Monitoring in AWS

Contents

- CloudWatch
- CloudWatch Logs
- CloudWatch Dashboard, Metrics
- CloudWatch Events
- CloudTrail

CloudWatch

AWS CloudWatch

- CloudWatch is an AWS managed service
- CloudWatch provides metrics for all services in AWS

AWS CloudWatch (cont.)

- CloudWatch concepts:
  - **Metric** is variable to monitor (CPUUltilization, NetworkIn…)
  - **Namespace** is a container for Metrics
  - **Dimension** is an attribute of metric (Instance ID, AZ, environment…)
  - **Time stamps** is attached to metric data point

EC2 detailed monitoring

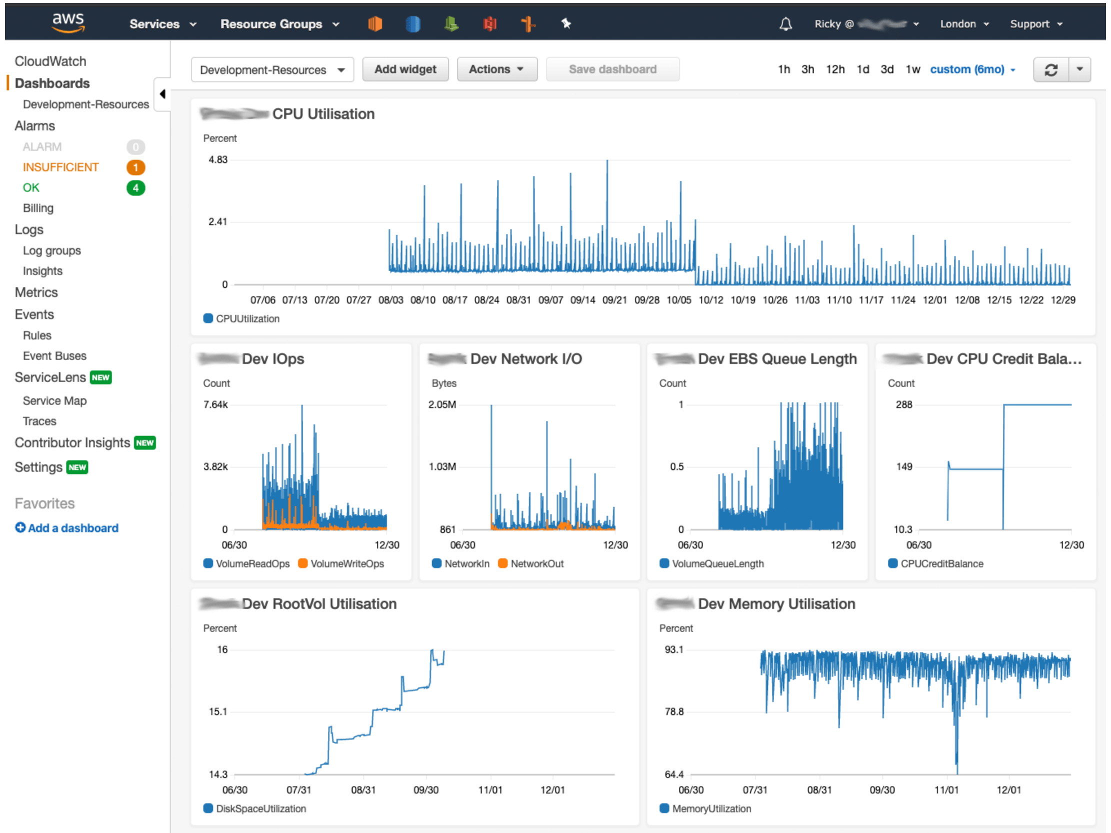
- EC2 instance metrics are collected every **5 minutes** (By default)
- Enable EC2 detailed monitoring to allow to collect metrics **every 1 minute**
- **Free Tier** allows to setup up to **10 detailed monitoring metrics**
- **EC2 memory usage** metric is not default metric, it is custom metric (collect and push by user script)

