

# Amazon CloudWatch

*Monitoring Service built for DevOps, SRE and IT Manager*

# Agenda

1. Monitoring Definition
2. CloudWatch Features
3. Labs :
  - a. Cloudwatch logs
  - b. EKS Monitoring
  - c. Prometheus & Grafana
  - d. Prometheus Metrix Collection

# Presentation of the Classroom

## Who am I ?

Computer Science Engineering Education,

Developer, project leader, IT Architect, Cloud Solution Architect, Cloud Security Architect

AWS Architect Associate Certified

16 years experience : Generali, ANPE, France Telecom, Airbus, NavBlue, AirFrance-KLM, AXA GO Operation, Roche Diagnostics

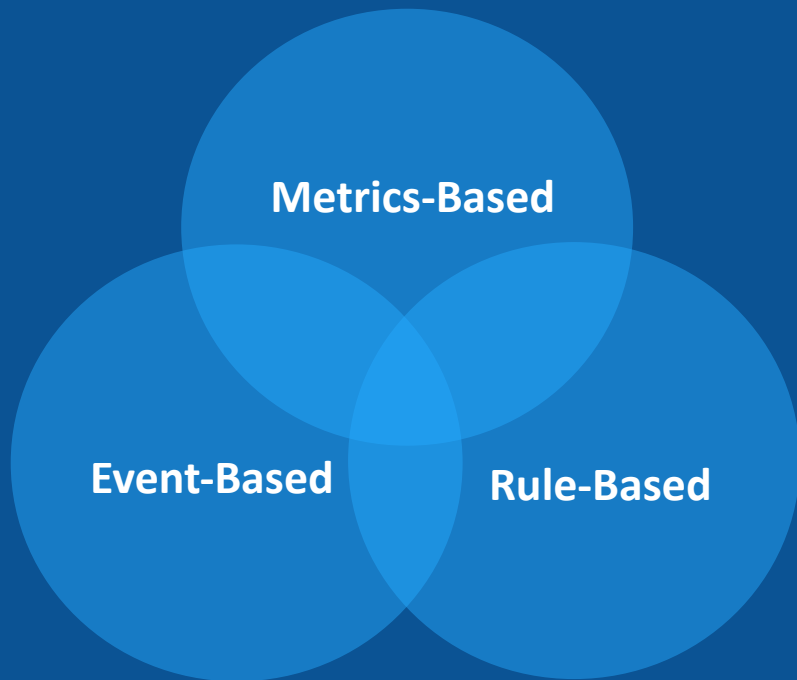
And now help Monaco Gouvernement to build its Cloud Sovereign

Freelancer from 10 years



# Monitoring Definition

# Monitoring is



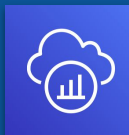
- **Metrics-Based**
  - Static (threshold base)
  - Dynamic (anomaly detection)
- **Event-Based**
  - Event driven
- **Rule-Based**
  - Compliance

