



# Security Essentials & Best Practices

Lijan Kuniyil

November 6, 2020



# Overview

Overview of the AWS cloud security concepts such as the AWS Security Center, Shared Responsibility Model, and Identity and Access Management.

What are your perceptions  
on cloud security?



# AWS Security

**At AWS, cloud security is job zero.**

All AWS customers benefit from a data center and network architecture built to satisfy the requirements of the most security-sensitive organizations.

# Gain access to a world-class security team

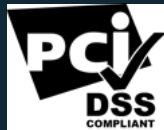
Where would some of the world's top security people like to work? At scale on huge challenges with huge rewards

So AWS has **world-class security and compliance** teams watching your back!

**Every customer benefits** from the tough scrutiny of other AWS customers



# Broad Accreditations & Certifications



Glacier Vault Lock  
& SEC Rule 17a-4(f)

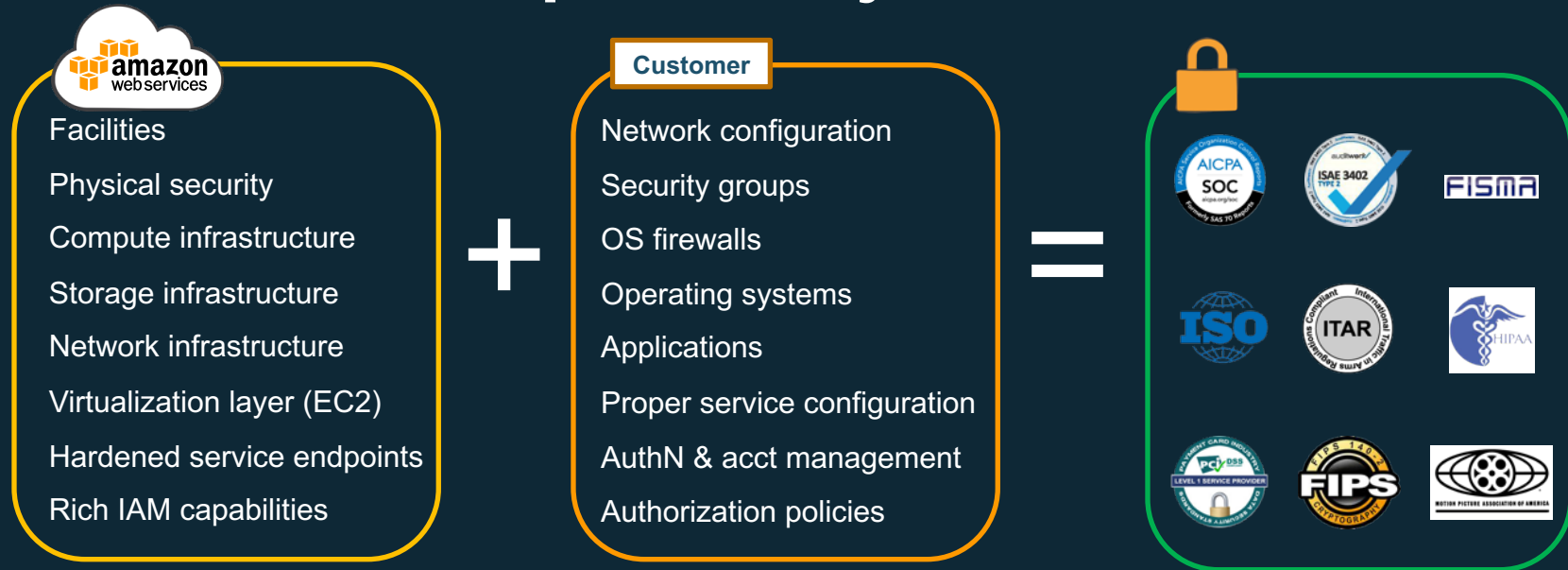
See <https://aws.amazon.com/compliance/programs/> for full list



# Shared Responsibility Model



# AWS Shared Responsibility Model



- Scope of responsibility depends on the type of service offered by AWS:  
**Infrastructure, Container, Abstracted Services**
- Understanding who is responsible for what is critical to ensuring your AWS data and systems are secure!

