
AWS Config

Developer Guide



AWS Config: Developer Guide

Copyright © 2017 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What Is AWS Config?	1
Ways to Use AWS Config	1
Resource Administration	1
Auditing and Compliance	2
Managing and Troubleshooting Configuration Changes	2
Security Analysis	2
Concepts	2
AWS Config Rules	3
AWS Resources	3
Configuration History	3
Configuration Items	3
Configuration Recorder	3
Configuration Snapshot	4
Configuration Stream	4
Resource Relationship	4
How Does AWS Config Work?	4
Deliver Configuration Items	5
Supported Resources, Configuration Items, and Relationships	6
Supported AWS Resource Types	7
Recording software configuration for managed instances	8
Components of a Configuration Item	6
Supported Resource Relationships	11
Getting Started	16
Signing up for AWS	16
Setting up AWS Config with the Console	17
Setting Up AWS Config Rules with the Console	19
Setting up AWS Config with the AWS CLI	20
Prerequisites	20
Turning on AWS Config	23
Verify that AWS Config Is On	24
Evaluating Resources With Rules	26
Specifying Triggers for AWS Config Rules	27
Trigger types	27
Example rules with triggers	27
Rule evaluations when the configuration recorder is turned off	28
About AWS Managed Config Rules	28
AWS Managed Config Rules	29
Working with AWS Managed Rules	46
Creating AWS Config Managed rules with AWS CloudFormation templates	47
Developing Custom Rules for AWS Config	48
Getting Started with Custom Rules	49
Developing a Custom Rule	51
Example Functions and Events	54
Viewing Configuration Compliance	62
Managing your AWS Config Rules	64
Using the Console	65
Using the AWS CLI	66
Using the AWS Config API	68
Deleting Evaluation Results	68
Manually Evaluate your Resources	68
Evaluating your Resources	68
Deleting Evaluation Results	69
Viewing AWS Resource Configurations and History	71
Looking Up Discovered Resources	71

Looking Up Resources (AWS Config Console)	71
Looking Up Resources (AWS CLI)	72
Looking up Resources (AWS Config API)	72
Viewing Configuration Details in the Console	73
View Configuration Details Using the CLI	74
View Configuration History	74
Deliver Configuration Snapshot	75
Example Amazon EBS Configuration History	77
Example Configuration Snapshot	79
Notifications that AWS Config sends	83
Monitoring Resource Changes by Email	84
Example Configuration Item Change Notifications	87
Example Configuration History Delivery Notification	95
Example Configuration Snapshot Delivery Started Notification	95
Example Configuration Snapshot Delivery Notification	96
Example Compliance Change Notification	97
Example Rules Evaluation Started Notification	98
Example Oversized Configuration Item Change Notification	98
Example Delivery Failed Notification	99
Using Amazon SQS to Monitor Resource Changes	101
Permissions for Amazon SQS	101
Managing	103
Managing the Delivery Channel	103
Updating the Delivery Channel	103
Renaming the Delivery Channel	105
Updating the IAM Role	106
Updating the IAM Role	106
Managing the Configuration Recorder	107
Managing the Configuration Recorder (Console)	107
Managing the Configuration Recorder (AWS CLI)	108
Selecting Which Resources are Recorded	109
Recording All Supported Resource Types	109
Recording Specific Resource Types	109
Selecting Resources (Console)	109
Selecting Resources (AWS CLI)	110
Permissions	113
Permissions for the IAM Role	113
Creating IAM Role Policies	113
Troubleshooting for recording S3 buckets	115
Permissions for the Amazon S3 Bucket	116
Required permissions for an Amazon S3 bucket in another account	116
Granting AWS Config access to an Amazon S3 bucket in another account	116
Permissions for the Amazon SNS Topic	117
Permissions for Users	118
Example policies	119
Logging API Calls	122
AWS Config Information in CloudTrail	122
Understanding AWS Config Log File Entries	123
DeleteDeliveryChannel	123
DeliverConfigSnapshot	123
DescribeConfigurationRecorderStatus	124
DescribeConfigurationRecorders	124
DescribeDeliveryChannels	125
GetResourceConfigHistory	125
PutConfigurationRecorder	126
PutDeliveryChannel	127
StartConfigurationRecorder	127

StopConfigurationRecorder	128
Resources	129
AWS Software Development Kits for AWS Config	129
Document History	131
AWS Glossary	139

What Is AWS Config?

