

# AWS Cloud for beginner

Instructor: Linh Nguyen

(Engineering Consultant, AWS Cloud Solution Architect)

Level: Beginner

*“Không có việc gì khó, chỉ sợ không biết làm”*

# Monitoring and Auditing CloudWatch, CloudTrail

Copyright@Linh Nguyen on Udemy

# Target

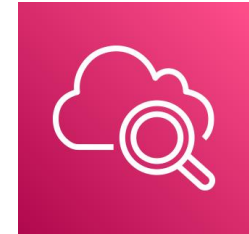
- Hiểu được tại sao lại cần Monitoring cho hệ thống?
- Các concept cơ bản về Monitoring.
- Hiểu được CloudWatch là gì? Các chức năng chính và usecase.
- Thành thạo việc cấu hình CloudWatch Alarm.
- Biết cách cài đặt CloudWatch Agent trên EC2 để collect các custom metrics và log.
- Nắm được concept cơ bản của CloudTrail, biết cách tra cứu một event khi cần thiết phục vụ mục đích audit.
- Thực hành enable trail export action log ra S3 bucket.

# Tại sao cần monitor (giám sát) hệ thống?

- Hệ thống được thiết kế và xây dựng tốt đến đâu thì vẫn sẽ tiềm ẩn các nguy cơ gặp sự cố, nhiệm vụ của giám sát (monitor) là theo dõi sức khỏe của hệ thống, phát hiện những vấn đề kịp thời, từ đó đưa ra các hành động hợp lý như thông báo cho quản trị viên hoặc recovery action.
- Nhu cầu truy cập, workload của các resource sẽ biến động không ngừng theo thời gian, cần có cơ chế giám sát để có hành động kịp thời, tránh các sự cố (không đủ tài nguyên, workload quá cao giảm trải nghiệm người dùng...)
- Việc giám sát liên tục trạng thái của các resource cũng là tiền đề để hệ thống có thể auto-scale.

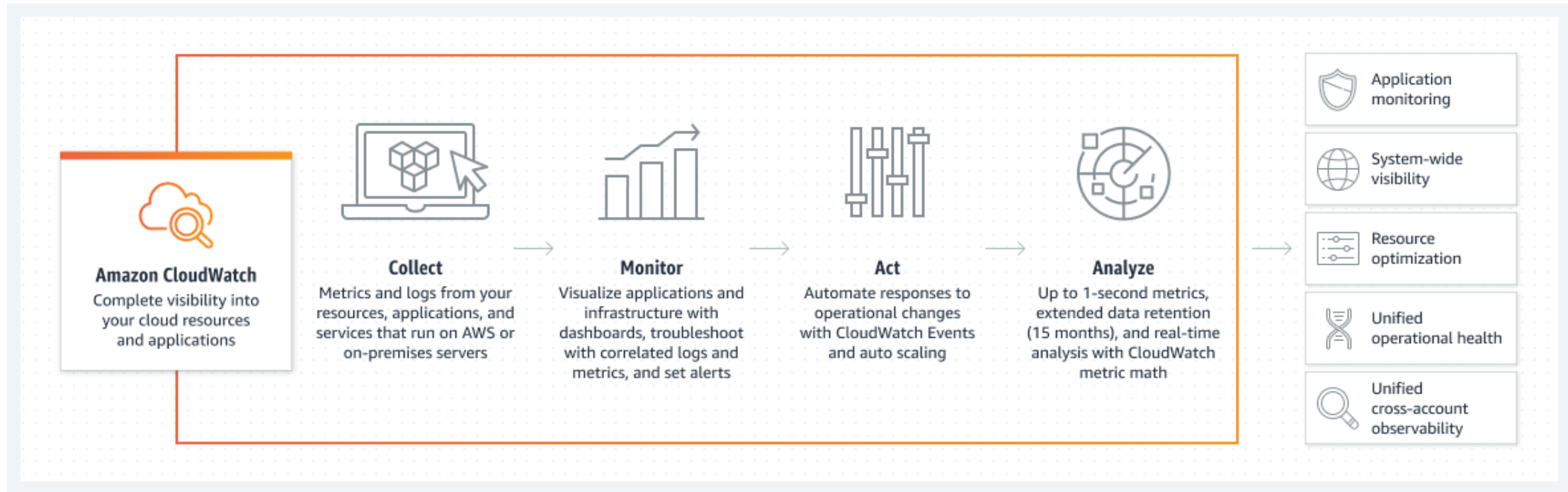
# CloudWatch là gì?

- AWS CloudWatch là một dịch vụ được thiết kế để giám sát và quản lý hệ thống và ứng dụng trên nền tảng AWS. Nó cung cấp khả năng thu thập, xử lý và hiển thị các thông tin liên quan đến hiệu suất, khả năng mở rộng và lỗi của các tài nguyên trong môi trường AWS.
- CloudWatch cho phép bạn theo dõi các thông số quan trọng như CPU usage, network traffic, storage, database. Nó cũng cung cấp các dịch vụ ghi log để lưu trữ và phân tích các sự kiện quan trọng từ các ứng dụng và hệ thống. Bạn có thể sử dụng CloudWatch để tạo ra các đồ thị và báo cáo để theo dõi hiệu suất và tình trạng của các ứng dụng và hệ thống trên AWS.
- CloudWatch cũng hỗ trợ các cảnh báo tự động (Alarm) dựa trên ngưỡng mà bạn đặt để thông báo khi các tài nguyên vượt quá giới hạn hoặc xảy ra lỗi. Điều này cho phép bạn tự động phản ứng kịp thời và giải quyết các vấn đề trong hệ thống của mình.



