# CloudWatch, CloudTrail

What is CloudWatch

How Amazon CloudWatch works

Amazon CloudWatch terminology

CloudWatch Metrics

CloudWatch Custom Metrics

CloudWatch Logs

CloudWatch Logs for EC2

CloudWatch Events

CloudWatch Dashboards

CloudWatch Alarms

AWS CloudTrail

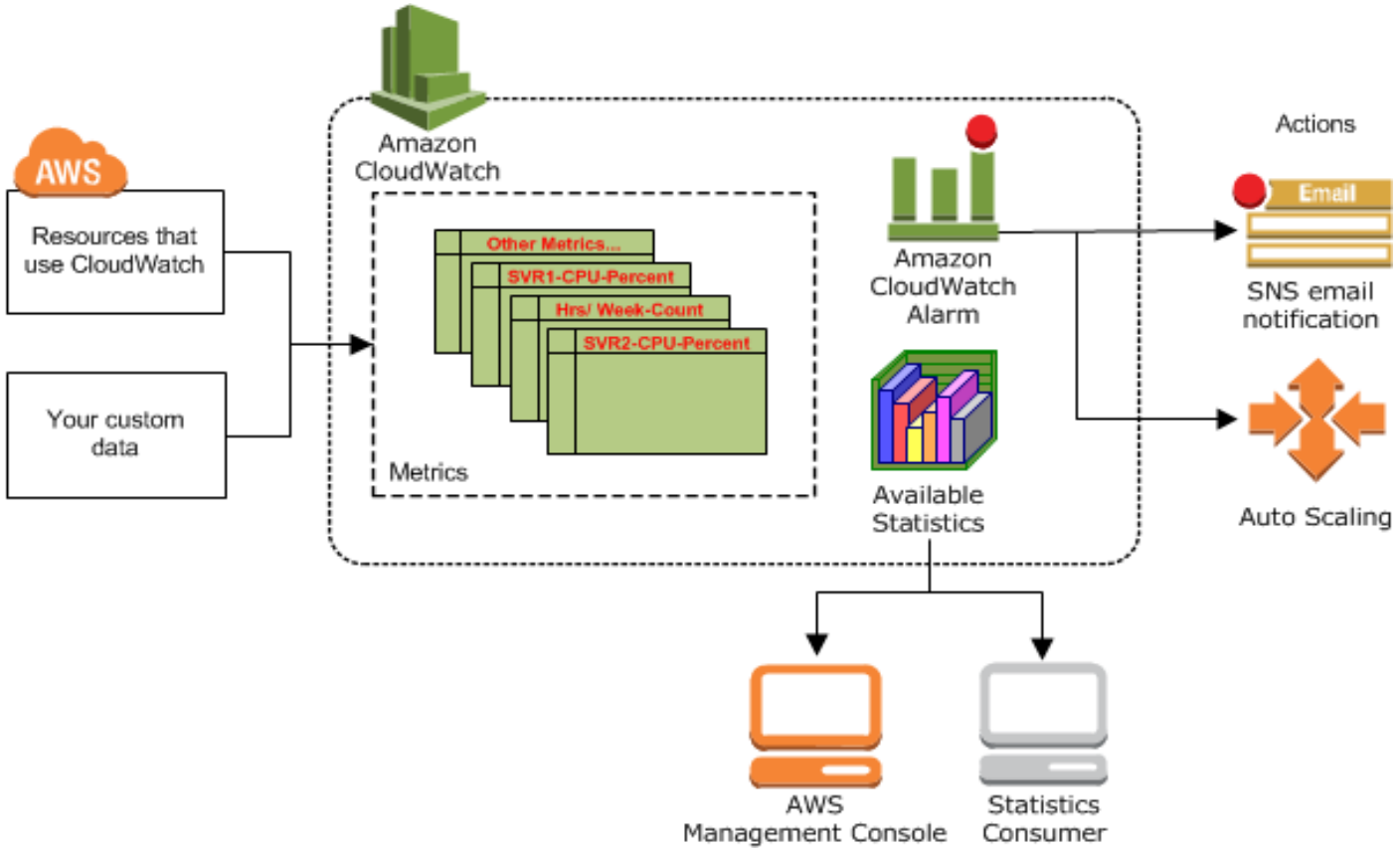
CloudTrail Events

# CloudWatch

- Amazon CloudWatch is a service that you can use to monitor your AWS resources and your applications in real time.
- With Amazon CloudWatch
  - Metrics: Collect and track key metrics
  - Logs: Collect, monitor, analyze and store log files
  - Events: Send notifications when certain events happen in your AWS
  - Alarms: React in real-time to metrics / events
- Amazon CloudWatch offers either basic or detailed monitoring for supported AWS products.
  - Basic monitoring sends data points to Amazon CloudWatch every five minutes for a limited number of preselected metrics at no charge.
  - Detailed monitoring sends data points to Amazon CloudWatch every minute and allows data aggregation for an additional charge. If you want to use detailed monitoring, you must enable it—basic is the default.

