Move Fast

AND

Stay Secure

Making life easier

- Choosing security does not mean giving up on convenience or introducing complexity

Security ownership as part of DNA

Distributed

Embedded

- Promotes culture of “everyone is an owner” for security
- Makes security a stakeholder in business success
- Enables easier and smoother communication

Strengthen your security posture

Over 30 global compliance certifications and accreditations

Security infrastructure built to satisfy military, global banks, and other high-sensitivity organizations

Get native functionality and tools

Benefit from AWS industry leading security teams 24/7, 365 days a year

Leverage security enhancements gleaned from 1M+ customer experiences

Why is Security Traditionally Hard?

Lack of visibility

Low degree of automation

New Tools in Your Toolbox – Security Controls

- Directive
- Preventive
- Detective
- Responsive

Security Controls

- Directive Controls

- Detective Controls

- Preventive Controls

- Responsive Controls

Understand AWS Security Practice

Prescriptive Approach

Understand AWS Security Practice

Build Strong Compliance Foundations

Integrate Identity & Access Management

Enable Detective Controls

Establish Network Security

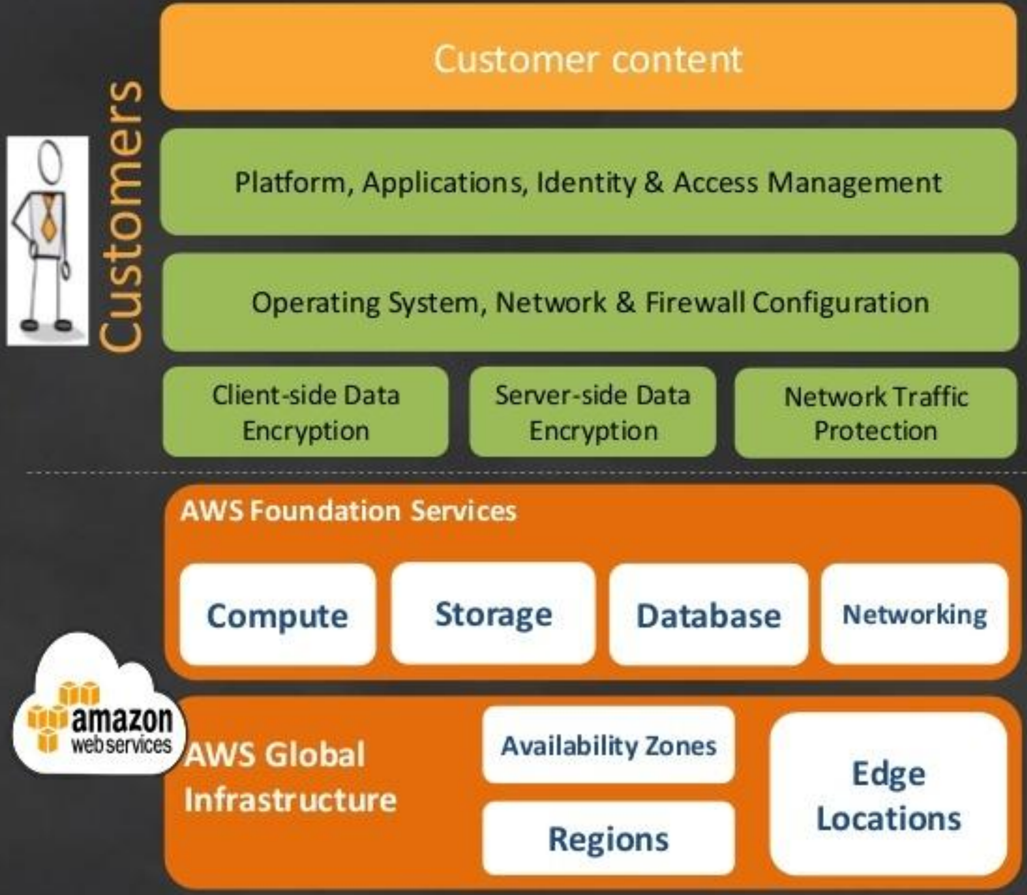
Implement Data Protection

Optimize Change Management

Automate Security Functions

https://aws.amazon.com/security/security-resources

Security is a shared responsibility



Customers

Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption

Server-side Data Encryption

Network Traffic Protection

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

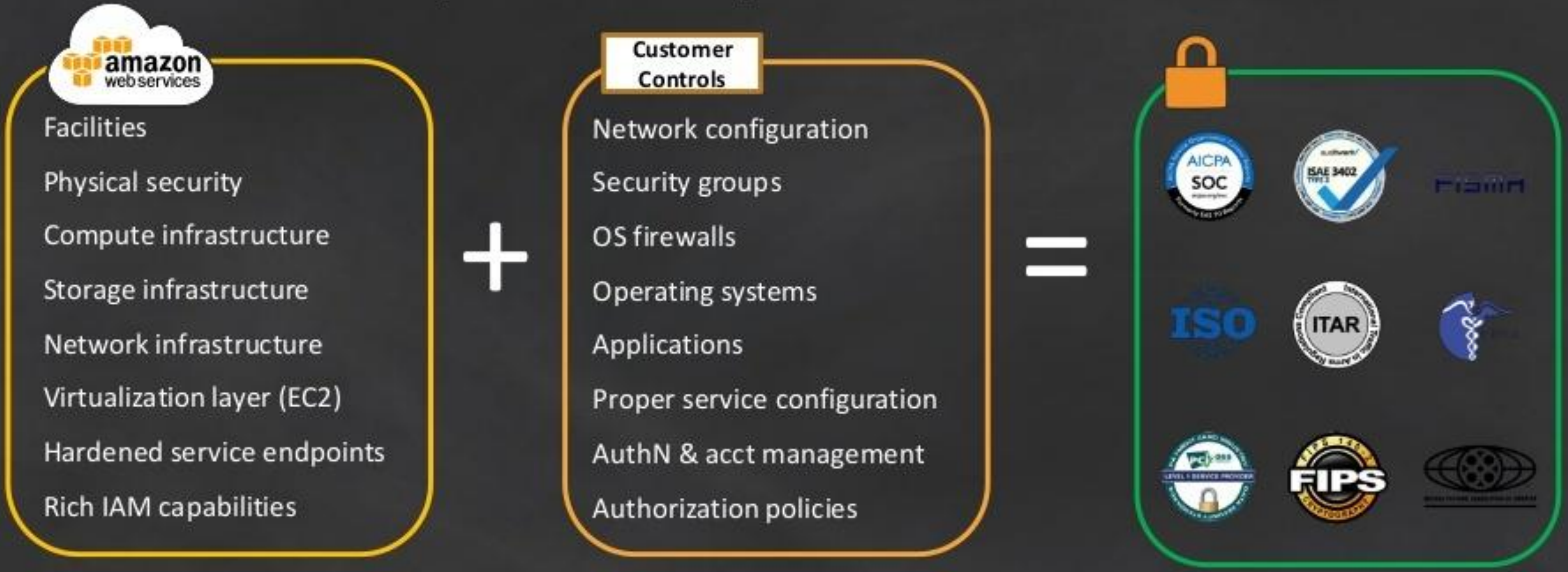
Edge Locations

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

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

Build Strong Compliance Foundations

AWS Shared Responsibility Model



Facilities

Physical security

Compute infrastructure

Storage infrastructure

Network infrastructure

Virtualization layer (EC2)