# Overview of AWS Monitoring Service



## AWS Trusted Advisor

- AWS Guidance on environmental optimization
- AWS Best Practices Evaluation



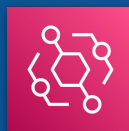
## AWS X-Ray

- Application monitoring
- Security automation / audit support



## AWS Config

- Configuration management / change management
- Compliance rule setting



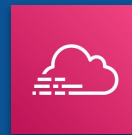
## AWS EventBridge

- Event monitoring
- Alert management



## Amazon CloudWatch

- Resource monitoring
- Log management



## AWS CloudTrail

- API activity monitoring
- Security automation / audit support



## Amazon GuardDuty

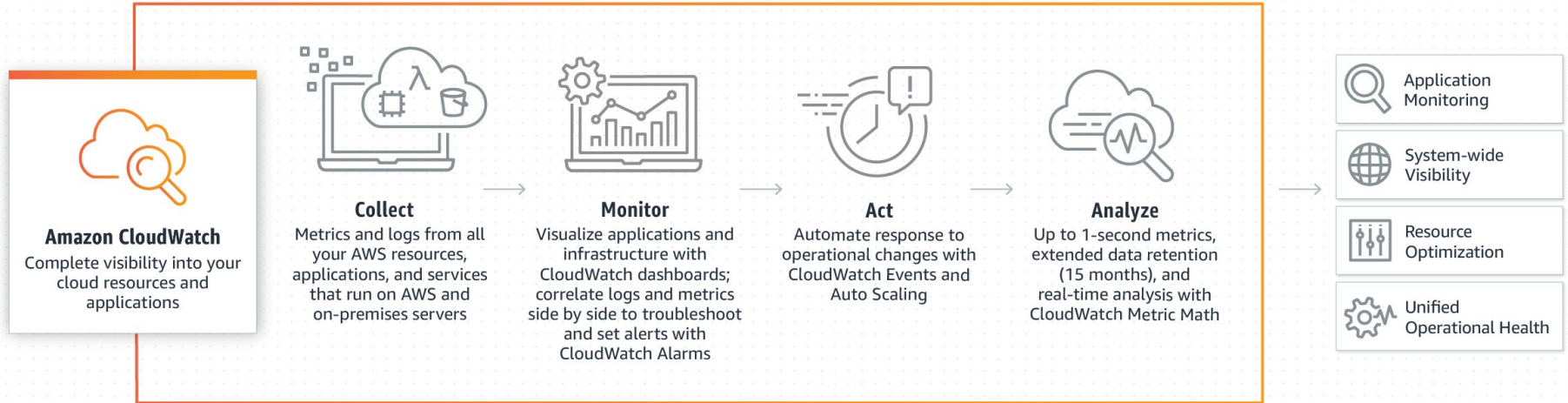
- Intelligent threat detection
- Workload protection using machine learning



## AWS Security Hub

- Integrated security management
- Features of high-priority security issues

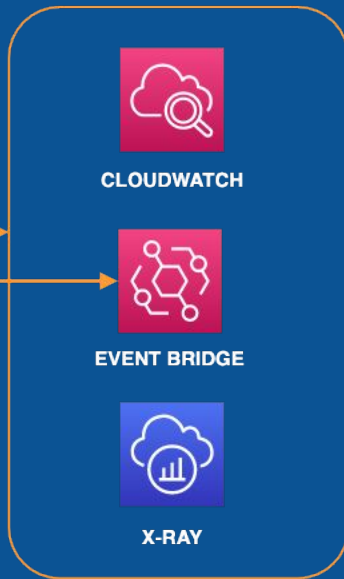
# AWS Cloudwatch



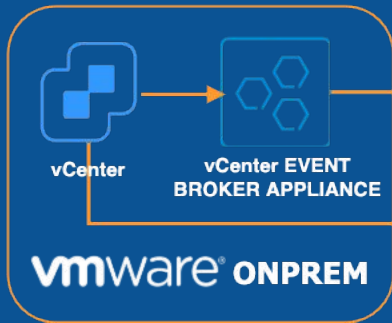
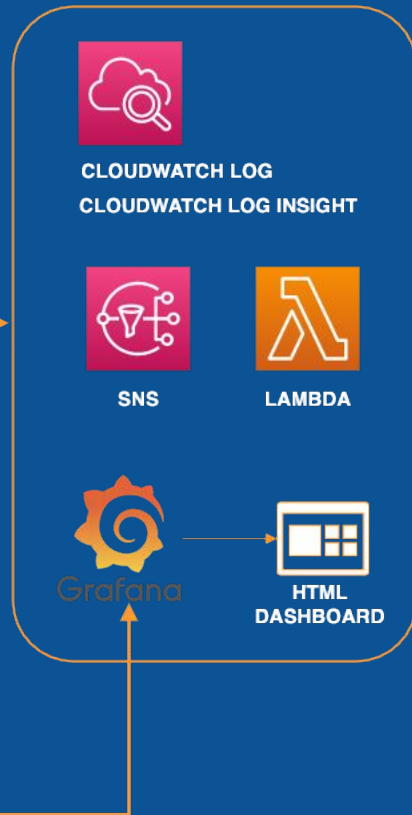
## SOURCES