# Shared Responsibility Model

Customer

Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data  
Encryption

Server-side Data  
Encryption

Network Traffic  
Protection

Customers are responsible for their security and compliance **IN** the Cloud

AWS

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global  
Infrastructure

Availability Zones

Regions

Edge Locations

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

# Meet your own security objectives

## Customer

Your own  
accreditation



Your own  
certifications



Your own  
external audits



**Customer scope and  
effort is reduced**

**Better results through  
focused efforts**

## AWS

**AWS Foundation Services**

**Compute**

**Storage**

**Database**

**Networking**

**AWS Global  
Infrastructure**

**Availability Zones**

**Regions**

**Edge Locations**

**Built on AWS  
consistent baseline  
controls**

# AWS Responsibilities

## Physical Security of Data Center

- **Amazon has been building large-scale data centers for many years.**
- **Important attributes:**
  - Non-descript facilities
  - Robust perimeter controls
  - Strictly controlled physical access
  - Two or more levels of two-factor authentication
- **Controlled, need-based access.**
- **All access is logged and reviewed.**
- **Separation of Duties**
  - Employees with physical access don't have logical privileges.



# AWS Responsibilities

## EC2 Security

- **Host (hypervisor) operating system**
  - Individual SSH keyed logins via bastion host for AWS admins
  - All accesses logged and audited
- **Guest (EC2 Instance) operating system**
  - Customer controlled (customer owns root/admin)
  - AWS admins cannot log in
  - Customer-generated keypairs
- **Stateful firewall**
  - Mandatory inbound firewall, default deny mode
  - Customer controls configuration via Security Groups



## Network Security

- IP Spoofing prohibited at host OS level.
- Packet sniffing (promiscuous mode) is ineffective (protected at hypervisor level).
- Unauthorized Port Scanning a violation of TOS and is detected/blocked.
- Inbound ports blocked by default.

# AWS Responsibilities

## Configuration Management

- Most updates are done in such a manner that they will not impact the customer.
- Changes are authorized, logged, tested, approved, and documented.
- AWS will communicate with customers, either via email, the AWS Service Health Dashboard (<http://status.aws.amazon.com/>), or the AWS Personal Health Dashboard (<https://phd.aws.amazon.com/>) when there is a potential for service being affected.

## Built for “Continuous Availability”

- **Scalable, fault tolerant services.**
- **All availability zones (AZs) are always on.**
  - There is no “Disaster Recovery Datacenter”
  - All managed to the same standards
- **Robust Internet connectivity**
  - Each AZ has redundant, Tier 1 ISP Service Providers
  - Resilient network infrastructure

# AWS Responsibilities

## Disk Management

- Proprietary disk management prevents customers from accessing each other's data.
- Disks wiped prior to use.
- Disks can also be encrypted by the customer for additional security.

## Storage Device Decommissioning

- All storage devices go through process using techniques from:
  - DoD 5220.22-M ("National Industrial Security Program Operating Manual").
  - NIST 800-88 ("Guidelines for Media Sanitization").
- Ultimately devices are:
  - Degaussed.
  - Physically destroyed.

# Under the AWS Shared Responsibility Model

## AWS Responsibility? or Customer Responsibility?

Configuring the Security Group rules that determine which ports are open on the EC2 Linux instance

Preventing packet sniffing at the hypervisor level

Patching the operating system with the latest security patches

Shredding disk drives before they leave a datacenter

Securing the internal network inside the AWS datacenters

Installing camera systems to monitor the physical datacenters

Toggling on the Server-side encryption feature for S3 buckets



# Under the AWS Shared Responsibility Model

## AWS Responsibility? or Customer Responsibility?

Configuring the Security Group rules that determine which ports are open on the EC2 Linux instance

Preventing packet sniffing at the hypervisor level

Patching the operating system with the latest security patches

Shredding disk drives before they leave a datacenter

Securing the internal network inside the AWS datacenters

Installing camera systems to monitor the physical datacenters

Toggling on the Server-side encryption feature for S3 buckets



# Identity and Access Management

# What is Identity Management?

“...the management of individual **principals**, their **authentication**, **authorization**, and **privileges** ...with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks.”  
(Wikipedia)

# AAA with AWS

## Authenticate

IAM Username/Password  
Access Key  
(+ MFA)  
Federation

## Authorize

IAM Policies

## Audit

CloudTrail

# Considerations for Layers of Principals

## Applications

- Identities: Application Users, Application Administrators



## Operating Systems

- Identities: Developers, and/or Systems Engineers



## Amazon Web Services

- Identities: Developers, Solutions Architects, Testers, Software/Platform
- Interaction of AWS Identities:
  - Provisioning/deprovisioning EC2 instances and EBS storage.
  - Configuring Elastic Load Balancers.
  - Accessing S3 Objects or data in DynamoDB.
  - Accessing data in DynamoDB.
  - Interacting with SQS queues.
  - Sending SNS notifications.



# AWS Principals

## Account Owner ID (Root Account)

- Access to all subscribed services.
- Access to billing.
- Access to console and APIs.
- Access to Customer Support.



## IAM Users, Groups and Roles

- Access to specific services.
- Access to console and/or APIs.
- Access to Customer Support (Business and Enterprise).



