



# AWS Config & AWS Config Rules

Tim Robinson – April 2019

# Inventory and Configuration Management

- Maintains a real-time inventory of cloud resources
- Maintains the current and historical configuration of cloud resources

# Inventory and Configuration Management

- What's currently out there? (Real-time resource inventory)
- What is the latest configuration state of my resources? (Configuration Snapshot)
- What relationships exist between my resources? (Resource relationships)
- What configuration changes occurred in the last 'X' days? (Configuration History)
- Which EC2 instances are built on top of a certain machine image (e.g. ami-234314)?

# Configuration Compliance Management

- Are my resources properly configured? (Best practice configuration checks)
- Do my resources comply with regulatory requirements (e.g. PCI, HIPAA etc.)
- How do I ensure continuous compliance? (check for policy violations immediately after a configuration change)
- How can I get notified in real-time if certain resources go out of compliance? (Real-time compliance change notifications)

# Summary

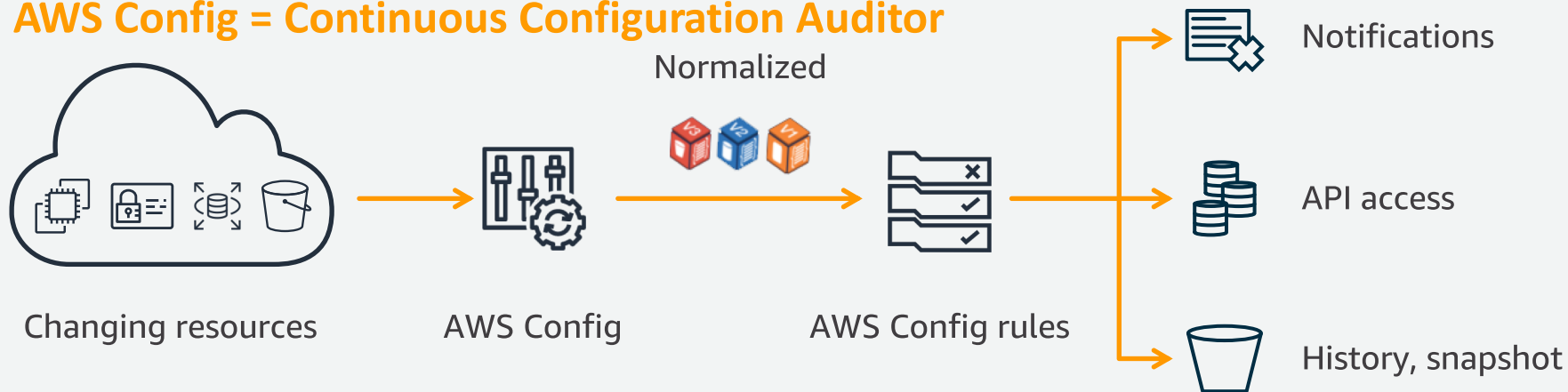
## Inventory & Configuration Management and Configuration Compliance Management

- Support governance initiatives by providing accurate configuration information to assist with decision making (for example, authorization of changes, release planning)
- Minimize the number of quality and compliance issues caused by incorrect or inaccurate configuration of services or resources

# AWS Config

- ✓ Continuously tracks resource configuration changes
- ✓ Evaluates the configuration against policies defined using AWS Config rules
- ✓ Alerts you if the configuration is noncompliant with your policies using Amazon SNS and Amazon CloudWatch Events

## AWS Config = Continuous Configuration Auditor



# Common Use Cases



## **Audit & compliance**

Maintain a history of all configuration changes for audits.