## ENGINES



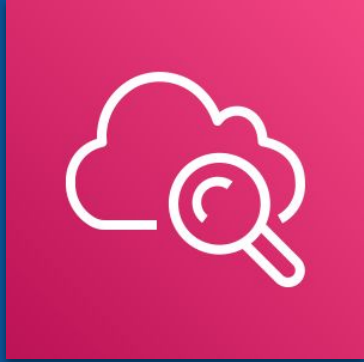
## DASHBOARDS ACTIONS





# CloudWatch Features

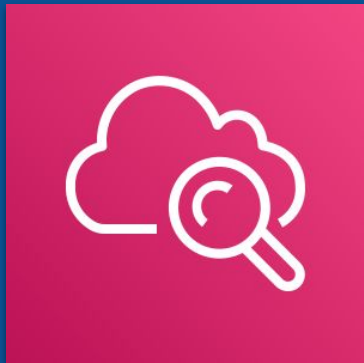
# Amazon CloudWatch



## Features

- Collect
- Monitor
- Act
- Analyse
- Compliance and Security

# Amazon CloudWatch



## Collect

*Log management platform service*

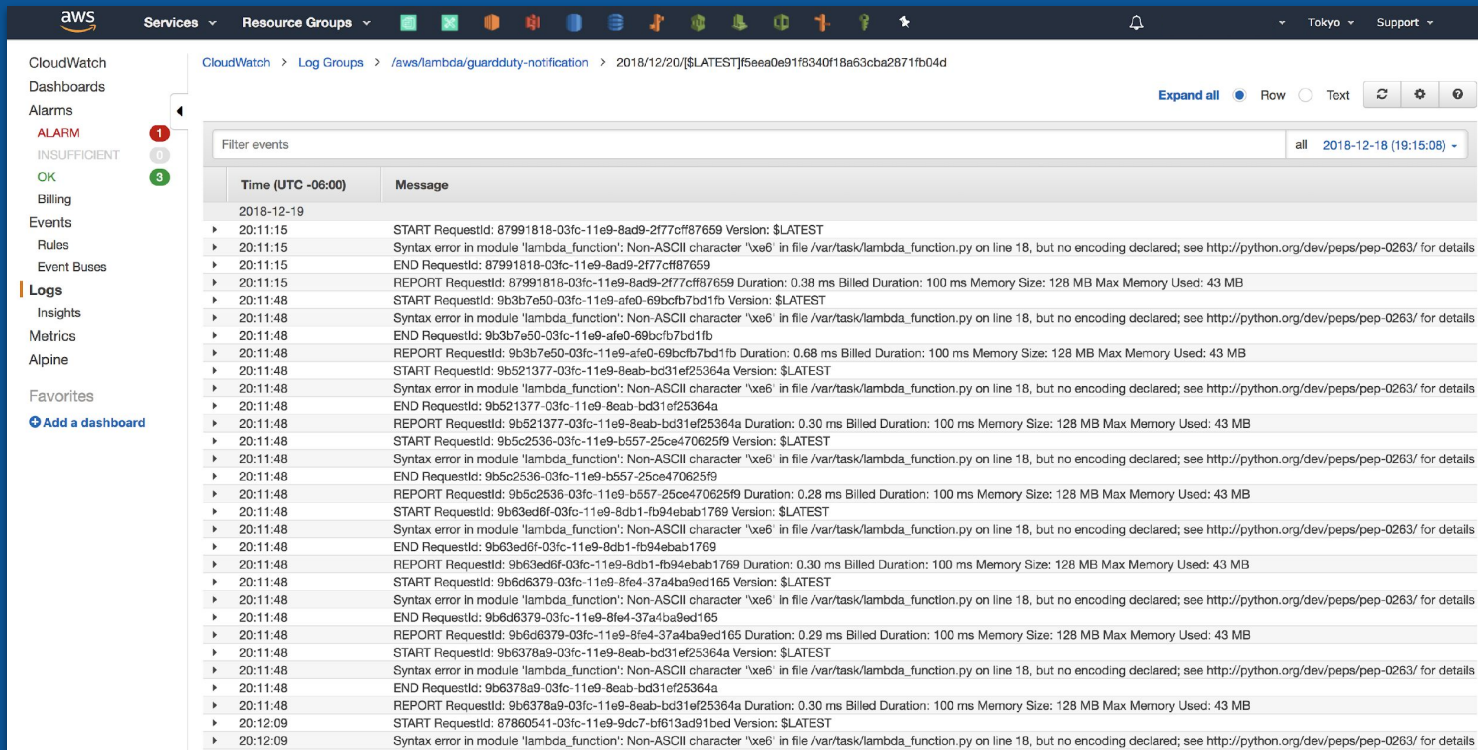
- ★ OS, APP log on EC2
- ★ AWS Managed Service Logs



