



Getting Started with AWS Security

Rahul Sareen
Sr. Consultant, AWS Professional Services

September 28th, 2016



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**

Understand AWS Security Practice

Why is Enterprise Security Traditionally Hard?



Lack of visibility



Low degree of automation

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

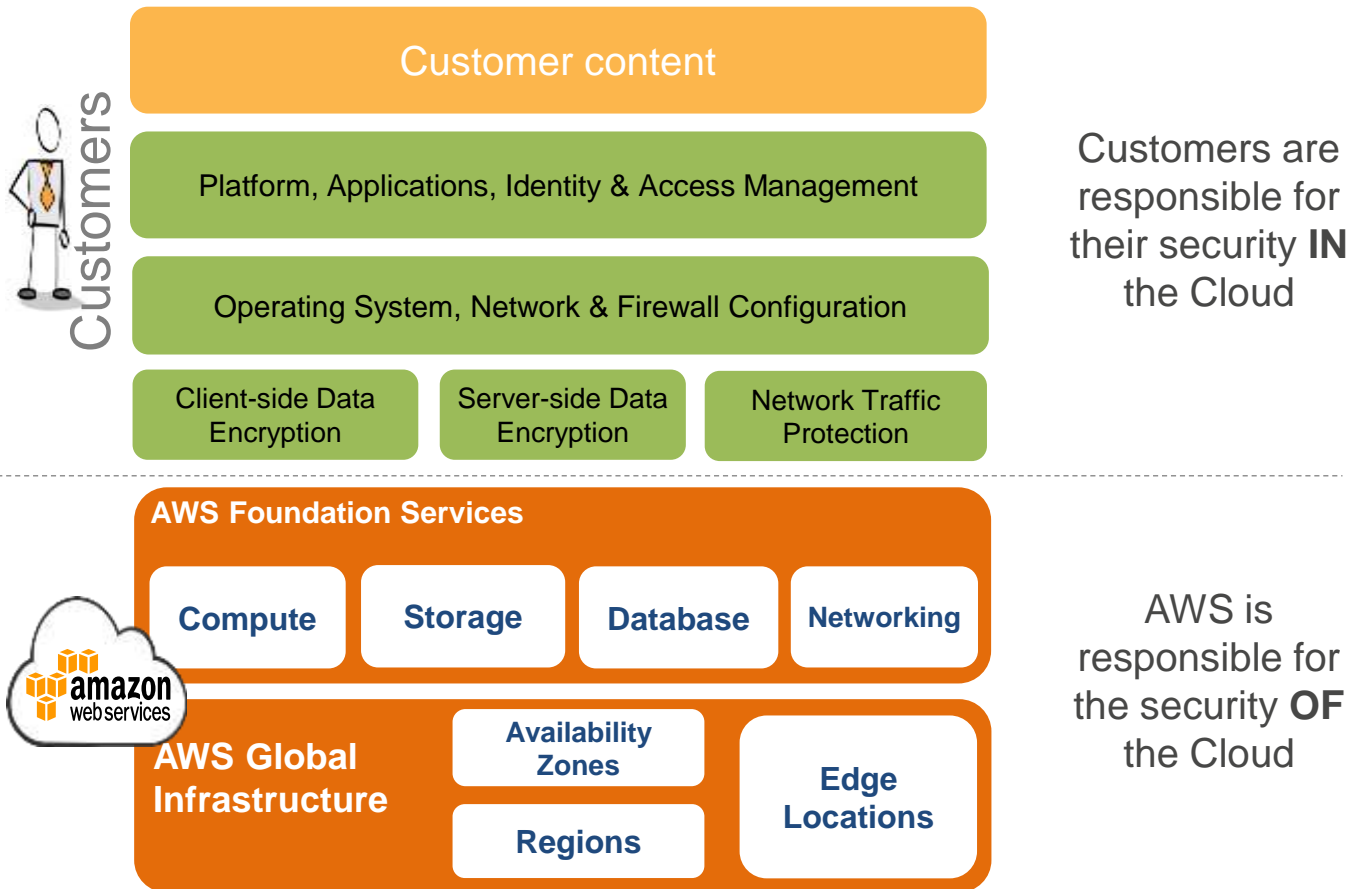


Benefit from AWS industry leading
security teams 24/7, 365 days a year

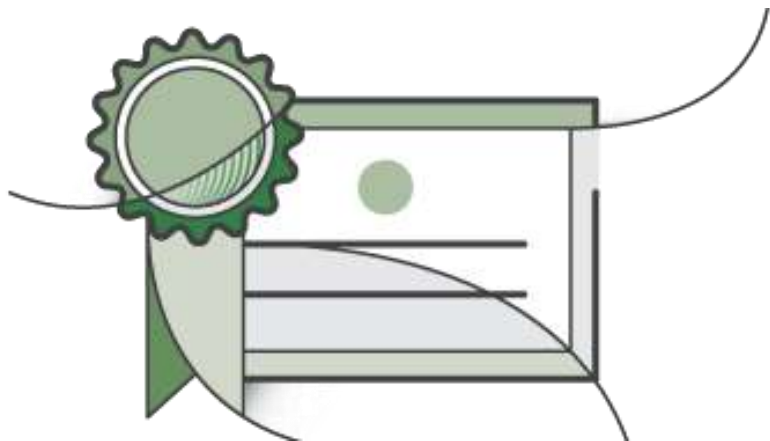


Leverage security enhancements gleaned
from 1M+ customer experiences

Security is a shared responsibility



Security Training



Security Fundamentals on AWS

(Free online course)

