Event-Driven Serverless Alerting System on AWS

Author: Abdul-Gafur Saeed
Date: September 2025

Table of Contents

1. Overview

This solution provides a scalable, serverless alerting pipeline that delivers real-time notifications for high-priority CloudWatch alarms. It is designed for developer teams seeking fast operational feedback without the overhead of persistent storage or dashboards.

The solution uses AWS native services including Amazon CloudWatch, Amazon EventBridge, Amazon SQS, AWS Lambda, and Amazon SNS. It is optimized for low-cost operation and can be deployed entirely within the AWS Free Tier for small to medium workloads.

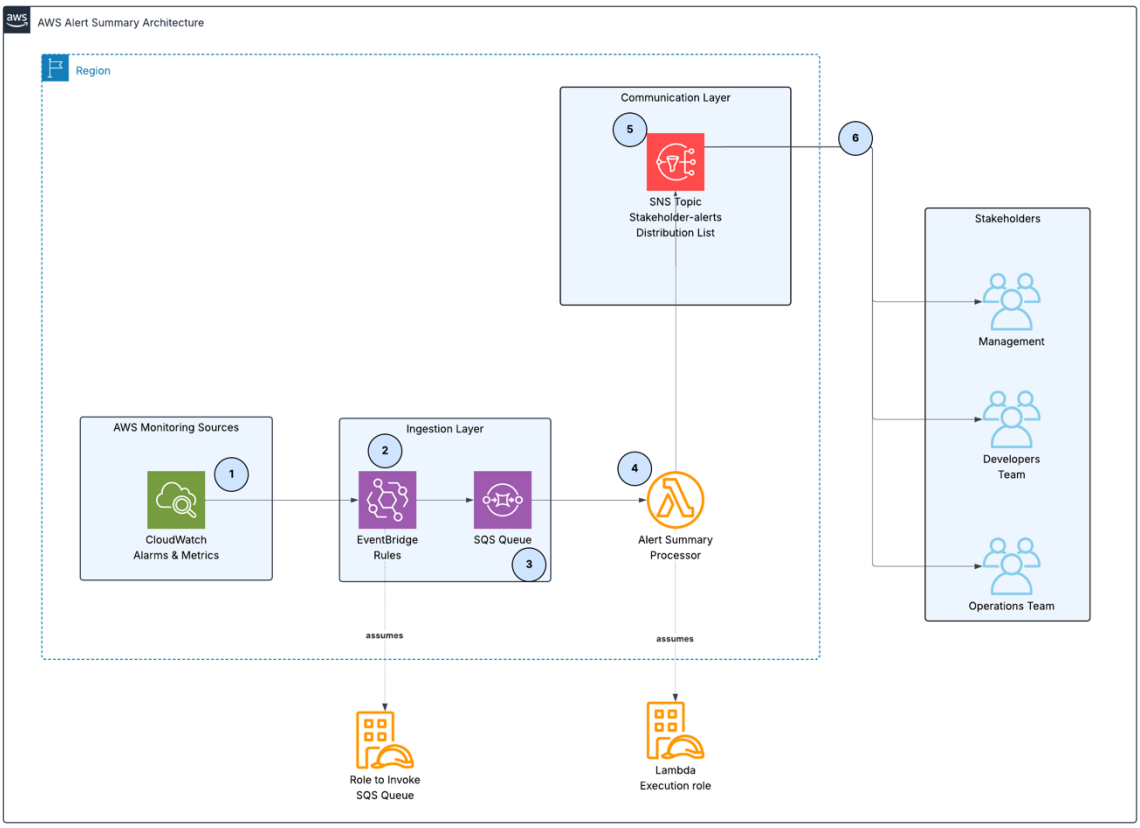
2. Problem Statement

In fast-paced development environments, critical alerts often get lost in noisy dashboards or delayed by manual triage. Developers need a lightweight, scalable system that:

- Detects high-priority events instantly
- Delivers structured notifications
- Avoids infrastructure overhead
- Remains cost-effective, even at scale

3. Architecture

3.1 Diagram



3.2 Components

Component	AWS Service	Description
Monitoring	Amazon CloudWatch	Detects metric thresholds and triggers alarms
Event Routing	Amazon EventBridge	Filters and forwards alarm events
Buffering	Amazon SQS	Decouples event flow and ensures delivery
Processing	AWS Lambda	Summarizes alerts and formats notifications
Notification	Amazon SNS	Publishes structured messages to subscribers

4. Deployment

4.1 Infrastructure

This solution is deployed using an AWS CloudFormation template. It provisions the following resources:

- CloudWatch alarm for a custom metric
- EventBridge rule to detect ALARM state transitions
- SQS queue to buffer alarm events
- Lambda function to process and summarize alerts
- SNS topic to publish alert summaries
- IAM roles for Lambda and EventBridge integration

4.2 Prerequisites

- AWS account with permissions to deploy CloudFormation stacks
- Basic familiarity with AWS monitoring and serverless services

4.3 Deployment Steps

1. Launch the CloudFormation stack in your preferred region
2. Monitor the stack creation process in the AWS CloudFormation console
3. Once deployed, simulate alerts using put-metric-data to test the pipeline
4. Subscribe to the SNS topic for notifications via email, SMS, or other endpoints

5. Cost

5.1 Free Tier Coverage

Service	Free Tier Limit (Monthly)
Lambda	1M requests, 400K GB-sec
SQS	1M requests
SNS	1M publishes
EventBridge	100K events
CloudWatch	10 metrics + 10 alarms

5.2 Paid Tier Example

For workloads exceeding the Free Tier, the following estimates apply:

Service	Usage	Estimated Monthly Cost
Lambda	2M requests, 128MB, 1s	~$2.50
SQS	2M messages	~$0.80

SNS	2M publishes	~$0.50
EventBridge	2M events	~$4.00
CloudWatch	30 metrics + 30 alarms	~$9.00

Total Estimated Cost: ~$16.80/month

Note: This cost breakdown would not be necessary because the solution will most at times be within the free tier, it's just to show the cost that would be incured if the services usage exceeds their free tiers.

6. Security

This solution follows AWS security best practices:

- IAM roles are scoped to least privilege
- Lambda functions are isolated and stateless
- EventBridge and SQS ensure secure event routing
- SNS supports encrypted delivery and access control

7. Customization

You can extend this solution by:

- Adding Slack or MS Teams integration via Lambda
- Storing alert history in Amazon DynamoDB or S3
- Filtering alerts by severity or service
- Visualizing metrics using Amazon QuickSight or Grafana

8. Troubleshooting

Issue	Resolution
No alerts received	Verify CloudWatch alarm threshold and EventBridge rule
Lambda not triggered	Check SQS permissions and EventSourceMapping
SNS notifications not delivered	Confirm subscription and topic permissions

9. Additional Resources

- AWS CloudWatch Documentation
- AWS Lambda Best Practices
- AWS Serverless Application Model