## Temporary Security Credentials

- Access to specific services.
- Access to console and/or APIs.

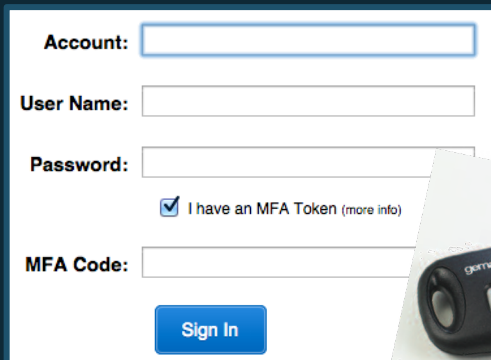


# AWS Identity Authentication

*Authentication: How do we know you are who you say you are?*

## AWS Management Console

Login with **Username/Password** with optional **MFA** (recommended)



The screenshot shows the AWS Management Console login interface. It includes fields for 'Account:', 'User Name:', 'Password:', and 'MFA Code:'. There is a checkbox labeled 'I have an MFA Token (more info)' which is checked. A blue 'Sign In' button is at the bottom. An image of a Gemalto security token is overlaid on the bottom right of the form.

For time-limited access: a **Signed URL** can provide temporary access to the Console

## API access

Access API using **Access Key** + **Secret Key**, with optional MFA

### ACCESS KEY ID

Ex: AKIAIOSFODNN7EXAMPLE

### SECRET KEY

Ex: Ut9FEMI/K7MDENG/bPxrFiCYE



For time-limited access: Call the AWS Security Token Service (STS) to get a temporary AccessKey + SecretKey + session token

# AWS Authorization and Privileges

*Authorization: What are you allowed to do?*

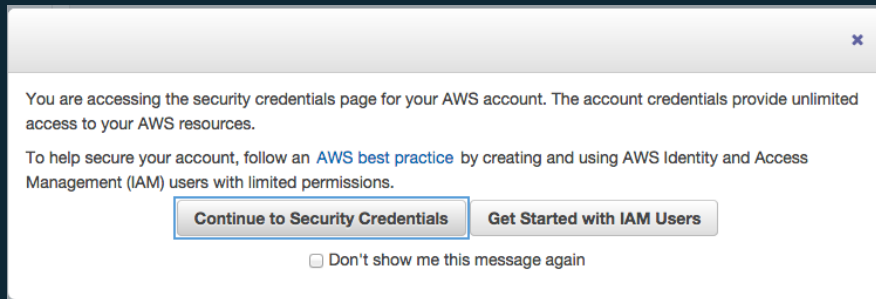
## Account Owner (Root)

- Privileged for all actions.

**Note:** Always associate the account owner ID with an MFA device and store it in a secured place!

## IAM Policies

- Privileges defined at User and Resource Level



▼ Permissions

This view shows all policies that apply to this User. This includes policies that are assigned to groups that this User belongs to.

**User Policies**

There are no policies attached to this user.

[Attach User Policy](#)

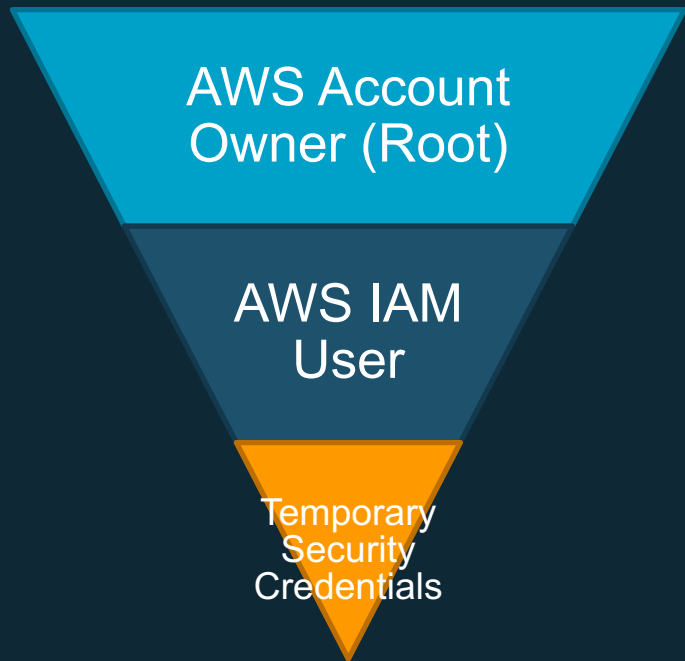
**Group Policies**

Policy Name	Group Name
AdministratorAccess-Administrators-201408161823 <a href="#">Show</a>	Administrators
AdministratorAccess-Demo-201410281057 <a href="#">Show</a>	Demo