CloudWatch Custom Metrics

- You can collect your own metrics to send to CloudWatch for monitoring
  - Ex: Total TCP Established connection, Total Openfiles, Memory Usage
- Ability to setup **Dimention** for metrics
- Metric Resolution
  - Standard: 1 minute (60s)
  - High Resolution: 1/5/30 second (s) (Higher cost cause by **PutDataMetric more frequently**)
- **Important:** Accept **Time stamps** of data point 2 weeks in the past or up to **2 hours** in the future

CloudWatch Dashboard

- You can setup a **Dashboard** that visualizes key, important metrics
- Dashboards are global
- Dashboard can visualizes Graphs from other AWS accounts
- Dashboard can be shared with non-AWS users

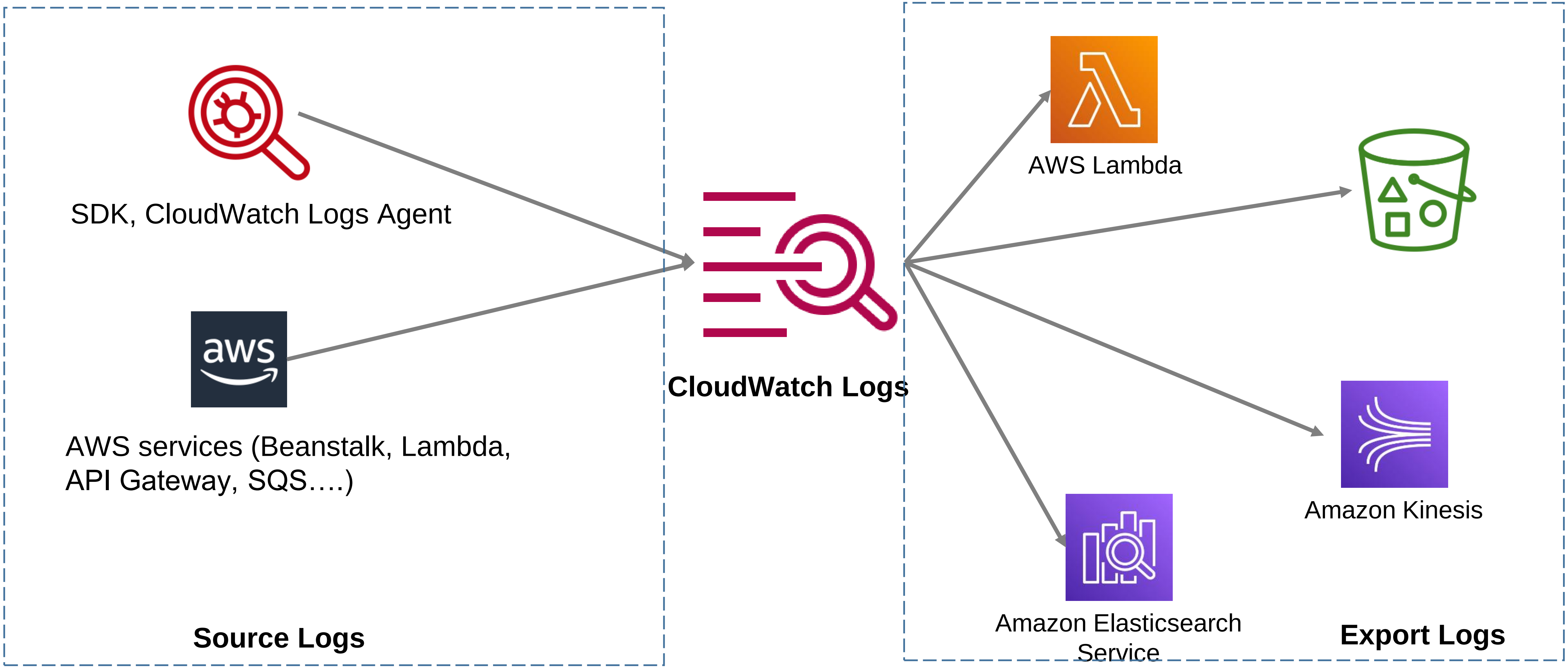


CloudWatch Logs

CloudWatch Logs

- CloudWatch Logs allows to collect logs from your system or AWS services
- Can define Logs expiration policies (30 days, 1 month or never expire)
- CloudWatch Logs can send logs to:
  - S3 (For Archiving purpose)
  - Kinesis Data Stream/Data Firehorse
  - AWS Lambda
  - ElasticSearch

CloudWatch Logs - Source



SDK, CloudWatch Logs Agent

AWS services (Beanstalk, Lambda, API Gateway, SQS….)