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

An AWS *resource* is an entity you can work with in AWS, such as an Amazon Elastic Compute Cloud (EC2) instance, an Amazon Elastic Block Store (EBS) volume, a security group, or an Amazon Virtual Private Cloud (VPC), for example. For a complete list of AWS resources supported by AWS Config, see [Supported AWS Resource Types](#) (p. 7).

With AWS Config, you can do the following:

- Evaluate your AWS resource configurations for desired settings.
- Get a snapshot of the current configurations of the supported resources that are associated with your AWS account.
- Retrieve configurations of one or more resources that exist in your account.
- Retrieve historical configurations of one or more resources.
- Receive a notification whenever a resource is created, modified, or deleted.
- View relationships between resources. For example, you might want to find all resources that use a particular security group.

Ways to Use AWS Config

When you run your applications on AWS, you usually use AWS resources, which you must create and manage collectively. As the demand for your application keeps growing, so does your need to keep track of your AWS resources. AWS Config is designed to help you oversee your application resources in the following scenarios:

Resource Administration

To exercise better governance over your resource configurations and to detect resource misconfigurations, you need fine-grained visibility into what resources exist and how these resources are configured at any

time. You can use AWS Config to notify you whenever resources are created, modified, or deleted without having to monitor these changes by polling the calls made to each resource.

You can use AWS Config rules to evaluate the configuration settings of your AWS resources. When AWS Config detects that a resource violates the conditions in one of your rules, AWS Config flags the resource as noncompliant and sends a notification. AWS Config continuously evaluates your resources as they are created, changed, or deleted.

Auditing and Compliance

You might be working with data that requires frequent audits to ensure compliance with internal policies and best practices. To demonstrate compliance, you need access to the historical configurations of your resources. This information is provided by AWS Config.

Managing and Troubleshooting Configuration Changes

When you use multiple AWS resources that depend on one another, a change in the configuration of one resource might have unintended consequences on related resources. With AWS Config, you can view how the resource you intend to modify is related to other resources and assess the impact of your change.

You can also use the historical configurations of your resources provided by AWS Config to troubleshoot issues and to access the last known good configuration of a problem resource.

Security Analysis

To analyze potential security weaknesses, you need detailed historical information about your AWS resource configurations, such as the AWS Identity and Access Management (IAM) permissions that are granted to your users, or the Amazon EC2 security group rules that control access to your resources.

You can use AWS Config to view the IAM policy that was assigned to an IAM user, group, or role at any time in which AWS Config was recording. This information can help you determine the permissions that belonged to a user at a specific time: for example, you can view whether the user `John Doe` had permission to modify Amazon VPC settings on Jan 1, 2015.

You can also use AWS Config to view the configuration of your EC2 security groups, including the port rules that were open at a specific time. This information can help you determine whether a security group blocked incoming TCP traffic to a specific port.

Concepts

Understanding the basic components of AWS Config will help you get the most out of this service.

Contents

- [AWS Config Rules \(p. 3\)](#)
- [AWS Resources \(p. 3\)](#)
- [Configuration History \(p. 3\)](#)
- [Configuration Items \(p. 3\)](#)
- [Configuration Recorder \(p. 3\)](#)
- [Configuration Snapshot \(p. 4\)](#)
- [Configuration Stream \(p. 4\)](#)

- [Resource Relationship \(p. 4\)](#)

AWS Config Rules

An AWS Config rule represents your desired configuration settings for specific AWS resources or for an entire AWS account. AWS Config provides customizable, predefined rules to help you get started. You can also create custom rules. While AWS Config continuously tracks your resource configuration changes, it checks whether these changes violate any of the conditions in your rules. If a resource violates a rule, AWS Config flags the resource and the rule as noncompliant, and AWS Config notifies you through Amazon SNS. For more information, see [Evaluating Resources With AWS Config Rules \(p. 26\)](#).

AWS Resources

AWS resources are entities that you create and manage using the AWS Management Console, the AWS Command Line Interface (CLI), the AWS SDKs, or AWS partner tools. Examples of AWS resources include Amazon EC2 instances, security groups, Amazon VPCs, and Amazon Elastic Block Store. AWS Config refers to each resource using its unique identifier, such as the resource ID or an [Amazon Resource Name \(ARN\)](#). For details, see [Supported AWS Resource Types \(p. 7\)](#).