Hardened service endpoints

Rich IAM capabilities

Customer Controls

Network configuration

Security groups

OS firewalls

Operating systems

Applications

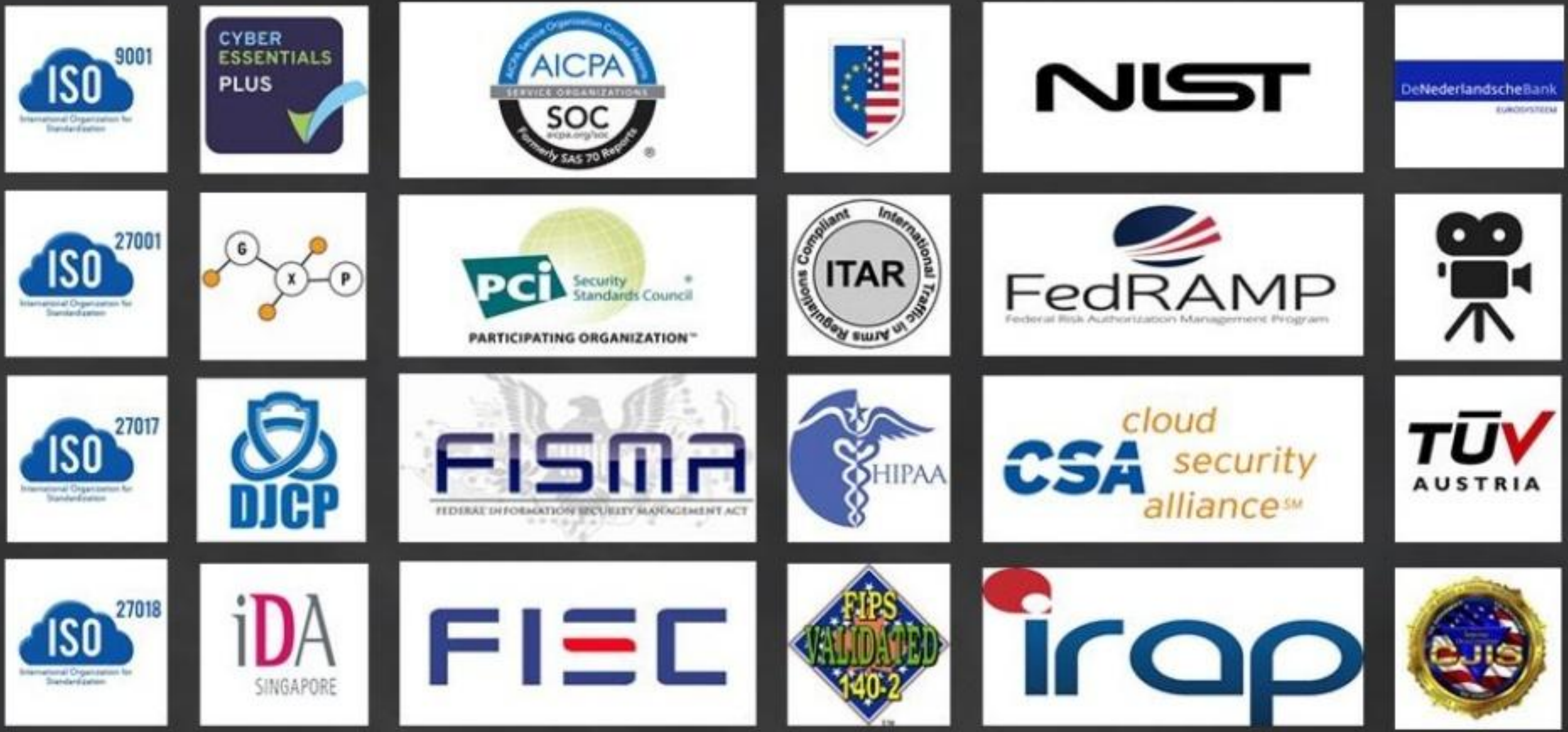
Proper service configuration

AuthN & acct management

Authorization policies

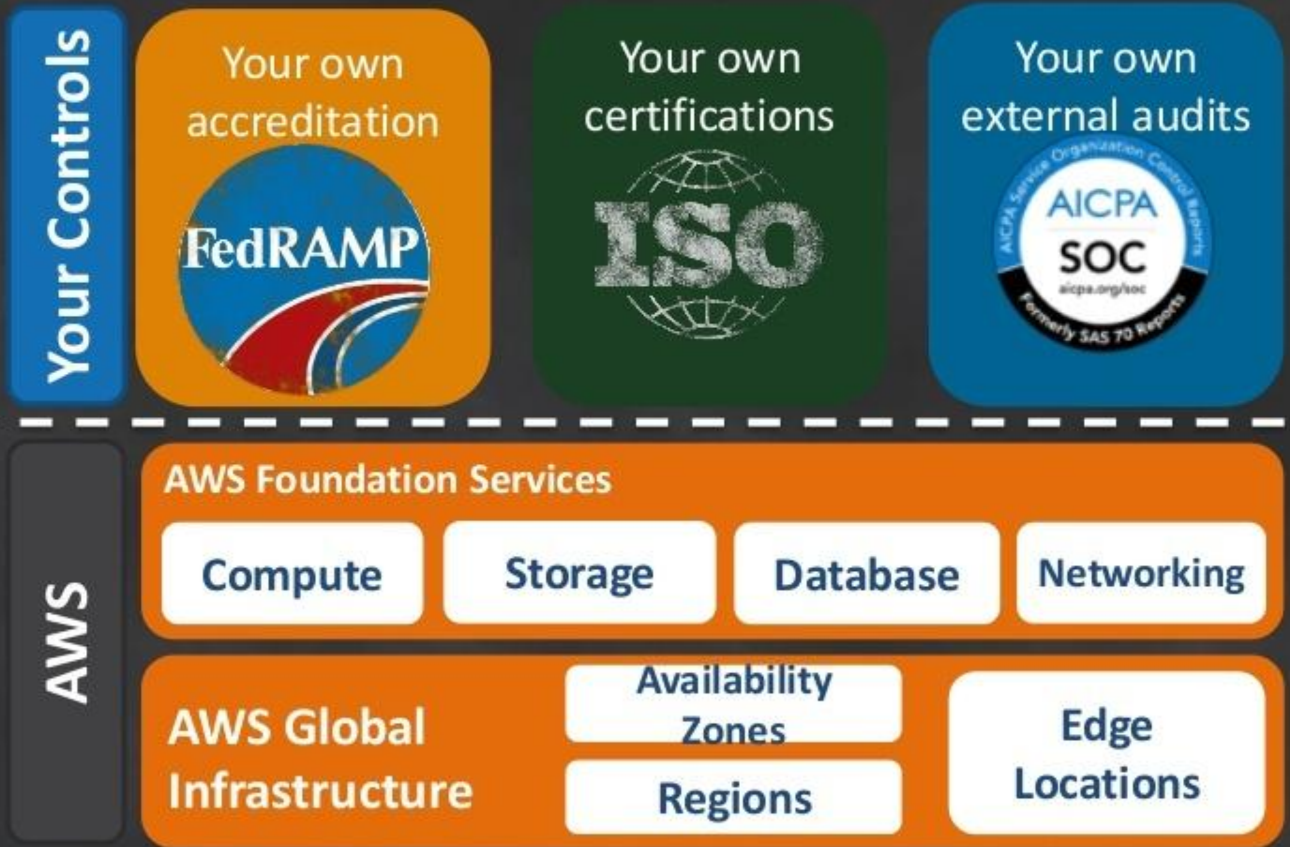
- Scope of responsibility depends on the type of service offered by AWS: **Infrastructure, Container, Abstracted Services**
- Understanding who is responsible for what is critical to ensuring your AWS data and systems are secure!

Broad Accreditations & Certifications


ISO 9001
International Organization for Standardization
CYBER ESSENTIALS PLUS
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports
NIST
DeNederlandscheBank
EUROSYSTEEM
ISO 27001
International Organization for Standardization
G X P
pci Security Standards Council
PARTICIPATING ORGANIZATION™
ITAR
Compliant International Traffic in Arms Regulations
FedRAMP
Federal Risk Authorization Management Program
ISO 27017
International Organization for Standardization
DJCP
FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
HIPAA
CSA cloud security alliance℠
TÜV AUSTRIA
ISO 27018
International Organization for Standardization
iDA SINGAPORE
FIEC
FIPS VALIDATED 140-2
irap
CJIS

https://aws.amazon.com/compliance/dod/

Meet your own security objectives



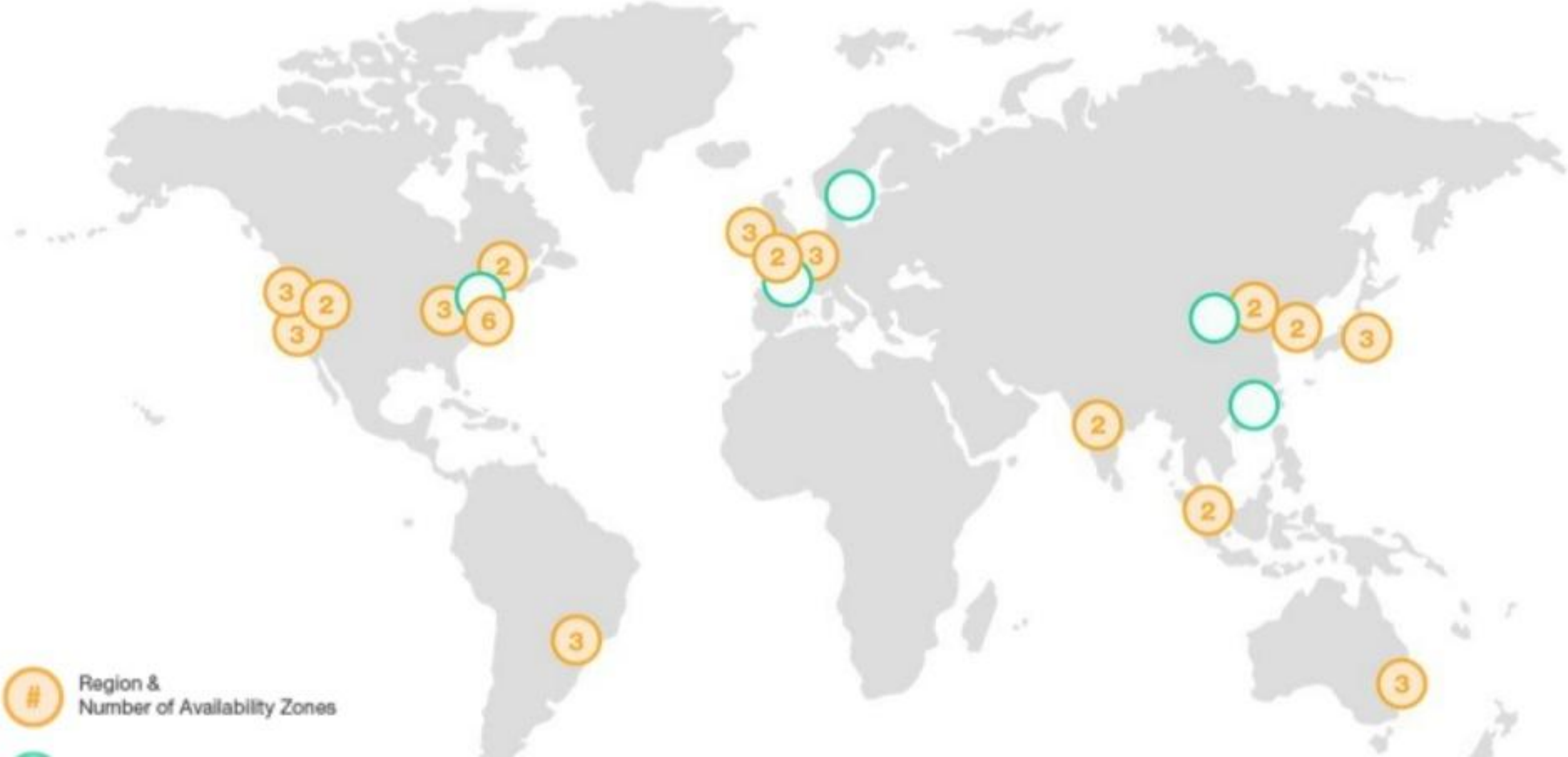
Customer scope and effort is reduced

Better results through focused efforts

Built on AWS consistent baseline controls

https://d0.awsstatic.com/whitepapers/compliance/AWS_DOD_CSM_Reference_Architecture.pdf

AWS Global Infrastructure



Directive Controls

Establish the governance, risk, and compliance models the environment will operate

Account Governance & Ownership

AWS Organizations

Centrally manage multiple accounts to help you scale.

- control which AWS services are available to individual accounts
- automate new account creation
- easily manage security and automation settings

AWS IAM

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

AWS Identity & Access Management

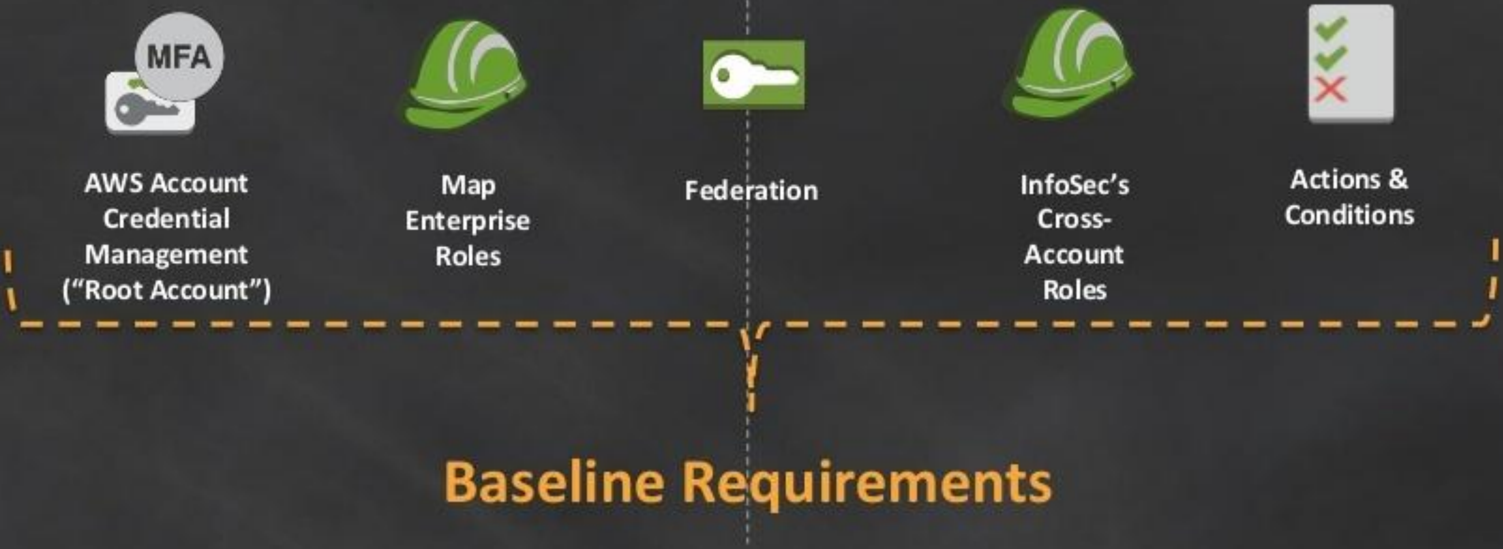
IAM Users

IAM Groups

IAM Roles

IAM Policies

Account Governance – New Accounts



AWS Account Credential Management ("Root Account")

Map Enterprise Roles

Federation

InfoSec's Cross-Account Roles

Actions & Conditions

Baseline Requirements

Preventive Controls

Protect your workloads and mitigate threats and vulnerabilities

Infrastructure Protection

Resources

security group

Virtual firewall that controls the traffic for one or more resources.

AWS CloudFormation

Easily create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion

AWS OpsWorks

Automate how servers are configured, deployed, and managed.

Network

Amazon VPC

Provision a logically isolated section of AWS cloud where you can launch AWS resources in a virtual network that you define.

