Amazon CloudWatch

- Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time.
- In Amazon CloudWatch, **metrics are data points that represent various aspects of resource performance or utilization.**
- They are a key feature of CloudWatch that help monitor applications, optimize resource use, and respond to performance changes.
- You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.
- The CloudWatch home page automatically displays metrics about every AWS service you use.

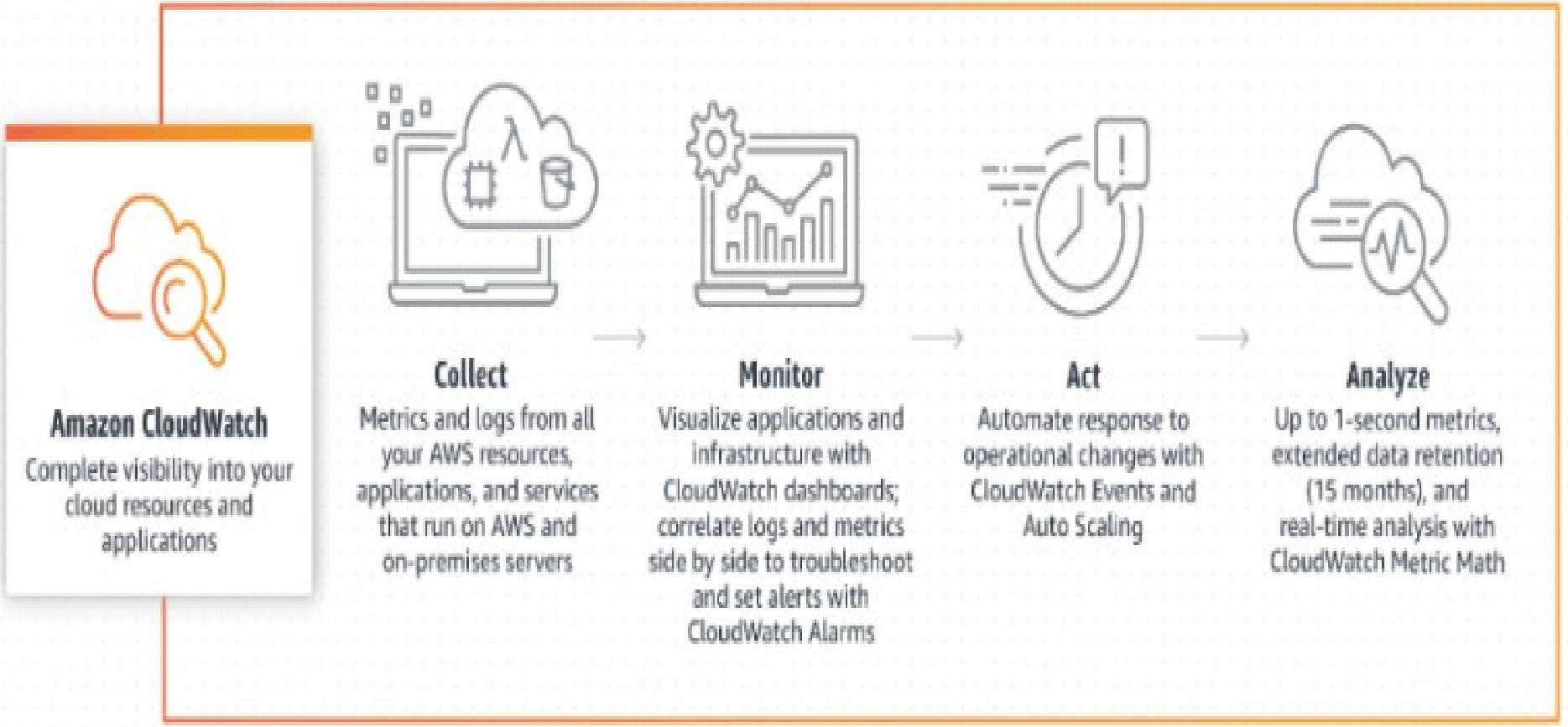
- You can additionally create custom dashboards to display metrics about your custom applications, and display custom collections of metrics that you choose.
- You can create alarms that watch metrics and send notifications or automatically make changes to the resources you are monitoring when a threshold is breached.
- With CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health.
- With Amazon CloudWatch, there is no up-front commitment or minimum fee; you simply pay for what you use. You will be charged at the end of the month for your usage.
- (https://calculator.aws/#/createCalculator/CloudWatch)