# AWS IAM Hierarchy of Privileges

*Enforce principle of least privilege with Identity and Access Management (IAM) users, groups, and policies and temporary credentials.*



Permissions	Example
Unrestricted access to all enabled services and resources.	Action: * Effect: Allow Resource: * (implicit)
Access restricted by Group and User policies	Action: ['s3:*', 'sts:Get*'] Effect: Allow Resource: *
Access restricted by generating identity and further by policies used to generate token	Action: ['s3:Get*'] Effect: Allow Resource: 'arn:aws:s3:::mybucket/*'

# AWS Identity and Access Management (IAM)

*Securely control access to AWS services and resources for your users.*

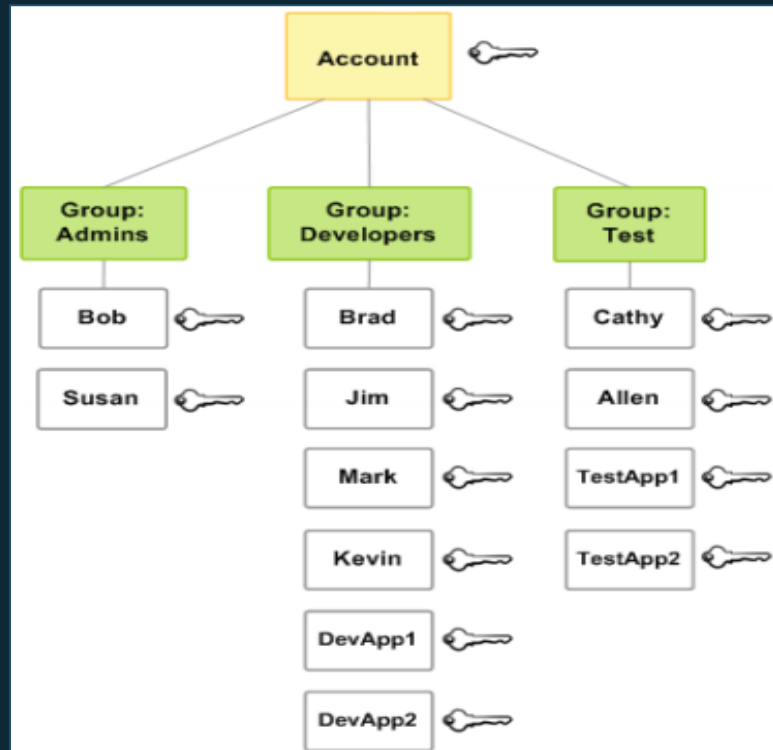
Username/  
User

Manage groups  
of users

Centralized  
Access Control

## Optional Configurations:

- Password for console access.
- Policies for controlling access AWS APIs.
- Two methods to sign API calls:
  - X.509 certificate
  - Access/Secret Keys
- Multi-factor Authentication (MFA)

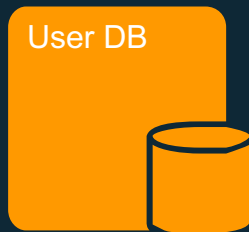


# Identity and Access Management

*Common approaches for Applications and Operating Systems*

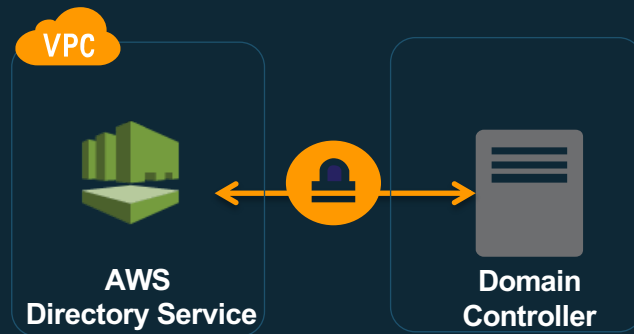
## Local User Databases

- Local Password (passwd) files
- Local Windows admin accounts
- User Databases



## LDAP Directories

- On-premise accessed over VPN.
- Replicated to AWS (read-only or read/write)
- Federated (one-way trusts, ADFS).
- Managed Samba-based directories via AWS Directory Services.





# AWS Directory Service

*Managed service for Active Directory*

Use your existing Corporate Credentials for

- AWS-based applications
- AWS Management Console



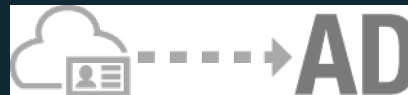
## Microsoft AD

Based on Microsoft Active Directory in Windows Server 2012 R2. Supports adding trust relationships with on-premises domains. Extend your schema using MS AD



## Simple AD

A Microsoft Active-Directory compatible directory powered by Samba 4.