- Collect & Store
  - Logs from resources, application and services in real time
  - over 30 AWS services
  - Custom Logs (application and on-premises resources)
- Built-in & Custom metrics
  - default metrics from over 70 AWS services
  - custom metrics from applications
- Collect and aggregate container metrics and logs
- Collect and aggregate Lambda metrics and logs



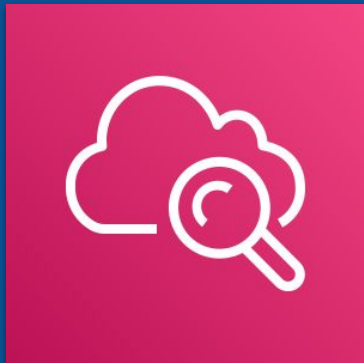
# CloudWatch Logs



The screenshot displays the AWS CloudWatch Logs console. The left sidebar shows navigation options: CloudWatch, Dashboards, Alarms, Billing, Events, Rules, Event Buses, Logs (selected), Insights, Metrics, and Alpine. The main content area shows the log group `/aws/lambda/guardduty-notification` for the function `2018/12/20[$LATEST]5eea0e91f8340f18a63cba2871fb04d`. The log events are filtered by time (UTC -06:00) and message. The events are listed in a table with columns for Time (UTC -06:00) and Message. The messages show various log entries, including syntax errors and report requests, with details like RequestId, Duration, Billed Duration, Memory Size, and Max Memory Used.

