Acme Manufacturing Cloud Migration: Monitoring & Alerting Configuration

Document Version: 1.0
Date: December 6, 2024

This document details the CloudWatch metrics, alarms, and dashboards configured to monitor the Acme Manufacturing cloud environment after the migration. Proactive monitoring is crucial for ensuring system stability, performance, and security.

I. Metrics:

CloudWatch collects various metrics to monitor the health and performance of the migrated systems. The following metrics are monitored:

A. EC2 Instance Metrics:

- **CPUUtilization:** Tracks CPU utilization of EC2 instances. Alarms are configured to trigger when utilization exceeds 80% for a sustained period (5 minutes).
- **NetworkIn:** Tracks inbound network traffic. Alarms trigger if there's a significant drop or spike in inbound traffic.
- **NetworkOut:** Tracks outbound network traffic. Alarms trigger if there's a significant drop or spike in outbound traffic.
- **DiskReadBytes:** Monitors disk read operations. Alarms are triggered if read operations exceed a specified threshold for a sustained period, indicating potential I/O bottlenecks.
- **DiskWriteBytes:** Monitors disk write operations. Alarms trigger if write operations exceed a specified threshold, indicating potential I/O bottlenecks.
- **StatusCheckFailed:** Monitors the instance status check. An alarm is triggered if the instance status check fails.

B. RDS Instance Metrics:

- **CPUUtilization:** Tracks CPU utilization of the RDS instance. Alarms trigger if CPU utilization exceeds 80% for a sustained period.
- **DatabaseConnections:** Monitors the number of active database connections. Alarms trigger if the number of connections exceeds a pre-defined threshold.
- **FreeableMemory:** Monitors available memory on the database instance. Alarms trigger if free memory falls below a certain threshold.
- **BinlogLag:** Monitors binary log lag for replication. Alarms are configured to trigger if the lag exceeds a defined threshold.
- **Deadlocks:** Monitors the number of deadlocks. Alarms trigger if deadlocks exceed a threshold.

C. DynamoDB Table Metrics:

- **ConsumedReadCapacityUnits:** Monitors consumed read capacity units (RCUs). Alarms trigger if RCUs exceed a defined threshold.
- **ConsumedWriteCapacityUnits:** Monitors consumed write capacity units (WCUs). Alarms trigger if WCUs exceed a defined threshold.
- **ThrottledRequests:** Monitors throttled requests. Alarms trigger if throttled requests exceed a threshold.

D. Lambda Function Metrics:

- **Invocations:** Monitors the number of Lambda function invocations.
- **Errors:** Monitors the number of errors. Alarms trigger if the error rate exceeds a defined threshold.
- **Duration:** Monitors execution time. Alarms trigger if execution time exceeds a defined threshold.

E. S3 Bucket Metrics:

- **NumberOfObjects:** Monitors the number of objects in the bucket.
- **BucketSizeBytes:** Monitors the total size of objects in the bucket.

F. CloudFront Metrics:

- **Requests:** Monitors the number of requests served by CloudFront.
- **4xxErrorRate:** Monitors the 4xx error rate. Alarms trigger if the 4xx error rate exceeds a defined threshold.
- **5xxErrorRate:** Monitors the 5xx error rate. Alarms trigger if the 5xx error rate exceeds a defined threshold.

II. Alarms:

Alarms are configured for each critical metric to notify the operations team via [Specify Notification Method, e.g., SNS, email] when a threshold is exceeded.

III. Dashboards:

CloudWatch dashboards provide a centralized view of key metrics and alarms, enabling quick identification of potential problems:

- **EC2 Instance Dashboard:** Visualizes key metrics for all EC2 instances.
- **RDS Instance Dashboard:** Visualizes key metrics for the RDS instance.
- **DynamoDB Dashboard:** Visualizes key metrics for DynamoDB tables.
- **Lambda Function Dashboard:** Visualizes key metrics for Lambda functions.
- **S3 Bucket Dashboard:** Visualizes key metrics for S3 buckets.
- **CloudFront Dashboard:** Visualizes key metrics for the CloudFront distribution.

IV. Log Monitoring:

CloudWatch Logs are used to monitor logs from EC2 instances, Lambda functions, and other AWS services. Log alerts are configured to notify the operations team of any critical errors or warnings.

This document provides a high-level overview of the monitoring and alerting configuration. Detailed configurations for each metric and alarm are maintained separately. Regular review and updates to the monitoring and alerting configuration are essential to ensure that the system remains stable and performs optimally. The dashboards provide a visual overview of the system's health.