Source Logs

CloudWatch Logs

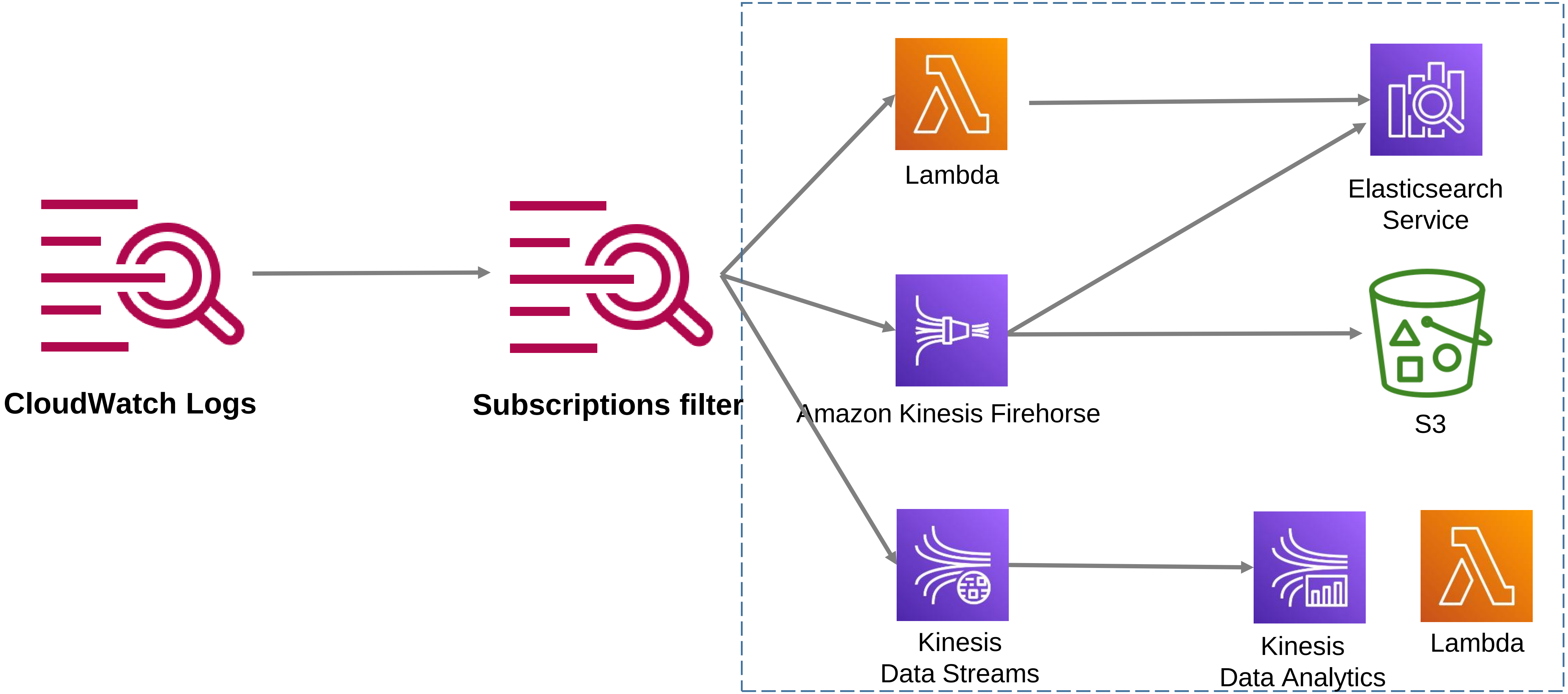
AWS Lambda

Amazon Kinesis

Amazon Elasticsearch Service

Export Logs

CloudWatch Logs Subscriptions

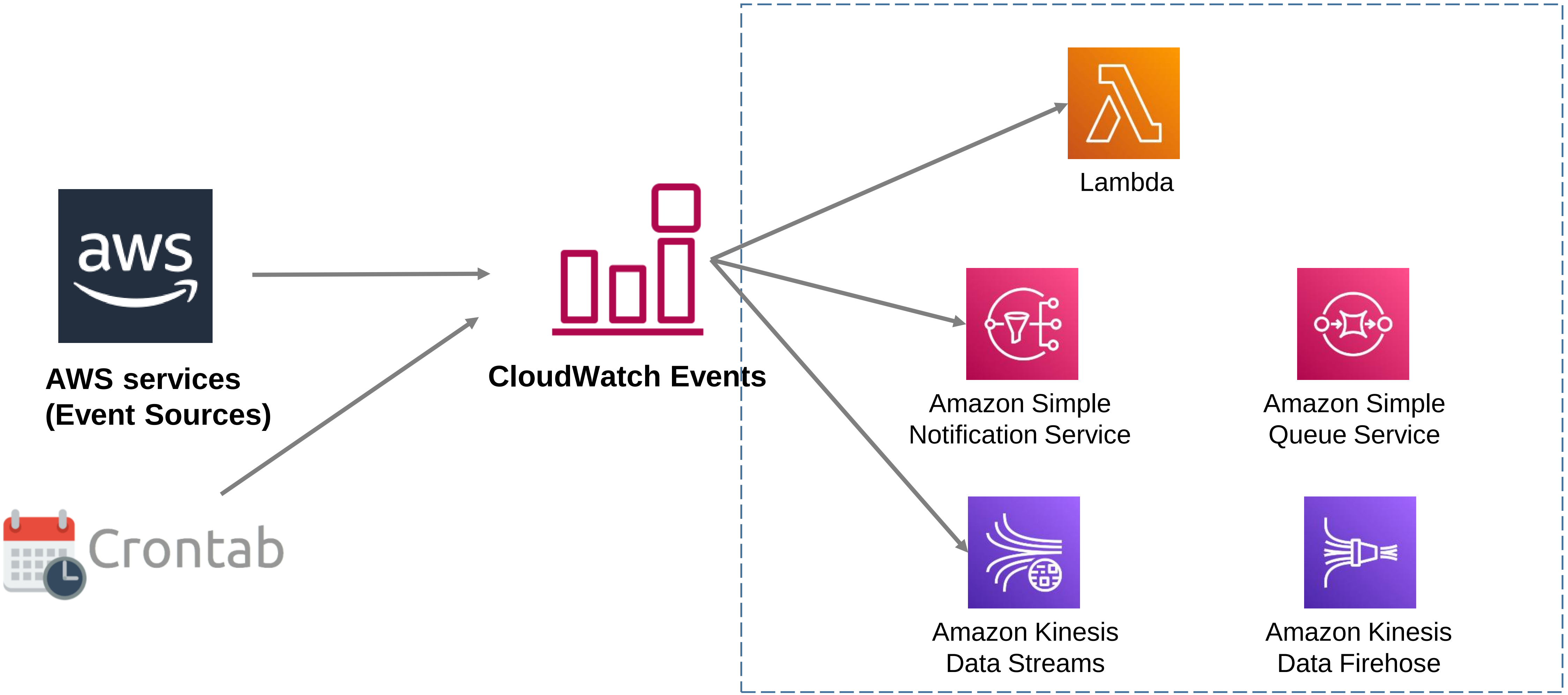


CloudWatch Event

CloudWatch Events

- Event Pattern: Responds to events of AWS resources (changes)
  - Example: AWS EC2 instances (Stopping, Pending), S3, Codebuild…
  - Can work with CloudTrail for intercept API call
- Schedule or Cron (Example: Create an event for every 5 minutes)
- A Payload data can send to target for futher processing