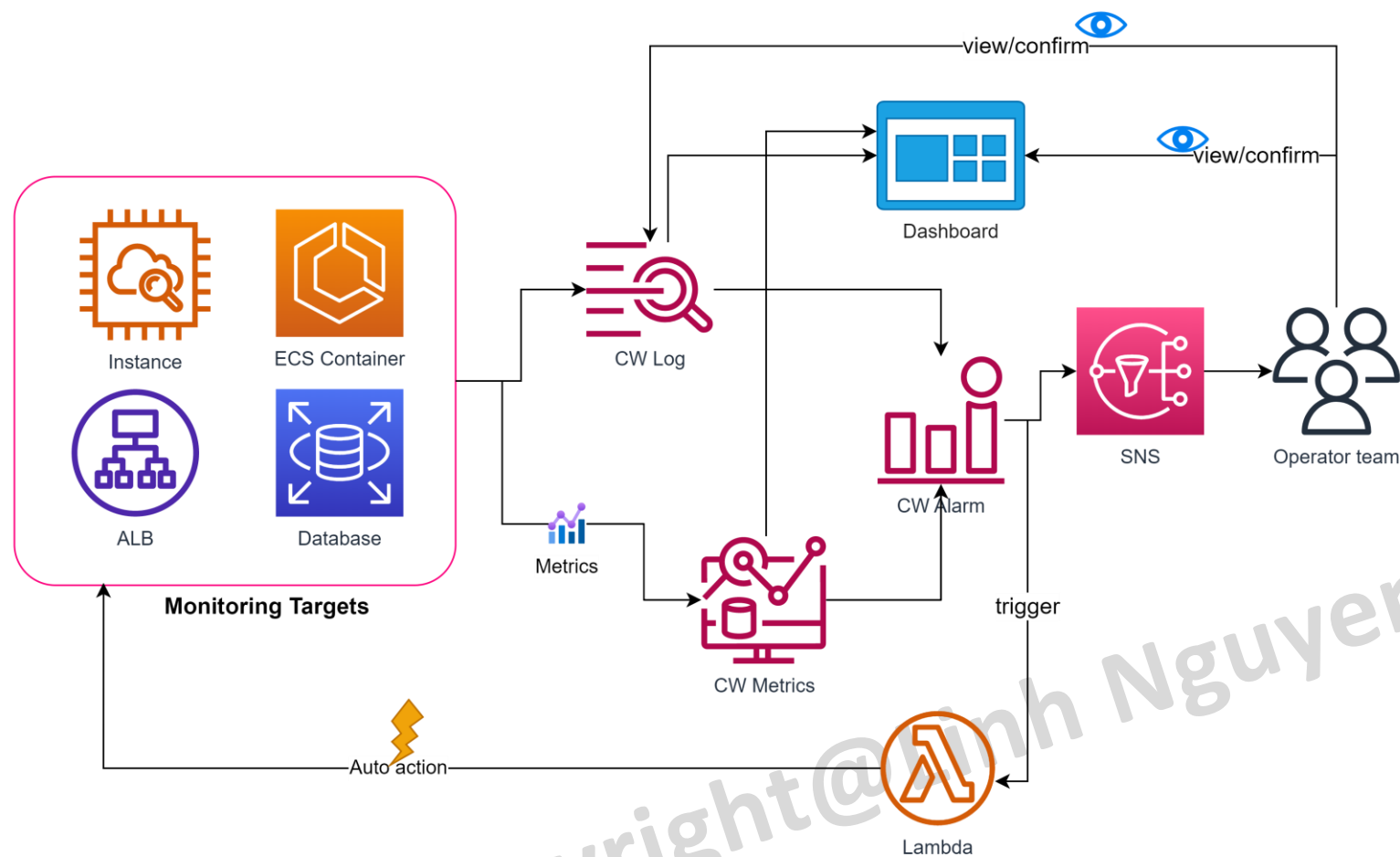
Amazon CloudWatch

# Hệ sinh thái CloudWatch



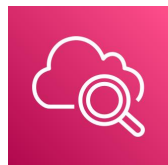
Nguồn: [https://aws.amazon.com/cloudwatch/?nc1=h\\_ls](https://aws.amazon.com/cloudwatch/?nc1=h_ls)

# CloudWatch overview



Ví dụ về một hệ thống có monitoring

# Các thành phần của CloudWatch



Amazon CloudWatch



Alarm



Rule



RUM



Cross-account  
observability



Event  
(time-based)



Event  
(event-based)



Evidently



Data protection



Logs



Synthetics



Metrics  
Insights



# CloudWatch Metrics

Metrics là các thông số đo lường được thu thập và lưu trữ bởi CloudWatch. Chúng đại diện cho các giá trị số hoặc các điểm dữ liệu liên quan đến hoạt động của các tài nguyên trong môi trường AWS, VD EC2, RDS, Elastic Load Balancer, hoặc các dịch vụ tạo ra bởi người dùng.

Metrics hiểu cơ bản là một tập hợp time-series data.

