CLOUDWATCH

**ApproximateNumberOfMessagesVisible** - This is a CloudWatch Amazon SQS queue metric. The number of messages in a queue might not change proportionally to the size of the Auto Scaling group that processes messages from the queue. Hence, this metric does not work for target tracking.

The minimum permissions required are as follows:

· “logs:CreateLogGroup” - Creates a log group with the specified name.

· “logs:CreateLogStream” - Creates a log stream for the specified log group.

· “logs:PutLogEvents” - Uploads a batch of log events to the specified log stream.

Q: What is Amazon CloudWatch?

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.

To get started with monitoring, you can use Automatic Dashboards with built-in AWS best practices, explore account and resource-based view of metrics and alarms, and easily drill-down to understand the root cause of performance issues.

Q: What kinds of things can I do with CloudWatch Logs?

CloudWatch Logs is capable of monitoring and storing your logs to help you better understand and operate your systems and applications. You can use CloudWatch Logs in a number of ways.

Real time application and system monitoring: You can use CloudWatch Logs to monitor applications and systems using log data. For example, CloudWatch Logs can track the number of errors that occur in your application logs and send you a notification whenever the rate of errors exceeds a threshold you specify. CloudWatch Logs uses your log data for monitoring; so, no code changes are required.

Long term log retention: You can use CloudWatch Logs to store your log data indefinitely in highly durable and cost effective storage without worrying about hard drives running out of space. The CloudWatch Logs Agent makes it easy to quickly move both rotated and non rotated log files off of a host and into the log service. You can then access the raw log event data when you need it

Q: What is the retention period of all metrics?

CloudWatch launched High Resolution Custom Metrics on July 26, 2017. This enables you to publish and store custom metrics down to 1-second resolution. Extended retention of metrics was launched on November 1, 2016, and enabled storage of all metrics for customers from the previous 14 days to 15 months. CloudWatch retains metric data as follows:

* Data points with a period of less than 60 seconds are available for 3 hours. These data points are high-resolution custom metrics.
* Data points with a period of 60 seconds (1 minute) are available for 15 days
* Data points with a period of 300 seconds (5 minute) are available for 63 days
* Data points with a period of 3600 seconds (1 hour) are available for 455 days (15 months)

Data points that are initially published with a shorter period are aggregated together for long-term storage. For example, if you collect data using a period of 1 minute, the data remains available for 15 days with 1-minute resolution. After 15 days this data is still available, but is aggregated and is retrievable only with a resolution of 5 minutes. After 63 days, the data is further aggregated and is available with a resolution of 1 hour. If you need availability of metrics longer than these periods, you can use the GetMetricStatistics API to retrieve the datapoints for offline or different storage.

Q: What is the minimum resolution for the data that Amazon CloudWatch receives and aggregates?

The minimum resolution supported by CloudWatch is 1-second data points, which is a high-resolution metric, or you can store metrics at 1-minute granularity. Sometimes metrics are received by Cloudwatch at varying intervals, such as 3-minute or 5-minute intervals. If you do not specify that a metric is high resolution, by setting the StorageResolution field in the PutMetricData API request, then by default CloudWatch will aggregate and store the metrics at 1-minute resolution.

Depending on the age of data requested, metrics will be available at the resolutions defined in the retention schedules above. For example, if you request for 1-minute data for a day from 10 days ago, you will receive the 1440 data points. However, if you request for 1-minute data from 5 months back, the UI will automatically change the granularity to 1-hour and the GetMetricStatistics API will not return any outpu

Q: Can I delete any metrics?

CloudWatch does not support metric deletion. Metrics expire based on the retention schedules described above.

Q: Will I lose the metrics data if I disable monitoring for an Amazon EC2 instance?

No. You can always retrieve metrics data for any Amazon EC2 instance based on the retention schedules described above. However, the CloudWatch console limits the search of metrics to 2 weeks after a metric is last ingested to ensure that the most up to date instances are shown in your namespace

Q: Can I access the metrics data for a terminated Amazon EC2 instance or a deleted Elastic Load Balancer?