Configuration History

A configuration history is a collection of the configuration items for a given resource over any time period. A configuration history can help you answer questions about, for example, when the resource was first created, how the resource has been configured over the last month, and what configuration changes were introduced yesterday at 9 AM. The configuration history is available to you in multiple formats. AWS Config automatically delivers a configuration history file for each resource type that is being recorded to an Amazon S3 bucket that you specify. You can select a given resource in the AWS Config console and navigate to all previous configuration items for that resource using the timeline. Additionally, you can access the historical configuration items for a resource from the API.

Configuration Items

A *configuration item* represents a point-in-time view of the various attributes of a supported AWS resource that exists in your account. The components of a configuration item include metadata, attributes, relationships, current configuration, and related events. AWS Config creates a configuration item whenever it detects a change to a resource type that it is recording. For example, if AWS Config is recording Amazon S3 buckets, AWS Config creates a configuration item whenever a bucket is created, updated, or deleted.

For details, see [Components of a Configuration Item \(p. 6\)](#).

Configuration Recorder

The configuration recorder stores the configurations of the supported resources in your account as configuration items. You must first create and then start the configuration recorder before you can start recording. You can stop and restart the configuration recorder at any time. For more information, see [Managing the Configuration Recorder \(p. 107\)](#).

By default, the configuration recorder records all supported resources in the region where AWS Config is running. You can create a customized configuration recorder that records only the resource types that you specify. For more information, see [Selecting Which Resources AWS Config Records \(p. 109\)](#).

If you use the AWS Management Console or the CLI to turn on the service, AWS Config automatically creates and starts a configuration recorder for you.

Configuration Snapshot

A configuration snapshot is a collection of the configuration items for the supported resources that exist in your account. This configuration snapshot is a complete picture of the resources that are being recorded and their configurations. The configuration snapshot can be a useful tool for validating your configuration. For example, you may want to examine the configuration snapshot regularly for resources that are configured incorrectly or that potentially should not exist. The configuration snapshot is available in multiple formats. You can have the configuration snapshot delivered to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. Additionally, you can select a point in time in the AWS Config console and navigate through the snapshot of configuration items using the relationships between the resources.

Configuration Stream

A configuration stream is an automatically updated list of all configuration items for the resources that AWS Config is recording. Every time a resource is created, modified, or deleted, AWS Config creates a configuration item and adds to the configuration stream. The configuration stream works by using an Amazon Simple Notification Service (Amazon SNS) topic of your choice. The configuration stream is helpful for observing configuration changes as they occur so that you can spot potential problems, generating notifications if certain resources are changed, or updating external systems that need to reflect the configuration of your AWS resources.

Resource Relationship

AWS Config discovers AWS resources in your account and then creates a map of relationships between AWS resources. For example, a relationship might include an Amazon EBS volume `vol-123ab45d` attached to an Amazon EC2 instance `i-a1b2c3d4` that is associated with security group `sg-ef678hk`.

For more information, see [Supported Resource Relationships \(p. 11\)](#).

How Does AWS Config Work?

When you turn on AWS Config, it first discovers the supported AWS resources that exist in your account and generates a [configuration item \(p. 3\)](#) for each resource.

AWS Config also generates configuration items when the configuration of a resource changes, and it maintains historical records of the configuration items of your resources from the time you start the configuration recorder. By default, AWS Config creates configuration items for every supported resource in the region. If you don't want AWS Config to create configuration items for all supported resources, you can specify the resource types that you want it to track.

AWS Config keeps track of all changes to your resources by invoking the Describe or the List API call for each resource in your account. The service uses those same API calls to capture configuration details for all related resources.

For example, removing an egress rule from a VPC security group causes AWS Config to invoke a Describe API call on the security group. AWS Config then invokes a Describe API call on all of the instances associated with the security group. The updated configurations of the security group (the resource) and of each instance (the related resources) are recorded as configuration items and delivered in a configuration stream to an Amazon Simple Storage Service (Amazon S3) bucket.

AWS Config also tracks the configuration changes that were not initiated by the API. AWS Config examines the resource configurations periodically and generates configuration items for the configurations that have changed.