CloudWatch Events

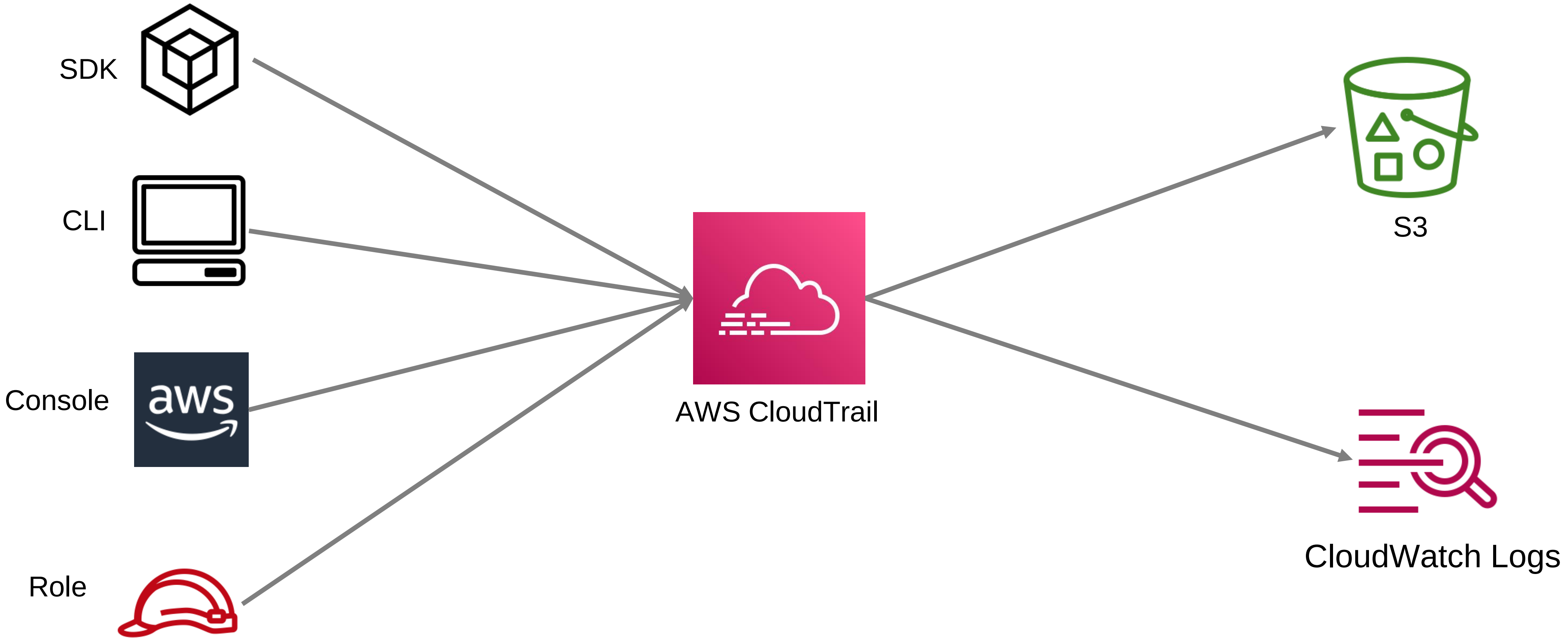

AWS services
(Event Sources)
Crontab
CloudWatch Events
Lambda
Amazon Simple Notification Service
Amazon Simple Queue Service
Amazon Kinesis Data Streams
Amazon Kinesis Data Firehose

CloudTrail

CloudTrail

- CloudTrail provides a tool to governance, tracking and audit in AWS account
- CloudTrail can record the events of API call made by:
  - Console
  - SDK
  - CLI
  - AWS services
- CloudTrail logs can put to S3 or CloudWatch Logs for audit purpose
- CloudTrail is enable by default