## AD Connector

Connect to your on-premises Active Directory. Integrates with existing RADIUS MFA solutions.



# Encryption

How are you currently encrypting your data?

# Encryption

*Protecting data in-transit and at-rest.*



## Encryption In-Transit

HTTPS

SSL/TLS

VPN / IPSEC

SSH

## Encryption At-Rest

Object

Database

Filesystem

Disk

*Details about encryption can be found in the AWS Whitepaper,  
["Securing Data at Rest with Encryption"](#).*

# Encryption at Rest

## Volume Encryption

EBS Encryption

Filesystem Tools

AWS  
Marketplace/Partner

## Object Encryption

S3 Server Side  
Encryption (SSE)

S3 SSE w/ Customer  
Provided Keys

Client-Side Encryption

## Database Encryption

RDS  
MSSQL  
TDE

RDS  
ORACLE  
TDE/HSM

RDS  
MYSQL  
KMS

RDS  
PostgreSQL  
KMS

Redshift  
Encryption



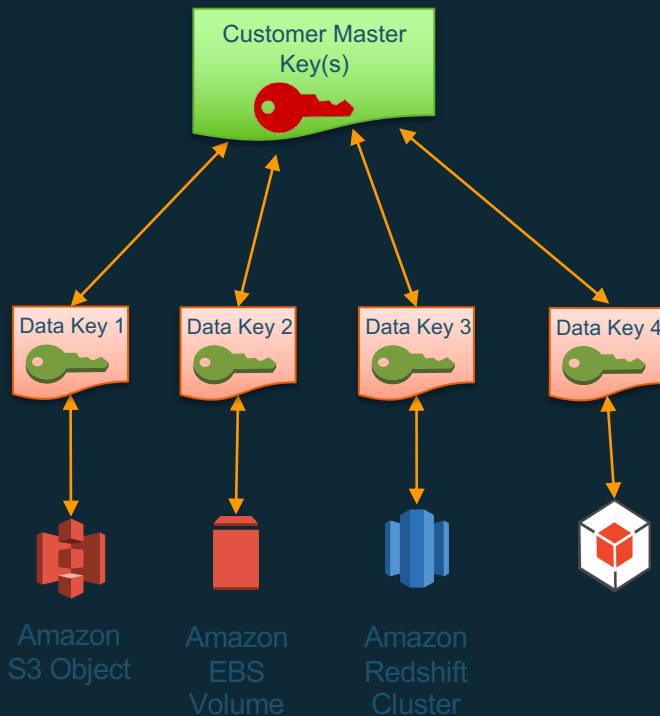
# AWS Certificate Manager



AWS Certificate Manager (ACM) makes it easy to provision, manage, deploy, and renew SSL/TLS certificates on the AWS platform.

# AWS Key Management Service

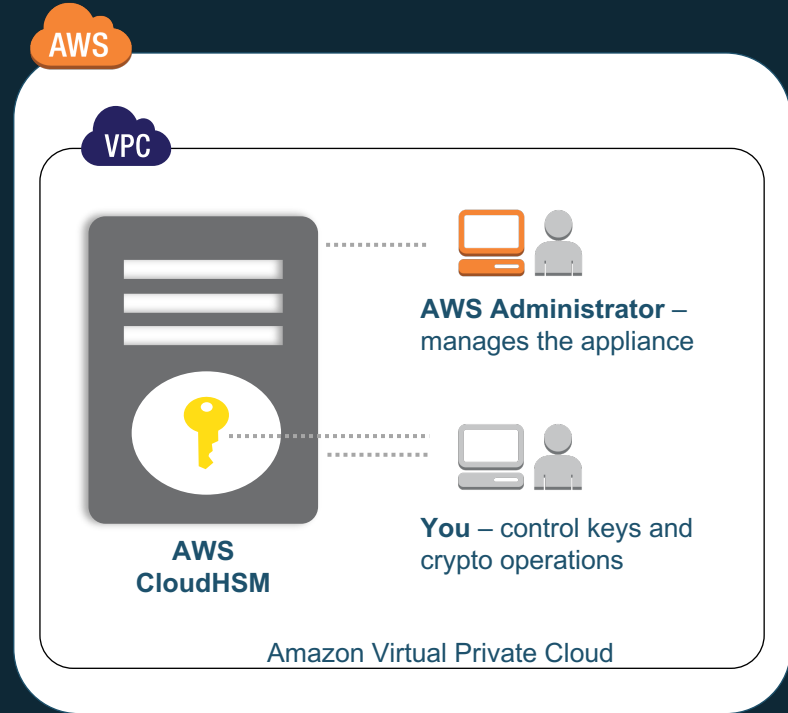
*Managed service to securely create, control, rotate, and use encryption keys.*



