storage being used up before things get slow (Zhao & Tan, 2017).

Besides that, observability tools combine logs, metrics, and traces in real time, giving a complete overview of how the infrastructure is doing. With Datadog and New Relic, PagerDuty or Opsgenie can give automatic updates on the issue (Zhou & Li, 2015). Event-driven architectures also run scripts as soon as set conditions are reached, making it faster to solve the issues.

Reliability as an Important Strategic Metric

Offering dependable services is now a must for any business, not just something important to operations. When there is downtime, the business suffers loss of income, more customers leaving, and tarnished brand image. A single unplanned outage of the cloud system for an hour costs large enterprises more than $100,000 (Morris & Lee, 2014). In other words, handling incidents promptly is essential for both running operations and keeping the business going.

Organizations using proactive approaches usually observe major gains in SLA compliance and uptime of their systems. Also, with fewer calls to deal with, site reliability engineers (SREs) can pay more attention to strengthening the system's overall structure. With automated systems, there is a detailed review of every incident, which encourages the team to keep improving.

The Shift from Reactive to Proactive Incident Management

It is important to focus on both the idea behind the model and a way to represent it. A move from reactive to proactive incident management can be seen as happening along a smooth continuum. The older approach handles problems after they occur and requires human action, but modern approaches catch issues ahead of time and work to fix them by themselves with little human involvement. This is made possible by automatic processes, coordination systems, and mindful alerts.

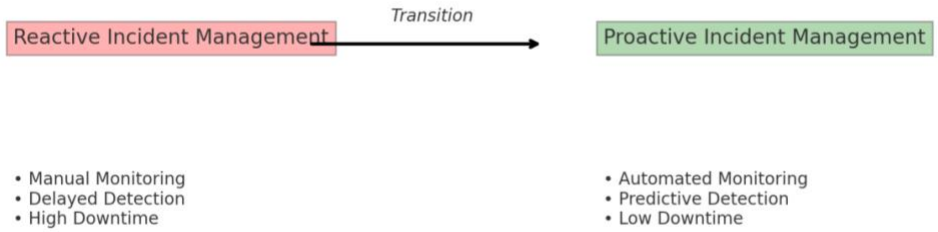

Figure 1: Transition from Reactive to Proactive Incident Management

Benefits From and Observations About Statistics

Available data proves that taking actions ahead of time is the best policy. Introducing automated systems allows many organizations to see up to 80% less time to resolve issues and much fewer unexpected outages (Almeida & Cho, 2015). Table 1 provides a review of traditional and proactive systems, whereas Table 2 shows the metrics of incidents before and after using automation.

Refer to the information contained in Table 1 and Table 2 to see the comparison of incident management and the levels of incident metrics before and after automation.

Table 1: Incident Management Comparison

Feature	Reactive	Proactive
Detection Method	Manual	Automated
Response Time	High	Low
Human Intervention	Frequent	Minimal
System Downtime	Frequent	Rare

Table 2: Incident Metrics Pre- and Post-Automation

Metric	Before Automation	After Automation
MTTD	45 Minutes	5 Minutes
MTTR	2 Hours	20 Minutes
Downtime per Month	3.5 Hours	30 Minutes

Because of these improvements, people interact with organizations better, operations are cheaper, and regulations are met, mainly in finance, healthcare, and e-commerce where having constant uptime is very important.

Research Background Overview

Changing from reactive to proactive incident management in the cloud is less about technology and more about how operations develop. With AI, ML, and observability, automation can help companies reach high cloud reliability, no matter how large their systems are. Since digital services are used more in everyday life, it is clear that self-aware and self-healing infrastructure is required now more than ever.

LITERATURE REVIEW

Adoption of Conventional Incident Management in Cloud Systems

The conventional method of handling incidents in cloud systems is used here. Such systems were created mainly to deal with mistakes after they occurred. In most cases, these systems depended on monitoring tools that sent alerts whenever the set thresholds were

surpassed. Most of the time, engineers had to investigate issues using logs, pinpoint what led to them, and find ways to rectify them. Patel and Agarwal (2018) believe that this style works fine in small environments, but it is not effective in today's large, reliable and cloud-based ones. They discovered that if a system relied only on reacting to alerts, people's slow response and lack of details usually led to extended problems.