Security Operations on AWS

(3-day class)

Details at aws.amazon.com/training

Build Strong Compliance Foundations

AWS Assurance Programs



FISMA



AWS maintains a formal control environment

- SOC 1 Type II
- SOC 2 Type II and public SOC 3 report
- ISO 27001, 27017, 27018 Certification
- Certified PCI DSS Level 1 Service Provider
- FedRAMP Authorization
- Architect for HIPAA compliance

AWS Account Relationship



AWS Account
Ownership



AWS Account
Contact
Information



AWS Sales
AWS Solutions Architects
AWS Support
AWS Professional Services
AWS Consulting Partners

AWS Trusted Advisor



AWS Trusted
Advisor



Integrate Identity & Access Management

AWS Identity & Access Management



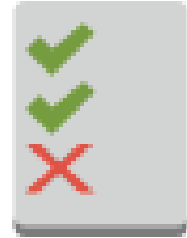
IAM Users



IAM Groups



IAM Roles



IAM Policies



Dashboard

Search IAM

Details

Groups

Users

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

Welcome to Identity and Access Management

IAM users sign-in link:

<https://rahulsareen.signin.aws.amazon.com/console>[Customize](#) | [Copy Link](#)

IAM Resources

Users: 3

Roles: 35

Groups: 3

Identity Providers: 0

Customer Managed Policies: 6

Security Status

 4 out of 5 complete.☒ Activate MFA on your root account☒ Create individual IAM users☒ Use groups to assign permissions☒ Apply an IAM password policy☐ Rotate your access keys

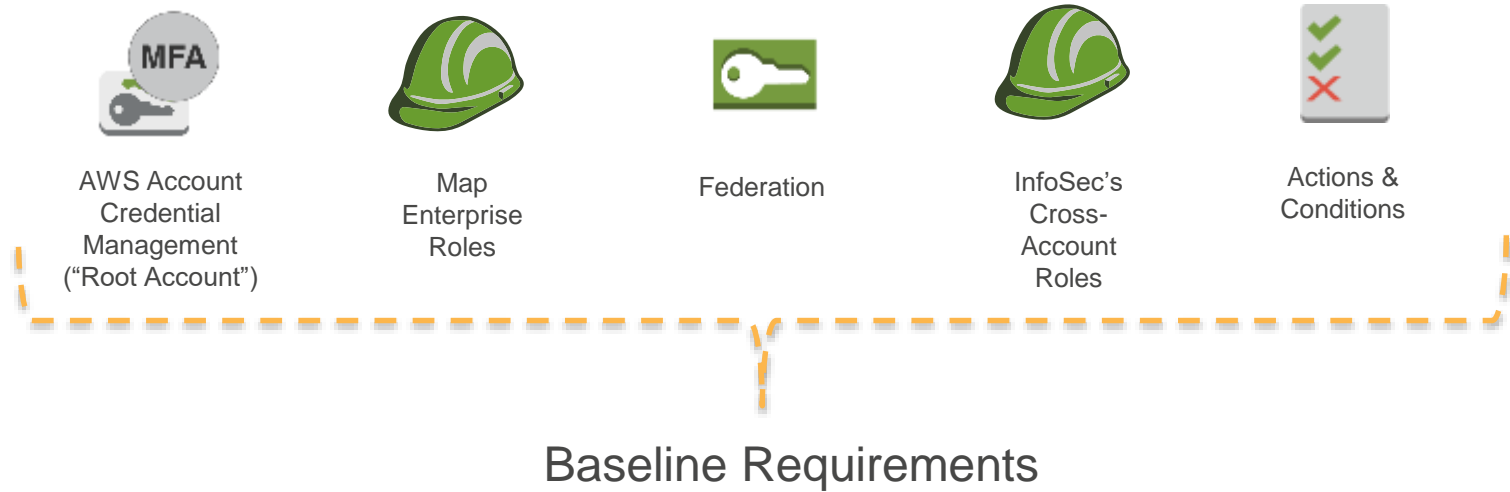
Feature Spotlight



Additional Information

[IAM documentation](#)[Web Identity Federation
Playground](#)[Policy Simulator](#)[Videos, IAM release history and
additional resources](#)