Verify configuration changes do not violate policies



## **Operational governance**

DevOps compliance (e.g. remove deleted or unused resources)

Ensure configuration changes are tied to approved change requests



## **Security intelligence**

Security incident/breach analysis

Identifying vulnerable resources



## **Integration with ITSM/CMDB**

Integration with asset/inventory management systems

Change management, incident management

# Supported services: 24 AWS services and 60+ resource types



Amazon VPC



Amazon EC2



Amazon S3



Classic Load  
Balancers



Application Load  
Balancers



Amazon EBS  
volumes



AWS CloudTrail



AWS IAM



Amazon Redshift



Amazon RDS



AWS Systems  
Manager



AWS Certificate  
Manager



Amazon CloudWatch  
alarms



AWS  
CloudFormation  
stacks



Amazon DynamoDB  
tables



AWS Auto Scaling  
groups



AWS CodeBuild



AWS CodePipeline



AWS WAF



Amazon CloudFront



AWS Elastic  
Beanstalk



AWS Lambda



AWS X-Ray



AWS Shield



# Continuous assessment using AWS Config rules



Analyze configuration changes

60+ pre-built rules provided by AWS

Custom rules using AWS Lambda

GitHub repo: community sourced rules

Aggregate compliance into a central account

Compliance history

# Configuration history timeline

aws

Services

Resource Groups

★

AWS Config > resources > myProdVPC1-rSecurityGroupSSHFromProd-1MNK0D85JSVIC > configuration

EC2 SecurityGroup sg-02096173

on October 28, 2017 3:31:17 PM Pacific Standard Time (UTC-08:00)