Có 2 loại metrics là default metrics (do AWS thu thập) và custom metrics (do người dùng tự định nghĩa).

Metrics được dùng để làm input cho Alarm hoặc hiển thị trên graph của dashboard phục vụ mục đích giám sát.

Copyright@Linh Nguyen on Udemy

# CloudWatch Metrics

CloudWatch Metrics có quy định về thời gian lưu trữ cho metrics, cụ thể như sau:

- 1 second metrics are available for 3 hours.
- 60 second metrics are available for 15 days.
- 5 minute metrics are available for 63 days.
- 1 hour metrics are available for 455 days (15 months).

Điều này đồng nghĩa với việc những khoảng thời gian càng lâu sẽ càng ít detail hơn (độ dày của data point ít hơn).

Copyright@Linh Nguyen on Udemy

# CloudWatch Metrics – Custom metrics

Một số thông số trên EC2 instance mặc định không thể được thu thập bởi AWS, cần phải cài đặt agent lên để thu thập và gửi metrics lên CloudWatch. VD về agent: CloudWatch Agent, Prometheus, Data dog agent, Telegraf, StatsD.

Các metrics có thể được tính toán để tạo ra một metrics khác phục vụ nhu cầu autoscaling, alarm.

VD: (số lượng instance) / (số lượng message trên SQS).

Copyright@Linh Nguyen on Udemy

# CloudWatch Alarm

- CloudWatch Alarm cho phép bạn tạo ra cảnh báo tự động dựa trên các giá trị Metrics. Khi một CloudWatch Alarm được định cấu hình, nó kiểm tra liên tục các giá trị Metrics và kích hoạt cảnh báo nếu các giá trị vượt quá hoặc thỏa mãn các ngưỡng xác định.
- Khi một CloudWatch Alarm được kích hoạt, nó có thể thực hiện các hành động xác định trước, bao gồm:
  - Gửi thông báo qua email (kết hợp với SNS, SES)
  - Gửi thông báo qua tin nhắn văn bản (SMS) khi kết hợp với SNS
  - Kích hoạt các hành động tự động: CloudWatch Alarm có thể kích hoạt các hành động tự động, chẳng hạn như restart EC2, adjust storage, hoặc call API đến các dịch vụ khác trong AWS.
  - Các CloudWatch Alarm có thể được tạo ra dựa trên nhiều điều kiện khác nhau, bao gồm giá trị Metrics vượt ngưỡng, giá trị Metrics thấp hơn ngưỡng, trung bình hay tổng hợp các giá trị Metrics trong một khoảng thời gian nhất định, và nhiều điều kiện khác nữa.

# CloudWatch Log

- CloudWatch Logs là một dịch vụ cho phép bạn lưu trữ, xem và phân tích các logs từ các ứng dụng và hệ thống trong môi trường AWS cũng như on-premise.
- Nhiều service của AWS có option cho export thẳng log ra CloudWatch, chỉ cần enable lên là có thể xem được.
- CloudWatch Log hỗ trợ các thao tác:
  - Xem các logs theo thời gian thực trong giao diện CloudWatch Logs hoặc sử dụng API để truy xuất logs.
  - Lọc và Tìm kiếm Logs: CloudWatch Logs cung cấp công cụ để lọc và tìm kiếm logs theo các điều kiện xác định. Bạn có thể tìm kiếm các mẫu, từ khóa hoặc các thuộc tính đặc biệt trong logs để tìm kiếm và phân tích thông tin cần thiết.
  - Lưu trữ Logs: CloudWatch Logs cho phép bạn lưu trữ logs trong một kho lưu trữ lâu dài để duy trì lịch sử và thực hiện các phân tích sau này.
  - Phân tích Logs: Bạn có thể sử dụng các dịch vụ và công cụ khác của AWS như Amazon Athena, Amazon Elasticsearch hoặc các công cụ khác để phân tích logs từ CloudWatch Logs và trích xuất thông tin hữu ích.

# CloudWatch Log - Concepts

- **Log Group:** Level cao nhất của CloudWatch Log. Thông thường mỗi nhóm service hoặc resource sẽ push log ra một log group cụ thể.
- **Log Stream:** Đơn vị nhỏ hơn trong log group.
- **Log Metrics Filter:** Định nghĩa các pattern của log để thống kê. Khi log message được set filter, đồng thời bạn cũng tạo ra một metrics trên log group đó.
- **Log retention:** Thời gian log tồn tại trên CloudWatch, được set riêng cho từng log group.
- **Log streaming and archive:** Bạn có thể export log ra các service như S3 nhằm mục đích lưu trữ lâu dài với giá rẻ hoặc stream sang Kinesis phục vụ mục đích realtime analytic.

# CloudWatch Log Insight

Một công cụ cho phép bạn truy vấn log thông qua một cú pháp do AWS định nghĩa.

Copyright@Linh Nguyen on Udemy

# CloudWatch Log Insight

## Logs Insights

Select log groups, and then run a query or [choose a sample query](#).

5m 30m

Select log group(s)

/aws/lambda/udemy-csv-to-dynamodb-employee-function X

1 fields @timestamp, @message, @LogStream, @log

2 | sort @timestamp desc

3 | limit 20

4 | filter @message like /Finish/

Run query

Cancel

Save

History

Queries are allowed to run for up to 60 minutes.