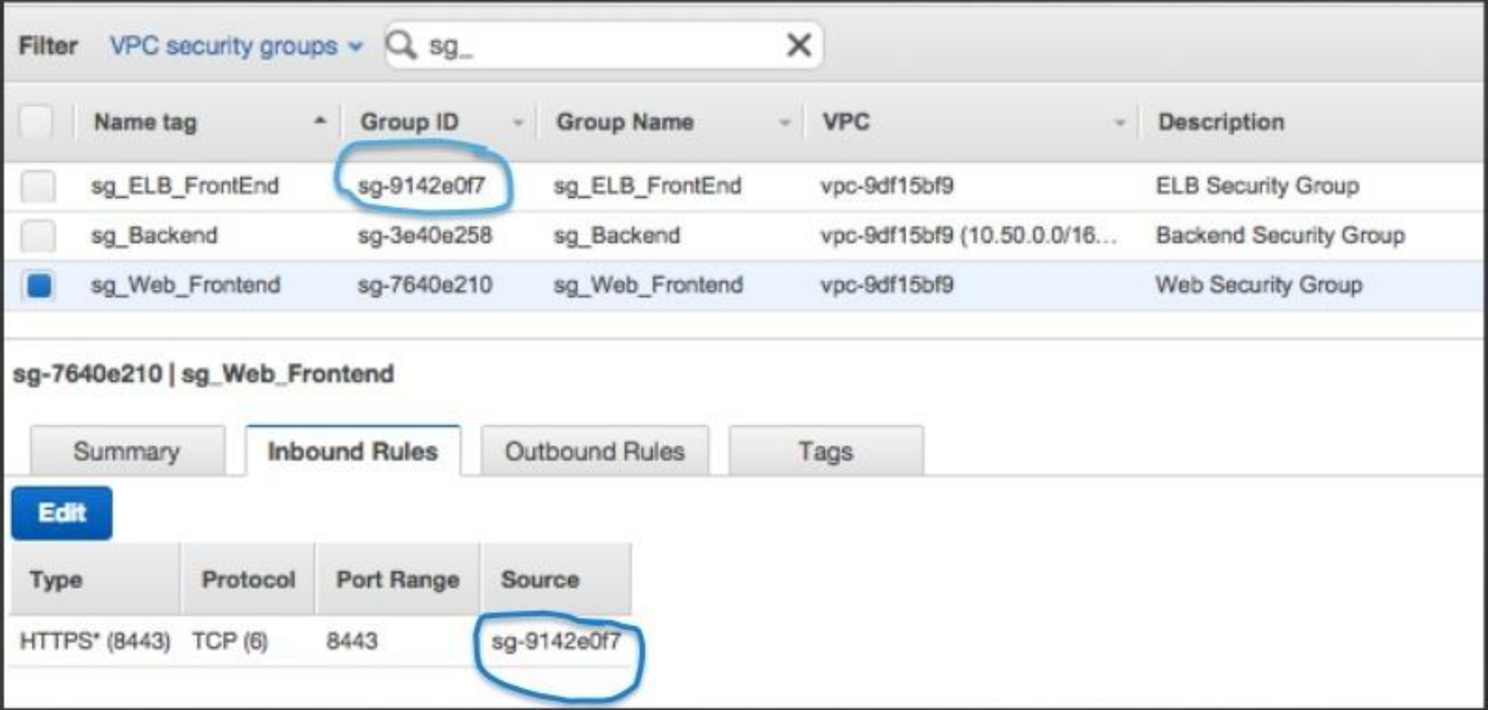
AWS Shield

DDoS protection service that safeguards web applications running on AWS

AWS WAF

Protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources

Security Groups

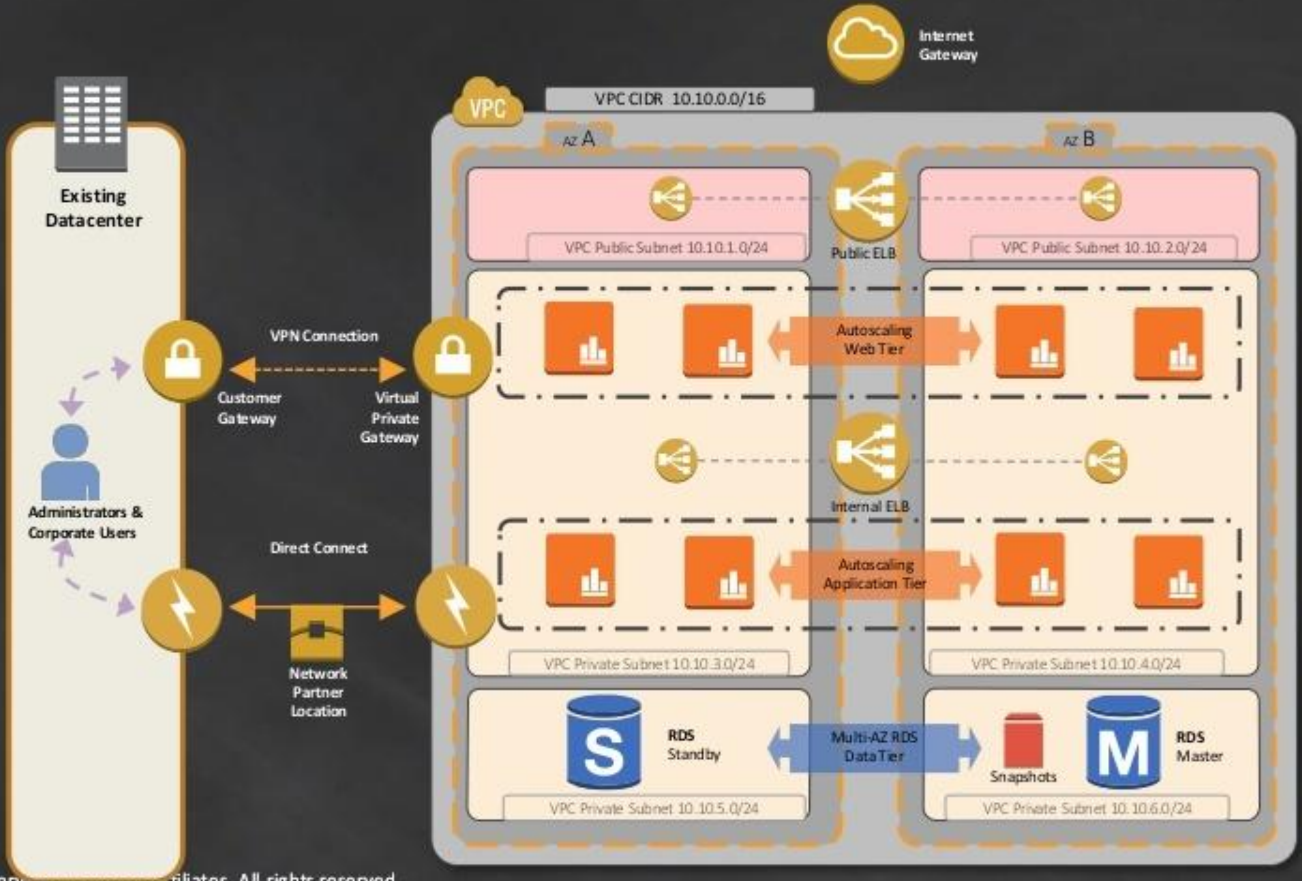


☐	Name tag	Group ID	Group Name	VPC	Description
☐	sg_ELB_FrontEnd	sg-9142e0f7	sg_ELB_FrontEnd	vpc-9df15bf9	ELB Security Group
☐	sg_Backend	sg-3e40e258	sg_Backend	vpc-9df15bf9 (10.50.0.0/16...	Backend Security Group
☑	sg_Web_Frontend	sg-7640e210	sg_Web_Frontend	vpc-9df15bf9	Web Security Group

sg-7640e210 | sg_Web_Frontend

Type	Protocol	Port Range	Source
HTTPS* (8443)	TCP (6)	8443	sg-9142e0f7

Amazon Virtual Private Cloud

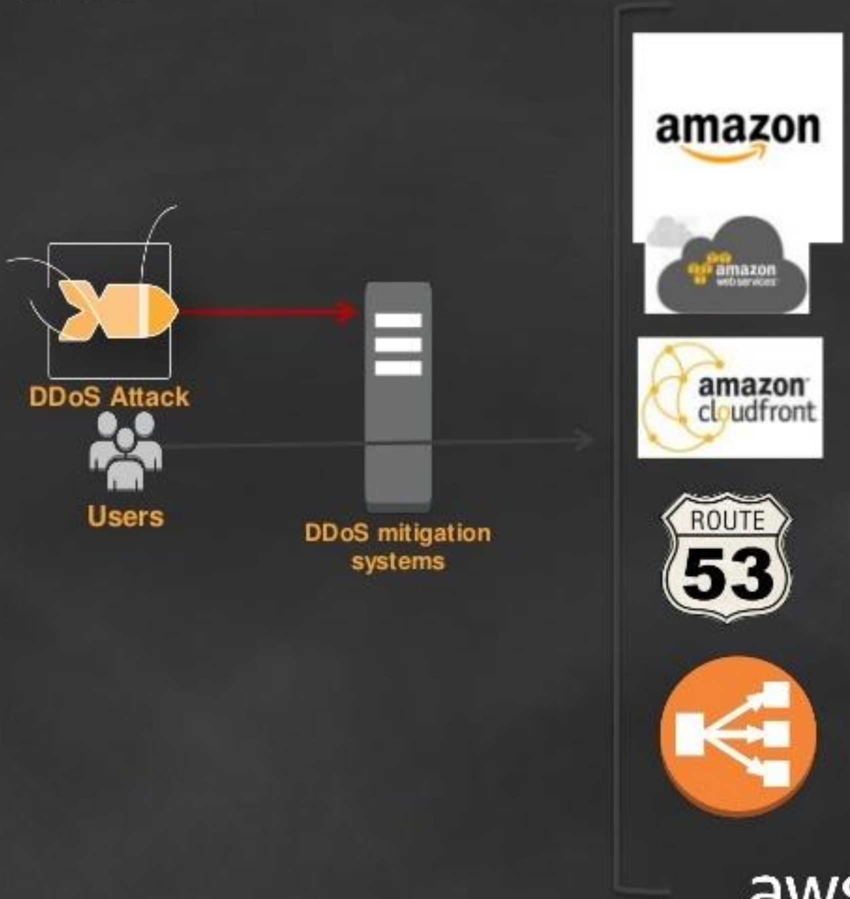


DDoS protections built into AWS

- Protection against most common infrastructure attacks

- SYN/ACK Floods, UDP Floods, Refection attacks etc.

- No additional cost



Advanced DDoS protection

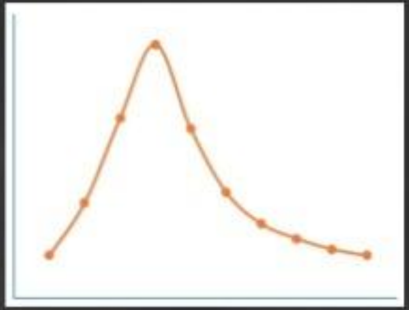
Layer 3/4 infrastructure protection

Layer 7 application protection

Layer 3/4 infrastructure protection

- Advanced mitigation techniques

Deterministic filtering



Traffic prioritization based on scoring

Advanced routing policies

AWS WAF – Layer 7 application protection

Web traffic filtering with custom rules

Malicious request blocking

Active monitoring and tuning

AWS Shield Standard

Protection against most common DDoS attacks, and access to tools and best practices to build a DDoS resilient architecture.

- Free of Cost
- Network Flow monitoring
- Quick Detection
- Inline Attack Mitigation
- DDoS protection best practices/architecture review
- Instant rule updates using Web Application Firewall (WAF)

AWS Shield Advanced

Additional protection against larger and more sophisticated attacks, visibility into attacks, and 24X7 access to DDoS experts for complex cases.