# AWS CloudHSM

*Help meet compliance requirements for data security by using a dedicated Hardware Security Module appliance with AWS.*

- Dedicated, single-tenant hardware device
- Can be deployed as HA and load balanced
- Customer use cases:
  - Oracle TDE
  - MS SQL Server TDE
  - Setup SSL connections
  - Digital Rights Management (DRM)
  - Document Signing

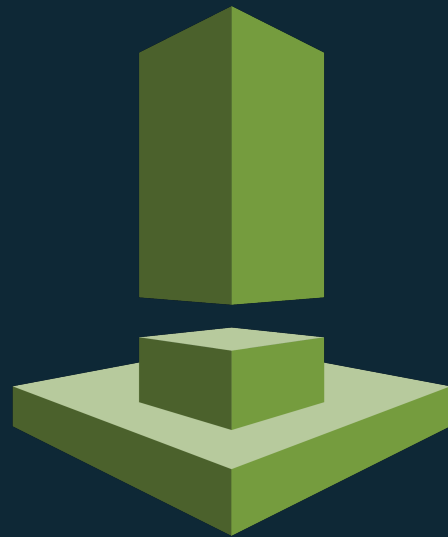




# Configuration Management

# Amazon Inspector

- Vulnerability Assessment Service
  - Built from the ground up to support DevSecOps
  - Automatable via APIs
  - Integrates with CI/CD tools
  - On-Demand Pricing model
  - Static & Dynamic Rules Packages
  - Generates Findings





## Web Traffic Filtering with Custom Rules

Create custom rules that can block, allow or monitor requests based on IP address, HTTP headers, or a combination of both.



## Malicious Request Blocking

AWS WAF can recognize and block common web application security risks like SQL injection (SQLi) and cross-site scripting (XSS).



## Active monitoring & tuning

Monitor and configure the requests that are being blocked and allowed by the Web ACL rules.

# AWS CloudTrail

*Web service that records AWS API calls for your account and delivers logs.*

Who?	When?	What?	Where to?	Where from?
Bill	3:27pm	Launch Instance	us-west-2	72.21.198.64
Alice	8:19am	Added Bob to admin group	us-east-1	127.0.0.1
Steve	2:22pm	Deleted DynamoDB table	eu-west-1	205.251.233.176

```
{
  "Records": [
    {
      "eventVersion": "1.0",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-03-25T18:45:11Z"
          }
        }
      },
      "eventTime": "2014-03-25T21:08:14Z",
      "eventSource": "iam.amazonaws.com",
      "eventName": "AddUserToGroup",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "AWSConsole",
      "requestParameters": {
        "userName": "Bob",
        "groupName": "admin"
      },
      "responseElements": null
    },
    ...additional entries
  ]
}
```

# AWS CloudWatch

*Monitoring services for AWS Resources and AWS-based Applications.*

## What does it do?

Collect and Track Metrics

Monitor and Store Logs

Set Alarms (react to changes)

View Graphs and Statistics



## How can you use it?

Monitor CPU, Memory, Disk I/O, Network, etc.

React to application log events and availability

Automatically scale EC2 instance fleet

View Operational Status and Identify Issues

CloudWatch Metrics

CloudWatch Logs / CloudWatch Events

CloudWatch Alarms

CloudWatch Dashboards



# VPC Flow Logs

- Agentless
- Enable per ENI, per subnet, or per VPC
- Logged to AWS CloudWatch Logs
- Create CloudWatch metrics from log data
- Alarm on those metrics