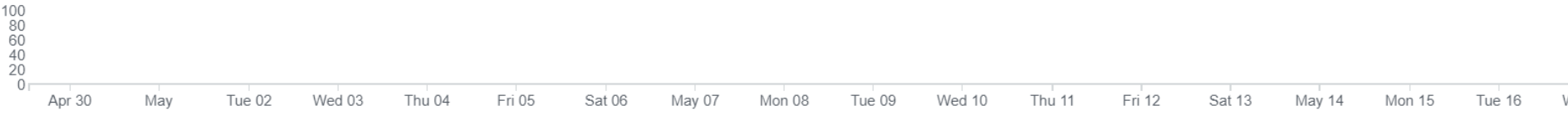
✔ Complete

Logs

Visualization

Export r

Showing 1 of 1 records matched ⓘ  
33 records (10.3 kB) scanned in 2.5s @ 13 records/s (4.1 kB/s)



#	@timestamp	@message	@logStream	@log
▶ 1	2023-05-04T21:46:17.07...	Finished insert data to DynamoDB	2023/05/04/[\$LATEST]b397b77023494409bf45bc240142d2e2	430950558682:/aws/lambda/udemy-csv-to-dynamodb-employee-function



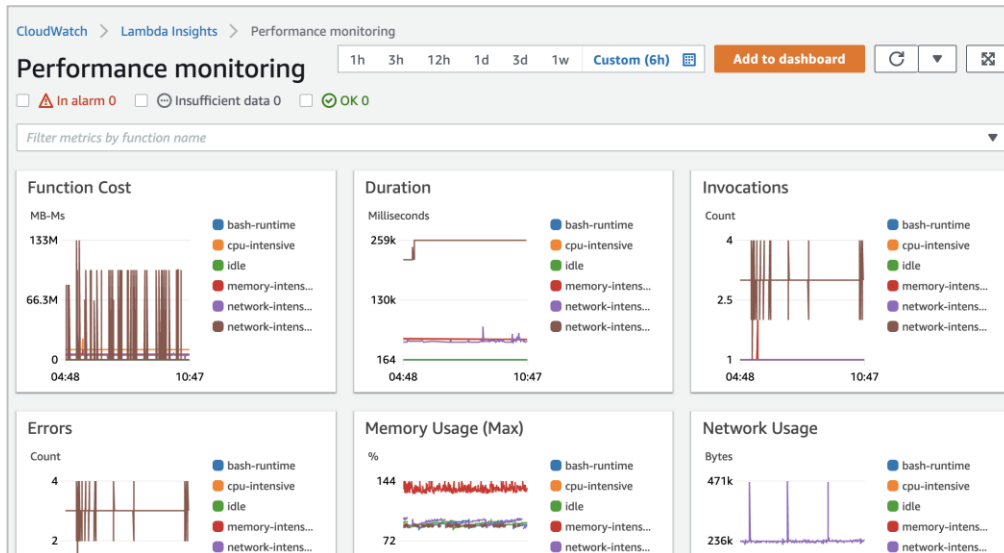
# CloudWatch Insight

Cung cấp công cụ hỗ trợ đơn giản hoá việc collect metrics và log một cách chi tiết.  
Áp dụng cho ứng dụng chạy trên **Container** và **Lambda**.