Time (UTC -06:00)	Message
2018-12-19	
20:11:15	START RequestId: 87991818-03fc-11e9-8ad9-2f77c0ff87659 Version: \$LATEST
20:11:15	Syntax error in module 'lambda_function': Non-ASCII character '\xe6' in file /var/task/lambda_function.py on line 18, but no encoding declared; see http://python.org/dev/peps/pep-0263/ for details
20:11:15	END RequestId: 87991818-03fc-11e9-8ad9-2f77c0ff87659
20:11:15	REPORT RequestId: 87991818-03fc-11e9-8ad9-2f77c0ff87659 Duration: 0.38 ms Billed Duration: 100 ms Memory Size: 128 MB Max Memory Used: 43 MB
20:11:48	START RequestId: 9b3b7e50-03fc-11e9-afe0-69bcfb7bd1fb Version: \$LATEST
20:11:48	Syntax error in module 'lambda_function': Non-ASCII character '\xe6' in file /var/task/lambda_function.py on line 18, but no encoding declared; see http://python.org/dev/peps/pep-0263/ for details
20:11:48	END RequestId: 9b3b7e50-03fc-11e9-afe0-69bcfb7bd1fb
20:11:48	REPORT RequestId: 9b3b7e50-03fc-11e9-afe0-69bcfb7bd1fb Duration: 0.68 ms Billed Duration: 100 ms Memory Size: 128 MB Max Memory Used: 43 MB
20:11:48	START RequestId: 9b521377-03fc-11e9-8eab-bd31ef25364a Version: \$LATEST
20:11:48	Syntax error in module 'lambda_function': Non-ASCII character '\xe6' in file /var/task/lambda_function.py on line 18, but no encoding declared; see http://python.org/dev/peps/pep-0263/ for details
20:11:48	END RequestId: 9b521377-03fc-11e9-8eab-bd31ef25364a
20:11:48	REPORT RequestId: 9b521377-03fc-11e9-8eab-bd31ef25364a Duration: 0.30 ms Billed Duration: 100 ms Memory Size: 128 MB Max Memory Used: 43 MB
20:11:48	START RequestId: 9b5c2536-03fc-11e9-b557-25ce470625f9 Version: \$LATEST
20:11:48	Syntax error in module 'lambda_function': Non-ASCII character '\xe6' in file /var/task/lambda_function.py on line 18, but no encoding declared; see http://python.org/dev/peps/pep-0263/ for details
20:11:48	END RequestId: 9b5c2536-03fc-11e9-b557-25ce470625f9
20:11:48	REPORT RequestId: 9b5c2536-03fc-11e9-b557-25ce470625f9 Duration: 0.28 ms Billed Duration: 100 ms Memory Size: 128 MB Max Memory Used: 43 MB
20:11:48	START RequestId: 9b63ed6f-03fc-11e9-8db1-fb94ebab1769 Version: \$LATEST
20:11:48	Syntax error in module 'lambda_function': Non-ASCII character '\xe6' in file /var/task/lambda_function.py on line 18, but no encoding declared; see http://python.org/dev/peps/pep-0263/ for details
20:11:48	END RequestId: 9b63ed6f-03fc-11e9-8db1-fb94ebab1769
20:11:48	REPORT RequestId: 9b63ed6f-03fc-11e9-8db1-fb94ebab1769 Duration: 0.30 ms Billed Duration: 100 ms Memory Size: 128 MB Max Memory Used: 43 MB
20:11:48	START RequestId: 9b6d6379-03fc-11e9-8fe4-37a4ba9ed165 Version: \$LATEST
20:11:48	Syntax error in module 'lambda_function': Non-ASCII character '\xe6' in file /var/task/lambda_function.py on line 18, but no encoding declared; see http://python.org/dev/peps/pep-0263/ for details
20:11:48	END RequestId: 9b6d6379-03fc-11e9-8fe4-37a4ba9ed165
20:11:48	REPORT RequestId: 9b6d6379-03fc-11e9-8fe4-37a4ba9ed165 Duration: 0.29 ms Billed Duration: 100 ms Memory Size: 128 MB Max Memory Used: 43 MB
20:11:48	START RequestId: 9b6378a9-03fc-11e9-8eab-bd31ef25364a Version: \$LATEST
20:11:48	Syntax error in module 'lambda_function': Non-ASCII character '\xe6' in file /var/task/lambda_function.py on line 18, but no encoding declared; see http://python.org/dev/peps/pep-0263/ for details
20:11:48	END RequestId: 9b6378a9-03fc-11e9-8eab-bd31ef25364a
20:11:48	REPORT RequestId: 9b6378a9-03fc-11e9-8eab-bd31ef25364a Duration: 0.30 ms Billed Duration: 100 ms Memory Size: 128 MB Max Memory Used: 43 MB
20:12:09	START RequestId: 87860541-03fc-11e9-9dc7-bf613ad91bed Version: \$LATEST
20:12:09	Syntax error in module 'lambda_function': Non-ASCII character '\xe6' in file /var/task/lambda_function.py on line 18, but no encoding declared; see http://python.org/dev/peps/pep-0263/ for details

# Amazon CloudWatch



## Monitor

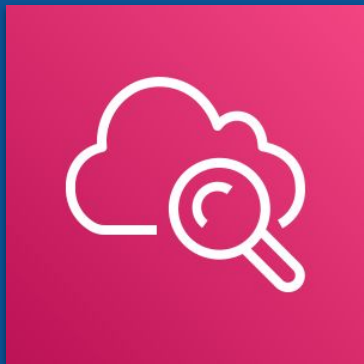
*AWS System monitoring service running on  
Life and death monitoring / performance  
monitoring / capacity monitoring*



- Unified operational view with dashboards
  - Re-usable graphs in unified view
  - graphs metrics, logs data in the same dashboard
- Composite Alarms
- High Resolution Alarms
- Logs & Metrics correlation
- Container monitoring insights
  - provides automatic dashboards
  - for EKS & k8s, dashboard for nodes/EC2 and namespaces
- Lambda monitoring insights
- Anomaly Detection
- ...