Interface

Source IP

Source port

Protocol

Packets

Destination IP

Destination port

Bytes

Start/end time

Accept or reject

Event Data

2

41747

eni-b30b9cd5

119.147.115.32

10.1.1.179

6000

22

6

1

40

1442975475

1442975535

REJECT OK

2

41747

eni-b30b9cd5

169.54.233.117

10.1.1.179

21188

80

6

1

40

1442975535

1442975595

REJECT OK

2

41747

eni-b30b9cd5

212.7.209.6

10.1.1.179

3389

3389

6

1

40

1442975596

1442975655

REJECT OK

2

41747

eni-b30b9cd5

189.134.227.225

10.1.1.179

39664

23

6

2

120

1442975656

1442975716

REJECT OK

2

41747

eni-b30b9cd5

77.85.113.238

10.1.1.179

0

0

1

1

100

1442975656

1442975716

REJECT OK

2

41747

eni-b30b9cd5

10.1.1.179

198.60.73.8

512

123

17

1

76

1442975776

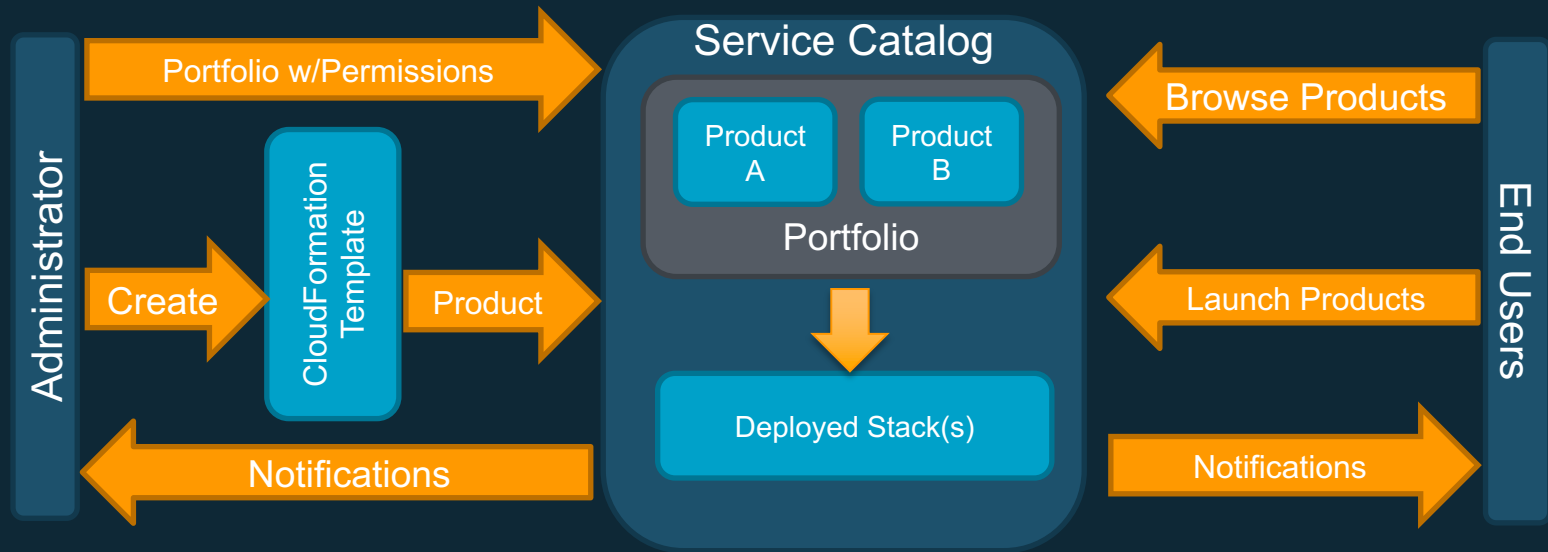
1442975836

ACCEPT OK

AWS account

# AWS Service Catalog

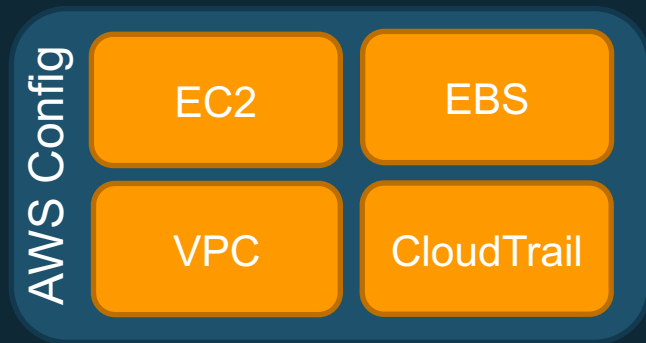
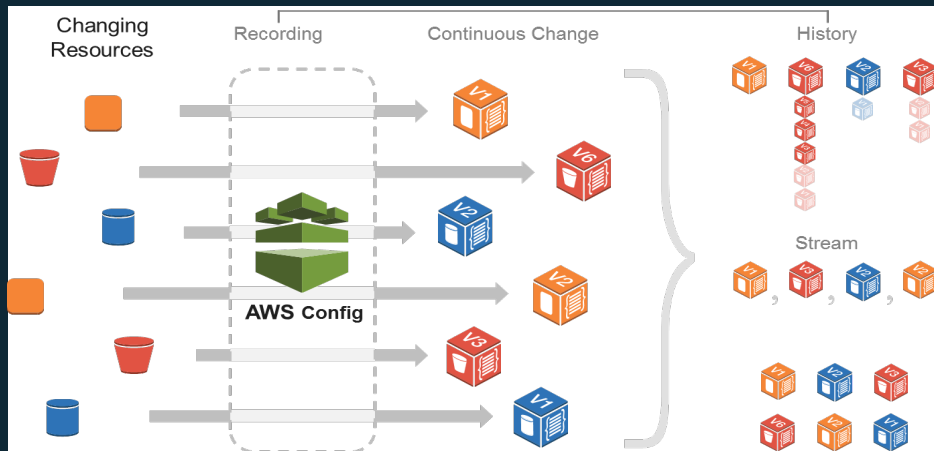
*Self-service portal for creating and managing resources in AWS.*



- Create and manage approved catalogs of resources.
- End users browse and launch products via self-service portal.
- Control user access to applications or AWS resources per compliance needs.
- Extensible via API to existing self-service frameworks.