Copyright@Linh Nguyen on Udemy

# CloudWatch Insight

Ví dụ về monitor Lambda có enable Insight



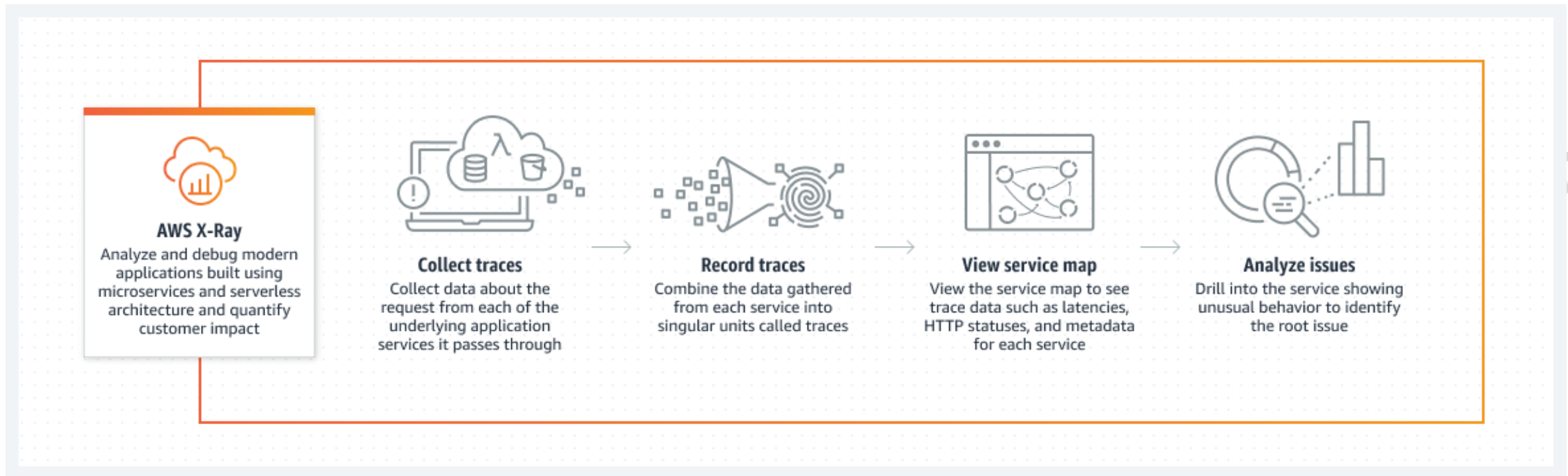
Function summary (6) Actions

< 1 > ⚙

<input type="checkbox"/>	Function name ▲	Invocations ▼	CPU time ▼	Network IO ▼	Max. memory ▼	Cold starts ▼
<input type="checkbox"/>	bash-runtime	360	132.9167ms	4770 kB	<div><div></div></div> 97%	3
<input type="checkbox"/>	cpu-intensive	359	6714.2897ms	4780 kB	<div><div></div></div> 43%	4
<input type="checkbox"/>	idle	359	120.2507ms	4746 kB	<div><div></div></div> 96%	3
<input type="checkbox"/>	memory-intensive	358	2385.9497ms	4794 kB	<div><div></div></div> 144%	4
<input type="checkbox"/>	network-intensive	359	781.0585ms	82008 kB	<div><div></div></div> 99%	3
<input type="checkbox"/>	network-intensive-vpc	43	2730.6977ms	95 kB	<div><div></div></div> 91%	43

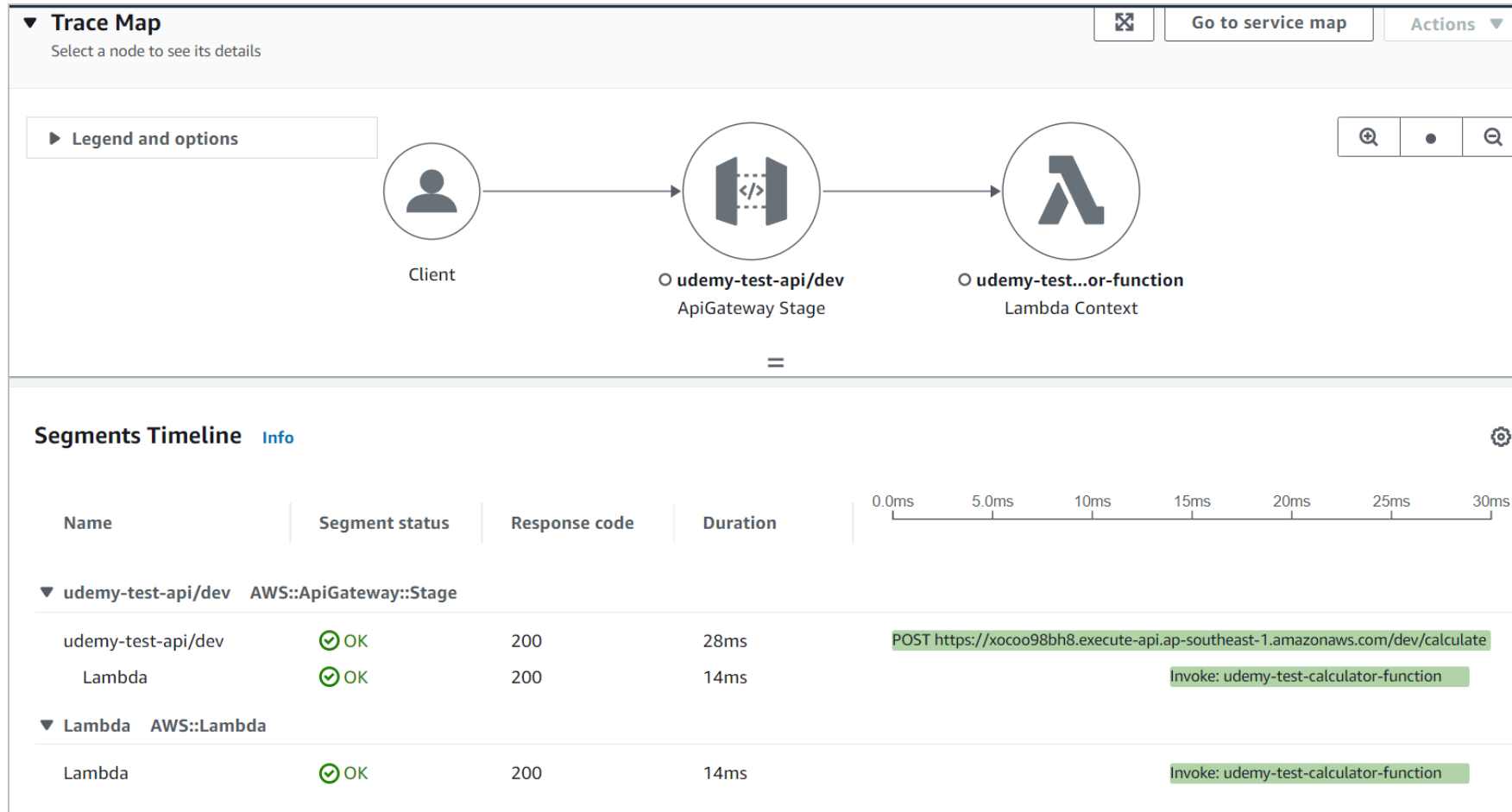
# X-ray

Cung cấp cái nhìn toàn cảnh và chi tiết đường đi của request trong application, giúp điều tra, visualize dựa theo function, api, service.