Accessing CloudWatch

You can access CloudWatch using any of the following methods:

- **Amazon CloudWatch console** – https://console.aws.amazon.com/cloudwatch/
- **AWS CLI** – For more information, see Getting Set Up with the AWS Command Line Interface in the *AWS Command Line Interface User Guide*.
- **CloudWatch API** – For more information, see the Amazon CloudWatch API Reference.
- **AWS SDKs** – For more information, see Tools for Amazon Web Services.

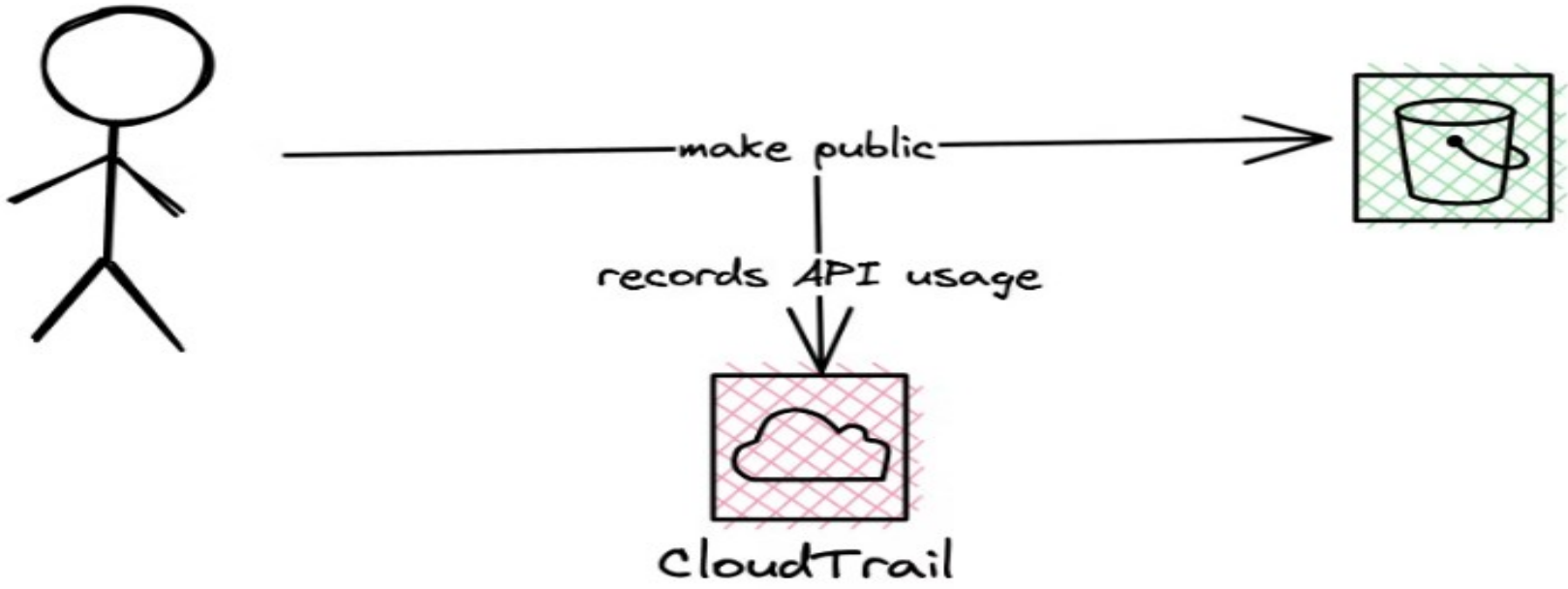
How CloudWatch works???