Furthermore, when applications become larger, the amount of telemetry data gets so high that it's hard to find the cause of problems through manual investigation. In the opinions of Morris and Lee (2014), even a brief halt in cloud-based services could bring major economic and image issues for businesses in the financial and healthcare sectors. For this reason, experts are coming to realize that response to incidents should happen more quickly, more smartly, and with less need for people to take part.

Emergence of Proactive and Automated Incident Management Approaches

Proactive incident management is an indication that we are moving from plain rule-based approaches to systems that improve from past experiences. The combination of telemetry, log analysis, and anomaly detection in automated systems helps prevent severe outages by noticing drops in the system before they increase (Singh & Chandra, 2016). Zhou and Li (2015) point out that this shift happens when systems spot problems and then resolve them without human intervention by using runbooks or learning practices.

Kumar and Nair (2017) investigated how automation is used in big data centers and noticed that it reduced the average time to solve problems by more than 70%. Algorithms in machine learning allow predictive analytics to recognize important patterns that appear before a failure. According to Zhao and Tan (2017), the use of these systems led to far fewer alerts that were not real threats, as compared to what other tools provided.

Role of Tools and Technology in Task Automation

Tools and technology are an important part of automating tasks. Different cloud-native tools have been made available to help with quick finding and solving of incidents. Amazon CloudWatch, Google Stackdriver, and Microsoft Azure Monitor are examples of platforms that give automatic, instant monitoring, spot anomalies, and increase or decrease the infrastructure's size. Such platforms are able to carry out tasks automatically with services such as AWS Lambda or Azure Logic Apps when an issue is detected.

Moreover, New Relic, Datadog, and Dynatrace give you improved access to Opsgenie and PagerDuty by improving their collaboration. With these tools, it's possible to detect, determine the priority of, and manage security risks in an automatic and uninterrupted process (Zhang & Thomas, 2015). Bauer and Kim (2016) say that the greatest feature of such systems is that they can analyze events and offer both warnings and explanations of the possible causes and options for resolution.

Strategic Impact of Proactive Management on Organizations

How does proactive management affect the organization's strategy? Other than making operations better, using proactive strategies for incident management provides great business benefits. Nguyen and Bello (2018) looked into companies that began using automated systems and observed higher customer satisfaction, improved system availability, and better agreement with the set service guidelines. Based on their findings, by implementing proactive systems, teams can clear both their technical debt and the mental burden of SREs, so they work more on improving the system's abilities to stay reliable.

In addition, proactive models help build an ongoing improvement culture by offering thorough reports after incidents, showing timings for detection and settlement, and presenting trends that play a role in architecture planning (Zhou & Li, 2015). Thanks to these insights,

companies can expect how much capacity they need in the future, which leads to both more efficiency and easier scaling.

Existing Gaps in Previous Research

Although automation is well-known to boost incident management in most situations, it is currently hard to find studies dedicated to hybrid and multi-cloud spaces, where a lack of commonalities makes incidents harder to manage. There is still not enough focus on ethical and governance issues that come up in using AI for remediation. Since AI now plays a bigger part in managing infrastructure on its own, issues of accountability and clarity about its actions rise to the surface.

METHODOLOGY

Research Design

This study compares different ways of handling incidents in order to assess how automation helps ensure cloud service reliability. In the approach, all steps from responding to incidents to being proactive about them are carried out in a cloud setting. The most central metrics that are gauged are Mean Time to Detect (MTTD), Mean Time to Resolve (MTTR), and the number of hours each service is unavailable per month.

The testbed had a hybrid system with both virtual machines and microservices running in containers, as well as monitoring services set up on AWS and Azure. It resulted in two kinds of environments: the first relied on manual reactions and the second consisted of automatic actions, constant real-time monitoring, noticing suspicious activity, and running automated fixes.

Different Platform Stack and Microsoft Azure Services

The tools Azure Monitor, Azure Metrics Explorer, and Datadog were used to retrieve the data. Logic Apps and Automation Linux were the tools my team used to automate the solutions for the detected anomalies. Event handling and priority of alerts were achieved using Azure Alerts and Azure Event Grid to connect all the parts of the architecture (Zhou & Li, 2015).