If you are using AWS Config rules, AWS Config continuously evaluates your AWS resource configurations for desired settings. Depending on the rule, AWS Config will evaluate your resources either in response to configuration changes or periodically. Each rule is associated with an AWS Lambda function, which contains the evaluation logic for the rule. When AWS Config evaluates your resources, it invokes the rule's AWS Lambda function. The function returns the compliance status of the evaluated resources. If a resource violates the conditions of a rule, AWS Config flags the resource and the rule as noncompliant. When the compliance status of a resource changes, AWS Config sends a notification to your Amazon SNS topic.

Deliver Configuration Items

AWS Config can deliver configuration items through one of the following channels:

Amazon S3 Bucket

AWS Config tracks changes in the configuration of your AWS resources, and it regularly sends updated configuration details to an Amazon S3 bucket that you specify. For each resource type that AWS Config records, it sends a *configuration history file* every six hours. Each configuration history file contains details about the resources that changed in that six-hour period. Each file includes resources of one type, such as Amazon EC2 instances or Amazon EBS volumes. If no configuration changes occur, AWS Config does not send a file.

AWS Config sends a *configuration snapshot* to your Amazon S3 bucket when you use the [deliver-config-snapshot](#) command with the AWS CLI, or when you use the [DeliverConfigSnapshot](#) action with the AWS Config API. A configuration snapshot contains configuration details for all resources that AWS Config records in your AWS account. The configuration history file and configuration snapshot are in JSON format.

Note

AWS Config only delivers the configuration history files and configuration snapshots to the specified S3 bucket; AWS Config doesn't modify the lifecycle policies for objects in the S3 bucket. You can use lifecycle policies to specify whether you want to delete or archive objects to Amazon Glacier. For more information, see [Managing Lifecycle Configuration](#) in the *Amazon Simple Storage Service Console User Guide*. You can also see the [Archiving Amazon S3 Data to Amazon Glacier](#) blog post.

Amazon SNS Topic

An Amazon Simple Notification Service (Amazon SNS) topic is a communication channel that Amazon SNS uses to deliver messages (or *notifications*) to subscribing endpoints such as an email address or clients such as an [Amazon Simple Queue Service](#) queue. Other types of Amazon SNS notifications include push notification messages to apps on mobile phones, Short Message Service (SMS) notifications to SMS-enabled mobile phones and smart phones, and HTTP POST requests. For best results, use Amazon SQS as the notification endpoint for the SNS topic and then process the information in the notification programmatically.

AWS Config uses the Amazon SNS topic that you specify to send you notifications. The type of notification that you are receiving is indicated by the value for the `messageType` key in the message body, as in the following example:

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

The notifications can be any of the following message types:

`ComplianceChangeNotification`

The compliance type of a resource that AWS Config evaluates has changed. The compliance type indicates whether the resource complies with a specific AWS Config rule, and it is represented

by the `ComplianceType` key in the message. The message includes `newEvaluationResult` and `oldEvaluationResult` objects for comparison.

`ConfigRulesEvaluationStarted`

AWS Config started evaluating your rule against the specified resources.

`ConfigurationSnapshotDeliveryStarted`

AWS Config started delivering the configuration snapshot to your Amazon S3 bucket. The name of the Amazon S3 bucket is provided for the `s3Bucket` key in the message.

`ConfigurationSnapshotDeliveryCompleted`

AWS Config successfully delivered the configuration snapshot to your Amazon S3 bucket.

`ConfigurationSnapshotDeliveryFailed`

AWS Config failed to deliver the configuration snapshot to your Amazon S3 bucket.

`ConfigurationHistoryDeliveryCompleted`

AWS Config successfully delivered the configuration history to your Amazon S3 bucket.

`ConfigurationItemChangeNotification`

A resource has been created, deleted, or changed in configuration. This message includes the details of the configuration item that AWS Config creates for this change, and it includes the type of change. These notifications are delivered within minutes of a change and are collectively known as the *configuration stream*.

`OversizedConfigurationItemChangeNotification`

This message type is delivered when a configuration item change notification exceeded the maximum size allowed by Amazon SNS. The message includes a summary of the configuration item. You can view the complete notification in the specified Amazon S3 bucket location.

`OversizedConfigurationItemChangeDeliveryFailed`

AWS Config failed to deliver the oversized configuration item change notification to your Amazon S3 bucket.

For example notifications, see [Notifications that AWS Config sends \(p. 83\)](#).