- **Application Traffic monitoring**
- **Additional DDoS mitigation capacity for large attacks**
- **Layer 3 / Layer 4 attack notification**
- **Layer 3 / Layer 4 / Layer 7 attack historical report**
- **Custom mitigations during attacks**
- **Post attack analysis**
- **DRT-driven application layer (Layer 7) mitigations**
- **Currently available to only Business and Enterprise Support customers**

Data Protection

AWS Certificate Manager

- Provision, manage, and deploy TLS certificates
- Use with Amazon ELB or Amazon CloudFront distribution

Amazon CloudHSM V2

- Fully Managed service
- Standards-compliant
- FIPS 140-2 Level 3
- AWS-Native

AWS KMS

- Deep integration with AWS Services
- CloudTrail
- AWS SDK for application encryption

Authenticating AWS to you and protecting confidentiality using TLS

- TLS can be used with every AWS API to protect data upload/download and configuration change
- You can provide your own certificates to be presented to your customers when using:
  - Elastic Load Balancing
  - Amazon CloudFront (content distribution network)

AWS Certificate Manager (ACM)

- Provision trusted SSL/TLS certificates from AWS for use with AWS resources:
  - Elastic Load Balancing
  - Amazon CloudFront distributions
- AWS handles the muck
  - Key pair and CSR generation
  - Managed renewal and deployment
- Domain validation (DV) through email
- Available through AWS Management Console, AWS Command Line Interface (AWS CLI), or API

Options for using encryption in AWS

Client-side encryption

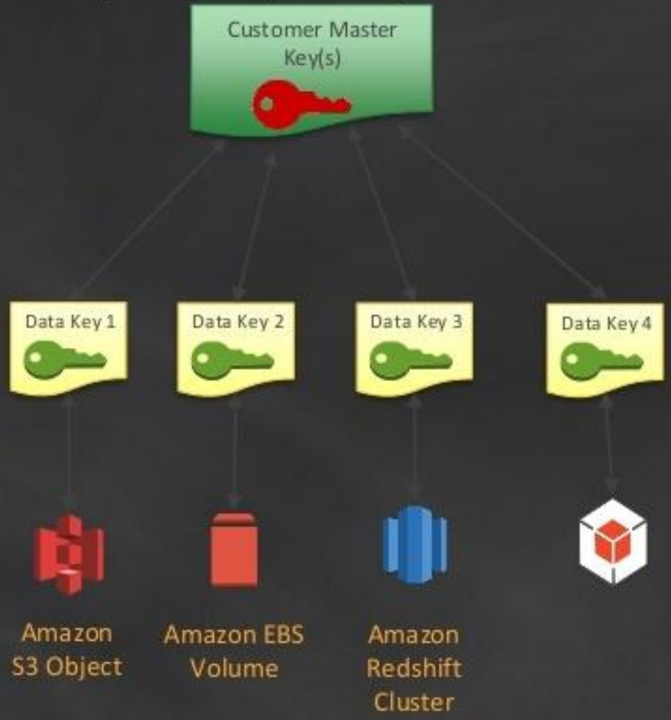
- You encrypt your data ***before*** data submitted to service
- You supply encryption keys OR use keys in your AWS account
- Available clients:
  - S3, EMR File System (EMRFS), DynamoDB, AWS Encryption SDK

Server-side encryption

- AWS encrypts data on your behalf ***after*** data is received by service
- 19 integrated services including S3, Snowball, EBS, RDS, Amazon Redshift, WorkSpaces, Amazon Kinesis Firehose, CloudTrail

AWS Key Management Service

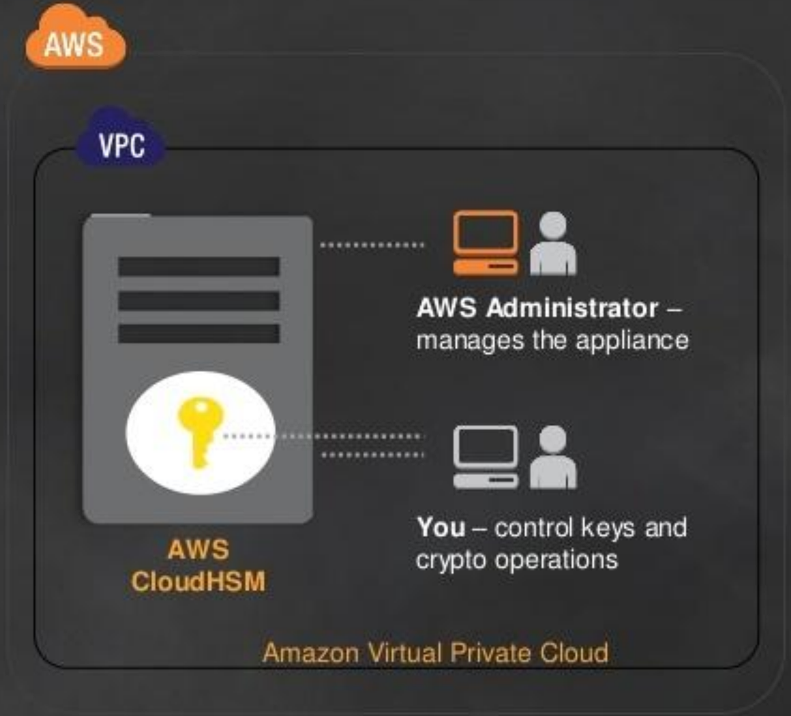
Managed service to securely create, control, rotate, and use encryption keys.



AWS CloudHSM

Help meet compliance requirements for data security by using clustered Hardware Security Module appliances with AWS.

- Hardware-enforced isolation of crypto operations and key storage.
- **Scalable managed service** – Provisioning, patching, high availability, and backups are all built-in and taken care of for you.
- **Standards-compliant**
  - PKCS #11
  - Java Cryptography Extension(JCE)
  - Microsoft CryptoNG (CNG).
- **FIPS 140-2 Level 3** support


AWS
VPC
AWS Administrator – manages the appliance
AWS CloudHSM
You – control keys and crypto operations
Amazon Virtual Private Cloud

Comparing CloudHSM with KMS

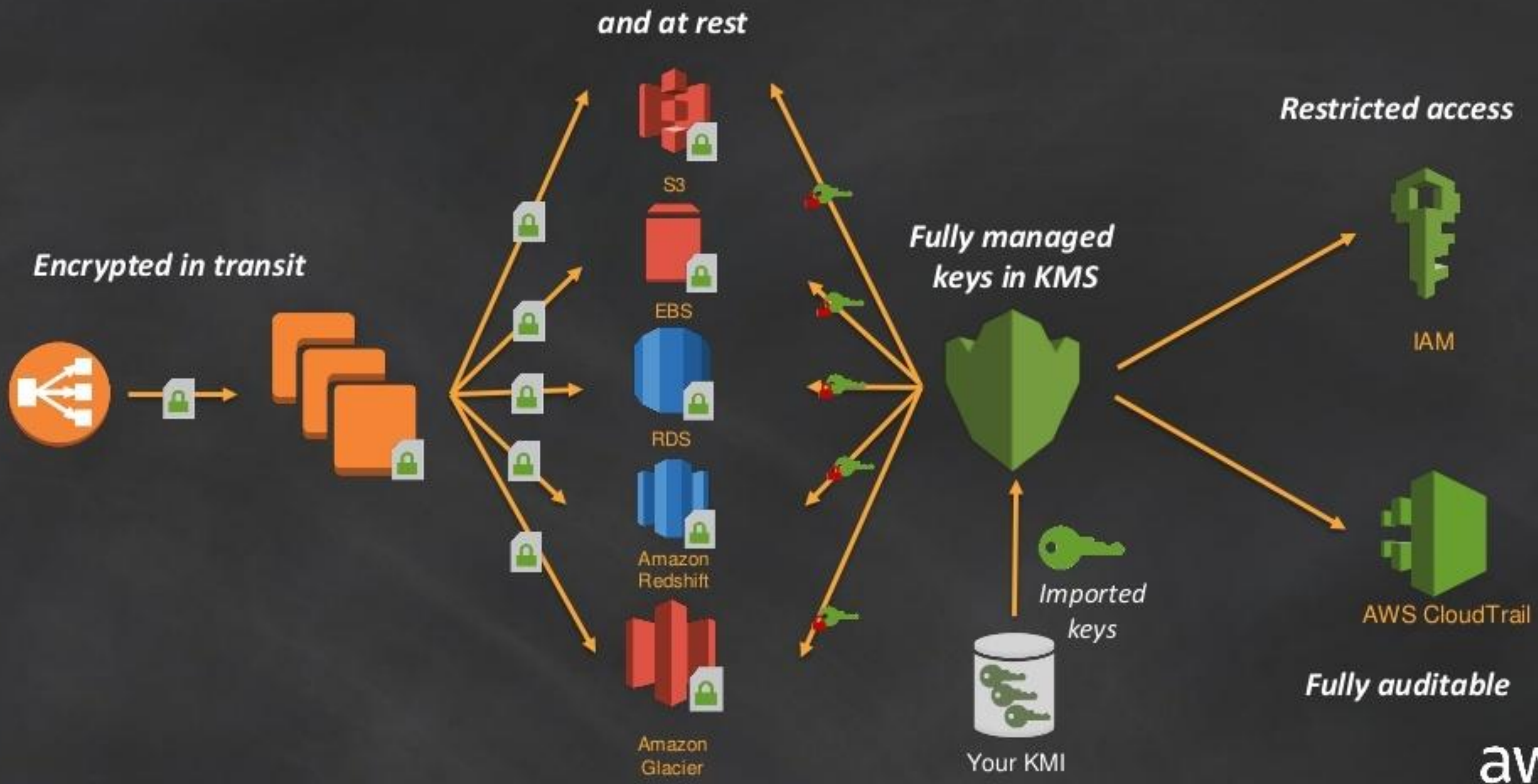
CloudHSM

- Access to one or more HSM devices that comply with government standards (for example, FIPS 140-2, Common Criteria)
- You control all access to your keys and the application software that uses them
- Supported applications:
  - Your custom software
  - Third-party software
  - AWS services: Amazon Redshift, RDS for Oracle

KMS

- Highly available and durable key storage, management, and auditable service
- Allows you to import keys
- Easily encrypt your data across AWS services and within your own applications based on policies you define
- Supported applications:
  - Your custom software built with AWS SDKs/CLI
  - AWS services (S3, EBS, RDS, Amazon Aurora, Amazon Redshift, WorkMail, WorkSpaces, CloudTrail, Elastic Transcoder)

Ubiquitous encryption



Data Loss Prevention

Amazon Macie

- Machine learning service to help customers prevent data loss in AWS.
- Analyzes S3 objects.
- Identifies and protects the data that attackers are likely to target.
- Automatically learns jargon, internal project names, and estimates the business value.

Database security with Amazon RDS

Database security

Amazon database solutions:

Amazon DynamoDB

Amazon Redshift

Amazon Aurora

AWS Database Migration Service

AWS database services and encryption at rest

Server-side encryption with KMS

- RDS MySQL
- RDS PostgreSQL
- RDS SQL Server
- RDS Oracle
- RDS MariaDB
- Amazon Aurora
- Amazon Redshift

Server-side encryption with CloudHSM

- Amazon Redshift
- RDS Oracle TDE
- Microsoft SQL TDE

Client-side encryption for row/column/field-level protection

- DynamoDB encryption client
- Build your own with AWS SDK
- third-party solutions

AWS data platforms - IAM and CloudTrail

- API permissions
  - Enforce separation of duties
- Resource-based permissions
  - Use tags by environment
- Integrated with CloudTrail
  - Alert on key management activities

Preventive Controls

```
{
 "Version": "2012-10-17",
 "Id": "key-consolepolicy-2",
 "Statement": [
  {
   "Sid": "Enable IAM User Permissions",
   "Effect": "Allow",
   "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
   "Action": "kms:*",
   "Resource": "*"
  },
  {
   "Sid": "Allow access for Key Administrators",
   "Effect": "Allow",
   "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KMSAdminUser",
    "arn:aws:iam::111122223333:role/KMSAdminRole"
   ]},
   "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms:Delete*",
    "kms:TagResource",
    "kms:UntagResource",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
   ],
   "Resource": "*"
```