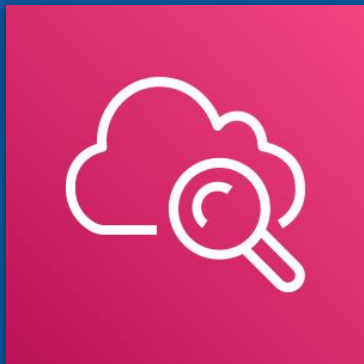
# Amazon CloudWatch



Monitor

- Unified operational view with dashboards
  - Re-usable graphs in unified view
  - graphs metrics, logs data in the same dashboard
- Composite Alarms
- High Resolution Alarms
- Logs & Metrics correlation
- Container monitoring insights
  - provides automatic dashboards
  - for EKS & k8s, dashboard for nodes/EC2 and namespaces
- Lambda monitoring insights
- Anomaly Detection
- ...

# Amazon CloudWatch

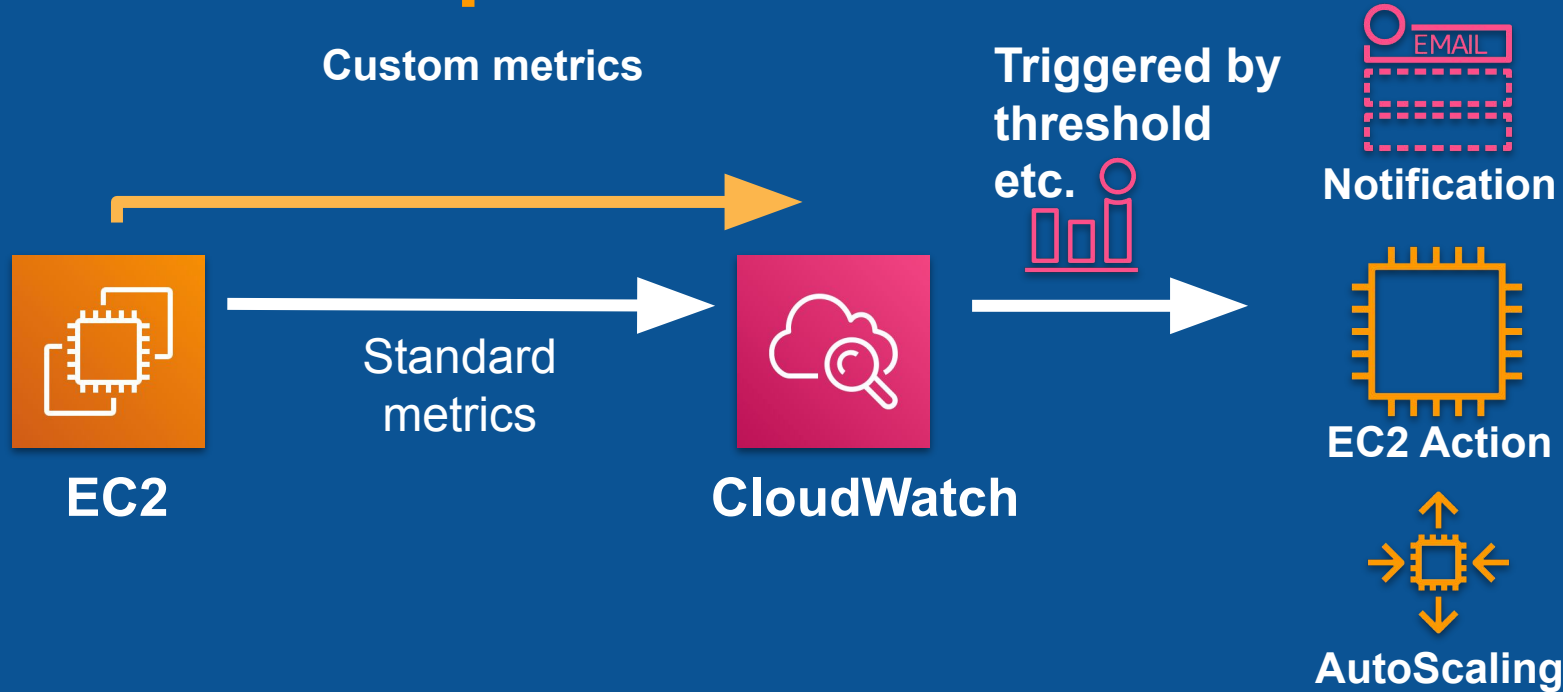


Act

- Auto Scaling
  - help to automate capacity and resource planning
- Automate response to operational changes with CloudWatch Events
- Alarm and automate actions on EKS, ECS, and k8s clusters
  - Container Insight allows to alarm on compute metrics to trigger auto-scaling policies