# X-ray

## Ví dụ về tracing đối với API Gateway + lambda



# CloudWatch Dashboard

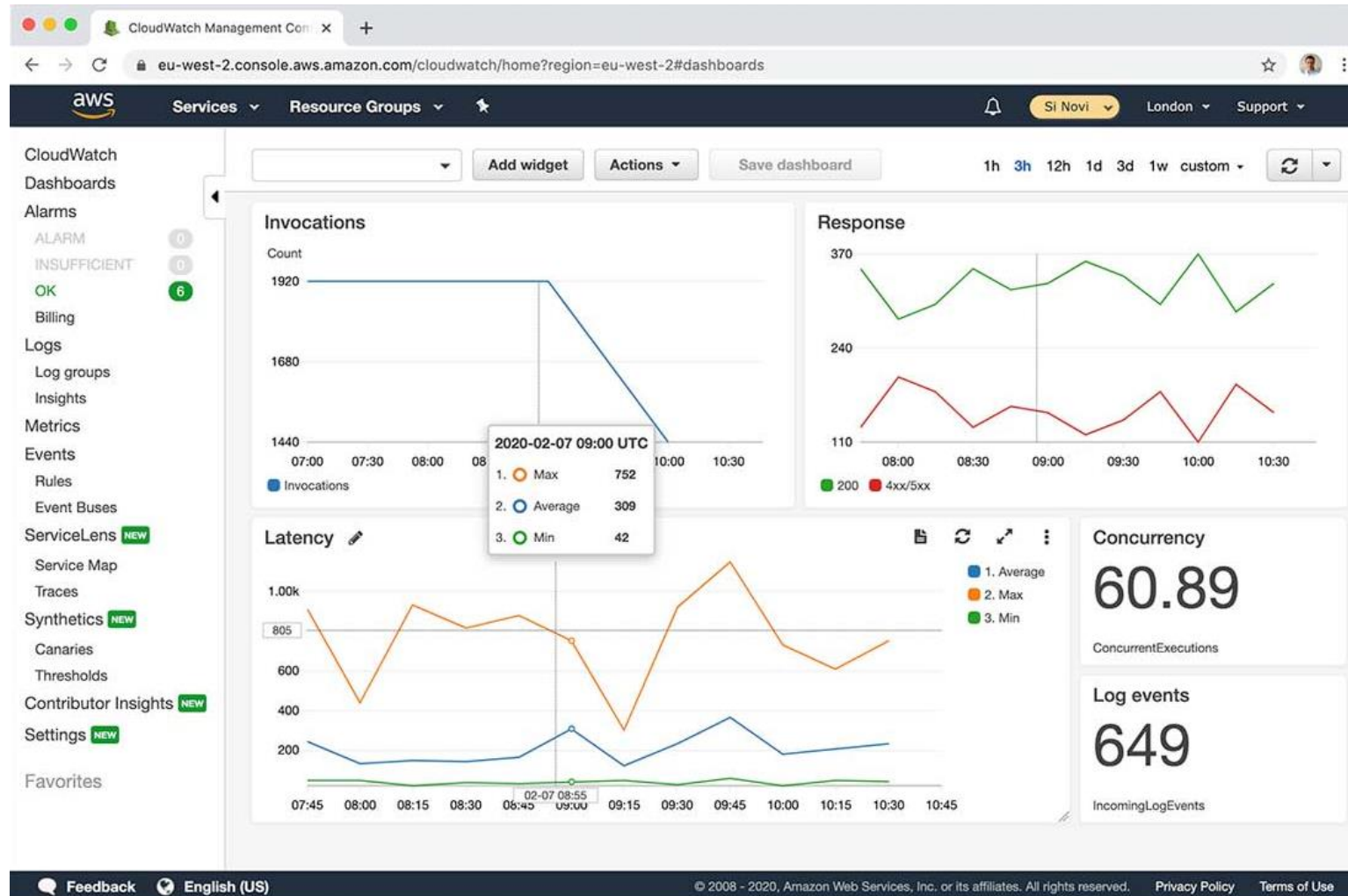
CloudWatch Dashboard cho phép bạn theo dõi nhiều resource (cross regions) trên một view duy nhất.

Bạn có thể add nhiều biểu đồ (widget) với nhiều hình dạng, customize size, màu sắc, title, đơn vị, vị trí...

Widget có thể là biểu đồ, con số biểu diễn một metrics của một resource hoặc danh sách log từ một log group.

Copyright@Linh Nguyen on Udemy

# CloudWatch Dashboard - Example



# Khi thiết kế monitor cần quan tâm những gì?

## **Đặt câu hỏi và trả lời các mục sau:**

- Hệ thống có những resource nào cần monitor?
- Với mỗi resource cần monitor những thông số nào?
- Những thông số nào cần set alarm? thông số nào cần visualize (dashboard)?
- Những resource nào cần collect log?
- Với mỗi resource có log, collect những loại log nào?
- Có set alarm cho log không?
- Metrics và Log lưu trữ ở đâu? (Native service or tự dựng?)
- Khi có alarm cần thông báo tới ai?
- Những yêu cầu khác liên quan quy trình vận hành...

# Lab 1 – CloudWatch Alarm

Yêu cầu tạo một alarm dành cho EC2 có notification sang email, giả lập usage cao (VD CPU, Network) và tiến hành test alarm.