CloudTrail Diagram



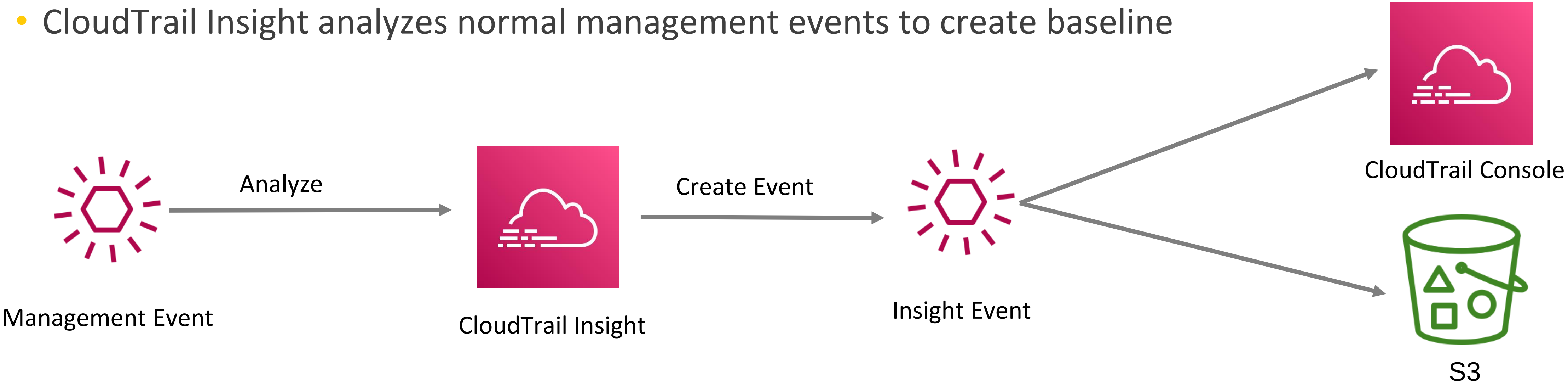
CloudTrail Events

- **Management Events**
  - Management operations on resources on AWS account
  - Example:
    - Configuring security (AWS IAM **AttachRolePolicy**)
    - Configuring rules for routing data (AWS EC2 **CreateSubnet**)
    - Setting up Logging (AWS CloudTrail **CreateTrail**)

- **Data Events**
- Resource operations on a resource on AWS account
- Data events are not enable by default
- Example:
  - Amazon S3, DynamoDB object-level API activity (GetObject, DeleteObject…)s

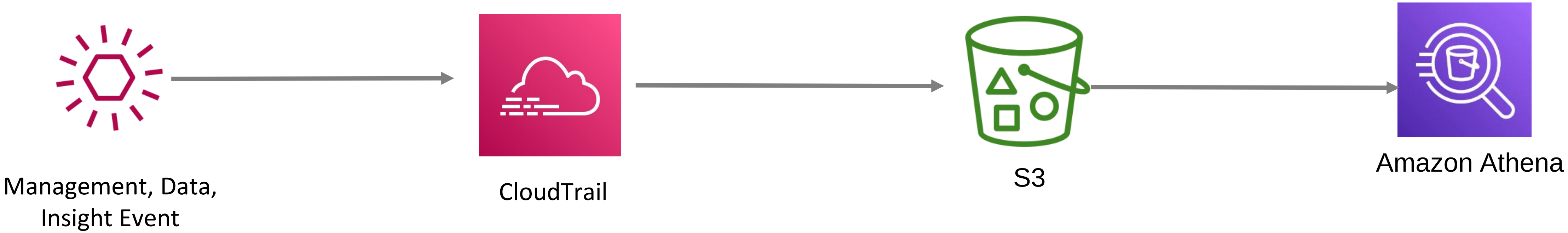
CloudTrail Events (cont.)

- **CloudTrail Insight Events**: Help to identify and respond to unusual activity in AWS account
  - Inaccurate resources provisioning
  - Bursts of AWS IAM action
  - Gaps in regular maintenance activity
- CloudTrail Insight analyzes normal management events to create baseline



CloudTrail Events Retention

- Events are stored in CloudTrail for 90 days
- Put events to S3 for long-term retention


Management, Data,
Insight Event
CloudTrail
S3
Amazon Athena