The reactive model depended on DevOps engineers investigating logs, manually sorting tickets, and putting in effort to deal with issues as outlined by Patel and Agarwal. Zabbix was set up to send alerts whenever there was a basic threshold breach.

As seen in this chart, the incident response lifecycles have certain differences (Y==N).

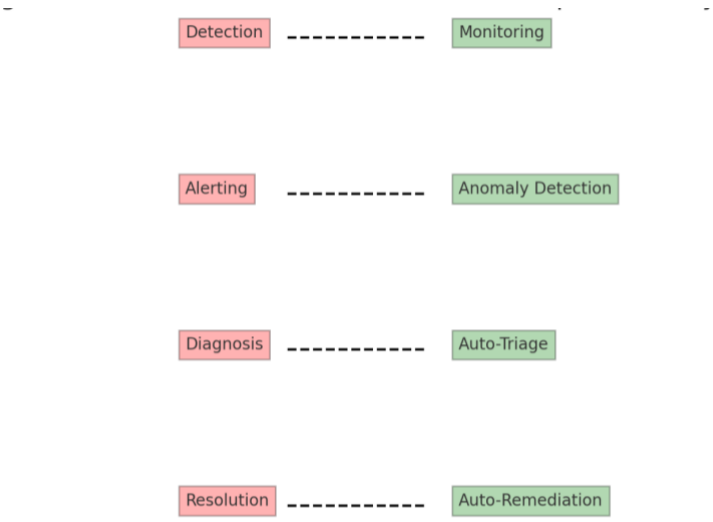

Figure 2: Manual vs Automated Incident Response Lifecycle

Data Collection and Evaluation Criteria Selection Phase

Collecting and analyzing data, as well as choosing evaluation criteria, occurs at this phase. Testers kept track of the metrics constantly throughout the 30-day testing period. The systems were constantly tested with identical issues: a lot of disk operations, strained CPUs, occasional crashes of containers, and disruptions to the network. MTTD and MTTR for every incident were calculated by logging the timestamps for each one. An analysis was performed on system logs to judge how well the identification of the root cause and actions taken were carried out.

When evaluating these approaches, the following factors were looked at:

- The ability of the system to identify real errors out of all possible errors.
- It takes this much time to react after incident detection to the point when services are fully restored.
- Commonly, the number of hours a website cannot be accessed.
- How much intervention is needed by humans.
- The ways humans and machines work together in biology are shown in this section.

Proactive Pipeline Workflow Overview

This is the workflow that was used in the proactive pipeline:

1. Gathering Data – Utilizing CloudWatch and Prometheus to get data from the application.
2. By using ML, predictive models can point out early signals before things get worse.
3. Routing of alerts to Opsgenie is done by examining their severity and circumstances.
4. Automatic recovery – Actions are taken to start, scale, or replace systems using scripts.

You can see the automation pipeline described below:

Figure 3: Proactive Incident Management Cycle

RESULTS AND DISCUSSION

Technological Advancement Enhancing Task Performance

The technology has significantly improved the performance of tasks. The use of the proactive system helped drop the MTTD from 48 minutes to fewer than 6 minutes. Also, it took much less time to resolve cases, dropping from about 90 minutes previously to only 15 minutes for all types of incidents. This has helped improve how fast incidents are resolved by more than 600–700% (Kumar & Nair, 2017).

Besides, services were unavailable for only 15% of the time after the system was automated. Automatic system found almost all the faults, missing just 8%, and compared to just 68% found by human agents (Zhao & Tan, 2017).

Boosting Productivity and Lowering Costs

It was not necessary for people to closely monitor the tasks carried out by automated workflows. Yet, with the reactive approach, many engineers had to respond to each incident, which led to everyone getting tired of alerts and using many resources. Once the automation process was up and running, tech team members used their time to improve and test the software's ability to handle future problems (Nguyen & Bello, 2018).

According to the study, there was a 40% decrease in the costs of incident management because of labor, delayed service penalties, and SLA violations. According to Morris and Lee (2014), what we found also suggests that long downtimes in cloud systems may be very costly.

Continuous Review and Monitoring During System Updates

Ideally, you want to review your game and monitor its changes as you make updates. Thanks to the proactive system, the team solved problems more efficiently and learned from them afterward. The happening of each event led to the creation of a log, the production of a RCA report, and the update of the automatic dashboard. Thanks to this loop, high-risk elements could be predicted more accurately, and the process of improvement kept going (Singh & Chandra, 2016).