Account Governance – New Accounts



Enable Detective Controls

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

Establish Network Security

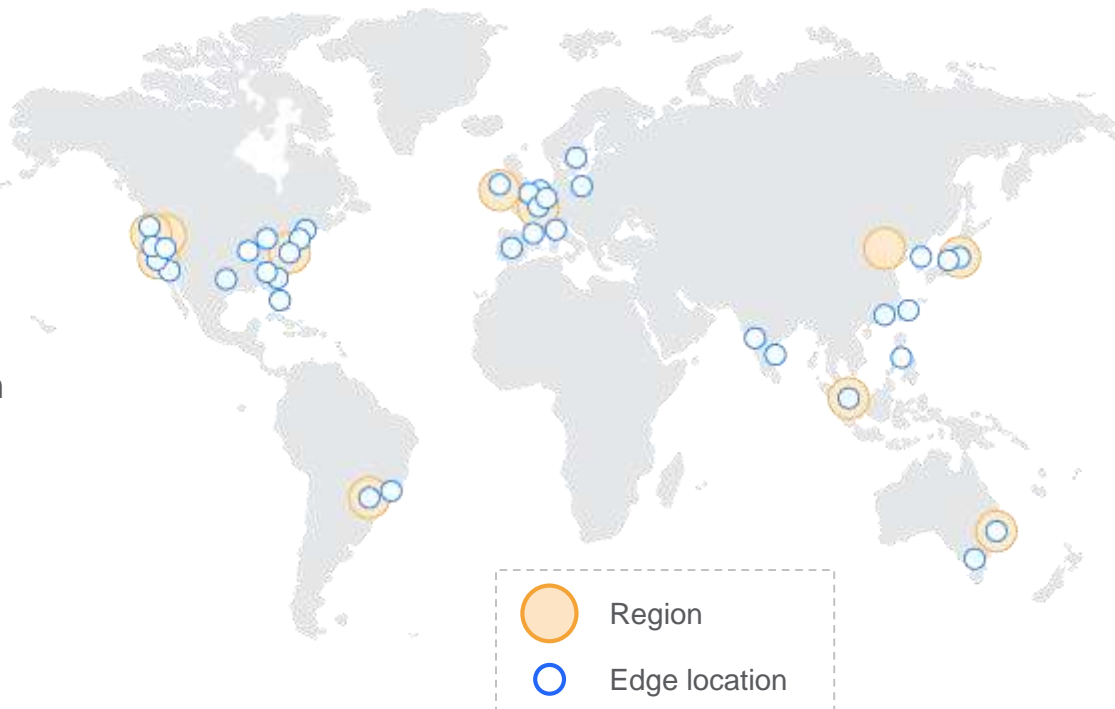
AWS Global Footprint

13 Regions (11 Public, China Region and GovCloud Region)

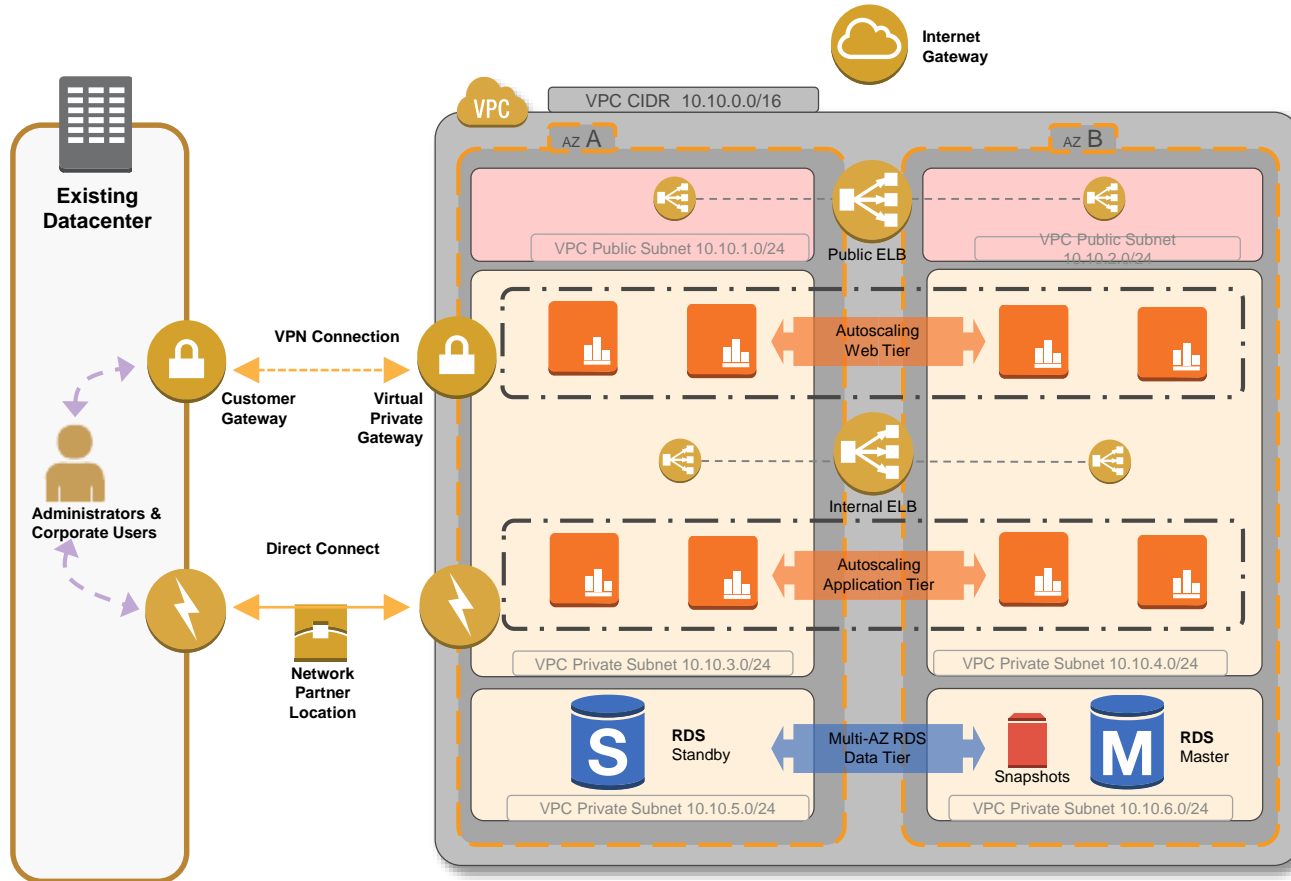
Canada, Ohio, UK and another China Region planned for 2016 and beyond