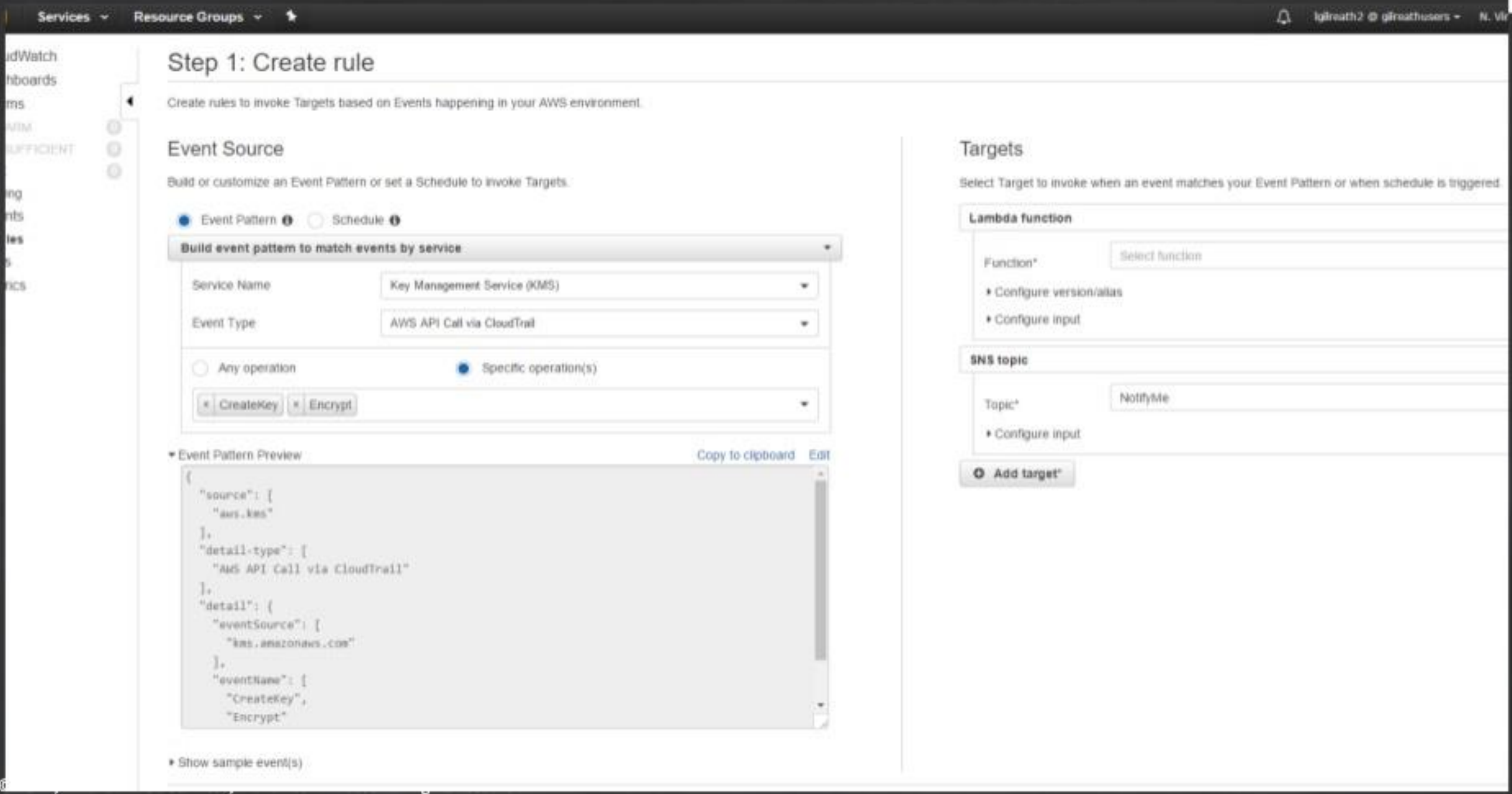
```
  },
  {
   "Sid": "Allow use of the key",
   "Effect": "Allow",
   "Principal": {"
                               KMSUser",
         111122223333:role/KMSRole",
    "arn:aws:iam::444455556666:root"
   ]},
   "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"

  {
   "Sid": "Allow attachment of persistent resources",
   "Effect": "Allow",
   "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KMSUser",
    "arn:aws:iam::111122223333:role/KMSRole",
    "arn:aws:iam::444455556666:root"
   ]},
   "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
   ],
   "Resource": "*",
   "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
  }
 ]
```

Allows the AWS account (root user) 111122223333 full access to the CMK, and thus enables IAM policies in the account to allow access to the CMK.

Allows IAM user KMSAdminUser and IAM role KMSAdminRole to administer the CMK.

Allows IAM user KMSUser, IAM role KMSRole, and AWS account 444455556666 to use the CMK.

Responsive Controls



Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

● Event Pattern ○ Schedule

Build event pattern to match events by service

Service Name: Key Management Service (KMS)

Event Type: AWS API Call via CloudTrail

○ Any operation ● Specific operation(s)

× CreateKey × Encrypt

Event Pattern Preview — Copy to clipboard — Edit

```
{
  "source": [
    "aws.kms"
  ],
  "detail-type": [
    "AWS API Call via CloudTrail"
  ],
  "detail": {
    "eventSource": [
      "kms.amazonaws.com"
    ],
    "eventName": [
      "CreateKey",
      "Encrypt"
```

Show sample event(s)

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered

Lambda function

Function*: Select function

Configure version/alias

Configure input

SNS topic

Topic*: NotifyMe

Configure input

Add target*

Track, detect, and take action

Tracking

- AWS Config rules
- Amazon CloudWatch Events
- AWS CloudTrail
- Amazon Inspector

Coordination

- Amazon SWF
- AWS CodePipeline

Execution

- AWS Lambda

Securing

- MFA
- IAM policies

Track/log

- Amazon CloudWatch Logs
- Amazon DynamoDB

Alert

- Amazon SNS

…

- You have options to implement data controls that meet your business needs
- Take advantage of managed services, and let us do the heavy lifting
- Protect your data but also track, detect, and take action on changes and events

Detective Controls

Full visibility and transparency over the operation of your deployments in AWS

VISIBILITY

Account

AWS CloudTrail

Web service that records AWS API calls for your account and delivers log files to you.

AWS Config

Resource inventory, configuration history, and configuration change notifications to enable security and governance

Resources

Amazon CloudWatch

Monitoring service for AWS cloud resources and the applications you run on AWS.

- collect and track metrics
- collect and monitor log files
- set alarms
- automatically react to changes in your AWS resources

Amazon Inspector

Automatically assesses applications for vulnerabilities or deviations from best practices

Network

Flow logs

Capture information about the IP traffic going to and from network interfaces in your VPC.

AWS CloudTrail & CloudWatch

AWS CloudTrail

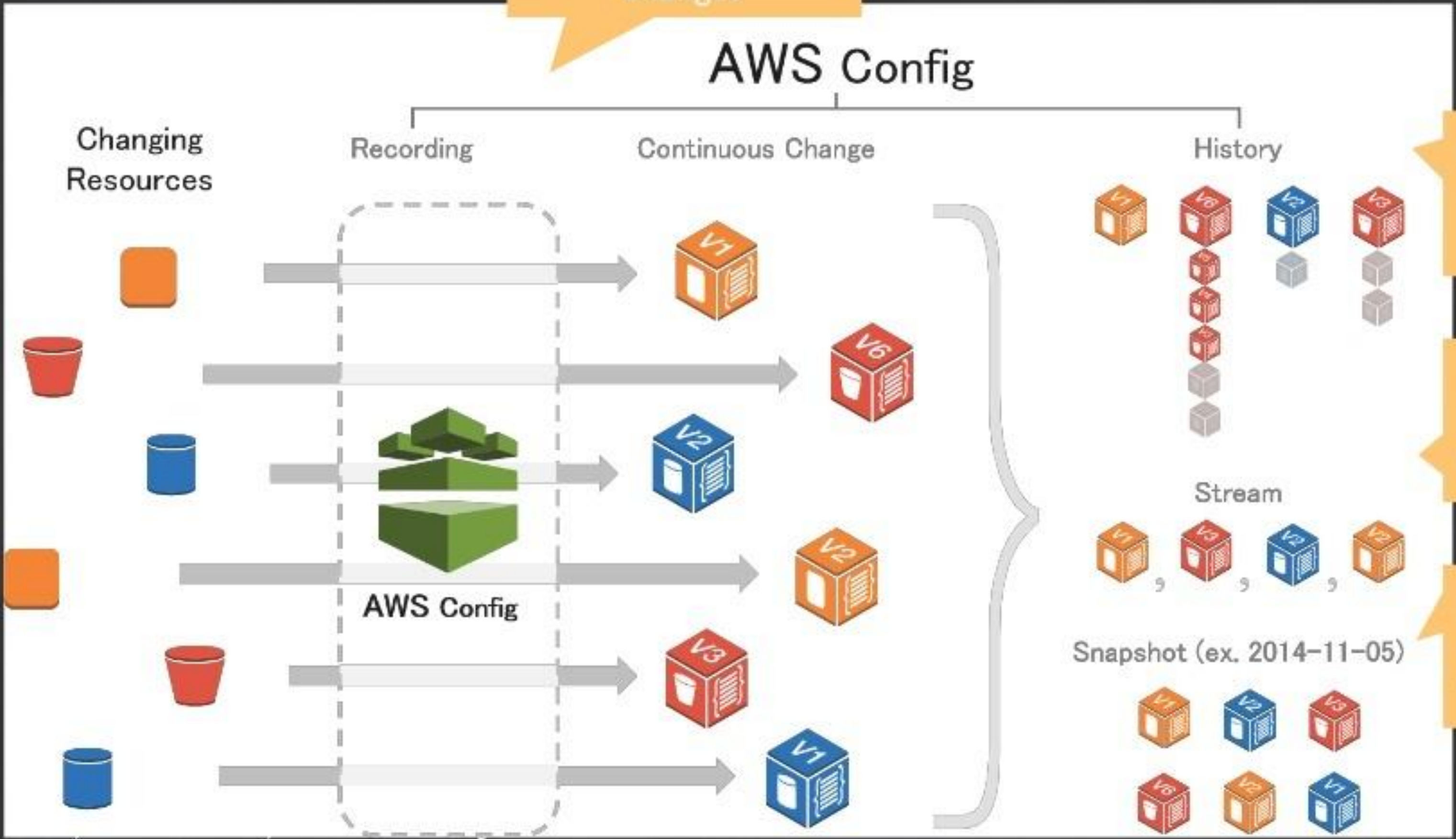
- ✓ Enable globally for all AWS Regions
- ✓ Encryption & Integrity Validation
- ✓ Archive & Forward

Amazon CloudWatch

- ✓ Amazon CloudWatch Logs
- ✓ Metrics & Filters
- ✓ Alarms & Notifications

AWS Config

record configuration changes

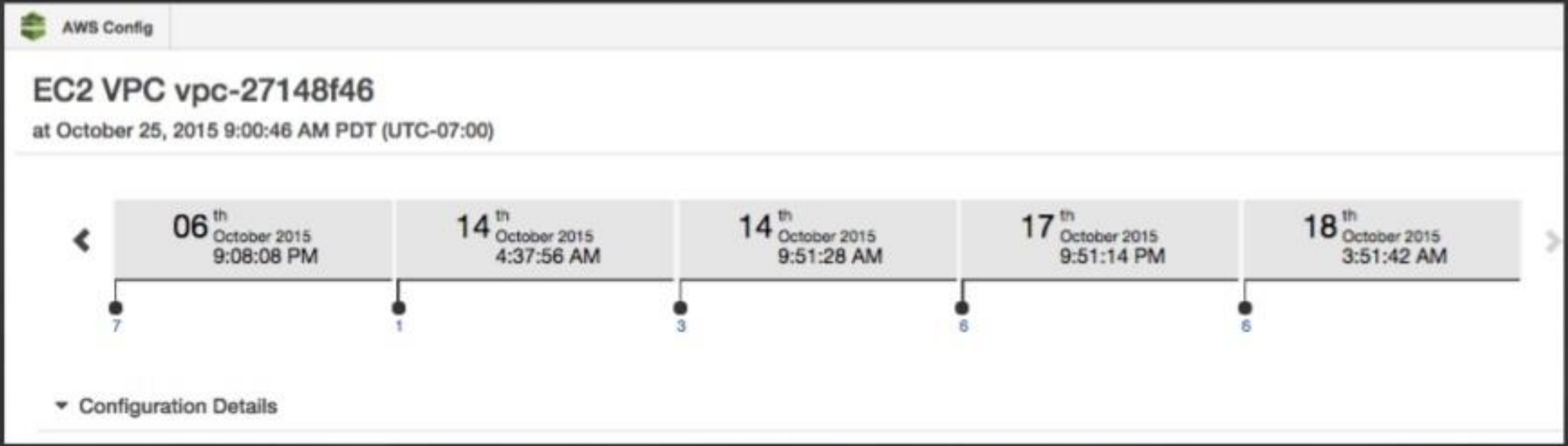


Configuration items can be viewed as a history

Stream of configuration items for all changes

Collection of configuration items for all resources

AWS Config



EC2 VPC vpc-27148f46

at October 25, 2015 9:00:46 AM PDT (UTC-07:00)

