

AWS Security Best Practices





Mohammad Mizanur Rahman

CTO, Brain Station 23

AWS Partner Network (APN) Ambassador



Advanced
Consulting
Partner

BRAIN STATION 23

Market Served:

UK, USA, Netherlands, Germany,
Norway, Denmark, Switzerland,
Spain, Australia, Canada, Japan,
Turkey, Middle East, Bangladesh.

Certified Professionals: **150+**

Project Delivered: **200+**

No of employees: **700+**

AWS Service Offers:

- DevOps
- Consultancy
- Managed Service
- Migration
- Well-Architected Framework Review



Website: <https://cloud-23.com>



Cloud As A Service

We Provide All In One Cloud Solution

We've completed **30+** Well Architecte Review for AWS in last 8 months.

We've successfully done **20** Migration project on AWS.

We've **50+** DevOps resources engaged in various projects.

We're engaged in **20+** Managed Service projects for our clients.

We've multiple **Hybrid Cloud** projects running in **Telco & Banks.**

We've completed **10+** EC2 for windows/Linux delivery projects.

We've given consultancy support for **200+** customers as of yet.

We are trusted billing partner for **50+** clients as of now.



We've built largest live gaming knowledge-based quiz app for the leading telco provider in Bangladesh. Which could serve more than 3 million advertisement views every day. ([Link](#))

We've built & migrated the complex environment for a clinical-stage biotechnology company in Norway. Who are also one of the largest pharmaceutical companies in the world. ([Link](#))

SECURITY IS **SHARED**



Build everything on a **constantly improving** security baseline



GxP
ISO 13485
AS9100
ISO/TS 16949



AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global
Infrastructure

Availability Zones

Regions

Edge Locations

AWS is
responsible for
the security **OF**
the Cloud



Security & compliance is a **shared responsibility**



Customers

Customer applications & content

Platform, Applications, Identity & Access Management

Operating System, Network, & Firewall Configuration

Client-side Data
Encryption

Server-side Data
Encryption

Network Traffic
Protection

Customers have
their choice of
security
configurations **IN**
the Cloud

AWS Foundation Services

Compute

Storage

Database

Networking

AWS is
responsible for
the security **OF**
the Cloud

AWS Global
Infrastructure

Availability Zones

Regions

Edge Locations



Security

- Key Areas
 - Visibility
 - Auditability
 - Controllability
 - Agility



Security is **Visible**

- Who is accessing the resources?
- Who took what action?
 - When?
 - From where?
 - What did they do?
 - Logs Logs Logs



AWS CLOUDTRAIL



You are making
API calls...



On a growing set of
services around the
world...



AWS CloudTrail
is continuously
recording API
calls...

User	Action	Time
Tim	Created	1:30pm
Sue	Deleted	2:40pm
Kat	Created	3:30pm

And delivering
log files to you

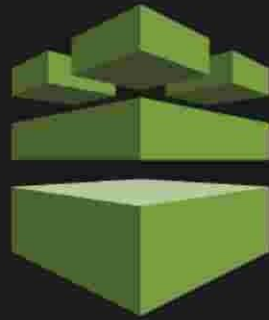
Use cases enabled by CloudTrail

- Security Analysis
 - ❖ Use log files as an input into log management and analysis solutions to perform security analysis and to detect user behavior patterns
- Track Changes to AWS Resources
 - ❖ Track creation, modification, and deletion of AWS resources such as Amazon EC2 instances, Amazon VPC security groups and Amazon EBS volumes
- Troubleshoot Operational Issues
 - ❖ Identify the most recent actions made to resources in your AWS account
- Compliance Aid
 - ❖ Easier to demonstrate compliance with internal policies and regulatory standards

