Monitor

CloudTrail, CloudWatch, CloudWatch Logs, CloudWatch Logs Insights, CloudWatch Events, AWS X-Ray, AWS Config, Trusted Advisor, AWS Personal Health Dashboard (PHD), Automated AWS Account Audits

Đà Nẵng, năm COVID thứ 2

CloudTrail 1

- Is an AWS service that records actions in AWS that were taken by any user, role or service.
- Events types:
  - Management events = control plane events.
  - Data events = data plane events. Supported on few services only (S3, Lambda).
  - Insights = unusual activity in your AWS account.
- Events history:
  - You can view, search, and download the past 90 days of activity in your AWS account.
- CloudTrail trails:
  - A trail is a configuration that enables delivery of events to an Amazon S3 bucket, CloudWatch Logs and CloudWatch Events.

CloudTrail 2

- Events delivery time:
  - Logs are delivered within an average of about 15 minutes of an API call. No SLA.
  - Events are delivered to the CloudWatch Events bus in near-realtime.
- Delivering log files to S3:
  - Log files are compressed JSON files.
- A trail can be applied to all Regions or a single Region.
- To create an alarm on some API activity, you should create a trail that sends the events to CloudWatch Logs and create an alarm in CloudWatch Logs.

CloudWatch 1

- Monitors AWS resources and your applications in real time to collect and track metrics.
- CloudWatch concepts: Namespaces, Metrics, Dimensions, Statistics, Percentiles, Alarms.
- Namespace:
  - A container for CloudWatch metrics. Example: "AWS/EC2".
- Metric:
  - A time-ordered set of data points that are published to CloudWatch.
- Dimension:
  - A dimension is a name/value pair that is part of the identity of a metric.
    - For example, you can get statistics for a specific EC2 instance by specifying the InstanceId dimension when you search for metrics.

CloudWatch 2

- Statistics:
  - Statistics are metric data aggregations over specified periods of time.
  - Example of statistics functions: min, max, average, sum, percentile.
- Percentile:
  - A percentile indicates the relative standing of a value in a dataset.
  - For example, the 95th percentile means that 95 percent of the data is lower than this value and 5 percent of the data is higher than this value.
- Alarm:
  - Automatically initiate actions on your behalf.
- Action:
  - An action can be triggered either when: - the alarm goes to an "In-Alarm" state, or - the alarm goes to an "OK" state, or, - the alarm goes to an "Insufficient data" state.
- CloudWatch agent: enables you to collect internal system-level metrics from Amazon EC2 instances and on-prem servers across operating systems.

CloudWatch Logs 1

- Collects and monitors log files from sources like EC2, CloudTrail and Route53.
- Logs can be viewed, searched, filtered and archived.
- A log event is a record of some activity. Composed of a timestamp and a raw message.
- A log stream is a sequence of log events that share the same source.
- Log groups define groups of log streams that share the same retention, monitoring, and access control settings.
- Metrics from logs:
  - You can search and filter the log data coming into CloudWatch Logs and create one or more metric filters.

CloudWatch Logs Insights:

- Enables you to search and analyze your log data in CloudWatch Logs.
- Includes a purpose-built query language.
- Automatically discovers fields in logs from many AWS services and from 3rd party JSON logs.

CloudWatch Events 1

- Delivers a near real-time stream of system events that describe changes in AWS resources.
- CloudWatch Event is based on one special event stream included in EventBridge for AWS system events.
- Events can be triggered in CloudWatch Events when:
  - A change happens in your AWS environment. For example, EC2 generates an event when the state of an EC2 instance changes from pending to running.
  - You make API calls. These events are published by CloudTrail.
  - You can generate custom application-level events and publish them to CloudWatch Events.
  - You set up scheduled events that are generated on a periodic basis.

CloudWatch Events 2

- Rules:
  - A rule matches incoming events and routes them to targets for processing.
  - A single rule can route to multiple targets, all of which are processed in parallel.
  - A rule can customize the JSON sent to the target, by passing only certain parts or by overwriting it with a constant.
- Targets:
  - A target processes events.
  - Targets can include EC2 instances, Lambda functions, Kinesis streams, ECS tasks, Step Functions state machines, SNS topics, SQS queues, and built-in targets.
  - A target receives events in JSON format.
- Event Patterns
  - Rules use event patterns to select events and route them to targets.

AWS X-Ray

- A service that collects data about requests that your application serves.

AWS Config

- Enables you to assess, audit, and evaluate the configurations of your AWS resources.
- You can review the changes history of your configurations.
- AWS Config can monitor your configurations with the following workflow: Triggers ==> Rules ==> Notification ==> Remediation.

Trusted Advisor

- Inspects your AWS environment, and then makes recommendations on:
  - **Cost optimization**. Examples:
    - EC2 Reserved Instances optimization.
    - Low utilization Amazon EC2 instances.
  - **Fault Tolerance**. Examples:
    - EBS snapshots.
    - EC2 availability zone balance.
  - **Performance**. Examples:
    - High utilization of EC2 CPU or EBS IOPS.
  - **Security**. Examples:
    - Security groups - Unrestricted access (0.0.0.0/0).
  - **Service Limits**: Checks whether your account approaches or exceeds the limits (quotas) for AWS services and resources.

AWS Personal Health Dashboard (PHD)

- Provides alerts and remediation guidance when AWS is experiencing events that may impact you.