Yes. Amazon CloudWatch stores metrics for terminated Amazon EC2 instances or deleted Elastic Load Balancers for 15 months.

Q: What resolution can I get from a Custom Metric?

A custom metric can be one of the following:

* Standard resolution, with data having one-minute granularity
* High resolution, with data at a granularity of one second

By default, metrics are stored at 1-minute resolution in CloudWatch. You can define a metric as high-resolution by setting the StorageResolution parameter to 1 in the PutMetricData API request. If you do not set the optional StorageResolution parameter, then CloudWatch will default to storing the metrics at 1-minute resolution.

When you publish a high-resolution metric, CloudWatch stores it with a resolution of 1 second, and you can read and retrieve it with a period of 1 second, 5 seconds, 10 seconds, 30 seconds, or any multiple of 60 seconds.

Custom metrics follow the same retention schedule listed above.

Q: What metrics are available at high resolution?

Currently, only custom metrics that you publish to CloudWatch are available at high resolution. High-resolution custom metrics are stored in CloudWatch at 1-second resolution. High resolution is defined by the StorageResolution parameter in the PutMetricData API request, with a value of 1, and is not a required field. If you do not specify a value for the optional StorageResolution field, then CloudWatch will store the custom metric at 1-minute resolution by default.

Q: When would I use a Custom Metric over having my program emit a log to CloudWatch Logs?

You can monitor your own data using custom metrics, CloudWatch Logs, or both. You may want to use custom metrics if your data is not already produced in log format, for example operating system processes or performance measurements. Or, you may want to write your own application or script, or one provided by an AWS partner. If you want to store and save individual measurements along with additional detail, you may want to use CloudWatch Logs.

Q: What log monitoring does Amazon CloudWatch provide?

CloudWatch Logs lets you monitor and troubleshoot your systems and applications using your existing system, application and custom log files.

With CloudWatch Logs, you can monitor your logs, in near real time, for specific phrases, values or patterns. For example, you could set an alarm on the number of errors that occur in your system logs or view graphs of latency of web requests from your application logs. You can then view the original log data to see the source of the problem. Log data can be stored and accessed for up to as long as you need in highly durable, low-cost storage so you don’t have to worry about filling up hard drives.

Q: What if I configure the CloudWatch Logs Agent to send non-text log data?

The CloudWatch Logs Agent will record an error in the event it has been configured to report non text log data. This error is recorded in the /var/logs/awslogs.log.

Q: What thresholds can I set to trigger a CloudWatch Alarm?

When you create an alarm, you first choose the Amazon CloudWatch metric you want it to monitor. Next, you choose the evaluation period (e.g., five minutes or one hour) and a statistical value to measure (e.g., Average or Maximum). To set a threshold, set a target value and choose whether the alarm will trigger when the value is greater than (>), greater than or equal to (>=), less than (<), or less than or equal to (<=) that value.

Q: My CloudWatch Alarm is constantly in the Alarm state, what did I do wrong?

Alarms continue to evaluate metrics against your chosen threshold, even after they have already triggered. This allows you to view its current up-to-date state at any time. You may notice that one of your alarms stays in the ALARM state for a long time. If your metric value is still in breach of your threshold, the alarm will remain in the ALARM state until it no longer breaches the threshold. This is normal behavior. If you want your alarm to treat this new level as OK, you can adjust the alarm threshold accordingly.

Q: What is CloudWatch Dashboards?

Amazon CloudWatch Dashboards allow you to create, customize, interact with, and save graphs of AWS resources and custom metrics.

Q: What are the advantages of Automatic Dashboards?

Automatic Dashboards are pre-built with AWS service recommended best practices, remain resource aware, and dynamically update to reflect the latest state of important performance metrics. You can now filter and troubleshoot to a specific view without adding additional code to reflect the latest state of your AWS resources. Once you have identified the root cause of a performance issue, you can quickly act by going directly to the AWS resource.