AWS Monitoring CloudWatch, CloudTrail, Config

CloudWatch

CloudWatch Metrics

CloudWatch provides metrics (variable that you want to monitor) for every services in AWS. A metric belong to namespaces which is per services.

10 Dimension per metrics, associated instance id, environments, ...etc.

You can even make your own custom metrics to say monitor the RAM usage for example

Metric stream

You can stream them outside of CloudWatch to a destination. It is near-time delivery and low latency which is Kinesis Firehose, then you can sent it to anywhere. Filtering option is also available so that you only stream a subset of the metrics.

C1's Splunk is how this is done basically.

CloudWatch logs groups

You can create log groups for your logs. Inside each group you will have stream which is the logs from the application.

You can have life cycle policy for logs, and logs can be send to different places. S3, Data Streams, Firehose, Lambda, OpenSearch all those are valid destinations.

You can sent logs to CloudWatch logs using SDK, Logs Agent, or Unified Agent.

ECS automatically collect logs from containers, Lambda as well, API Gateway too so most services have logs pre-configured.

Metric filter

You can filter the logs to search for specifically the line that you want, then it can be created as a new metric!

Metric filter can also trigger CloudWatch alarms because it is a custom metric!

Exporting logs to S3

If you export straight from logs to S3 it won't be near real-time or real time. Instead you want to put a subscription filter then sent it to other places say Lambda, Kinesis Data firehose, and Data stream.

CloudWatch Agent and Logs Agent

By default no logs are going from EC2 instance to cloudWatch. You need to install an agent on EC2 to push those log files that you want to CloudWatch.

EC2 instance must have the appropriate IAM role to sent the logs. The agent can also be on-premise which is really nice.

Logs agent: Both for virtual server. Can only sent logs to CloudWatch logs

Unified agent (new): Will also collect system-level metrics like RAM, processes to CloudWatch. Have centralized configuration.

CPU metrics, Disk metrics, RAM, Netstat, Processes, swap space can be collected by Unified agent.

CloudWatch Alarms

Used to trigger action from any metrics even filter metrics.

- Ok: Not triggered
- Insufficient data: Not enough data
- Alarm: Triggered

Alarm have three main targets that you can do the action to.

1. EC2 instances: Stop it, terminate it, reboot, or recover
2. ASG: Trigger auto scaling action
3. SNS: Sent notification to SNS then you can do whatever you want with those subscriber that subscribed to the topic

Composite alarm

CloudWatch are on single metric. Composite alarm monitor the states of multiple other alarms. Combining different alarms together using AND and OR conditions.

EventBridge

Formerly known as CloudWatch event

You can schedule CRON job, scripts to run periodically.

You can also use it to react to a service doing something. React to say IAM Root user sign in event, sent a message to SNS topic saying that the root user has signed in.

EventBridge rules

All services when doing something can sent the event through EventBridge. You will write rules to react to those events.

Then you can set up "destinations" to react to those events. Events are in JSON, which the destination will receive.

There is the default event bus that is created for each account. You can sent the event to this bus if you like, or to your custom event bus.

You can select to sent EVERY EVENT that occurred in AWS to a bus, but this is very expensive. You should only nick pick only the event that you care about.

Partner event bus can receive events from third party software like Datadog and Zendesk to EventBridge as well. So it can react to event outside of AWS as well!

You can also sent your own application's event to EventBridge!

Schema registry

EventBridge analyze the events in your bus and infer the schema.

The schema registry let you write code so that it will know in advance how data is structured in the event bus that is sent to the destination.

Basically the JSON file that defines how the event that is going to sent to the destination looks like.

Resource-based policy

Set permission for a specific event bus. Allow / deny event from another AWS account or AWS region.

CloudWatch insights

CloudWatch container insights

You can collect metrics and logs from containers. From ECS, EKS, Kubernetes.

For EKS the metrics and logs are collected using a containerized version of the CloudWatch Agent to find those containers.

CloudWatch lambda insights

Monitoring and troubleshooting solutions for serverless application on lambda.

It collects CPU time, memory, disk, network, cold starts for lambda.

CloudWatch contributor insights

See contributor data from time series. Find top talkers and understand who or what is impacting system performance.

Finding bad host who is doing malicious thing.

CloudWatch application insights

Give automated dashboards that show potential problems with monitored applications. The apps running on EC2 instances can be monitored but only certain technologies.

Those apps can link to other AWS services, and application insights can show you what issues those services connected can have. Helps troubleshooting.

CloudTrail

Audit logs for your AWS account. It provides you a history of events / API calls made within your AWS.

Console, SDK, CLI, and AWS services. You can store the logs to S3 or CloudWatch.

You can monitor all region or single region.

If resources are deleted then look into CloudTrail! To check who did it!

Events

Management events: Those are operation that performed on resources in your AWS. Two kinds read events (that doesn't modify resources) and write events (that may modify resources). You

read IAM roles, or you add an IAM role, these are management events.

Data events: These are not logged by default. You get events on S3 object levels. GetObject, DeleteObject, PutObject, and again you can eparate read and write events. It also monitor lambda function execution invoke API.

CloudTrail insights events: Detect unusal activity in your account.
It looks like historical data, what normal activity looks like in your account, then find those unusual usage pattersn. You need to pay for this events.

Event retentions

By default stored for 90 days in CloudTrail. To store it longer put it into S3, then use Athena for analytics.

Intercept API calls

Any API call will be logged in CloudTrail, then the event will be stored into EventBridge, then you can set up rules to alert to SNS topic for a specific API call usage.

AWS Config

This helps monitor compliance of your AWS resources. It will give you a dashboard on the resources that you are monitoring

- I want this bucket not public -> Compliance or not compliance
- Every EBS disk is type gp2
- Each EC2 instance I deploy must be t2.micro

You can define rules or use the one provided by AWS

It doesn't do the remediation for you! It will just tell you that it isn't compliance. You can set up SSM **automation document** to do remediation. It can have retries in case remediation failed.

To receive notification on non-compliance resources you can set up on EventBridge. Or you can filtere it in SNS.

Summary

CloudWatch: Used for performance monitoring, you can also receive logs and analysis on specific metrics.

CloudTrail: Used for API call auditing. Define trail for more specific resources, it is a global service

Config: Record configuration changes for you resources, and also define what is compliance and what is not.

Revision #1
Created 2023-02-25 18:36:37 UTC by Tamarine
Updated 2023-02-26 00:39:01 UTC by Tamarine