SECURITY IS **AUDITABLE**

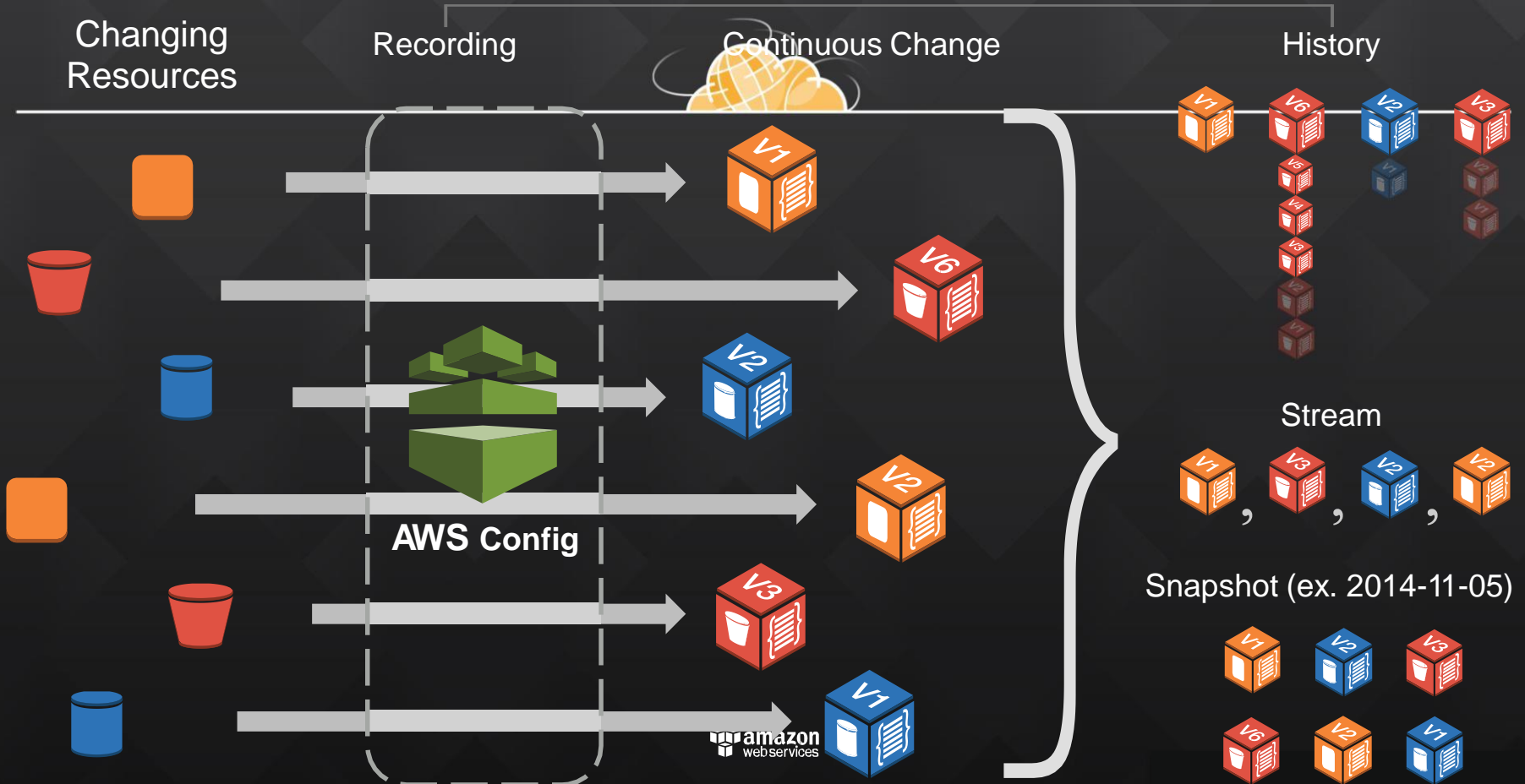


AWS Config



*AWS Config is a fully managed service that provides you with an inventory of your AWS resources, lets you audit the resource configuration history **and notifies you** of resource configuration changes.*

AWS Config



Use cases enabled by Config

- Security Analysis: Am I safe?
- Audit Compliance: Where is the evidence?
- Change Management: What will this change affect?
- Troubleshooting: What has changed?



Am I safe?

- Properly configured resources are critical to security
- Config enables you to continuously monitor the configurations of your resources and evaluate these configurations for potential security weaknesses



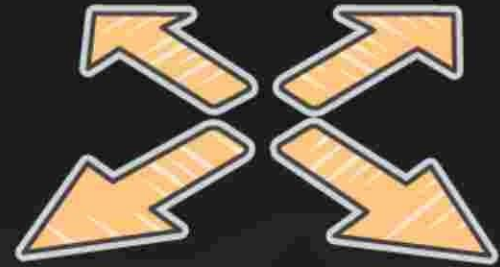
Where is the evidence?

- Many compliance audits require access to the state of your systems at arbitrary times (i.e. PCI, HIPAA)
- A complete inventory of all resources and their configuration attributes is available for any point in time



What will this change affect?

- When your resources are created, updated, or deleted, these configuration changes are streamed to Amazon SNS
- Relationships between resources are understood, so that you can proactively assess change impact



SECURITY PROVIDES CONTROL



First class security and compliance starts (but doesn't end!) with **encryption**



Automatic encryption with managed keys

Bring your own keys

Dedicated hardware security modules

Encryption & Best Practices with AWS

Managed key encryption

Key storage with AWS CloudHSM

Customer-supplied key encryption

DIY on Amazon EC2

Create, store, & retrieve keys securely

Rotate keys regularly

Securely audit access to keys



AWS Key Management Service



- A managed service that makes it easy for you to create, control, and use your encryption keys
- Integrated with AWS SDKs and AWS services including Amazon EBS, Amazon S3, and Amazon Redshift
- Integrated with AWS CloudTrail to provide auditable logs to help your regulatory and compliance activities