For more information about Amazon SNS, see the [Amazon Simple Notification Service Developer Guide](#).

Supported Resources, Configuration Items, and Relationships

AWS Config supports the following AWS resources, configuration items, and resource relationships.

Contents

- [Supported AWS Resource Types \(p. 7\)](#)
- [Recording software configuration for managed instances \(p. 8\)](#)
- [Components of a Configuration Item \(p. 6\)](#)
 - [Amazon S3 Bucket Attributes \(p. 10\)](#)
- [Supported Resource Relationships \(p. 11\)](#)

Supported AWS Resource Types

AWS Config supports the following AWS resources.

AWS Service	Resource Type	resourceType Value
AWS Certificate Manager	Certificate	AWS::ACM::Certificate
AWS CloudTrail	Trail	AWS::CloudTrail::Trail
Amazon Elastic Block Store	Amazon EBS volume	AWS::EC2::Volume
Amazon Elastic Compute Cloud	EC2 Dedicated host ¹	AWS::EC2::Host
	EC2 Elastic IP (VPC only)	AWS::EC2::EIP
	EC2 instance	AWS::EC2::Instance
	EC2 network interface	AWS::EC2::NetworkInterface
	EC2 security group	AWS::EC2::SecurityGroup
Amazon EC2 Systems Manager	Managed instance inventory ²	AWS::SSM::ManagedInstanceInventory
Elastic Load Balancing	Application load balancer	AWS::ElasticLoadBalancingV2::LoadBalancer
AWS Identity and Access Management ³	IAM user ⁴	AWS::IAM::User
	IAM group ⁴	AWS::IAM::Group
	IAM role ⁴	AWS::IAM::Role
	IAM customer managed policy	AWS::IAM::Policy
Amazon Redshift	Cluster	AWS::Redshift::Cluster
	Cluster parameter group	AWS::Redshift::ClusterParameterGroup
	Cluster security group	AWS::Redshift::ClusterSecurityGroup
	Cluster snapshot	AWS::Redshift::ClusterSnapshot
	Cluster subnet group	AWS::Redshift::ClusterSubnetGroup
	Event subscription	AWS::Redshift::EventSubscription
Amazon Relational Database Service	RDS DB instance	AWS::RDS::DBInstance
	RDS DB security group	AWS::RDS::DBSecurityGroup
	RDS DB snapshot	AWS::RDS::DBSnapshot
	RDS DB subnet group	AWS::RDS::DBSubnetGroup
	Event subscription	AWS::RDS::EventSubscription
Amazon Simple Storage Service	Amazon S3 bucket ⁵	AWS::S3::Bucket

AWS Service	Resource Type	resourceType Value
Amazon Virtual Private Cloud	Customer gateway	AWS::EC2::CustomerGateway
	Internet gateway	AWS::EC2::InternetGateway
	Network access control list (ACL)	AWS::EC2::NetworkAcl
	Route table	AWS::EC2::RouteTable
	Subnet	AWS::EC2::Subnet
	Virtual private cloud (VPC)	AWS::EC2::VPC
	VPN connection	AWS::EC2::VPNConnection
	VPN gateway	AWS::EC2::VPNGateway

Notes

1. AWS Config records the configuration details of Dedicated hosts and the instances that you launch on them. As a result, you can use AWS Config as a data source when you report compliance with your server-bound software licenses. For example, you can view the configuration history of an instance and determine which Amazon Machine Image (AMI) it is based on. Then, you can look up the configuration history of the host, which includes details such as the numbers of sockets and cores, to verify that the host complies with the license requirements of the AMI. For more information, see [Tracking Configuration Changes with AWS Config](#) in the *Amazon EC2 User Guide for Linux Instances*.
2. To learn more about managed instance inventory, see [Recording software configuration for managed instances](#) (p. 8).
3. AWS Identity and Access Management (IAM) resources are *global resources*. Global resources are not tied to an individual region and can be used in all regions. The configuration details for a global resource are the same in all regions. For more information, see [Selecting Which Resources AWS Config Records](#) (p. 109).
4. AWS Config includes inline policies with the configuration details that it records.
5. If you configured AWS Config to record your S3 buckets, and are not receiving configuration change notifications, verify your S3 bucket policies have the required permissions. For more information, see [Troubleshooting for recording S3 buckets](#) (p. 115).

