AWS Management Tools

Agenda

AWS CloudWatch

- Introduction of CloudWatch
- CloudWatch Features and Benefits
- CloudWatch Workflow
- List of Monitoring AWS resources
- CloudWatch Concepts
- CloudWatch Custom Metrics

AWS CloudTrail

- Introduction to AWS CloudTrail
- CloudTrail Use cases
- CloudTrail Worflow
- Managing CloudTrail

Introduction of CloudWatch

- CloudWatch is a monitoring service for AWS resources & applications running on AWS
- CloudWatch can collect and track metrics from AWS resources
- CloudWatch will send notification based on CloudWatch Alarm
- CloudWatch will integrated with AWS SNS to alert based on thresholds

- With CloudWatch we can gain application performance, operational health
- We can access CloudWatch using Amazon CloudWatch console, AWS CLI, CloudWatch API, AWS SDKs

CloudWatch Features and Benefits

Monitor AWC EC2

Monitor Other AWS Resources

Monitor Custom Metrics

View Graphs and Statistics

Monitor and Store Logs

Set Alarms

Monitor and React to Resource Changes

CloudWatch – List of Monitoring AWS resources

Compute & Networking

- EC2
- Auto Scaling
- ELB
- Route 53

Storage & Content Delivery

- EBS PIOPS (SSD) volumes
- EBS General Purpose (SSD) volumes
- EBS Magnetic volumes
- AWS Storage Gateways
- AWS CloudFront

Databases & Analytics

- DynamoDB
- ElastiCache
- RDS
- Elastic MapReduce
- Redshift

Other services

- SNS topics
- SQS queues
- Opsworks
- CloudWatch Logs
- AWS Billing

CloudWatch Monitor

Monitored AWS resources	Frequency	Charge
EC2 instance(basic)	Every 5 mins	Free
EC2 instance(detail)	Every 1 min	Additional
EBS volumes	Every 5 mins	Free
Elastic Load Balancers	Every 5 mins	Free
RDS DB instance	Every 1 min	Free
SQS queues	Every 5 mins	Free
SNS topics	Every 5 mins	Free

Introduction to AWS CloudTrail

- CloudTrail service used to enable logging in AWS account
- It helps for operational auditing, risk auditing and compliance
- We can use AWS CloudTrail to get a history of AWS API calls & related events for our AWS account

- It can capture all API call logs which made through AWS management console, AWS SDKs, APIs, and command line tools
- We can identify which users and accounts called AWS for services that support CloudTrail, the source IP address the calls were made from, when the calls occurred

CloudTrail - Use Cases

- Using CloudTrail IT and security administrators can perform security analysis
- Also, IT administrators and DevOps engineers can track the changes to AWS resources
- DevOps engineers can troubleshoot operational issues
- IT auditors can use the log files generated by CloudTrail as a compliance aid

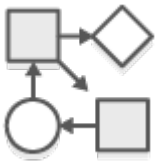
CloudTrail - Benefits

Simplified Compliance

Visibility Into User and Resource Activity

Security Analysis and Troubleshooting

Security Automation



CloudTrail - Workflow

- **Trail –** Configuration to enables logging of AWS API calls
- We can 2 types of Trails
    - *A trail that applies to all regions* – It create trails that applies to all region
    - *A trail that applies to one region* – It will create trail on one region which you mentioned

- **Creating a trail -** CloudTrail store the log files to AWS S3 bucket.
- Trail which created in AWS management Console, default it will applies to all regions

- **Create & Subscribe to an Amazon SNS** - Subscribe to a SNS topic for receiving the notifications about log file delivery to your bucket

CloudTrail - Workflow

- **Viewing log files –** AWS S3 retrieve logs file from CloudTrail and stores into buckets, When new trail created, we can see log files in S3 buckets within 15 minutes

- **Manage User Permissions -** Using AWS IAM manage permissions to create, configure, or delete trails; start and stop logging; and access buckets that have log files

- **Monitoring events with CloudWatch Logs** - Here, we can configure the trail to send the events to a CloudWatch Logs log group

Managing CloudTrail

- We can create and manage CloudTrail using
  - CloudTrail Console
  - CloudTrail CLI
  - CloudTrail APIs
  - AWS SDKs

- **Access to CloudTrail -** Using IAM to create individual users for anyone who needs access to AWS CloudTrail.

CloudTrail Supported Regions

Region Name	Region	Endpoint	Protocol	AWS Account ID	Support Date
US East (Ohio)	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS		
US East (N. Virginia)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS		
US West (N. California)	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS		
US West (Oregon)	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS		
Canada (Central)	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS		
Asia Pacific (Mumbai)	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS		
Asia Pacific (Seoul)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS		
Asia Pacific (Singapore)	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS		
Asia Pacific (Sydney)	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS		
Asia Pacific (Tokyo)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS		
EU (Frankfurt)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS		
EU (Ireland)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS		
EU (London)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS		
South America (São Paulo)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS		

CloudTrail Log File

- CloudTrail monitors events for your account and then delivers those events as log files to your Amazon S3 bucket

- **CloudTrail Log File Name Format -** CloudTrail uses the following file name format for the log file objects that it delivers to your Amazon S3 bucket:

AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.File NameFormat

- **Example CloudTrail Log File Name**

111122223333_CloudTrail_us-east-2_ _Mu0KsOhtH1ar15ZZ.json.gz

Log File Examples

- A log file contains one or more records. The following examples are snippets of logs that show the records for an action that started the creation of a log file.

Amazon EC2 Log Examples


```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "accountId": "123456789012",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:22:54Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]}},
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 0,
            "name": "pending"
        },
        "previousState": {
            "code": 80,
            "name": "stopped"
        }
    }]}}
}]}
```

CloudWatch and CloudTrail Hands-on

CloudWatch

- Create Alarm
- Create Events Rule
- Create Dashboard

CloudTrail

- Create trail

Thank you