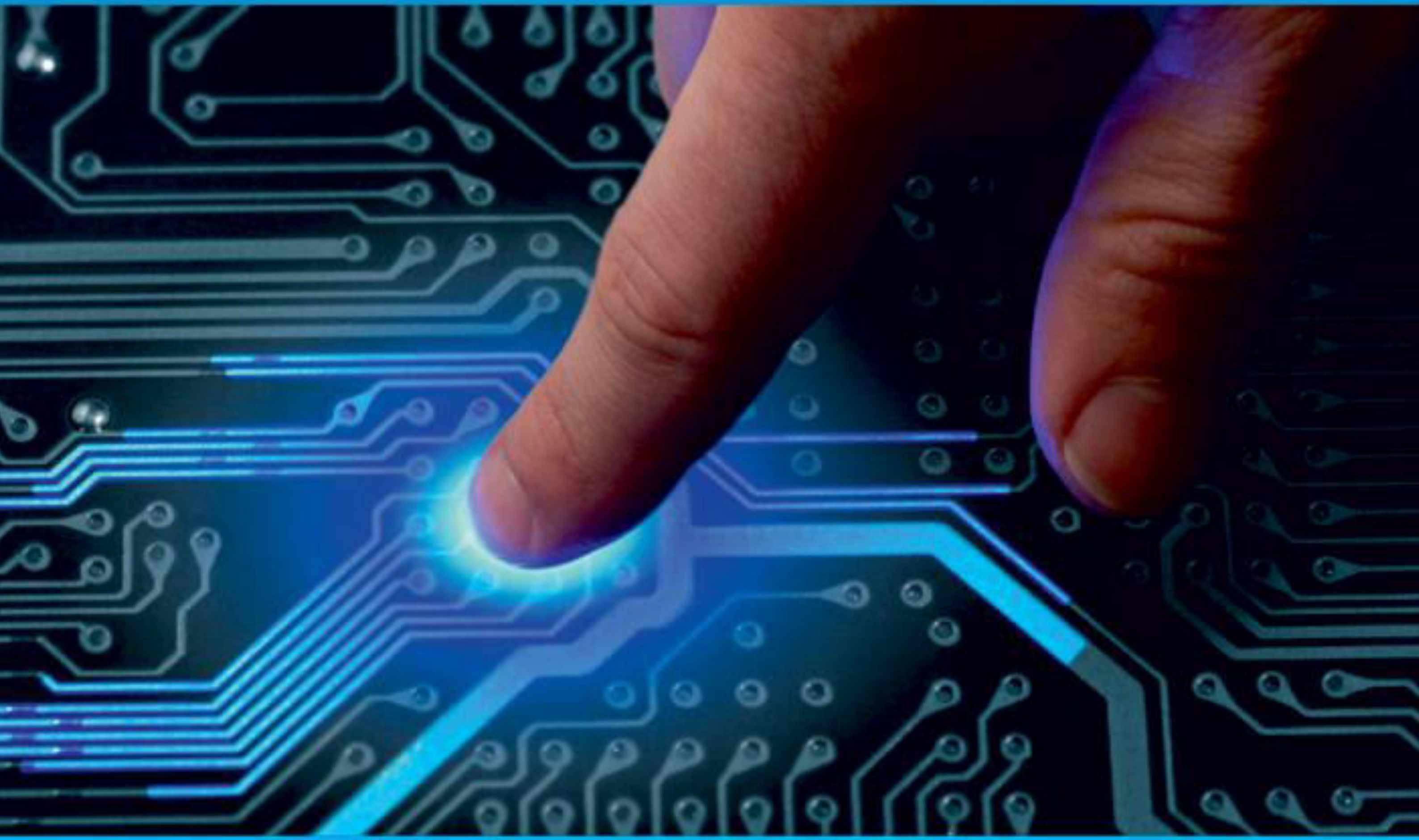
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 11, November 2021

Impact Factor: 7.542

| DOI: 10.15680/IJIRCCE.2021.0911028 |

5 Pillars of AWS Well-Architected Framework

Priyanka [1], Varsha [2], Nitin Kamble[3]

Student, School of Engineering, Ajeenkya D Y Patil University, Pune, India [1,2]

Assistant Professor, School of Engineering, Ajeenkya D Y Patil University, Pune, India [3]

ABSTRACT: Creating a software system is very similar to building a building; If the foundation is not strong, structural problems can affect the integrity and function of the building. If the five pillars of operational excellence, security, reliability, performance efficiency, and cost optimization are neglected when designing technology solutions on Amazon Web Services (AWS), it can be difficult to create a system that meets your expectations and needs. The integration of these pillars into your architecture contributes to stable and efficient systems [5].