Recording software configuration for managed instances

You can use AWS Config to record software inventory changes on EC2 instances and on-premises servers. This enables you to see the historical changes to software configuration. For example, when a new Windows update is installed on a managed Windows instance, AWS Config records the changes and then sends the changes to your delivery channels, so that you are notified about the change. With AWS Config, you can see the history of when Windows updates were installed for the managed instance and how they changed over time.

You must complete the following steps to record software configuration changes:

- Turn on recording for the managed instance inventory resource type in AWS Config
- Configure EC2 and on-premises instances as *managed instances*
- Initiate collection of software inventory from your managed instances

You can also use AWS Config rules to monitor software configuration changes and be notified whether the changes are compliant or noncompliant against your rules. For example, if you create a rule that checks whether your managed instances have a specified application, and an instance doesn't have that application installed, AWS Config flags that instance as noncompliant against your rule. For a list of AWS Config managed rules, see [AWS Managed Config Rules](#) (p. 29).

To enable recording of software configuration changes in AWS Config:

1. Turn on recording for all supported resource types or selectively record the managed instance inventory resource type in AWS Config. For more information, see [Selecting Which Resources AWS Config Records](#) (p. 109).
2. Launch an Amazon EC2 instance with an IAM role and the **AmazonEC2RoleforSSM** policy. You may also need to install an **SSM Agent**. For more information, see [Systems Manager Prerequisites](#) in the *Amazon EC2 User Guide for Linux Instances* or [Systems Manager Prerequisites](#) in the *Amazon EC2 User Guide for Windows Instances*.
3. Initiate inventory collection as described in [Configuring Inventory Collection](#) in the *Amazon EC2 User Guide for Linux Instances*. The procedures are the same for Linux and Windows instances.

AWS Config can record configuration changes for the following inventory types:

- **Applications** – A list of applications for managed instances, such as antivirus software.
- **AWS components** – A list of AWS components for managed instances, such as the AWS CLI and SDKs.
- **Instance information** – Instance information such as OS name and version, domain, and firewall status.
- **Network configuration** – Configuration information such as IP address, gateway, and subnet mask.
- **Windows Updates** – A list of Windows updates for managed instances (Windows instances only).

Note

AWS Config doesn't support recording the custom inventory type at this time.

Inventory collection is one of many Amazon EC2 Systems Manager capabilities, which also includes applying operating system patches and configuring instances at scale. For more information, see [Amazon EC2 Systems Manager](#) in the *Amazon EC2 User Guide for Linux Instances* or [Amazon EC2 Systems Manager](#) in the *Amazon EC2 User Guide for Windows Instances*.

Components of a Configuration Item

A configuration item consists of the following components.

Component	Description	Contains
Metadata	Information about this configuration item	<ul style="list-style-type: none">• Version ID• Configuration item ID• Time when the configuration item was captured• Status of the configuration item indicating whether the item was captured successfully• State ID indicating the ordering of the configuration items of a resource• A unique MD5Hash representing the state of a configuration item that can be used

Component	Description	Contains
		to compare two states of two or more configuration items of the same resource
Attributes ¹	Resource attributes	<ul style="list-style-type: none"> Resource ID List of key–value tags for this resource Resource type; see Supported AWS Resource Types (p. 7) Amazon Resource Name (ARN) Availability Zone that contains this resource, if applicable Time the resource was created
Relationships	How the resource is related to other resources associated with the account	Description of the relationship, such as Amazon EBS volume <code>vol-1234567</code> is attached to an Amazon EC2 instance <code>i-a1b2c3d4</code>
Current configuration	Information returned through a call to the Describe or List API of the resource	<p>For example, <code>DescribeVolumes</code> API returns the following information about the volume:</p> <ul style="list-style-type: none"> Availability Zone the volume is in Time the volume was attached ID of the EC2 instance it is attached to Current status of the volume State of <code>DeleteOnTermination</code> flag Device the volume is attached to Type of volume, such as <code>gp2</code>, <code>io1</code>, or <code>standard</code>
Related events	The AWS CloudTrail events that is related to the current configuration of the resource	CloudTrail event ID

Notes

1. A configuration item relationship does not include network flow or data flow dependencies. Configuration items cannot be customized to represent your application architecture.
2. AWS Config also records the following attributes for the Amazon S3 bucket resource type. For more information about the attributes, see [Bucket Configuration Options](#) in the *Amazon Simple Storage Service Developer Guide*.