32+ Availability zones (adding more in 2016 across new Regions)

55+ Edge locations

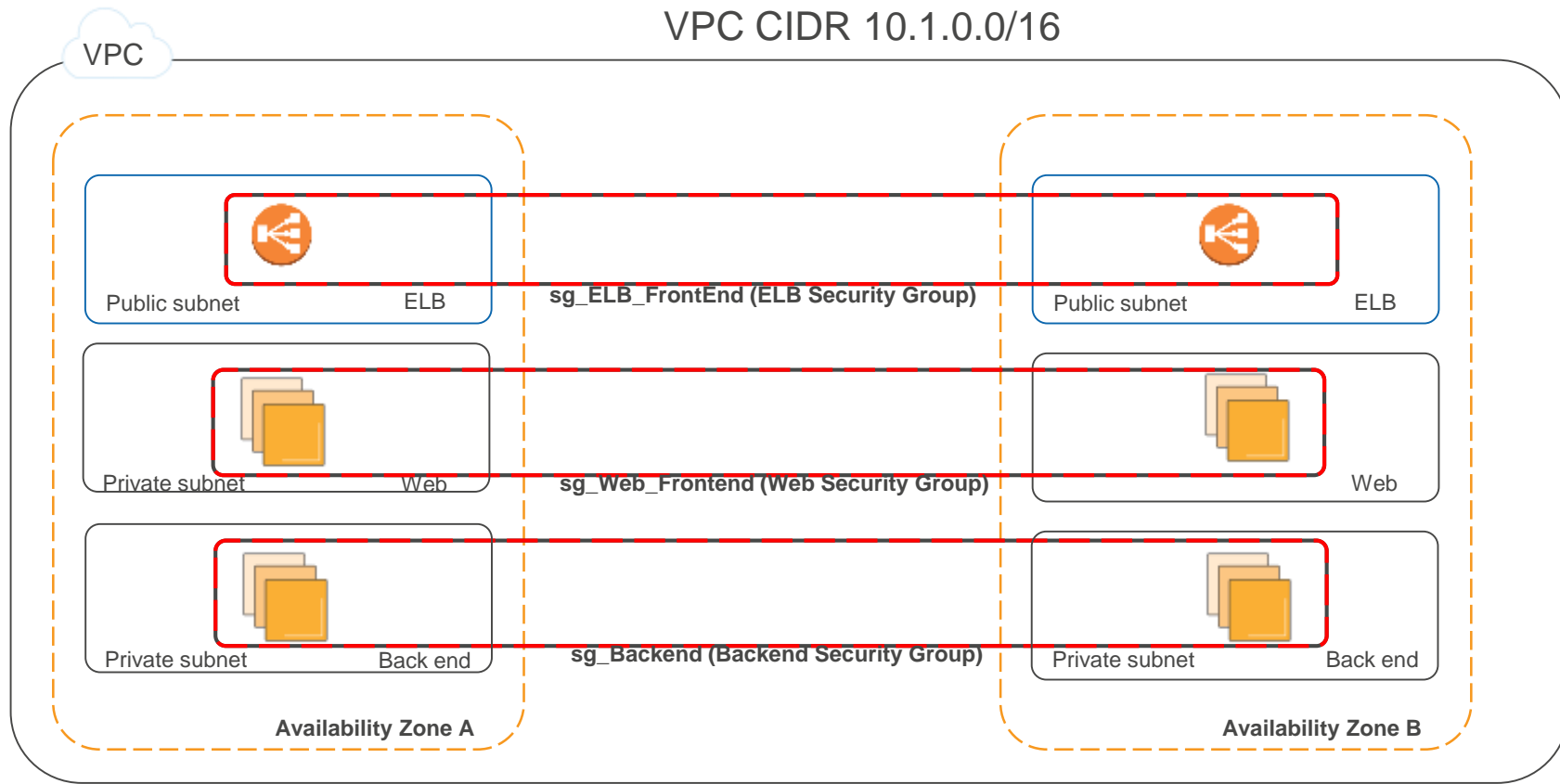


Amazon Virtual Private Cloud



Security Groups

VPC CIDR 10.1.0.0/16



Security Groups

VPC Dashboard

Filter by VPC:

None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

DHCP Options Sets

Create Security Group

Delete Security Group

Filter VPC security groups

sg_

X

<input type="checkbox"/>	Name tag	Group ID	Group Name	VPC	Description
<input type="checkbox"/>	sg_ELB_FrontEnd	sg-9142e0f7	sg_ELB_FrontEnd	vpc-9df15bf9 (10.50.0.0/16...	ELB Security Group
<input type="checkbox"/>	sg_Backend	sg-3e40e258	sg_Backend	vpc-9df15bf9 (10.50.0.0/16...	Backend Security Group
<input type="checkbox"/>	sg_Web_Frontend	sg-7640e210	sg_Web_Frontend	vpc-9df15bf9 (10.50.0.0/16...	Web Security Group