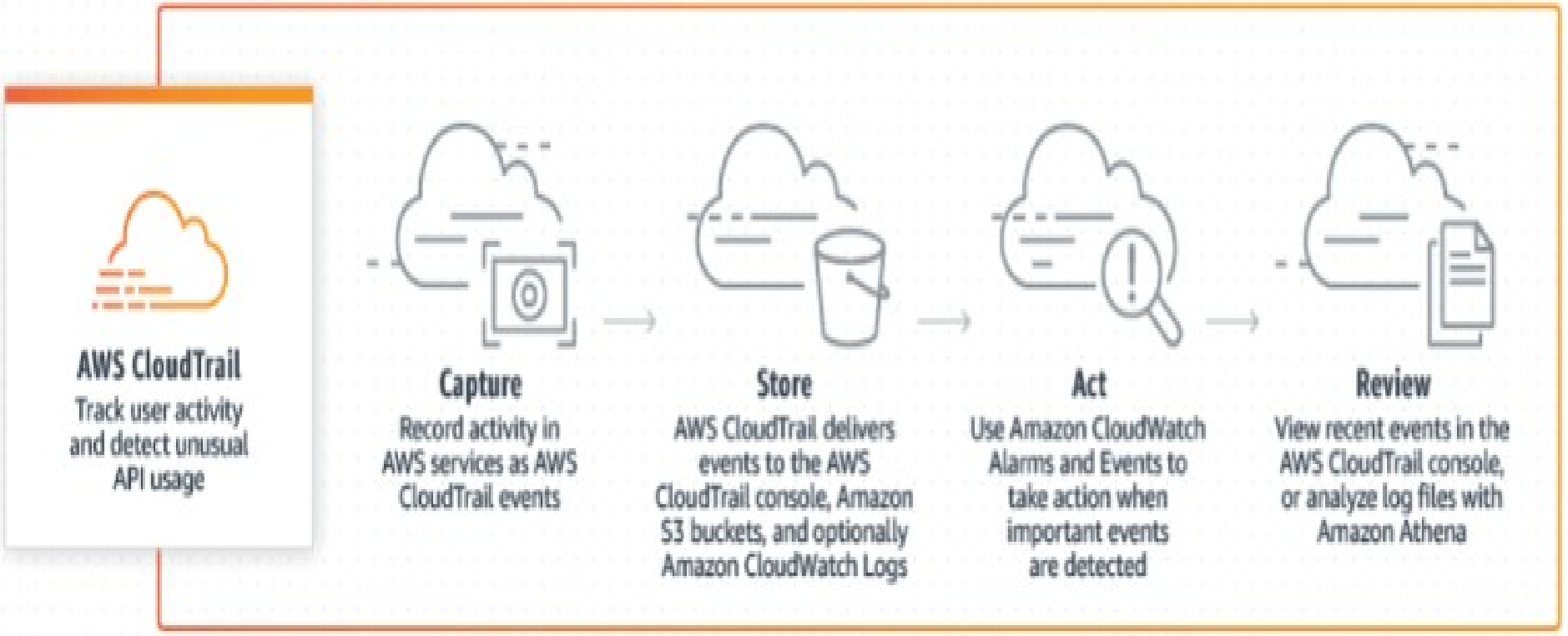
What Is AWS CloudTrail?

- It is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account.
- Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.
- Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

- CloudTrail is active in your AWS account when you create it.
- When activity occurs in your AWS account, that activity is recorded in a CloudTrail event



How does CloudTrail work?



Different ways to record events

- **Event history** – The **Event history** provides a viewable, searchable, downloadable, and immutable record of the past 90 days of management events in an AWS Region. You can search events by filtering on a single attribute. You automatically have access to the **Event history** when you create your account.