KEYWORDS: Operational Excellence, Security, Reliability, Performance Efficiency and Cost Optimization

I. INTRODUCTION

The AWS Well Architected framework helps you understand the pros and cons of the decisions you make when developing workloads on AWS by Using the framework, you will learn operational and architectural best practices for developing and running cloud workloads. that are reliable, safe, efficient and affordable. It allows you to continuously compare your operations and facilities with best practices and uncover opportunities for improvement. We believe that having Well Architected workloads designed with operations in mind dramatically increases the chances of business success.

The framework is based on five pillars:

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization

This research paper focuses on the 5 Pillars of the AWS Well Architected Framework and how to apply it as the foundation for well-architected solutions. Operational excellence is difficult to achieve in environments where operations are seen as an isolated function, separate from the lines of business and the development teams it supports. By adopting the practices described in this document, you can create architectures that provide state information, are enabled for effective and efficient operations and event response, and can continue to improve and support your business goals. This document is intended for people in technology roles such as CTOs, architects, developers and members of the operations team. After reading this document, you will understand the AWS best practices and strategies to use when designing cloud architectures for operational excellence. This document does not provide implementation details or architectural models. However, it does include references to appropriate resources for this information [1],[2].

II. OPERATIONAL EXCELLENCE PILLAR

Areas Of Operational Excellence

Amazon describes operational excellence in the cloud through three areas:

- Preparation
- Operation

- Evolution

Let’s dig into these areas.

Preparation

Operational excellence cannot be achieved in a vacuum. It requires a detailed understanding of each workload, what it is trying to accomplish, and how it will achieve those goals. Without this information, it is impossible to design a system that brings out its state or to create a procedure that effectively supports that system.

Preparation: Operational Priorities

Successful operations teams are enlightened operations teams. They have a complete understanding of:

- Workloads they’re responsible for
- Shared business goals
- Their role in achieving the goals
- Regulatory or compliance requirements

Preparation: Design for Operations

Well-designed workloads are carefully designed with provisioning, upgrades, and operations in mind. They are observable by design, with built-in logging, instrumentation, and metrics that are ready to use out of the box. With AWS, you can code all of your workload, including applications, infrastructure, policies, governance, and operations. By applying rigorous engineering discipline not just to your application code but to your entire stack, you ensure that you have been designed from the ground up. AWS offers a variety of tools and services to enable you to design for operations, including CloudFormation and AWS Developer Tools.

Preparation: Operational Readiness

Operational excellence is more than technology, it is also about processes and procedures. Teams mastered in operational excellence will create and maintain a consistent, repeatable, and well-maintained process to implement and operate their workloads, and track it to actually execute the process. Does that look similar?

- Documentation that accurately reflects the process, including checklists, runbooks, and playbooks.
- A well-trained team of the appropriate size to cover its operational activities. There are no shortcuts here! The team must be familiar with your procedures, workloads, and the underlying AWS infrastructure.
- Governance that ensures no trade-offs are made before starting your workload.

Operation

What does operational success look like? Based on shared business goals, operations teams should create, publish and agree on key metrics and outcomes to define the operational success of their business and workload. Clear definitions help teams react to events quickly and in a way that directly impacts your business goals. To function successfully, your team must first understand and then react [2-5].

Operation: Understanding Operational Health

At Mission, we manage large-scale workloads on behalf of hundreds of customers with varying expectations, requirements and use cases. Some of our customers' workloads require extremely low latency, high throughput performance and will prioritize these requirements above all, including cost. Others are willing to sacrifice some level of performance to provide high availability in a cost-effective manner. Therefore, the definition of operational integrity varies from workload to workload, so it is essential for us to understand the key metrics that correctly capture the definition of customer operational success! Likewise, your teams must engage with the main stakeholders of your company to define these key measures in the results. What are your business priorities? Performance, costs, availability, latency, etc. must be balanced to adequately support your business goals. With these turnkey metrics, your team can get to work collecting data to understand the operational status of your workloads at a glance.