Configuration timeline

Compliance timeline

<

10<sup>th</sup> July 2017

10:40:31 AM

28<sup>th</sup> October 2017

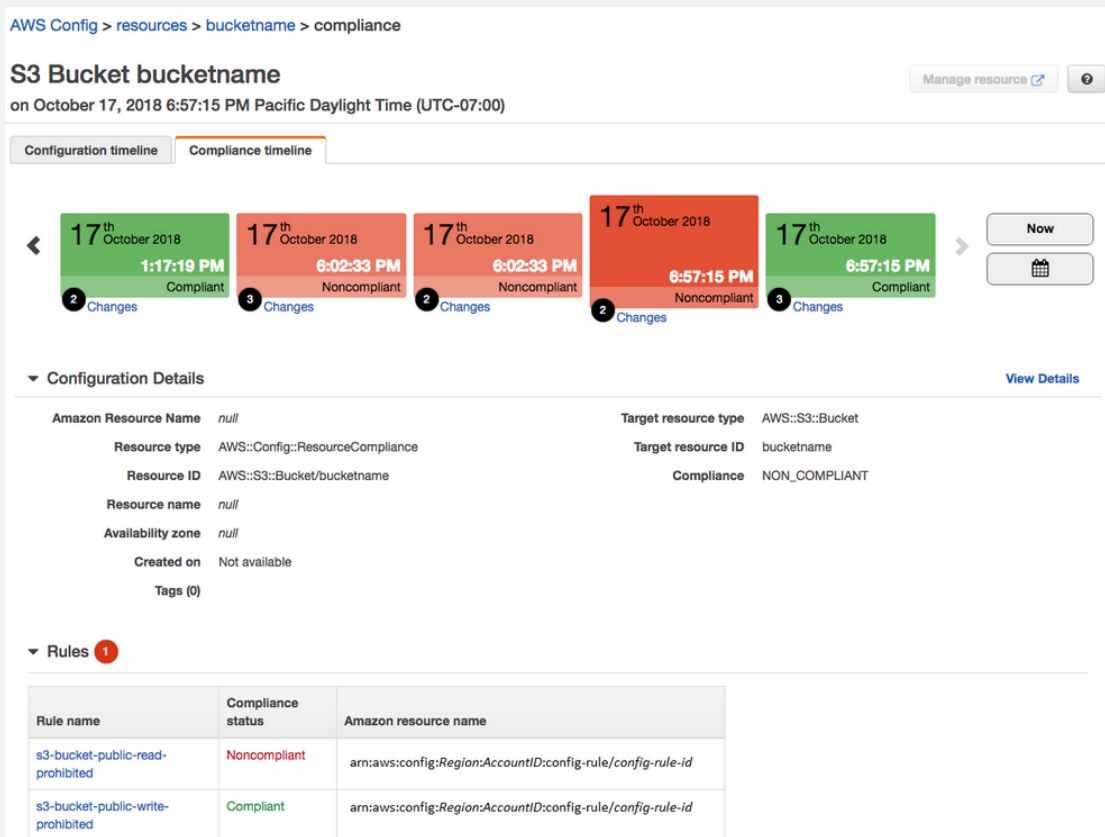
3:31:17 PM

2 Changes

▼ Configuration Details

Amazon Resource Name	arn:aws:ec2:us-east-1:899668315585:security-group/sg-02096173	Group name	myProdVPC1-rSecurityG
Resource type	AWS::EC2::SecurityGroup	Group description	Enable SSH access via
Resource ID	sg-02096173		
Resource name	myProdVPC1-rSecurityGroupSSHFromProd-1MNK0D85JSVIC		
Availability zone	Not Applicable		
Created on	Not available		
Tags (6)	<div>aws.cloudfo...aws.cloudfo...Environmen...aws.cloudfo...Criticality:Hi...Name:sg-en...</div>		
			<pre>▼ prefixListIds: Array [0] [] toPort: 22 ▼ userIdGroupPairs: Array [0] [] ▼ ipv4Ranges: Array [1] ▼ 0: Object   cidrIp: "0.0.0.0/0" ▼ ipRanges: Array [1]   0: "0.0.0.0/0"</pre>
Configuration.IpPermissions.0	<pre>▼ Object   fromPort: 22   ipProtocol: "tcp"   ▼ ipv6Ranges: Array [0]     []   ▼ prefixListIds: Array [0]     []   toPort: 22   ▼ userIdGroupPairs: Array [0]     []   ▼ ipv4Ranges: Array [1]   ▼ 0: Object     cidrIp: "10.100.0.0/16"   ▼ ipRanges: Array [1]     0: "10.100.0.0/16"</pre>		

# Compliance history timeline



# Demo

# AWS Config dashboard

## AWS Config

### Dashboard

[Rules](#)[Resources](#)[Settings](#)[What's new 2](#)










### Learn More

[Documentation](#)[Partners](#)[Pricing](#)[FAQs](#)

### Resources

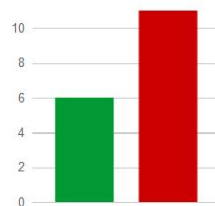
Total resources 200

Top 10 resource types Total

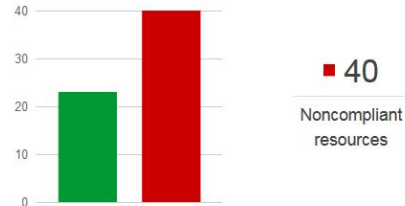
 CloudWatch Alarm	38
 RDS DBSnapshot	26
 EC2 SecurityGroup	25
 EC2 NetworkInterface	18
 S3 Bucket	17
 EC2 Subnet	16
 EC2 RouteTable	12
 EC2 NetworkAcl	8
 EC2 Volume	7
 EC2 EIP	5

[View all 200 resources](#)

### Config rule compliance



### Resource compliance



### Top 5 noncompliant rules

Rule name	Compliance
<a href="#">s3-bucket-ssl-requests-only</a>	14 noncompliant resource(s)
<a href="#">s3-bucket-logging-enabled</a>	13 noncompliant resource(s)
<a href="#">restricted-ssh</a>	12 noncompliant resource(s)
<a href="#">s3-bucket-versioning-enabled</a>	9 noncompliant resource(s)
<a href="#">encrypted-volumes</a>	4 noncompliant resource(s)

[View all 11 noncompliant rules](#)

# Useful links

## Product Documentation:

<https://docs.aws.amazon.com/config/latest/developerguide/getting-started.html>

<https://docs.aws.amazon.com/config/latest/developerguide/aggregate-data.html>

<https://docs.aws.amazon.com/config/latest/developerguide/resource-config-reference.html>

<https://aws.amazon.com/config/partners/>

## Blogs:

<https://aws.amazon.com/blogs/aws/aws-config-update-aggregate-compliance-data-across-accounts-regions/>

<https://aws-blogs-prod.amazon.com/mt/aws-config-best-practices/>

<https://aws.amazon.com/blogs/mt/how-to-query-your-aws-resource-configuration-states-using-aws-config-and-amazon-athena/>