1. Tạo một EC2 server, sử dụng script để cài httpd, test truy cập thành công.
2. Tạo một alarm cho Network In, threshold 2000, notify đến email.
3. Tạo một alarm cho CPU Usage, threshold 20%, notify đến email.
4. Truy cập liên tục website, confirm alarm Network gửi đến email.
5. Giả lập CPU usage cao, confirm alarm CPU gửi đến email.

Copyright@Linh Nguyen on Udemy



# CloudWatch Alarm

## Một số chú ý cho CW Alarm trong quá trình thiết kế và setting

- Naming rule: dễ đọc, dễ hiểu, nhìn vô biết ngay là hệ thống nào, môi trường nào, resource nào, vấn đề gì.

Tham khảo naming rule: <system-name>-<env>-<resource>-<alarm>

VD: [ABCBank-dev-master\\_database-CPU-is-higher-80%-in-10-mins](#)

- Threshold phải hợp lý. Điều này phải được kiểm chứng thông qua quá trình performance test và turning, rất khó để setting kiểu “*một phút ăn ngay*”.
- Phân chia notification target cho những nhóm resource và người phụ trách phù hợp. Có thể tách mỗi nhóm resource thành 1 topic SNS.
- Xác nhận với khách hàng/người thiết kế về những thông số cần collect/set alarm từ giai đoạn sớm của dự án.

## Lab 2 – CloudWatch Agent

Yêu cầu: Tạo một EC2 instance, thực hiện cài đặt CWAgent lên trên đó, cấu hình CWAgent đẩy các thông số như Memory, Disk, Log lên CloudWatch.

1. Tạo một EC2 instance với AMI Amazon linux 2 2023, cài httpd, test truy cập.
2. Cấp IAM Role phù hợp cho EC2 Instance (**CloudWatchAgentServerPolicy**)
3. Cài đặt CloudWatch Agent
4. Cấu hình CloudWatch Agent (collect access log của httpd, Memory, Disk usage)
5. Enable service CW Agent khởi động cùng OS và theo dõi log của CW Agent xem hoạt động thành công.
6. Thử access website, confirm log được gửi lên CW Log?
7. Xem metrics có được gửi lên CloudWatch metrics thành công?

## Lab 3 – Log Metrics filters

Yêu cầu: Metrics filter trên log group “access\_log”, setting alarm nếu xuất hiện ERROR log trên 3 lần trong 1 phút thì thông báo notification.

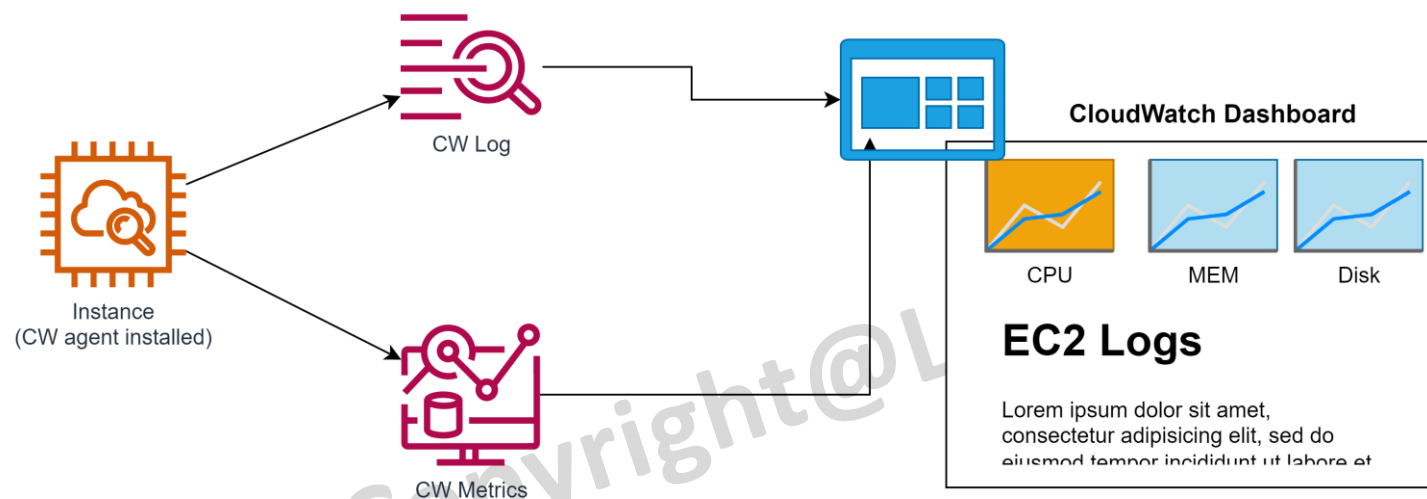
1. Tạo một Log Metrics filter trên log group “access\_log” với keyword là “**ERROR**”.
2. Tạo một Alarm dựa trên Metrics filter vừa tạo.
  - Theshold: 3
  - Duration: 1 min
  - Statistic: Sum
3. Thử ghi log dummy có keyword **ERROR** vào trong “access\_log” file.
4. Confirm alarm được kích hoạt và gửi email.

Copyright@Linh Nguyen on Udemy

# Lab 4 – CloudWatch Dashboard

Yêu cầu: Tạo một dashboard trên CloudWatch, add một vài widget vào dashboard.