Operation: Responding to Events

Being operationally excellent doesn't guarantee that you won't have to deal with operational events. That said, operational excellence requires that you adequately predict what failures will occur and be prepared to respond quickly and effectively by leveraging your operational health metrics, processes, and procedures.

Evolution

In my experience leading operations teams, the passion for learning is the most important predictor of success. Teams seeking operational excellence need to cultivate a culture of curiosity and continuous improvement, where each experience is an opportunity to learn first, and then to share those lessons far and wide.

Evolution: Learning from Experience

While no operations team eagerly awaits production issues, I have found that the best teams love to learn from failures. As a leader, encouraging operational teams to analyse, experiment and improve will pay big dividends over time. AWS provides a broad platform for analysis and experimentation:

- Amazon CloudWatch and CloudTrail can be combined with Amazon Elasticsearch with Kibana.
- Exporting large amounts of data to Amazon S3 enables analytics with Amazon Athena and Amazon Quick Sight, including advanced visualizations to help your teams gain insight.

As you experiment and evolve, be sure to involve other parts of the activity to add their own perspectives. Often, new opportunities for improvement emerge when other perspectives are called upon.

Evolution: Share Learnings

With Mission status as an AWS Certified MSP, we have the ability to learn from hundreds of workloads and dozens of use cases. Mission engineers appreciate little more than evolving our platform based on these lessons. Every improvement we make extends to all of our customers over time, providing maximum benefit to all of our customers.

Likewise, many organizations have multiple product and operations teams. By widely sharing the courses, you allow the whole company to benefit from your development. AWS enables the sharing of best practices. Your teams can define shared libraries for implementing best practices, including CloudFormation models, Chef cookbooks or Ansible reading books, Lambda functions for common operational tasks, and more. When sharing resources, it uses AWS IAM to set permissions for controlled access [4].

III. SECURITY

Amazon describes security in the cloud through five key areas of concern:

- Identity and access management
- Detective controls
- Infrastructure protection
- Data protection
- Incident response

Let's dig into these areas.

Identity and Access Management Perhaps the most fundamental element of security, identity, and access management is making sure that only properly authorized and authenticated clients have valid access to your resources. Identification and access management is primarily concerned with defining your “principles” (users, groups, services, and roles that will perform actions on your account), policies, and managing them. Identity and Access Management Best Practices are divided into two main topics: AWS Credential Protection and Detailed Authorization.

Detective Controls Forensic audits were an integral part of security long before the advent of the cloud, but in a cloud-centric world, they are becoming an even more essential aspect of security. By using forensic controls, you can completely avoid security threats and potential incidents. Additionally, investigative controls improve governance, compliance, and forensic investigations in the event of an incident. AWS discusses detective checks in two sections of the Security Pillar White Paper: Capturing and Analysing Logs, and Integrating Audit Controls with Notification and Workflows.

Infrastructure Protection Infrastructure security is a broad set of auditing methodologies that help you meet industry best practices and compliance / regulatory obligations. It is also a critical part of any information security practice, as it helps ensure that the systems in your workload are not unauthorized or vulnerable to breaches. Infrastructure security includes limitations at the host and network level, hardening at the operating system level, and more. AWS divides infrastructure security into three broad categories of approach: securing host and network boundaries, configuring and maintaining system security, and enforcing service-level security.

Data Protection Following recent high profile data breaches and the transition and implementation of GDPR, data protection is more important than ever. The architecture of secure systems requires a diligent and in-depth approach to data protection, and it all starts with classifying and categorizing data based on sensitivity levels. Once your data is classified, a number of best practices must be applied to secure it: encryption / tokenization, protection of inactive data, protection of data in transit, and data backup / replication / recovery.

Incident Response No matter how good your security practices, you should always have a plan for responding to security incidents, including a mitigation plan. By putting your tools, processes, and procedures in place before an incident occurs, you can dramatically reduce the impact of security events and the time it takes to restore operations to a known good state. In addition, by practicing incident response, your teams will be well prepared to act calmly in the event of an accident.

AWS recommends using asset tagging to help organize your teams during incident response, tagging assets based on the sensitivity and classification of their data, the team responsible for mitigation, and other information, you can help your team maintain situational awareness. Additionally, these beacons can help ensure that the right people gain access to them in a timely manner to help mitigate, contain, and then conduct forensic investigations.

