Digital Cloud Guru

Monitoring and Logging Services

CloudWatch

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS

CloudWatch is for performance monitoring (CloudTrail is for auditing)

Used to collect and track metrics, collect and monitor log files, and set alarms

Automatically react to changes in your AWS resources

Monitor resources such as:

- EC2 instances
- DynamoDB tables
- RDS DB instances
- Custom metrics generated by applications and services
- Any log files generated by your applications

Gain system-wide visibility into resource utilization

Monitor application performance

Monitor operational health

CloudWatch is accessed via API, command-line interface, AWS SDKs, and the AWS Management Console

CloudWatch integrates with IAM

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

CloudWatch Logs can be used for real time application and system monitoring as well as long term log retention

CloudWatch Logs keeps logs indefinitely by default

CloudTrail logs can be sent to CloudWatch Logs for real-time monitoring

CloudWatch Logs metric filters can evaluate CloudTrail logs for specific terms, phrases or values

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)

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

Alarms can be used to monitor any Amazon CloudWatch metric in your account

Events are a stream of system events describing changes in your AWS resources

Logs help you to aggregate, monitor and store logs

Basic monitoring = 5 mins (free for EC2 Instances, EBS volumes, ELBs and RDS DBs)

Detailed monitoring = 1 min (chargeable)

Metrics are provided automatically for a number of AWS products and services

There is no standard metric for memory usage on EC2 instances

A custom metric is any metric you provide to Amazon CloudWatch (e.g. time to load a web page or application performance)

Options for storing logs:

- CloudWatch Logs

- Centralized logging system (e.g. Splunk)
- Custom script and store on S3

Do not store logs on non-persistent disks:

Best practice is to store logs in CloudWatch Logs or S3

CloudWatch Logs subscription can be used across multiple AWS accounts (using cross account access)

Amazon CloudWatch uses Amazon SNS to send email

CloudTrail

AWS CloudTrail is a web service that records activity made on your account and delivers log files to an Amazon S3 bucket

CloudTrail is for auditing (CloudWatch is for performance monitoring)

CloudTrail is about logging and saves a history of API calls for your AWS account

Provides visibility into user activity by recording actions taken on your account

API history enables security analysis, resource change tracking, and compliance auditing

Logs API calls made via:

- AWS Management Console
- AWS SDKs
- Command line tools
- Higher-level AWS services (such as CloudFormation)

CloudTrail records account activity and service events from most AWS services and logs the following records:

- The identity of the API caller
- The time of the API call
- The source IP address of the API caller
- The request parameters
- The response elements returned by the AWS service

CloudTrail is not enabled by default

CloudTrail is per AWS account

You can consolidate logs from multiple accounts using an S3 bucket:

1. Turn on CloudTrail in the paying account
2. Create a bucket policy that allows cross-account access
3. Turn on CloudTrail in the other accounts and use the bucket in the paying account

You can integrate CloudTrail with CloudWatch Logs to deliver data events captured by CloudTrail to a CloudWatch Logs log stream

CloudTrail log file integrity validation feature allows you to determine whether a CloudTrail log file was unchanged, deleted, or modified since CloudTrail delivered it to the specified Amazon S3 bucket

AWS Certified Solutions Architect – Associate

AWS Certified Cloud Practitioner

- **Cloud Computing Concepts**
- **AWS Global Infrastructure**
- **Identity and Access Management**
- **AWS Compute**
- **AWS Storage**
- **AWS Networking**
- **AWS Databases**
- **Elastic Load Balancing and Auto Scaling**
- **Content Delivery and DNS Services**
- **Monitoring and Logging Services**
- **Notification Services**
- **AWS Billing and Pricing**
- **Cloud Security**
- **AWS Shared Responsibility Model**
- **Architecting for the Cloud**
- **Additional AWS Services & Tools**

Categories