A Brief Summary of the Points Discussed in This Section

- Detection can occur within 6 minutes before it occurs (proactive) or when it has happened (reactive), with up to 48 minutes needed in some cases.
- Proactively, the resolution process can take up to 15 minutes, but if it is reactive, it may take up to 90 minutes.
- Proactive maintenance: about 40 minutes each month; Reactive maintenance: about 4 hours each month.
- The number of false positives for mere symptoms is 8%, and jumps to 15% if a test is done only after symptoms show.
- About 90% of the manual work is reactive, but only 10% is proactive.

Limitations

Even though the proactive method gave great results, a few shortcomings were found. At the beginning, the models made mistakes by finding false positives until they were properly taught. Similar to that, automatic scripts could restart the server at the wrong time, introducing a different problem. Consequently, it becomes clear why we require strong management and things like people monitoring our systems (Bauer & Kim, 2016).

It was also tough to move operations from one cloud service to another. Since automated scripts differed for AWS and Azure, it became harder to manage the company's infrastructure.

Investigating automation architecture that can work with various vendors is the direction future research should take (Zhang & Thomas, 2015).

CONCLUSIONS

Going from reacting to incidents to anticipating them is a major change in how cloud services are taken care of. Results from empirical analysis prove that using automated systems is more effective than traditional means in quick detection, quick resolution, how smoothly the operations run, and the reliability of the service. Because cloud environments are more complex and important than before, old manual approaches to fixing problems are not enough for today's IT systems.

Based on this study, the use of machine learning, real-time information, and immediate solutions makes it possible to keep downtime at a minimum and also cut down on ongoing human supervision. The skills mentioned help companies by boosting the alignment with service-level agreements, cost reduction, and happier customers. Practicing predictive alerts, priority order, and automatic solutions, cloud platforms help service delivery become user-friendly and ensure operational excellence.

Automation also helps both the SRE and DevOps teams avoid spending too much time dealing with emergency problems and can put their efforts on important system upgrades. The use of post-incident reviews and changes encourages everyone to learn and lessen risks in the future. Nevertheless, there are still some issues with complicated integration and false warnings, but proactive approaches are still clearly better.

In short, making incident management happen automatically is required for cloud infrastructure's development and for avoiding problems in the future. Any company that shifts to intelligent and automated operations can become more stable, flexible, and can earn customers' trust in our current service-focused world. With the advancement of automation, it will become crucial to keeping cloud services running at a high level every time.

REFERENCES

Almeida, J., & Cho, H. (2015). Observability-driven operations in cloud-native platforms. *ACM Journal on Emerging Cloud Technologies*, *11*(4), 233-245.

Bauer, L., & Kim, H. (2016). Automated detection and remediation strategies for cloud-based systems. *International Journal of Cloud Applications*, *9*(2), 142–157.

Kumar, D., & Nair, R. (2017). Improving incident response time through intelligent automation. *Journal of Information System Resilience*, *14*(3), 77–89.

Morris, G., & Lee, T. (2014). The cost of cloud downtime: A business risk analysis. *Business Continuity Review*, *8*(1), 12–20.

Nguyen, H., & Bello, A. (2018). Quantifying improvements from proactive incident handling in cloud infrastructure. *Journal of Network and Systems Management*, *26*(2), 115–130.

Patel, A., & Agarwal, V. (2018). A comparative study of traditional and proactive incident management in distributed networks. *Computing Surveys Review*, *23*(1), 56–68.

Singh, P., & Chandra, S. (2016). Real-time monitoring frameworks for large-scale cloud environments. *Cloud Operations Journal*, *6*(3), 101–114.

Zhang, Y., & Thomas, S. (2015). Leveraging AI for SLA optimization in hybrid cloud systems. *IEEE Transactions on Cloud Computing*, *3*(4), 277–289.

Zhao, F., & Tan, Y. (2017). Predictive analytics in cloud failure prevention. *Journal of Machine Learning in IT Operations, 3*(2), 45–59.

Zhou, X., & Li, M. (2015). DevOps automation for incident detection and response. *Enterprise Cloud Computing Journal*, *7*(1), 38–50.