Security Groups

Filter VPC security groups

<input type="checkbox"/>	Name tag	Group ID	Group Name	VPC	Description
<input checked="" type="checkbox"/>	sg_ELB_FrontEnd	sg-9142e0f7	sg_ELB_FrontEnd	vpc-9df15bf9	ELB Security Group
<input type="checkbox"/>	sg_Backend	sg-3e40e258	sg_Backend	vpc-9df15bf9 (10.50.0.0/16...	Backend Security Group
<input type="checkbox"/>	sg_Web_Frontend	sg-7640e210	sg_Web_Frontend	vpc-9df15bf9	Web Security Group

sg-9142e0f7 | sg_ELB_FrontEnd

Summary

Inbound Rules

Outbound Rules

Tags

Edit

Type	Protocol	Port Range	Source
HTTP (80)	TCP (6)	80	0.0.0.0/0
HTTPS (443)	TCP (6)	443	0.0.0.0/0

Security Groups

Filter VPC security groups

<input type="checkbox"/>	Name tag	Group ID	Group Name	VPC	Description
<input type="checkbox"/>	sg_ELB_FrontEnd	sg-9142e0f7	sg_ELB_FrontEnd	vpc-9df15bf9	ELB Security Group
<input type="checkbox"/>	sg_Backend	sg-3e40e258	sg_Backend	vpc-9df15bf9 (10.50.0.0/16...	Backend Security Group
<input checked="" type="checkbox"/>	sg_Web_Frontend	sg-7640e210	sg_Web_Frontend	vpc-9df15bf9	Web Security Group

sg-7640e210 | sg_Web_Frontend

Summary Inbound Rules Outbound Rules Tags

Edit

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

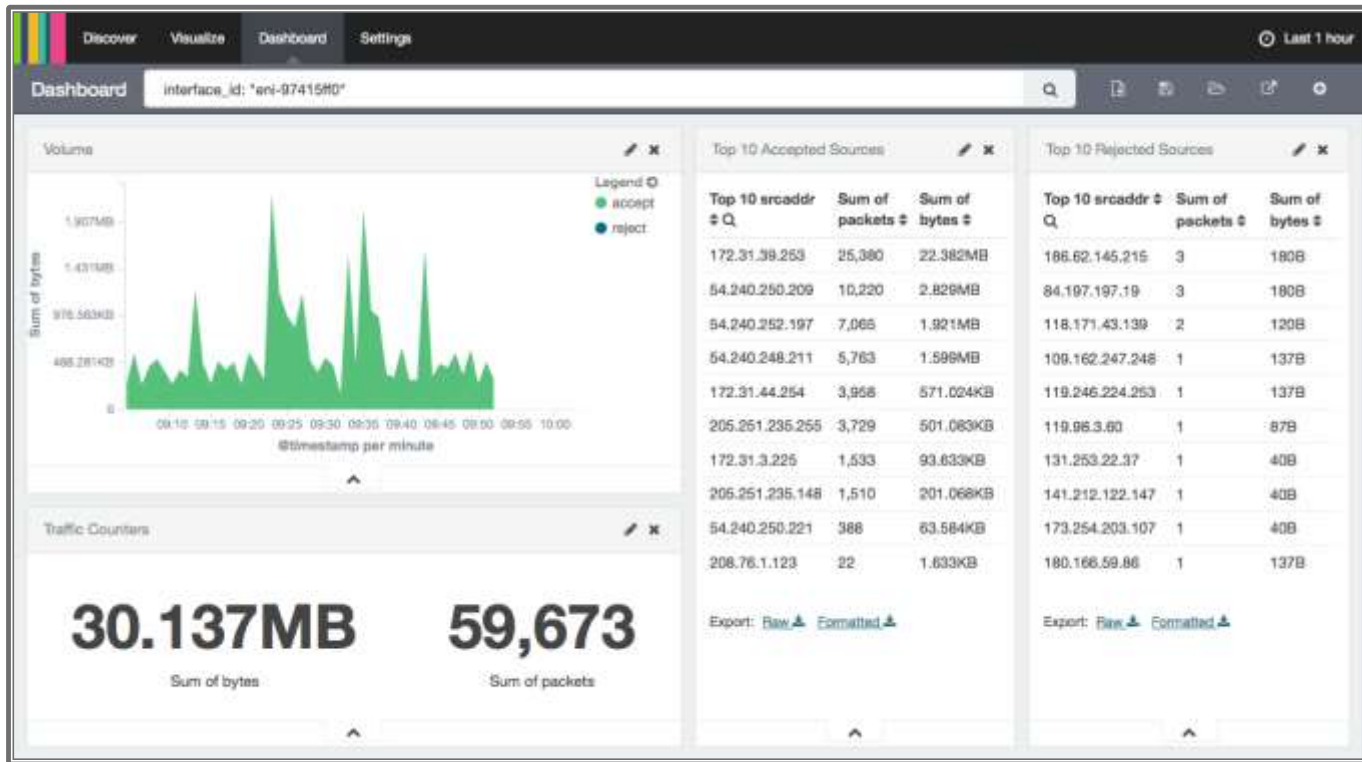
VPC Flow Logs

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

The diagram illustrates the structure of VPC Flow Log data. It features a table of event data with several fields annotated by orange arrows and labels. The labels include 'Interface', 'Source IP', 'Source port', 'Protocol', 'Packets', 'AWS account', 'Destination IP', 'Destination port', 'Bytes', 'Start/end time', and '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 1442975655 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

VPC Flow Logs



- 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 than 100 rejects

Whenever: SG-Rejected

is: \geq 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: CloudTrailNotifier

[New list](#) [Enter list](#) ⓘ

This notification list is managed in the SNS console.