# AWS Config

*Managed service for tracking AWS inventory and configuration, and configuration change notification.*



Security  
Analysis

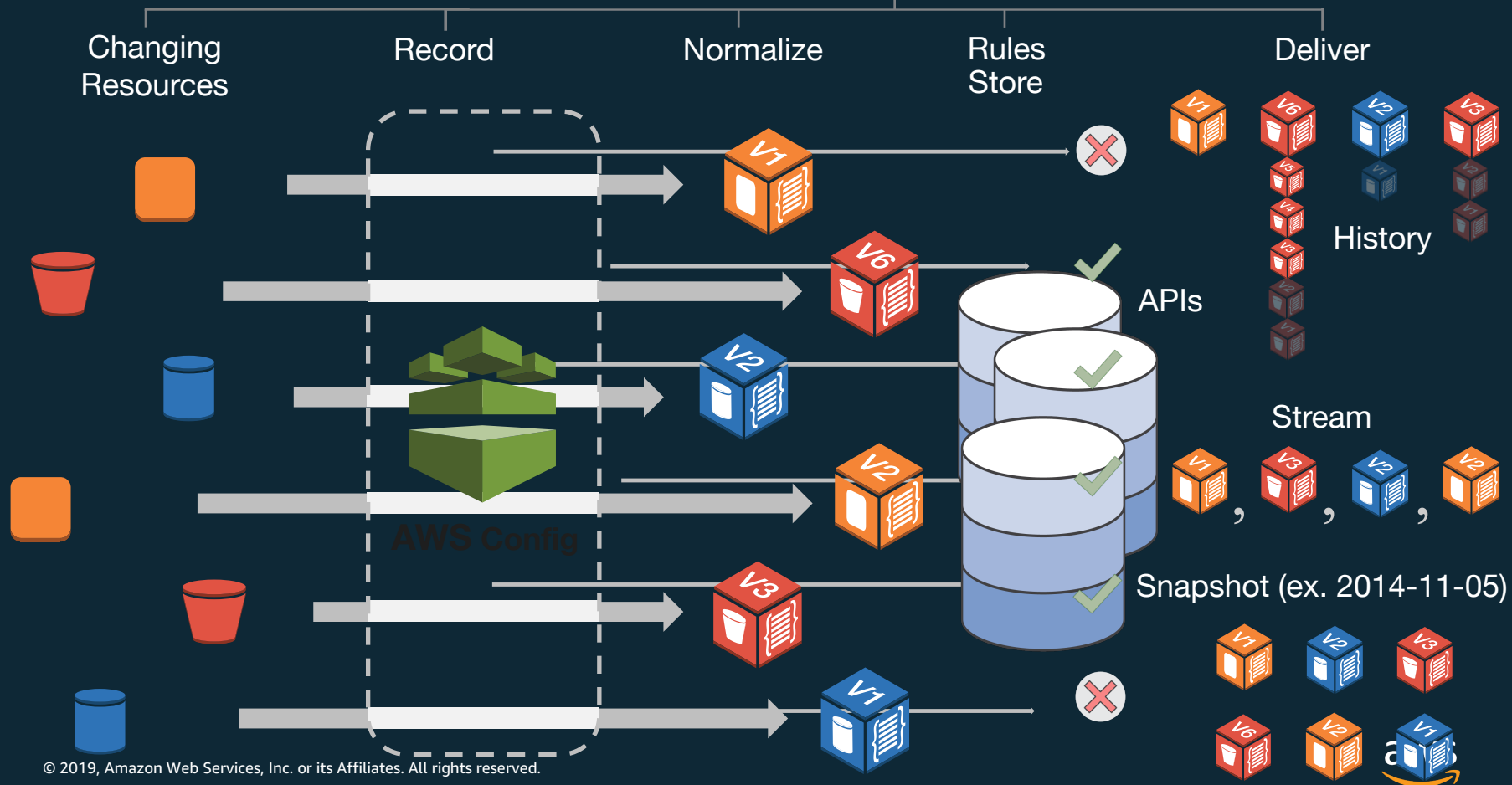
Audit  
Compliance

Change  
Management

Troubleshooting

Discovery

# AWS Config & Config Rules



# Any Questions?