06th October 2015 9:08:08 PM

14th October 2015 4:37:56 AM

14th October 2015 9:51:28 AM

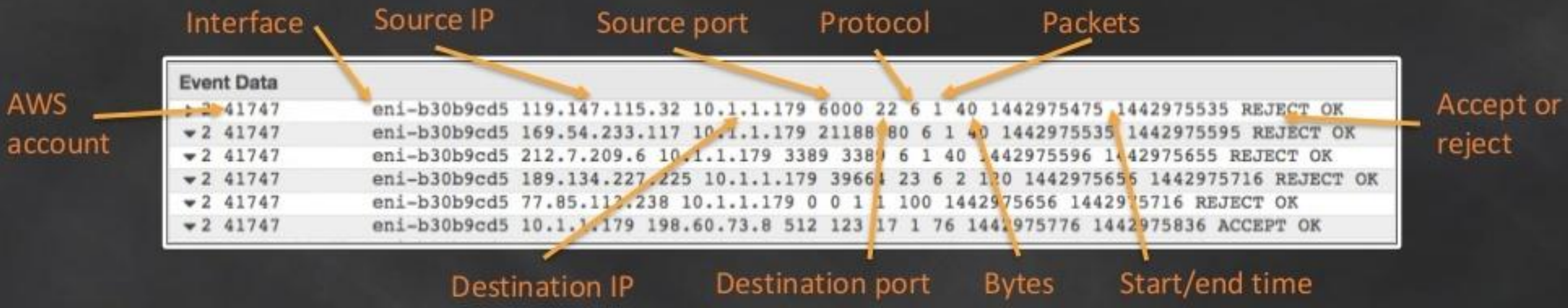
17th October 2015 9:51:14 PM

18th October 2015 3:51:42 AM

▾ Configuration Details

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

AWS account

Accept or reject

Destination IP

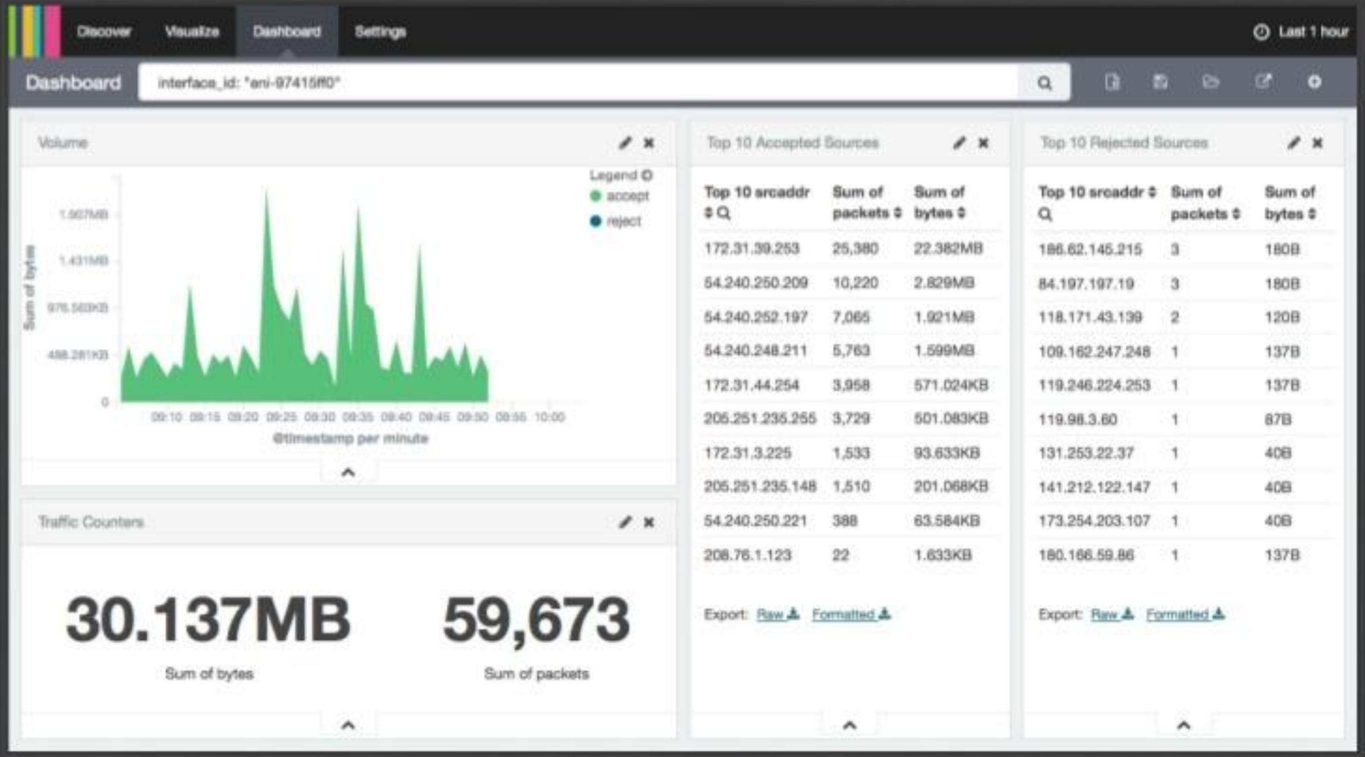
Destination port

Bytes

Start/end time

```
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 77.85.112.238 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
```

VPC Flow Logs



interface_id: "eni-97415ff0"

Top 10 Accepted Sources

Top 10 srcaddr ⇕	Sum of packets ⇕	Sum of bytes ⇕
172.31.39.253	25,380	22.382MB
54.240.250.209	10,220	2.829MB
54.240.252.197	7,065	1.921MB
54.240.248.211	5,763	1.599MB
172.31.44.254	3,958	571.024KB
205.251.235.255	3,729	501.083KB
172.31.3.225	1,533	93.633KB
205.251.235.148	1,510	201.068KB
54.240.250.221	388	63.584KB
208.76.1.123	22	1.633KB

Export: Raw Formatted

Top 10 Rejected Sources

Top 10 srcaddr ⇕	Sum of packets ⇕	Sum of bytes ⇕
186.62.145.215	3	180B
84.197.197.19	3	180B
118.171.43.139	2	120B
109.162.247.248	1	137B
119.246.224.253	1	137B
119.98.3.60	1	87B
131.253.22.37	1	40B
141.212.122.147	1	40B
173.254.203.107	1	40B
180.166.59.86	1	137B

Export: Raw Formatted

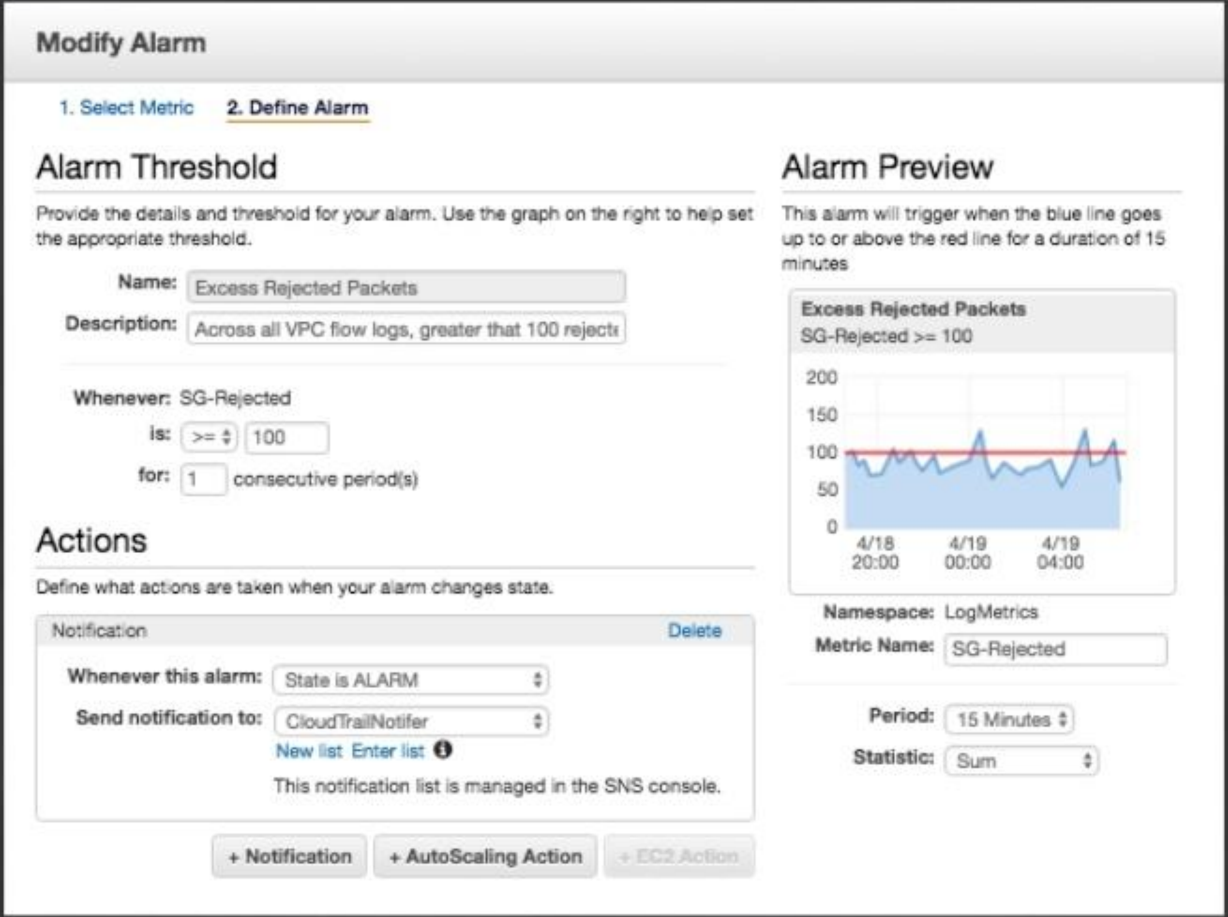
Traffic Counters

30.137MB
Sum of bytes

59,673
Sum of packets

- Amazon Elasticsearch Service
- Amazon CloudWatch Logs subscriptions

VPC Flow Logs – CloudWatch Alarms



Modify Alarm

1. Select Metric 2. Define Alarm

Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name: Excess Rejected Packets

Description: Across all VPC flow logs, greater that 100 rejecte

Whenever: SG-Rejected

is: >= 100

for: 1 consecutive period(s)

Actions

Define what actions are taken when your alarm changes state.

Notification Delete

Whenever this alarm: State is ALARM

Send notification to: CloudTrailNotifer

New list Enter list

This notification list is managed in the SNS console.

Alarm Preview

This alarm will trigger when the blue line goes up to or above the red line for a duration of 15 minutes

Excess Rejected Packets
SG-Rejected >= 100

Namespace: LogMetrics

Metric Name: SG-Rejected

Period: 15 Minutes

Statistic: Sum

Responsive Controls

Drive remediation of potential deviations from your security baselines

AUDITABILITY

AWS Trusted Advisor

Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.

- reduce cost
- increase performance
- improve security

An Introduction to AWS Trusted Advisor
Business Leaders
Developers
Cost Optimization
Performance
Security
Fault Tolerance
No Problems Detected
Action Recommended
Investigation Recommended

Config Rules enables you to create rules that automatically check the configuration of AWS resources recorded by AWS Config.

AWS Config rule

AWS Config & Config Rules

AWS
Config

- ✓ Record configuration changes continuously
- ✓ Time-series view of resource changes
- ✓ Archive & Compare

Amazon
Config Rules

- ✓ Enforce best practices
- ✓ Automatically roll-back unwanted changes
- ✓ Trigger additional workflow

AWS Trusted Advisor

Cost Optimization

Performance

Security

Fault Tolerance

Core Checks and Recommendations

Available to all AWS customers

Access to the six core Trusted Advisor checks to help increase the security and performance of your environment.