# How Amazon CloudWatch works

- Amazon CloudWatch is basically a metrics and logs repository.
- An AWS service such as Amazon EC2, Load balancer, puts metrics into the repository, and you retrieve statistics based on those metrics.
- If you put your own custom metrics into the repository, you can retrieve statistics on these metrics as well.



# Amazon CloudWatch terminology

- **Namespaces:** It is a container for CloudWatch metrics. Metrics in different namespaces are isolated from each other.
- **Metrics:** It represents a time-ordered set of data points that are published to CloudWatch
- **Dimensions:** A dimension is a name/value pair that is part of the identity of a metric. You can assign up to 10 dimensions to a metric
- **Statistics:** Statistics are metric data aggregations over specified periods of time. CloudWatch provides statistics based on the metric data points provided.
- **Alarms:** You can use an alarm to automatically initiate actions on your behalf. An alarm watches a single metric over a specified time period, and performs one or more specified actions, based on the value of the metric relative to a threshold over time.

# CloudWatch Metrics

- Metrics are data about the performance of your systems
- CloudWatch provides metrics for every services in AWS.
  - Ex: CPUUtilization, NetworkIn, DiskReadBytes, NetworkPacketsOut
- Metrics belong to namespaces
- Dimension is an attribute of a metric (instance id, environment, etc…).
- Up to 10 dimensions per metric
- Metrics have timestamps
- Can create CloudWatch dashboards of metrics

# CloudWatch Custom Metrics

- You can publish your own metrics to CloudWatch using the AWS CLI or an API.
- You can view statistical graphs of your published metrics with the AWS Management Console.
- CloudWatch stores data about a metric as a series of data points. Each data point has an associated time stamp
- Use API call PutMetricData
- AWS CLI
  - aws cloudwatch **put-metric-data** --metric-name Buffers --namespace MyNameSpace --unit Bytes --value 231434333 --dimensions InstanceId=1-23456789,InstanceType=m1.small

# CloudWatch Logs

- Amazon CloudWatch Logs used to monitor, store, and access log files from EC2 instances, AWS CloudTrail, Route 53, and other sources
- CloudWatch can collect log from:
  - Elastic Beanstalk: collection of logs from application
  - ECS: collection from containers
  - AWS Lambda: collection from function logs
  - VPC Flow Logs: VPC specific logs
  - API Gateway
  - CloudTrail based on filter
  - CloudWatch log agents: for example on EC2 machines
  - Route53: Log DNS queries

# CloudWatch Logs for EC2

- By default, no logs from your EC2 machine will go to CloudWatch
- You need to run a CloudWatch agent on EC2 to push the log files you want
- Make sure IAM permissions are correct
- The CloudWatch log agent can be setup on-premises too

# Amazon CloudWatch Alarms

# AWS CloudWatch Events

- Schedule: Cron jobs
- Event Pattern: Event rules to react to a service doing something
- Triggers to Lambda functions, SQS/SNS/Kinesis Messages
- CloudWatch Event creates a small JSON document to give information about the change
- ECS Batch job

# CloudWatch Dashboards

- Amazon CloudWatch dashboards are customizable home pages in the CloudWatch console that you can use to monitor your resources in a single view.
- CloudWatch dashboards is to create customized views of the metrics and alarms for your AWS resources
- You can create dashboards by using the console, the AWS CLI, or the PutDashboard API.
- Demo

# AWS CloudTrail

- Provides governance, compliance, and operational and risk auditing of your AWS account.
- Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.
- Get an Events history that include actions taken in the
  - AWS Management Console
  - AWS Command Line Interface
  - AWS SDKs and APIs.
- When activity occurs in your AWS account, that activity is recorded in a CloudTrail event

# AWS CloudTrail

- AWS CloudTrail records user activity by recording API calls made on your account.
- It records important information about each API call, including the name of the API, the identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS service.
- This information helps you to track changes made to your AWS resources and to troubleshoot operational issues.
- You can create a trail with the AWS CloudTrail console, the AWS Command Line Interface (CLI), or the AWS CloudTrail API.
- A trail is a configuration that enables logging of the AWS API activity and related events in your account

# CloudTrail Events

- An event in CloudTrail is the record of an activity in an AWS account
- CloudTrail **events** provide a history of both API and non-API account activity made through
  - AWS Management Console
  - AWS SDKs
  - command line tools
  - other AWS services.
- There are three types of events
  - Management Events
  - Data Events
  - CloudTrail Insights events

# CloudTrail Events

- Management Events
  - Management events provide information about management operations that are performed on resources in your AWS account. Ex:
    - Configuring security - IAM AttachRolePolicy
    - Setting up logging - CloudTrail CreateTrail
  - Can also include non-API events - Ex: Console login
- Data Events
  - Data events provide information about the resource operations performed on or in a resource. Ex
    - Amazon S3 - GetObject, DeleteObject, and PutObject API operations
    - AWS Lambda function execution - Invoke API
    - Amazon EBS APIs - PutSnapshotBlock, GetSnapshotBlock, and ListChangedBlocks
  - Not logged by default
  - To record CloudTrail data events, you must explicitly add to a trail the supported resources
- CloudTrail Insights events
  - CloudTrail Insights events capture unusual activity in your AWS account