III. RELIABILITY

The Reliability pillar encompasses the ability of a workload to correctly and consistently perform its intended function, when scheduled. This includes the ability to use and test the workload throughout its lifecycle. This document provides detailed guidance and best practices for deploying reliable workloads on AWS.

The reliability pillar provides an overview of design principles, best practices and questions. Prescriptive implementation advice can be found in the Trust Pillar Whitepaper.

Topics

- Design Principles
- Definition

Design Principles

There are five design principles for reliability in the cloud:

- **Automatically recover from failure**:
  By monitoring a workload for key performance indicators (KPIs), you can trigger automation when a threshold is exceeded. These KPIs should be a measure of business value, not the technical aspects of how the service works. This enables automatic error notification and monitoring and automated recovery processes that bypass or repair the error. With more sophisticated automation, errors can be anticipated and corrected before they occur.
- **Test recovery procedures**: In an on-premises environment, testing is often performed to demonstrate that the workload is working in a particular scenario. Tests are generally not used to validate recovery strategies. In the

cloud, you can check how your workload is failing and you can validate your recovery procedures. Automation can be used to simulate various failures or to recreate scenarios that led to failures before. This approach exposes error paths that can be tested and corrected before a true failure scenario occurs, thereby reducing risk.

Definition

There are four best practice areas for reliability in the cloud:

- Foundations
- Workload Architecture
- Change Management
- Failure Management

Foundations

The fundamental requirements are those whose scope extends beyond a single workload or project. For more reliability, there are specific patterns that you should follow.

With AWS, workload developers can choose which languages and technologies to use. AWS SDKs simplify coding by providing language-specific APIs for AWS services. These SDKs, in addition to the choice of languages, allow developers to implement the reliability best practices listed here. Developers can also read and learn about how Amazon creates and manages software in the Amazon Builders library.

Workload Architecture

A reliable workload starts with upfront design decisions for both software and infrastructure. Your architecture choices will impact your workload behaviour across all five Well-Architected pillars. For reliability, there are specific patterns you must follow.With AWS, workload developers have their choice of languages and technologies to use. AWS SDKs take the complexity out of coding by providing language-specific APIs for AWS services. These SDKs, plus the choice of languages, allow developers to implement the reliability best practices listed here. Developers can also read about and learn from how Amazon builds and operates software in The Amazon Builders' Library.

Change Management

Changes in the workload or its environment must be anticipated and adapted to ensure reliable operation of the workload. Changes include those imposed on the workload, such as peak demand, as well as internal changes, such as feature implementations and security fixes. Using AWS, you can monitor the behaviour of a workload and automate the response to KPIs.For example, the workload can add additional servers as a workload gains more users. You can control who is allowed to make workload changes and view the history of those changes.

Failure Management

In any system of reasonable complexity, errors are expected to occur. Reliability requires that the workload be aware of errors as they occur and take action to avoid any impact on availability. Workloads must be able to both resist errors and automatically fix problems.With AWS, you can take advantage of automation to respond to monitoring data. For example, when a certain metric exceeds a threshold, you can trigger an automated action to resolve the issue. Also, instead of trying to diagnose and repair a failed resource that is part of your production environment, you can replace it with a new one and perform an out of band scan on the failed resource. Full system versions at low cost, automated tests can be used to verify full recovery processes.

IV. PERFORMANCE EFFICIENCY

The performance efficiency pillar focuses on the efficient use of computing resources to meet requirements, and how to maintain efficiency as demand changes and technologies evolve.

Topics

- Design Principles
- Definition

Design Principles

The following design principles can help you achieve and maintain efficient workloads in the cloud.

- **Democratize advanced technologies**: Simplify the implementation of advanced technologies for your team by delegating complex tasks to the cloud provider. Rather than having your IT team learn how to host and run new technology, consider using technology as a service. For example, NoSQL database, multimedia transcoding, and machine learning are all technologies that require specialized skills. In the cloud, these technologies become services your team can use, allowing your team to focus on product development rather than provisioning and resource management.
- **Go global in minutes**: Distributing your workload across multiple AWS Regions around the world enables you to deliver lower latency and a better experience for your customers at minimal cost.
- **Uses serverless architectures:** Serverless architectures eliminate the need to run and maintain physical servers for traditional computing tasks. For example, serverless storage services can act like static websites (eliminating the need for web servers) and event services can host code. This eliminates the operational burden of managing physical servers and can reduce transaction costs as managed services run cloud-scale.
- **Experiment More Often:** With virtual and automatable resources, you can quickly run benchmarks using different types of instances, storage, or configurations.