AWS Key Management Service

Integrated with AWS IAM Console



Services ▾

Edit ▾

Dashboard

Details

S
Groups

Users

Roles

Identity Providers

Password Policy

Credential Report

Encryption Keys

Create Key

Key Actions ▾

Filter: US East (N. Virginia) ▾

Search

	Alias	Key ID	Status
	HighlyConfidentialData	arn:aws:kms:us-east-1:123456789012:key:12345678-9abc-def0-110bc8011638	Enabled
	CriticalData	arn:aws:kms:us-east-1:123456789012:key:12345678-9abc-def0-110bc8011638	Enabled
	ApplicationXYZ	arn:aws:kms:us-east-1:123456789012:key:12345678-9abc-def0-110bc8011638	Enabled
	aws/redshift:	arn:aws:kms:us-east-1:123456789012:key:12345678-9abc-def0-110bc8011638	Enabled
	aws/elb	arn:aws:kms:us-east-1:123456789012:key:12345678-9abc-def0-110bc8011638	Enabled
	aws/s3	arn:aws:kms:us-east-1:123456789012:key:12345678-9abc-def0-110bc8011638	Enabled

AWS Key Management Service

Integrated with Amazon EBS

Create Volume

X

Type

General Purpose (SSD)

Size (GiB)

100

(Min(MiB) 1 GiB; Max 1024 GiB)

IOPS

300 / 3000

(3000 IOPS bursts and baseline of 3 IOPS per GB)

Availability Zone

us-east-1b

Snapshot ID

Snapshot (ebs-elastic)

Encryption

☒ Encrypt this volume

Master Key

11111111

Key Details

Description

This key protects critical data in my account

Account

This account (██████████)

KMS Key ID

██████████-a0ec-33d40cacf295

Cancel

Create

SECURITY IS **AGILE**



Everyone's **an owner**

When the problem is “mine” rather than
“hers” there's a much higher likelihood I'll do
the right thing



Preferred Culture:

Measure constantly, report regularly, and hold senior executives **accountable** for security – have them drive the right culture



Culture:

Apply more effort to the “why” rather than the “how”

Why is what really matters

When something goes wrong, ask the “five whys”



Culture:

Test, **CONSTANTLY**

- Inside/outside
- Privileged/unprivileged
- Black-box/white-box
- Vendor/self



Culture:

Make your compliance team **a part of** your security operations



Culture:

Base decisions on **facts, metrics, & detailed understanding** of your environment and adversaries






Simple Security Controls

Easy to Get Right

Easy to Audit

Easy to Enforce



AWS security best practices by service			
	High Risk 	Medium Risk 	Low Risk 
AWS IAM	<p>(1) IAM policies should not allow full “*” administrative privileges</p> <p>(4) IAM root user access key should not exist</p> <p>(6) Hardware MFA should be enabled for the root user</p>	<p>(3) IAM users’ access keys should be rotated every 90 days or less</p> <p>(5) MFA should be enabled for all IAM users that have a console password</p> <p>(7) Password policies for IAM users should have strong configurations</p> <p>(8) Unused IAM user credentials should be removed</p>	<p>(2) IAM users should not have IAM policies attached</p>
Amazon S3	<p>(10) S3 buckets should have server-side encryption enabled</p>	<p>(9) S3 Block Public Access setting should be enabled</p> <p>(11) S3 Block Public Access setting should be enabled at the bucket level</p>	

<u>AWS CloudTrail</u>	<u>(12)</u> CloudTrail should be enabled and configured with at least one multi-Region trail	<u>(13)</u> CloudTrail should have encryption at rest enabled <u>(14)</u> Ensure CloudTrail log file validation is enabled	
<u>AWS Config</u>	<u>(15)</u> AWS Config should be enabled		
<u>Amazon EC2</u>	<u>(16)</u> Attached EBS volumes should be encrypted at rest <u>(19)</u> EBS default encryption should be enabled		<u>(17)</u> VPC flow logging should be enabled in all VPCs <u>(18)</u> The VPC default <u>security group</u> should not allow inbound and outbound traffic
<u>AWS DMS</u>	<u>(20)</u> AWS Database Migration Service replication instances should not be public		
<u>Amazon EBS</u>	<u>(21)</u> Amazon EBS snapshots should not be public, determined by the ability to be restorable by anyone		
<u>Amazon OpenSearch Service</u>	<u>(22)</u> Elasticsearch domains should have encryption at rest enabled		

Amazon SageMaker		(23) SageMaker notebook instances should not have direct internet access	
AWS Lambda		(24) Lambda functions should use supported runtimes	
AWS KMS		(25) AWS KMS keys should not be unintentionally deleted	
Amazon GuardDuty		(26) GuardDuty should be enabled	

Recommendation: AWS Well Architected Review



OPERATIONAL
EXCELLENCE



SECURITY



RELIABILITY



PERFORMANCE
EFFICIENCY



COST
OPTIMIZATION



SUSTAINABILITY

Thank you!

Q & A ?



BRAIN STATION-23