- **Trails** – *Trails* capture a record of AWS activities, delivering and storing these events in an Amazon S3 bucket, with optional delivery to CloudWatch Logs and Amazon EventBridge.
- You can input these events into your security monitoring solutions.
- You can also use your own third-party solutions or solutions such as Amazon Athena to search and analyze your CloudTrail logs.
- You can create trails for a single AWS account or for multiple AWS accounts by using AWS Organizations.

- **AWS CloudTrail Lake** - is a managed data lake for capturing, storing, accessing, and analyzing user and API activity on AWS for audit and security purposes.
- CloudTrail Lake converts existing events in row-based JSON format to Apache ORC format.

CloudTrail Lake event data stores

- When you create an event data store, you choose the type of events to include in your event data store.
- Includes : CloudTrail events (management events, data events, network activity events (in preview)), CloudTrail Insights events, AWS Config configuration items, AWS Audit Manager evidence, or events from outside of AWS.
- Each event data store can only contain a specific event category (for example, AWS Config configuration items), because the event schema is unique to the event category.
- You can store events from an organization in AWS Organizations in an organization event data store, including events from multiple Regions and accounts.
- You can also run SQL queries across multiple event data

- You can copy trail events to a new or existing event data store to create a point-in-time snapshot of events logged

Scenario	How do I accomplish this in the console?
Analyze and query historical trail events in CloudTrail Lake without ingesting new events	Create a new event data store and choose the **Copy trail events** option as part of event data store creation. When creating the event data store, deselect **Ingest events** (In the procedure) to ensure the event data store contains only the historical events for your trail and no future events.
Replace your existing trail with a CloudTrail Lake event data store	Create an event data store with the same event selectors as your trail to ensure that the event data store has the same coverage as your trail. To avoid duplicating events between the source trail and destination event data store, choose a date range for the copied events that is earlier than the creation of the event data store. After your event data store is created, you can turn off logging for the trail to avoid additional charges.

CloudWatch	CloudTrail
CloudWatch is basically a monitoring service for AWS resources and applications.	CloudTrail is a web service that is mainly concerned with what is done on AWS and by whom.
By default, CloudWatch offers free basic services like monitoring our AWS resources.	CloudTrail is also enabled by default when we create our AWS Free Tier account.
Using CloudWatch we can track metrics and monitor logs.	CloudTrail provides greater visibility into user activity by tracking AWS console actions including who made the call, from which IP address, and when.
CloudWatch records the application logs.	CloudTrail provides information about what occurred in your AWS account.
CloudWatch delivers metric data in 1 minute period for detailed monitoring and 5-minute periods for basic monitoring.	CloudTrail delivers an event within 15 minutes of the API call.
CloudWatch stores data in its own dashboard in form of metrics and logs.	CloudTrail centralizes all the logs across the regions and stores them on an S3 bucket.

AWS Config

- AWS Config provides a detailed view of the configuration of AWS resources in your AWS account.
- This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

Ways to Use AWS Config

- When you run your applications on AWS, you usually use AWS resources, which you must create and manage collectively. As the demand for your application keeps growing, so does your need to keep track of your AWS resources. AWS Config is designed to help you oversee your application resources in the following scenarios:

Resource Administration : You can use AWS Config to notify you whenever resources are created, modified, or deleted without having to monitor these changes by polling the calls made to each resource.

Auditing and Compliance : You might be working with data that requires frequent audits to ensure compliance with internal policies and best practices. To demonstrate compliance, you need access to the historical configurations of your resources. This information is provided by AWS Config.

Managing and Troubleshooting Configuration Changes : When you use multiple AWS resources that depend on one another, a change in the configuration of one resource might have unintended consequences on related resources. With AWS Config, you can view how the resource you intend to modify is related to other resources and assess the impact of your change.