+ Notification

+ AutoScaling Action

+ EC2 Action

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 \geq 100



Namespace: LogMetrics

Metric Name: SG-Rejected

Period: 15 Minutes

Statistic: Sum

Implement Data Protection

Cryptographic Services



**AWS
KMS**

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



**Amazon
CloudHSM**

- ✓ Dedicated HSM
- ✓ Integrate with on-premises HSMs
- ✓ Hybrid Architectures

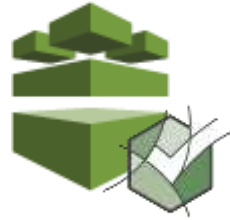
Optimize Change Management

AWS Config & Config Rules



**AWS
Config**

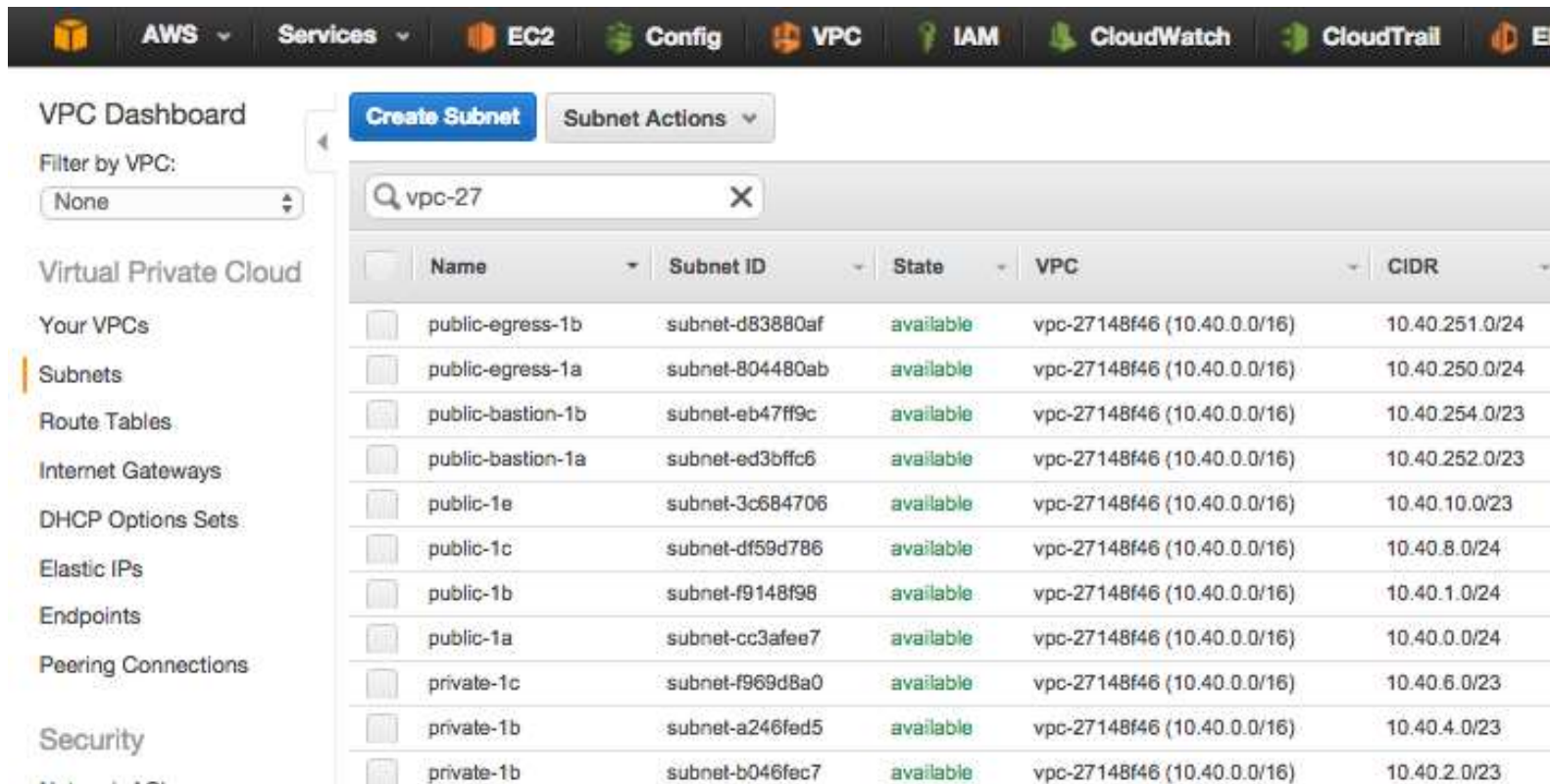
- ✓ Record configuration changes continuously
- ✓ Time-series view of resource changes
- ✓ Archive & Compare



**Amazon
Config
Rules**

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

AWS Config



The screenshot displays the AWS VPC Dashboard. The top navigation bar includes icons and labels for AWS, Services, EC2, Config, VPC, IAM, CloudWatch, and CloudTrail. On the left, the 'VPC Dashboard' sidebar is visible, with 'Subnets' selected under the 'Virtual Private Cloud' section. The main content area shows a 'Create Subnet' button and a 'Subnet Actions' dropdown. A search bar contains 'vpc-27'. Below the search bar is a table listing subnets associated with VPC vpc-27148f46 (10.40.0.0/16). The table has columns for Name, Subnet ID, State, VPC, and CIDR. All subnets listed are in an 'available' state.