Checks include:
Security: Security Groups - Specific Ports Unrestricted, IAM Use, MFA on Root Account, EBS Public Snapshots, RDS Public Snapshots

Performance: Service Limits

Core Checks and Recommendations

Available with Business or Enterprise support plans

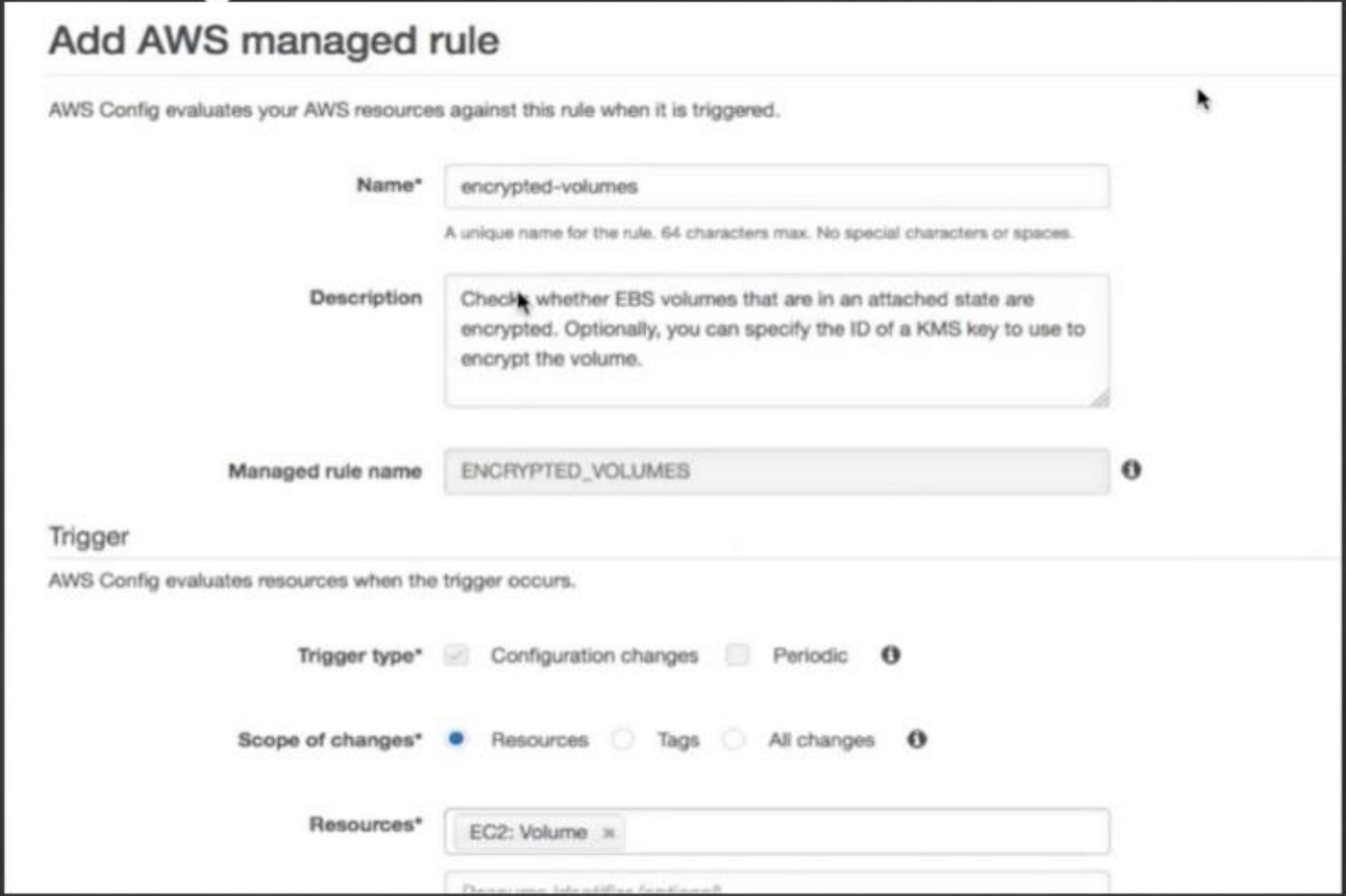
Access to the full set of Trusted Advisor checks to help optimize your entire AWS infrastructure.

Additional benefits include:

Notifications: Stay up-to-date with your AWS resource deployment with weekly updates.

Programmatic access: Retrieve and refresh Trusted Advisor results programmatically using AWS Support API.

AWS Config Rules – Enforce Volume Encryption



Add AWS managed rule

AWS Config evaluates your AWS resources against this rule when it is triggered.

Name*: encrypted-volumes

A unique name for the rule. 64 characters max. No special characters or spaces.

Description: Check whether EBS volumes that are in an attached state are encrypted. Optionally, you can specify the ID of a KMS key to use to encrypt the volume.

Managed rule name: ENCRYPTED_VOLUMES

Trigger

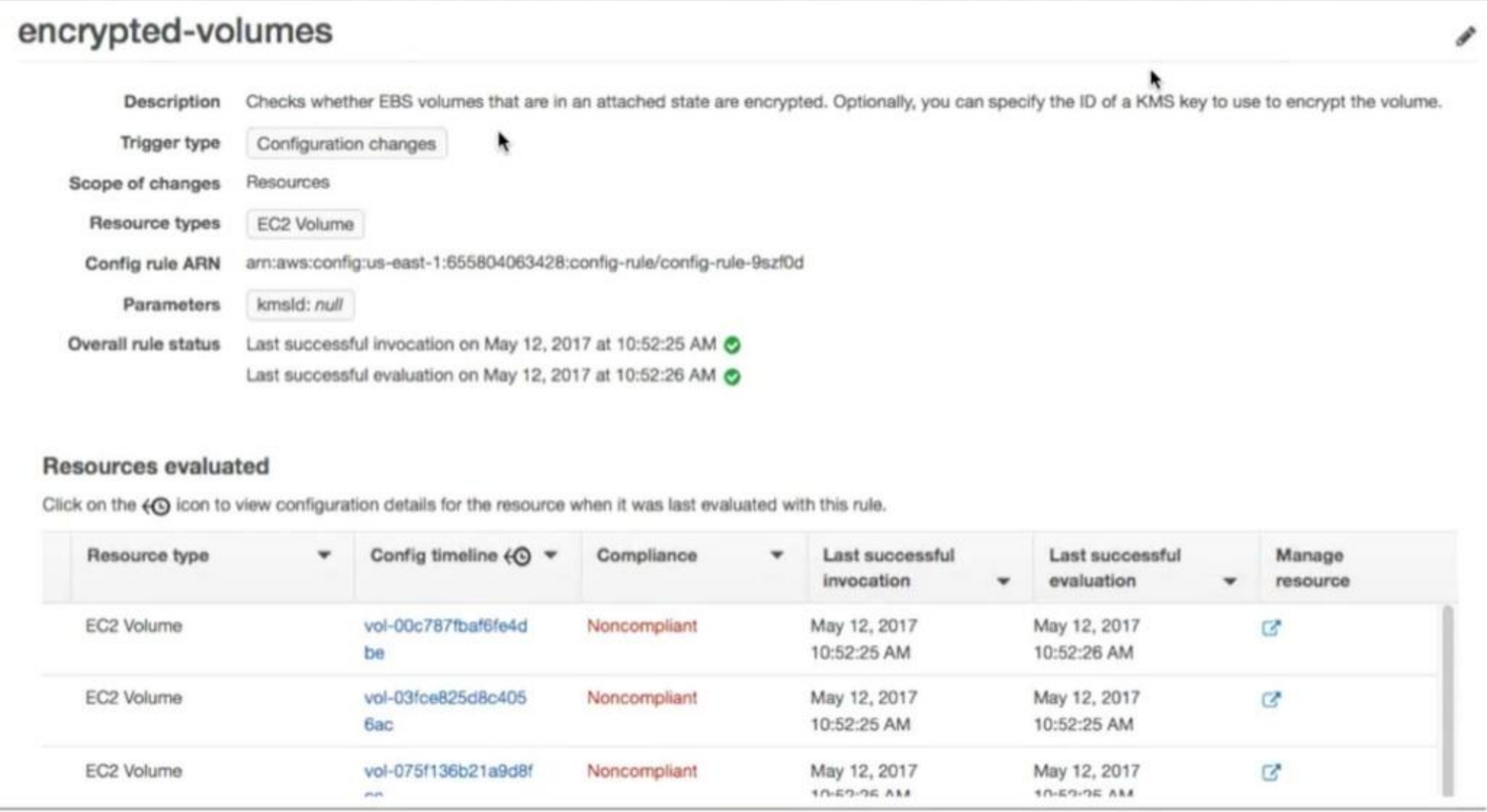
AWS Config evaluates resources when the trigger occurs.

Trigger type*: ☑ Configuration changes □ Periodic

Scope of changes*: ● Resources ○ Tags ○ All changes

Resources*: EC2: Volume ×

Resource identifier (optional)



encrypted-volumes

Description Checks whether EBS volumes that are in an attached state are encrypted. Optionally, you can specify the ID of a KMS key to use to encrypt the volume.

Trigger type Configuration changes

Scope of changes Resources

Resource types EC2 Volume

Config rule ARN arn:aws:config:us-east-1:655804063428:config-rule/config-rule-9szf0d

Parameters kmsId: *null*

Overall rule status Last successful invocation on May 12, 2017 at 10:52:25 AM ✓
Last successful evaluation on May 12, 2017 at 10:52:26 AM ✓

Resources evaluated

Click on the icon to view configuration details for the resource when it was last evaluated with this rule.

Resource type	Config timeline	Compliance	Last successful invocation	Last successful evaluation	Manage resource
EC2 Volume	vol-00c787fbaf6fe4dbe	Noncompliant	May 12, 2017 10:52:25 AM	May 12, 2017 10:52:26 AM	
EC2 Volume	vol-03fce825d8c4056ac	Noncompliant	May 12, 2017 10:52:25 AM	May 12, 2017 10:52:25 AM	
EC2 Volume	vol-075f136b21a9d8f	Noncompliant	May 12, 2017	May 12, 2017	

AWS Artifact

- Audit and compliance portal for on-demand access to download AWS’ compliance reports and manage select agreements for ISO, PCI, SOC, and other regulatory standards.

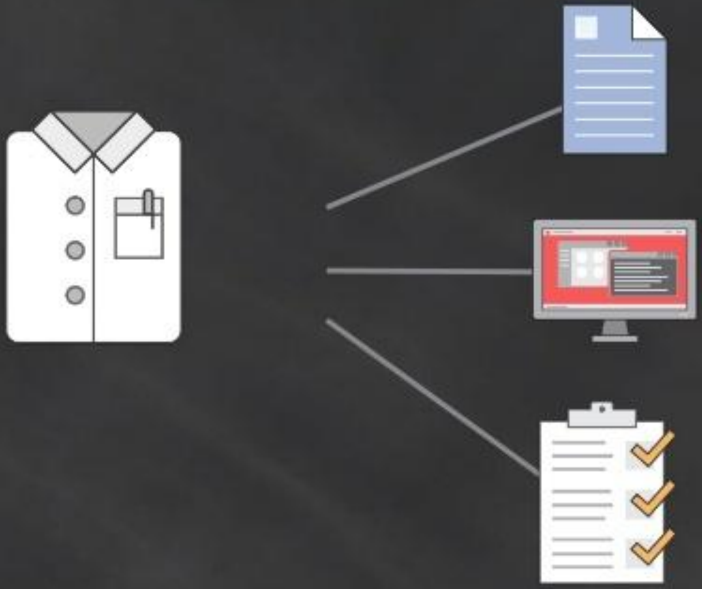
- Benefits:
  - Reports On-Demand
  - Globally Available
  - Easy Identification
  - Quick Assessments
  - Continuous Monitoring
  - Enhanced Transparency

Automate Security Functions

Evolving the Practice of Security Architecture

- Security architecture as a separate function can no longer exist

Current Security Architecture Practice

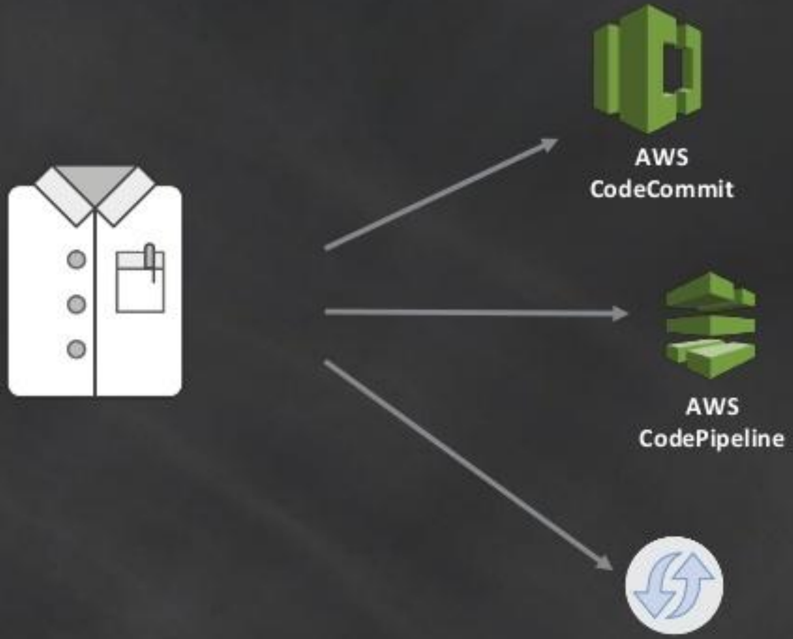


- Static position papers, architecture diagrams & documents
- UI-dependent consoles and technologies
- Auditing, assurance, and compliance are decoupled, separate processes

Evolving the Practice of Security Architecture

- Security architecture can now be part of the ‘maker’ team

Evolved Security Architecture Practice



- Architecture artifacts (design choices, narrative, etc.) committed to common repositories
- Complete solutions account for automation
- Solution architectures are living audit/compliance artifacts and evidence in a closed loop