Security Analysis : To analyze potential security weaknesses, you need detailed historical information about your AWS resource configurations, such as the AWS Identity and Access Management (IAM) permissions that are granted to your users, or the Amazon EC2 security group rules that control access to your resources.

AWS Config Benefits

- AWS Config makes it easier to track your resource’s configuration without the need for upfront investments and avoiding the complexity of installing and updating agents for data collection or maintaining large databases.
- Once you enable AWS Config, you can view continuously updated details of all configuration attributes associated with AWS resources.
- You are notified through Amazon Simple Notification Service (SNS) of every configuration change.

How AWS Config help with audits

- AWS Config gives you access to resource configuration history.
- You can relate configuration changes with AWS CloudTrail events that possibly contributed to the change in configuration.
- This information provides you full visibility, right from details, such as, “Who made the change?” and “From what IP address?”, to the effect of this change on AWS resources and related resources.
- You can use this information to generate reports to aid auditing and assessing compliance over a period.

AWS Systems Manager

- AWS Systems Manager is a collection of capabilities that enable visibility and control of your AWS resources.
- AWS Systems Manager allows you to safely automate common and repetitive IT operations and management tasks across multiple accounts and AWS Regions.

- The following Systems Manager capabilities work with Organizations across all of the AWS accounts in your organization:

- Systems Manager Explorer : is a customizable operations dashboard that reports information about your AWS resources. You can synchronize operations data across all AWS accounts in your organization by using Organizations and Systems Manager Explorer.
- Systems Manager Change Manager : is an enterprise change management framework for requesting, approving, implementing, and reporting on operational changes to your application configuration and infrastructure.

- **Systems Manager OpsCenter** provides a central location where operation engineers and IT professionals can view, investigate, and resolve operational work items (OpsItems) related to AWS resources.

  - When you use OpsCenter with Organizations it supports working with OpsItems from a management account and one other account during a single session.

- Once configured, users can perform the following types of actions:

1. Create, view, and update OpsItems in another account.
2. View detailed information about AWS resources that are specified in OpsItems in another account.
3. Start Systems Manager Automation runbooks to remediate issues with AWS resources in another account.

Enabling/Disabling trusted access with Systems Manager

- You can enable trusted access by using either the AWS Organizations console, by running a AWS CLI command, or by calling an API operation in one of the AWS SDKs.
- Systems Manager requires trusted access with AWS Organizations to synchronize operations data across AWS accounts in your organization.
- If you disable trusted access, then Systems Manager fails to synchronize operations data and reports an error.
- You can disable trusted access using only the Organizations tools.

AWS Management Console | AWS CLI, AWS API

To enable trusted service access using the Organizations console

1. Sign in to the AWS Organizations console. You must sign in as an IAM user, assume an IAM role, or sign in as the root user (not recommended) in the organization's management account.
2. In the navigation pane, choose **Services**.
3. Choose **AWS Systems Manager** in the list of services.
4. Choose **Enable trusted access**.
5. In the **Enable trusted access for AWS Systems Manager** dialog box, type **enable** to confirm it, and then choose **Enable trusted access**.
6. If you are the administrator of only AWS Organizations, tell the administrator of AWS Systems Manager that they can now enable that service using its console to work with AWS Organizations.

Enabling a delegated administrator account for Systems Manager

- When you designate a member account as a delegated administrator for the organization, users and roles from that account can perform administrative actions for Systems Manager that otherwise can be performed only by users or roles in the organization's management account.
- This helps you to separate management of the organization from management of Systems Manager.
- If you use Change Manager across an organization, you use a delegated administrator account.
- This is the AWS account that has been designated as the account for managing change templates, change requests, change runbooks and approval workflows in Change Manager.
- The delegated account manages change activities across your organization. When you set up your organization for use with Change Manager, you specify which of your accounts serves in this role.
- It does not have to be the organization's management account. The delegated administrator account is not required if you use Change