AWS Management

# IAM – Identity and Access Management

IAM is global – not regional

Every User that is created in IAM starts with – NO Permissions

Default Access Level for new user in IAM – NO Access to any services

Additional ways to secure accounts of AWS Root user and other Users – Use MFA

Components of IAM – Users, Groups, Roles

Policy Documents are written in – JSON

Root User Access -

Administrator User Access -

Power User Access – Access to all AWS Services except management of users & groups in IAM

Deny Policy will Override Allow Policy

## IAM Interaction with Corporate Network

SAML -

# CloudWatch

CloudWatch Logs

CloudWatch Metrics

CloudWatch Alarms

CloudWatch Dashboard

CloudWatch Events

# CloudTrail

Introduction to AWS CloudTrail and use-cases

Deep dives on use-cases

CloudTrail for multiple AWS accounts

Encryption using KMS and Log File Integrity validation

AWS Partner Solutions integrated with CloudTrail

## What is it?

Web-service that records activity made on account and delivers log files to Amazon S3 bucket

Records API calls made by Users via Console, SDK and CLI on AWS Services (Ex: S3, EC2, VPC, IAM etc.), writes to S3 Bucket. The logs can be used to Troubleshoot issues. We can also setup CloudWatch

### Advantages

* Trail of all account related activity useful for Audit
* Who, Which services, actions performed, parameters, AWS response etc.
* Helps in Compliance with Internal policies and Regulatory standards

### Who uses CloudTrail for what?

IT and Security Administrators – Security Analysis

IT Admins and DevOps Engineers – Track changes to AWS Resources

DevOps Engineers – Troubleshoot Operational Issues

IT Auditors – Compliance Aid

### What does a CloudTrail Event contain?

**Who** made the API call?

**When** was the API call made?

**What** was the API call?

**Which resources** were acted upon in the API call?

**Where** was the API call made from and made to?

How to turn on Cloud Trail?

Create a Trail

Specify S3 bucket where the logs have to be stored

Start logging

### CloudTrail log files as compliance Aid

CloudTrail logs -> S3 bucket -> Lifecyle policies -> Glacier

### CloudTrail Event Monitoring

Monitor specific events recorded by CloudTrail and receive notifications from CloudWatch

### Which Events?

Specifically, Security and Network related events that have a high blast-radius

Examples:

1. Creation/Deletion/Modification of Security Groups and VPCs
2. Changes to IAM Policies or S3 Bucket Policies
3. Failed AWS Management console sign-in events
4. API calls that resulted in Authorization Failures
5. Launching, Terminating, Stopping, Starting and Rebooting EC2 Instances

### Receive Email Notifications of Specific API Activity

(CloudTrail + CloudWatch) -> SNS -> Email/SQS Message-> (CreateTicket/Follow Up with User etc.)

How many days of activity? How to increase?

Shows last 90 days of activity

Can I select what to log and what not? Can I filter results?

## Security

CloudTrail logs are by default encrypted.

Organizations

OpsWorks

CloudFormation