Name	Subnet ID	State	VPC	CIDR
public-egress-1b	subnet-d83880af	available	vpc-27148f46 (10.40.0.0/16)	10.40.251.0/24
public-egress-1a	subnet-804480ab	available	vpc-27148f46 (10.40.0.0/16)	10.40.250.0/24
public-bastion-1b	subnet-eb47ff9c	available	vpc-27148f46 (10.40.0.0/16)	10.40.254.0/23
public-bastion-1a	subnet-ed3bffc6	available	vpc-27148f46 (10.40.0.0/16)	10.40.252.0/23
public-1e	subnet-3c684706	available	vpc-27148f46 (10.40.0.0/16)	10.40.10.0/23
public-1c	subnet-df59d786	available	vpc-27148f46 (10.40.0.0/16)	10.40.8.0/24
public-1b	subnet-f9148f98	available	vpc-27148f46 (10.40.0.0/16)	10.40.1.0/24
public-1a	subnet-cc3afee7	available	vpc-27148f46 (10.40.0.0/16)	10.40.0.0/24
private-1c	subnet-f969d8a0	available	vpc-27148f46 (10.40.0.0/16)	10.40.6.0/23
private-1b	subnet-a246fed5	available	vpc-27148f46 (10.40.0.0/16)	10.40.4.0/23
private-1b	subnet-b046fec7	available	vpc-27148f46 (10.40.0.0/16)	10.40.2.0/23

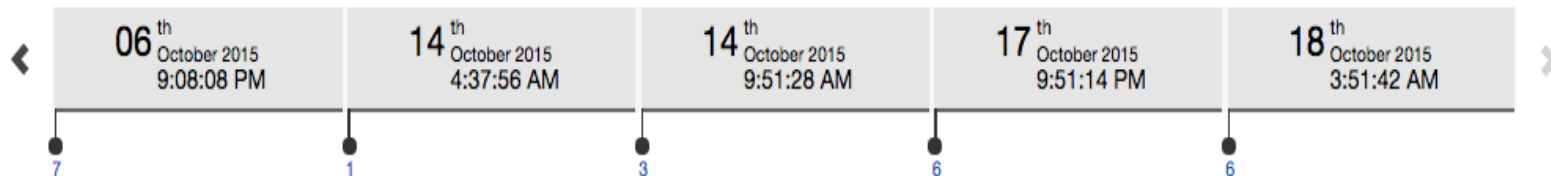
AWS Config



AWS Config

EC2 VPC vpc-27148f46

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



▼ Configuration Details

AWS Config Rules – Tenancy Enforcement Example

Trigger

AWS Config evaluates resources when the trigger occurs.

Trigger type* ☒ Configuration changes ☐ Periodic ⓘ

Scope of changes* ☒ Resources ☐ Tags ☐ All changes ⓘ

Resources*

EC2: Instance ✕

Resource identifier (optional)

This rule can be triggered only when recorded resources are created, changed, or deleted. Specify which resources are recorded on the Settings page.



Rule parameters

Rule parameters define attributes for which your resources are evaluated; for example, a required tag or S3 bucket.


Key	Value	
desiredTenancyType	dedicated	✕
Key	Value	



AWS Config Rules – Tenancy Enforcement Example

HIPAA-dedicatedTenancy

Description	Ensure that instances are running in Dedicated Tenancy
Trigger type	Configuration changes
Scope of changes	Resources
Resource types	EC2 Instance
Config rule ARN	arn:aws:config:us-east-1:663354267581:config-rule/config-rule-qq8nj7
Parameters	desiredTenancyType: dedicated
Rule status	Last successful invocation at Feb 8 8:51 PM 
	Last successful evaluation at Feb 8 8:51 PM 

Resources evaluated

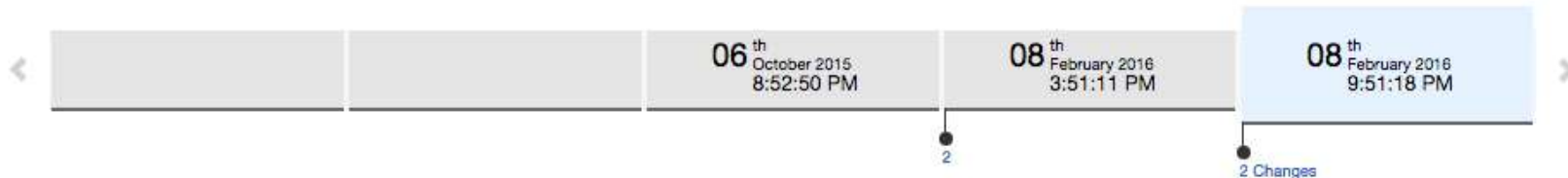
Click on the  icon to view configuration details for the resource when it was last evaluated with this rule.