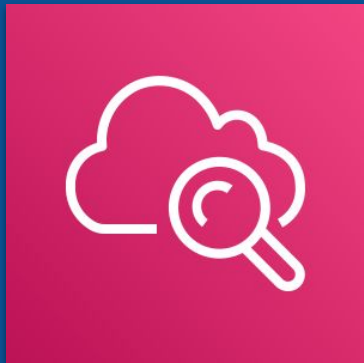
# Amazon CloudWatch Action function

## EC2 Example





# Amazon CloudWatch



## Analyse

*Log Insight : Fast and interactive log analysis*

- Granular data and extended retention
  - 15 months of metrics data (storage & retention)
  - Historical analysis
  - 1 second of health metrics
- Custom operations on metrics
- Log analytics
- Analyze container metrics, logs, and traces
- Analyze Lambda metrics, logs, and traces
- Contributor Insights

# CloudWatch Logs Insights

The screenshot displays the AWS CloudWatch Logs Insights interface. On the left, a navigation menu includes CloudWatch, Dashboards, Alarms (with a red '1' badge), INSUFFICIENT (0), OK (3), Billing, Events, Rules, Event Buses, Logs, Insights (selected), Metrics, and Alpine. Below the menu is a 'Favorites' section with an 'Add a dashboard' button.

The main content area features a 'Query editor' with a dropdown menu set to 'CloudTrail/DefaultLogGroup' and a time range of '15m 30m 1h 6h 12h 1d custom'. The query text is `stats count(*) by eventSource, eventName, awsRegion`. Below the editor are buttons for 'Run query', 'Sample queries', and a link to 'Have feedback? Email us.'.

Below the query editor, there are two tabs: 'Logs' and 'Visualization'. The 'Visualization' tab is active, showing a bar chart titled 'Distribution of log events over time'. The chart's x-axis represents time from 03 AM to 02 PM, and the y-axis represents the number of events from 0 to 1k. The chart shows a relatively steady distribution of events with some fluctuations.

Below the chart, a summary line states: '86,861 records matched | 87,025 records (103.1 MB) scanned in 5.9s @ 14,685 records/s (17.4 MB/s)'. Below this is a table with the following columns: #, eventSource, eventName, awsRegion, and count(\*).

#	eventSource	eventName	awsRegion	count(*)
1	ec2.amazonaws.com	DescribeInstances	ap-southeast-1	721
2	ecs.amazonaws.com	ListClusters	ap-southeast-1	384
3	ecs.amazonaws.com	ListContainerInstances	ap-southeast-1	768
4	ec2.amazonaws.com	DescribeInstanceStatus	ap-southeast-1	1683
5	logs.amazonaws.com	DescribeLogGroups	ap-southeast-1	180
6	elasticloadbalancing.amazonaws.com	DescribeTargetGroups	ap-southeast-1	96
7	ecs.amazonaws.com	ListServices	ap-southeast-1	288
8	monitoring.amazonaws.com	DescribeAlarmHistory	ap-southeast-1	144
9	rds.amazonaws.com	DescribeDBInstances	ap-southeast-1	242
10	elasticloadbalancing.amazonaws.com	DescribeTags	ap-southeast-1	120
11	rds.amazonaws.com	DescribeEvents	ap-southeast-1	241
12	s3.amazonaws.com	GetBucketTagging	ap-southeast-1	108
13	logs.amazonaws.com	DescribeLogStreams	ap-northeast-1	2700
14	ec2.amazonaws.com	DescribeInstanceStatus	ap-northeast-1	5648
15	ssm.amazonaws.com	UpdateInstanceInformation	ap-northeast-1	1440

On the right side of the console, there is a 'Query help' section. It includes a 'Commands' section with a list of fields: @logStream, @message, @timestamp, awsRegion, eventId, eventName, eventSource, eventTime, eventType, eventVersion, recipientAccountId, sourceIPAddress, userAgent, useridentity.type, requestId, useridentity.accountId, useridentity.principalId, useridentity.am, useridentity.sessionContext.attrib..., useridentity.sessionContext.attrib..., useridentity.sessionContext.sessi..., useridentity.sessionContext.sessi..., useridentity.sessionContext.sessi..., and useridentity.sessionContext.sessi... Each field is followed by a percentage indicating its frequency in the results.