Definition

Focus on the following areas to achieve performance efficiency in the cloud:

- Selection
- Review
- Monitoring
- Trade-offs

SelectionThe optimal solution for a given workload varies, and solutions often combine multiple approaches. Well-organized workloads use multiple solutions and enable various features to improve performance. AWS resources come in many types and configurations so you can easily find an approach that suits your needs. You may also find options that are not easily accessible with the local infrastructure. For example, a managed service like Amazon DynamoDB offers a fully managed NoSQL database with single-digit millisecond latency on any scale.

ReviewWhen architecting workloads, there are finite options that you can choose from. However, over time, new technologies and approaches become available that could improve the performance of your workload. In the cloud, it’s much easier to experiment with new features and services because your infrastructure is code.

MonitoringAfter you implement your architecture, you must monitor its performance so that you can remediate any issues before they impact your customers. Monitoring metrics should be used to raise alarms when thresholds are breached.

Active monitoring simulates user activity in scripted user journeys across critical paths in your product. AM should be continuously performed in order to test the performance and availability of a workload. AM complements PM by being continuous, lightweight, and predictable. It can be run across all environments (especially pre-production environments) to identify problems or performance issues before they impact end users.

Passive monitoring is commonly used with web-based workloads. PM collects performance metrics from the browser (non-web-based workloads can use a similar approach).

Trade-offs When designing solutions, think about compromises to ensure optimal focus. Depending on your situation, you can change consistency, shelf life, and spacing by time or latency for better performance.

With AWS, you can go global in minutes and provision resources in multiple locations around the world to be closer to your end users. You can also dynamically add read-only replicas to information stores (such as database systems) to reduce the load on the primary.

V. COST OPTIMIZATION

Cost optimization is a continual process of refinement and improvement over the span of a workload's lifecycle. The practices in this paper help you build and operate cost-aware workloads that achieve business outcomes while minimizing costs and allowing your organization to maximize its return on investment [3].

Topics

- Design Principles

Design Principles

Consider the following design principles for cost optimization:

Implement cloud financial management: To achieve financial success and accelerate business value realization in the cloud, you must invest in Cloud Financial Management. Your organization must dedicate the necessary time and resources for building capability in this new domain of technology and usage management. Similar to your Security or Operations capability, you need to build capability through knowledge building, programs, resources, and processes to help you become a cost-efficient organization.

Adopt a consumption model: Pay only for the computing resources you consume, and increase or decrease usage depending on business requirements. For example, development and test environments are typically only used for eight hours a day during the work week. You can stop these resources when they're not in use for a potential cost savings of 75% (40 hours versus 168 hours).

Analyze and attribute expenditure: The cloud makes it easier to accurately identify the cost and usage of workloads, which then allows transparent attribution of IT costs to revenue streams andindividual workload owner.

VI. CONCLUSION

The AWS Well Architected Framework provides architectural best practices on the five pillars for designing and operating reliable, secure, efficient, and profitable systems in the cloud. The framework provides a series of questions that allow you to examine an existing or proposed architecture. It also provides a set of AWS best practices for each pillar. Using the Framework in your architecture helps you produce stable and efficient systems that allow you to focus on functional requirements.

REFERENCES

1)Soltys, M., 2020. Cloudifying the Curriculum with AWS. *arXiv preprint arXiv:2002.04020*.
2)Soltys, M., 2020. Cybersecurity in the AWS Cloud. *arXiv preprint arXiv:2003.12905*.
3) Dineva, K. and Atanasova, T., 2021. Design of Scalable IoT Architecture Based on AWS for Smart Livestock. *Animals*, *11*(9), p.2697.
4) Marcelo, L.A., Rossi, J.L., Lara, J.A.C. and Mucsi, C.S., Analysis of Resistance Spot Welding (RSW) on 22MnB5 material after hot stamping for automotive applications (B-pillar).
5)Mikami, M., Ichijo, H., Matsubara, K., Duc, L.X. and Anh, H., 2020. A proposal of AWS maintenance and periodic calibration tools and installation of ARGs for Radar QPE calibration. *VN J. Hydrometeorol*, *5*, pp.13-35.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details