Resource type	Resource identifier	Compliance	Config timeline
EC2 Instance	i-0ae51ca8	Noncompliant	
EC2 Instance	i-0e9b60da	Noncompliant	
EC2 Instance	i-15e969c7	Noncompliant	
EC2 Instance	i-2565a487	Noncompliant	
EC2 Instance	i-2f3438f8	Noncompliant	
EC2 Instance	i-50e79ca1	Noncompliant	
EC2 Instance	i-a03dfc02	Noncompliant	
EC2 Instance	i-bf16af36	Noncompliant	
EC2 Instance	i-c683db6a	Noncompliant	
EC2 Instance	i-f32e9727	Noncompliant	
EC2 Instance	i-a8bde51f	Compliant	

AWS Config Rules – Tenancy Enforcement Example

EC2 Instance i-089b60dc

at February 08, 2016 9:51:18 PM PDT (UTC-07:00)



▼ Configuration Details

Amazon Resource Name arn:aws:ec2:us-east-1:663354267581:instance/i-089b60dc

Resource type AWS::EC2::Instance

Resource ID i-089b60dc

Availability zone us-east-1b

Created at October 06, 2015 8:43:50 PM

Tags (2)

Instance Type t2.micro

Instance state running

Private DNS ip-10-40-3-32.ec2.internal

Private Ips 10.40.3.32

Public DNS null

AMI ID ami-e3106686

Platform null

Launch time 2015-10-07T03:43:50.000Z

Lifecycle null

Monitoring disabled

► Relationship

AWS Config Partners



AWS CloudFormation – Infrastructure as Code



**AWS
CloudFormation**



Template



Stack

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

- ✓ JSON-based text file describing infrastructure

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

Change Sets – Create Change Set

Create change set for r53filtersalarms stack

Select Template

Specify Details

Options

Review

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

Other Acti

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`

► Change set input

▼ Changes

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

Filter

Viewing 2 of 2

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

Change Sets

ChangeSet-04192016-1235

Other Actions ▾

Execute

Overview

ID `arn:aws:cloudformation:us-east-1:663354267581:changeSet/ChangeSet-04192016-1235/e42489f4-f307-42e5-9ad4-ae78097b98b4`

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.

Filter

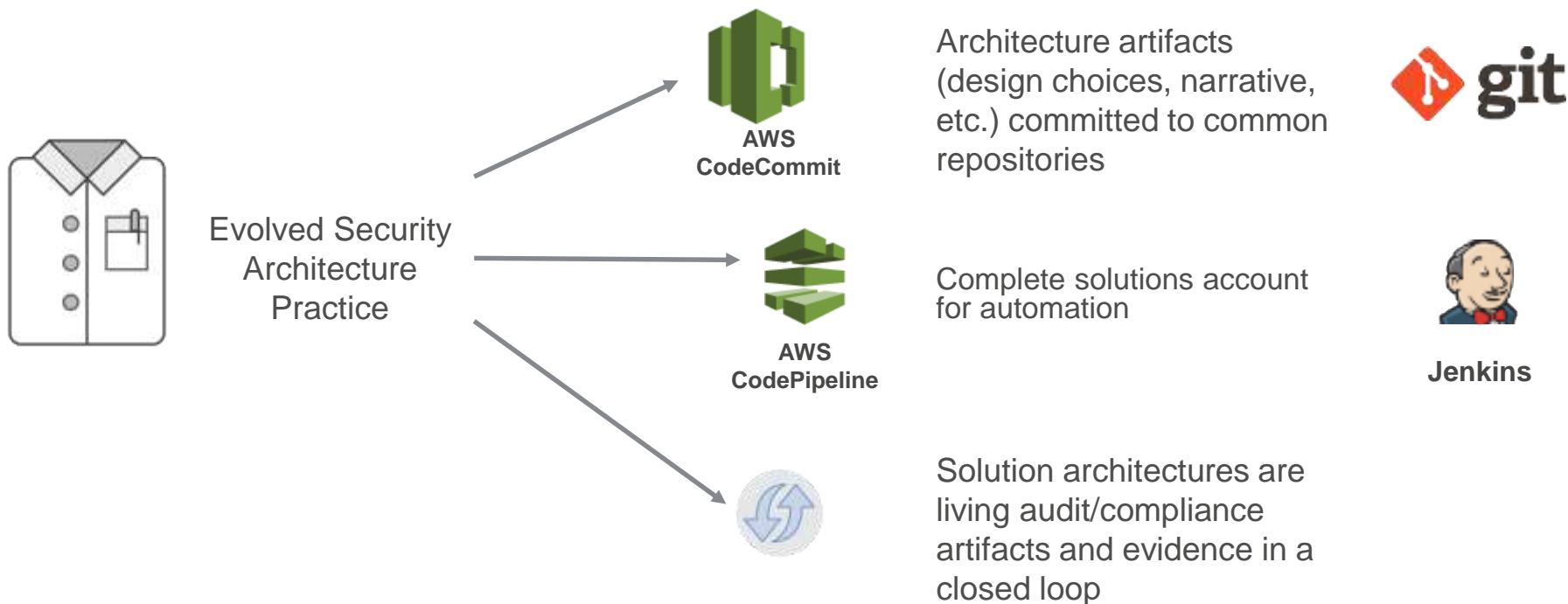
Viewing 2 of 2

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

Automate Security Functions

Evolving the Practice of Security Architecture

Security architecture can now be part of the 'maker' team



AWS Marketplace Security Partners

Infrastructure Security



Logging & Monitoring



Identity & Access Control



Configuration & Vulnerability Analysis



Data Protection



Prescriptive Approach – Get Started!



**Understand
AWS
Security
Approach**



**Build Strong
Compliance
Foundations**



**Integrate Identity
& Access
Management**



**Enable
Detective
Controls**



**Establish
Network
Security**



**Implement
Data
Protection**



**Optimize
Change
Management**



**Automate
Security
Functions**



Thank you!