AWS CloudFormation – Infrastructure as Code

AWS CloudFormation

- Orchestrate changes across AWS Services
- Use as foundation to Service Catalog products
- Use with source code repositories to manage infrastructure changes

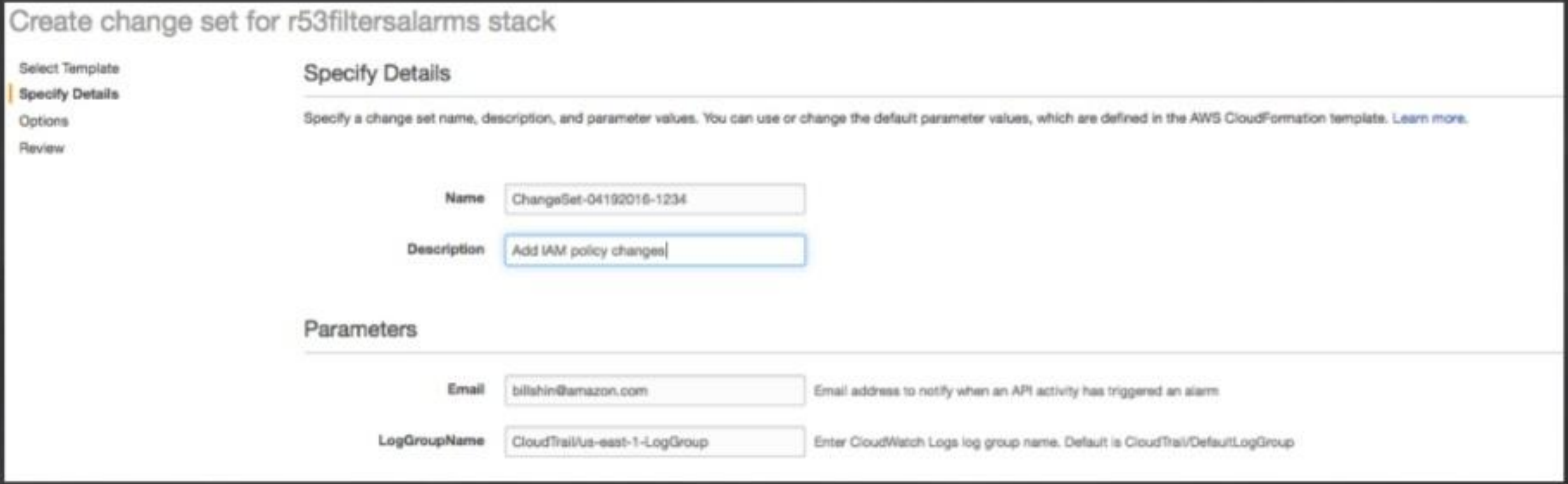
Template

- JSON-based text file describing infrastructure

Stack

- Resources created from a template
- Can be updated
- Updates can be restricted

Change Sets – Create Change Set



Create change set for r53filtersalarms stack

Specify Details

Specify a change set name, description, and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Name: ChangeSet-04192016-1234

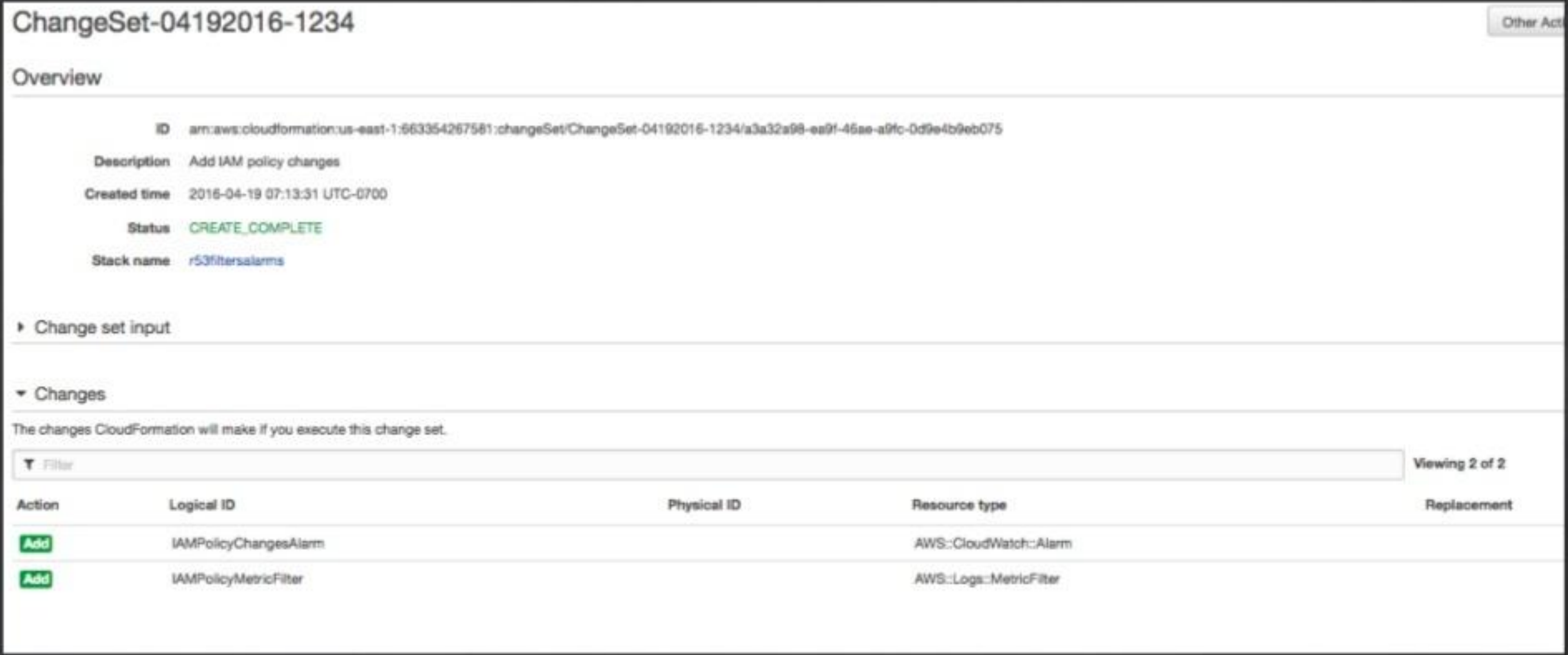
Description: Add IAM policy changes

Parameters

Email: billshin@amazon.com — Email address to notify when an API activity has triggered an alarm

LogGroupName: CloudTrail/us-east-1-LogGroup — Enter CloudWatch Logs log group name. Default is CloudTrail/DefaultLogGroup

Change Sets



ChangeSet-04192016-1234

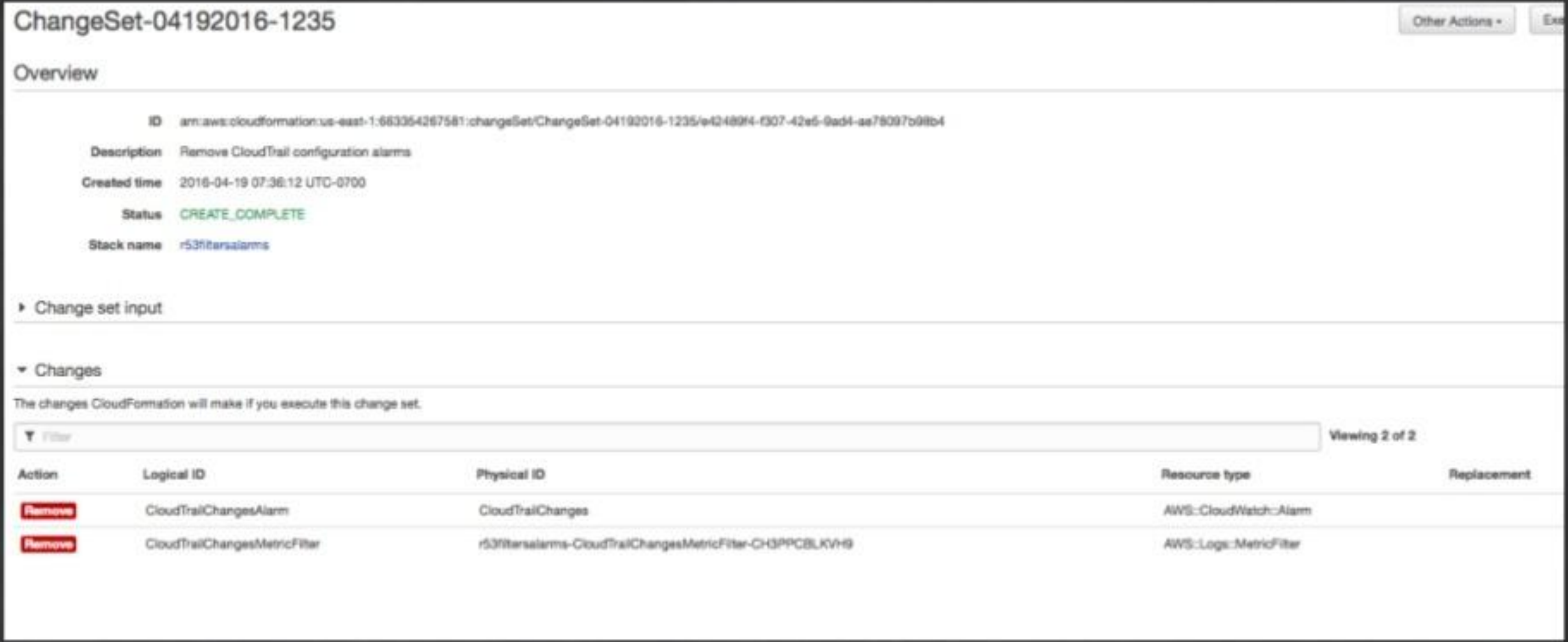
Overview

ID	arn:aws:cloudformation:us-east-1:663354267581:changeSet/ChangeSet-04192016-1234/a3a32a98-ea9f-46ae-a9fc-0d9e4b9eb075
Description	Add IAM policy changes
Created time	2016-04-19 07:13:31 UTC-0700
Status	CREATE_COMPLETE
Stack name	r53filtersalarms

The changes CloudFormation will make if you execute this change set.

Action	Logical ID	Physical ID	Resource type	Replacement
Add	IAMPolicyChangesAlarm		AWS::CloudWatch::Alarm	
Add	IAMPolicyMetricFilter		AWS::Logs::MetricFilter	

Change Sets



ChangeSet-04192016-1235

Overview

ID	arn:aws:cloudformation:us-east-1:683354267581:changeSet/ChangeSet-04192016-1235/e42489f4-f307-42e5-9ad4-aa78097b98b4
Description	Remove CloudTrail configuration alarms
Created time	2016-04-19 07:36:12 UTC-0700
Status	CREATE_COMPLETE
Stack name	r53filtersalarms

▸ Change set input

▾ Changes

The changes CloudFormation will make if you execute this change set.

Action	Logical ID	Physical ID	Resource type	Replacement
Remove	CloudTrailChangesAlarm	CloudTrailChanges	AWS::CloudWatch::Alarm	
Remove	CloudTrailChangesMetricFilter	r53filtersalarms-CloudTrailChangesMetricFilter-CH3PPCBLKVH9	AWS::Logs::MetricFilter	

AWS Marketplace Security Partners

Infrastructure Security

- CISCO
- f5
- CiTRiX
- SOPHOS
- Barracuda
- FORTINET
- intel Security
- paloalto networks
- Check Point SOFTWARE TECHNOLOGIES LTD We Secure the Internet
- IMPERVA

Logging & Monitoring

- ALERTLOGIC Security Compliance Cloud
- splunk>
- sumologic
- CloudPassage
- loggly

Identity & Access Control

- okta
- CIPHERGRAPH networks
- Elastic SSO
- conjur
- onelogin

Configuration & Vulnerability Analysis

- QUALYSGUARD
- TREND MICRO
- tenable network security
- RAPID7
- evident.io

Data Protection

- gemalto security to be free
- Vormetric Data Security Simplified
- HYTRUST Cloud Under Control
- KeyNexus
- Townsend SECURITY
- druva

Security is a service team, not a blocker

Security is everyone's job

Allow flexibility and freedom
but control the flow and result.

aws | Pop-up Loft

THANK YOU!