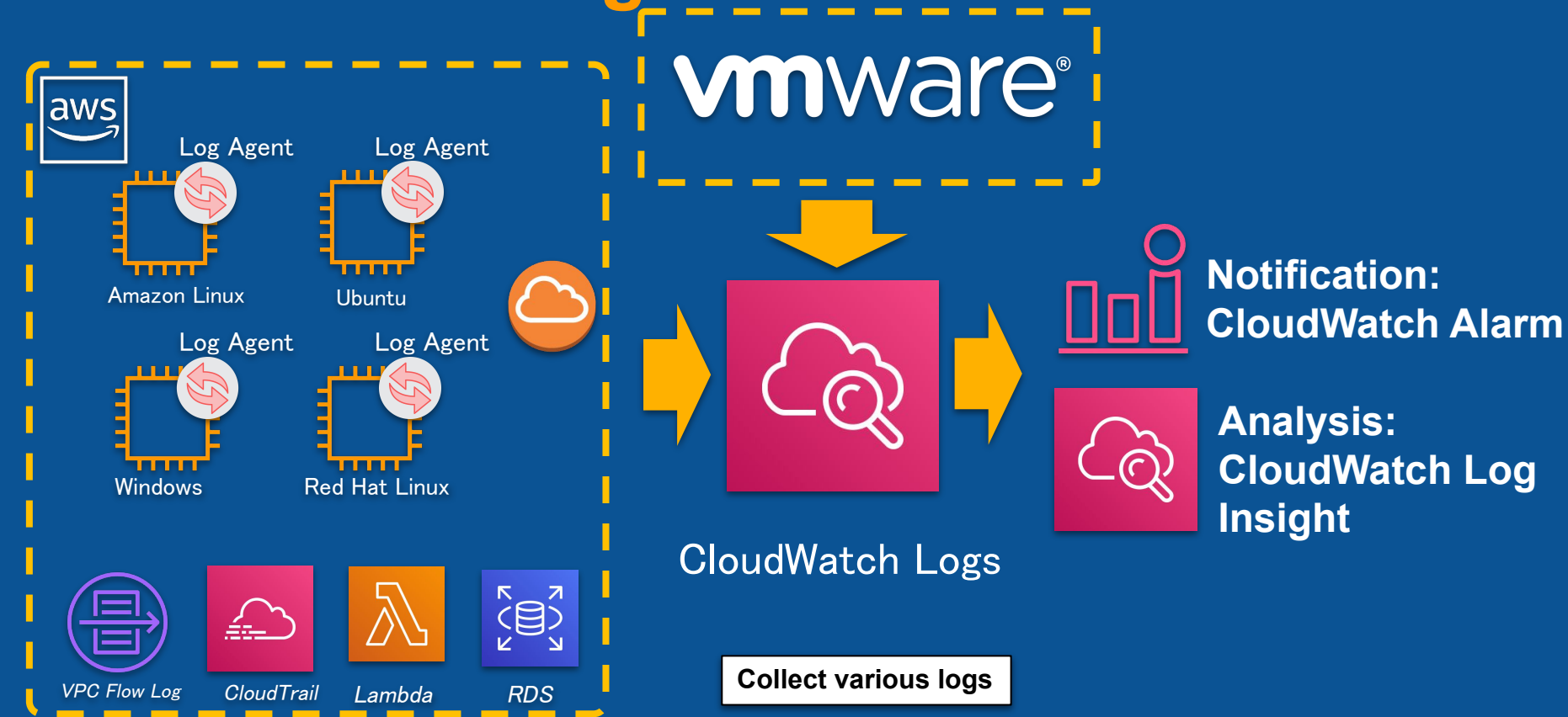
# Amazon CloudWatch



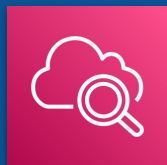
Compliance  
and Security

- IAM Integration
  - Control users and resources permission access

# CloudWatch Logs



# AWS Elasticity : AWS Cloudwatch



## Amazon Cloudwatch Architecture