- CPU
- Memory (custom metrics)
- Disk usage (custom metrics)
- Log (lấy từ CloudWatch agent gửi lên)



# Lab 4 – CloudWatch Dashboard

*Yêu cầu đã làm bài Lab2, cài đặt CW Agent trên EC2 thành công.*

## **Steps:**

1. Truy cập vào CloudWatch, Dashboard, tạo một Dashboard mới.
2. Add CPU Usage widget
3. Add Memory Usage widget
4. Add Disk Usage widget
5. Add Log message widget
6. Lưu Dashboard lại.

Copyright@Linh Nguyen on Udemy

# CloudWatch pricing

CloudWatch tính tiền dựa trên các yếu tố:

- Số lượng metrics: \$0.3/metrics/month
- Số lượng Alarm: \$0.1/alarm/month
  - \*Metrics và Alarm sẽ bị tính phí cao hơn nếu sd high resolution.*
- Số lượng Dashboard: \$3/dashboard/month
- Số lượng event push lên CloudWatch
- Dung lượng log lưu trữ trên CloudWatch: \$0.7/GB
- Dung lượng log scan khi sd CloudWatch Log Insight
- *and more...*

*Chi tiết hơn có tại: <https://aws.amazon.com/cloudwatch/pricing/>*

# Cost saving for CloudWatch

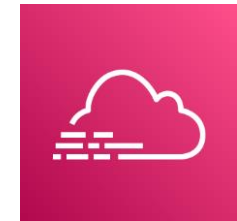
Có một số phương án tiết kiệm cost cho CloudWatch

- Chỉ monitor những thông số cần thiết thay vì monitor toàn bộ thông số.
- Sử dụng metrics resolution phù hợp (vd 60s thay vì 5s), bởi không phải metrics nào cũng cần phải monitor với tần suất cao.
- Đặt retention phù hợp cho các log group (vd 30d, 90d,...) thay vì để unlimited.
- Archive những log cũ không có nhu cầu tra cứu xuống S3, S3-Glacier để giảm cost nhưng vẫn đảm bảo compliance về lưu trữ.
- Tắt log DEBUG, INFO không cần thiết trên môi trường production để giảm lượng log gửi lên CloudWatch.

# CloudTrail

CloudTrail là một dịch vụ quản lý và giám sát log (log) hoạt động của resource trong môi trường AWS. CloudTrail ghi lại và theo dõi các hoạt động của người dùng, tài khoản, dịch vụ và tài nguyên trong tài khoản AWS của bạn. Dịch vụ này giúp bạn hiểu rõ hơn về những gì đã xảy ra trong tài khoản AWS của bạn, bảo mật hơn và giúp tuân thủ security compliance.

Khác với CloudWatch có mục đích giám sát tình trạng của resource, CloudTrail có mục đích ghi lại những hành động đã được thực thi trong môi trường AWS (who did what?).



AWS CloudTrail

Copyright@Linh Nguyen on Udemy



# Các chức năng cơ bản của CloudTrail

Một số chức năng và lợi ích của AWS CloudTrail bao gồm:

1. Ghi lại các sự kiện quan trọng: CloudTrail ghi lại các sự kiện như việc create, update, delete resource, truy cập vào resource, tạo, sửa đổi hoặc xóa IAM roles, và các hoạt động khác liên quan đến tài nguyên AWS.
2. Giám sát và kiểm tra tuân thủ: CloudTrail cung cấp thông tin chi tiết về các hoạt động trong tài khoản AWS, giúp bạn kiểm tra và đảm bảo tuân thủ các quy định, chính sách và quy trình an ninh nội bộ.
3. Phân tích và bảo mật: Dữ liệu log của CloudTrail có thể được sử dụng để phân tích hoạt động, phát hiện sự cố bảo mật, theo dõi và phản ứng kịp thời đối với các sự kiện không mong muốn hoặc đe dọa bảo mật.
4. Tương thích với các dịch vụ khác: CloudTrail tích hợp với các dịch vụ AWS khác như IAM, AWS Config và Amazon CloudWatch, tạo ra khả năng theo dõi và quản lý toàn diện.
5. CloudTrail cung cấp các log record được lưu trữ trong S3 của AWS, nơi bạn có thể truy cập và phân tích dữ liệu log theo nhu cầu.

# Giới thiệu Cloud Trail trên console.

*\*Mời các bạn xem AWS Console*

Copyright@Linh Nguyen on Udemy

# Lab CloudTrail – Bật trail và output log ra S3

Login vào console, CloudTrail

1. Tạo một Trail, setting output log ra S3
2. Thực hiện một vài hành động có thay đổi resource, vd Tạo EC2 Instance, Tạo & Xóa EBS Volume.
3. Kiểm tra xem CloudTrail log có được output ra S3 không?
4. Download về và xem nội dung.

Copyright@Linh Nguyen on Udemy

# Clear resources

1. Login to AWS console
2. Terminate instance (nếu có)
3. Xoá Elastic IP (nếu còn lại)
4. Xoá snapshot (nếu còn lại)
5. Xoá volume (nếu còn lại)
6. Xoá hết các log group hoặc set retention về 7 days
7. Xoá hết các Alarm
8. Xoá hết các Dashboard
9. Xoá Cloud Trail

Copyright@Linh Nguyen on Udemy