KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **Cloud Deployment and Operations**

Title : WGUCloud Deployment and Operations

Version : DEMO

1.Which CloudWatch metric filter includes log events with the word ERROR but excludes log events with the word WARNING?
A. ?ERROR ?WARN
B. "ERROR" WARN
C. ERROR -WARN
D. ERROR WARN
Answer: C
Explanation:
A metric filter in Amazon CloudWatch Logs can be used to search for specific terms in log data and create metrics based on the matches. To include log events with the word "ERROR" and exclude those with the word "WARNING," the correct syntax involves using a filter pattern with a positive match for "ERROR" and a negation for "WARNING." The correct pattern is "ERROR -WARN," where the minus sign (-) indicates exclusion of log events containing "WARN." According to the WGU Cloud Deployment and Operations Study Guide (Section 4.2, CloudWatch Logs), metric filters use a pattern-based syntax where terms are included or excluded using positive matches and the negation operator (-). This ensures that only logs with "ERROR" and without "WARN" are processed into the metric.

2.Which AWS solution can send email based on CloudWatch alarms?
A. Simple Queue Service (SQS
B. Simple Notification Service (SNS
C. Amplify
D. Kinesis
Answer: B
Explanation:
Amazon CloudWatch alarms can trigger notifications when a metric breaches a defined threshold. The AWS solution designed to send emails based on these alarms is Amazon Simple Notification Service (SNS). SNS supports sending notifications via email, SMS, and other protocols when subscribed endpoints are triggered by CloudWatch alarms. The WGU Cloud Deployment and Operations Study Guide (Section 4.3, Monitoring and Alarms) states that SNS is the primary service for delivering notifications from CloudWatch, allowing users to configure email subscriptions for alarm states. Other options like SQS, Amplify, and Kinesis are not designed for this purpose.

3.How are custom metrics grouped in CloudWatch?
A. Namespace
B. Service
C. Date
D. Value
Answer: A
Explanation:
In Amazon CloudWatch, custom metrics are organized and grouped using namespaces. A namespace is a container for CloudWatch metrics that allows you to isolate and categorize metrics from different applications or services. According to the WGU Cloud Deployment and Operations Study Guide (Section 4.1, CloudWatch Metrics), each custom metric must be assigned to a namespace, which acts as a unique identifier to prevent naming collisions and facilitate metric management.

Options like Service, Date, and Value are not used for grouping metrics in this context.

4.Which action must be used to create a metric filter in the Amazon CloudWatch console?
A. Enable an alarm
B. Define a trace
C. Select a log group
D. Specify a stream
Answer: C
Explanation:
To create a metric filter in the Amazon CloudWatch console, the first step is to select a log group from which the log data will be analyzed. A log group contains log streams, and metric filters are applied to the log data within these groups to extract metrics based on patterns. The WGU Cloud Deployment and Operations Study Guide (Section 4.2, CloudWatch Logs) specifies that the process begins by navigating to the CloudWatch console, selecting a log group, and then defining the filter pattern. Actions like enabling an alarm, defining a trace, or specifying a stream are subsequent or unrelated steps.

5.A cloud engineer needs to notify the response team whenever a high-security web server responds with a 403 Forbidden error.
Which two steps can enable this functionality? Choose 2 answers.
A. Define a metric filter for Apache logs in CloudWatch
B. Bind a Lambda function to an Apache process
C. Create an alarm for the metric filter to deliver alerts using Amazon SNS
D. Send alarms from the Lambda function using Amazon SQS
Answer: A, C
Explanation:
To notify a response team when a high-security web server returns a 403 Forbidden error, two key steps are required. First, define a metric filter for Apache logs in CloudWatch to detect the 403 error code within the log data. This involves setting up a filter pattern to match "403" in the Apache access logs. Second, create an alarm for the metric filter and configure it to deliver alerts using Amazon SNS, which supports email or other notifications to the response team. The WGU Cloud Deployment and Operations Study Guide (Section 4.2, CloudWatch Logs and Alarms) confirms that metric filters and SNS-integrated alarms are the standard approach for monitoring and alerting on log-based events. Options B and D are incorrect as they involve unnecessary or unsupported configurations (e.g., binding Lambda to Apache or using SQS for alarms).