Amazon S3 Bucket Attributes

Attributes	Description
<code>AccelerateConfiguration</code>	Transfer acceleration for data over long distances between your client and a bucket.
<code>BucketAcl</code>	Access control list used to manage access to buckets and objects.
<code>BucketPolicy</code>	Policy that defines the permissions to the bucket.
<code>CrossOriginConfiguration</code>	Allow cross-origin requests to the bucket.

Attributes	Description
LifecycleConfiguration	Rules that define the lifecycle for objects in your bucket.
LoggingConfiguration	Logging used to track requests for access to the bucket.
NotificationConfiguration	Event notifications used to send alerts or trigger workflows for specified bucket events.
ReplicationConfiguration	Automatic, asynchronous copying of objects across buckets in different AWS Regions.
RequestPaymentConfiguration	Requester pays is enabled.
TaggingConfiguration	Tags added to the bucket to categorize. You can also use tagging to track billing.
WebsiteConfiguration	Static website hosting is enabled for the bucket.
VersioningConfiguration	Versioning is enabled for objects in the bucket.

Supported Resource Relationships

AWS Config supports the following relationships between different resources.

Note

AWS Config can create multiple configuration items when a resource is changed and that resource is related to other resources. For more information, see [Configuration Items for Resources with Relationships \(p. 89\)](#).

Resource	Relationship	Related Resource
Amazon EBS volume	is attached to	EC2 instance
Amazon Redshift cluster	is associated with	Cluster parameter group
		Cluster security group
		Cluster subnet group
		Security group
		Virtual private cloud (VPC)
Amazon Redshift cluster snapshot	is associated with	Cluster

Resource	Relationship	Related Resource
		Virtual private cloud (VPC)
Amazon Redshift cluster subnet group	is associated with	Subnet
		Virtual private cloud (VPC)
Application load balancer	is associated with	EC2 security group
	is attached to	Subnet
	is contained in	Virtual private cloud (VPC)
Customer gateway	is attached to	VPN connection
EC2 Dedicated host	contains	EC2 instance
EC2 Elastic IP (EIP)	is attached to	EC2 instance
		Network interface
EC2 instance	contains	EC2 network interface
	is associated with	EC2 security group
	is attached to	Amazon EBS volume
		EC2 Elastic IP (EIP)
	is contained in	EC2 Dedicated host
		Route table
		Subnet

Resource	Relationship	Related Resource
		Virtual private cloud (VPC)
EC2 network interface	is associated with	EC2 security group
	is attached to	EC2 Elastic IP (EIP)
		EC2 instance
	is contained in	Route table
		Subnet
		Virtual private cloud (VPC)
EC2 security group	is associated with	EC2 instance
		EC2 network interface
		Virtual private cloud (VPC)
IAM user	is attached to	IAM group
		IAM customer managed policy
IAM group	contains	IAM user
	is attached to	IAM customer managed policy
IAM role	is attached to	IAM customer managed policy
IAM customer managed policy	is attached to	IAM user
		IAM group
		IAM role

Resource	Relationship	Related Resource
Internet gateway	is attached to	Virtual private cloud (VPC)
Managed instance inventory	is associated with	EC2 instance
Network ACL	is attached to	Subnet
	is contained in	Virtual private cloud (VPC)
RDS DB instance	is associated with	EC2 security group
		RDS DB security group
		RDS DB subnet group
RDS DB security group	is associated with	EC2 security group
		Virtual private cloud (VPC)
RDS DB snapshot	is associated with	Virtual private cloud (VPC)
RDS DB subnet group	is associated with	EC2 subnet
		Virtual private cloud (VPC)
Route table	contains	EC2 instance
		EC2 network interface
		Subnet
		VPN gateway

Resource	Relationship	Related Resource
	is contained in	Virtual private cloud (VPC)
Subnet	contains	EC2 instance
		EC2 network interface
	is attached to	Network ACL
	is contained in	Route table
		Virtual private cloud (VPC)
Virtual private cloud (VPC)	contains	EC2 instance
		EC2 network interface
		Network ACL
		Route table
		Subnet
	is associated with	Security group
	is attached to	Internet gateway
		VPN gateway
VPN connection	is attached to	Customer gateway
		VPN gateway
VPN gateway	is attached to	Virtual private cloud (VPC)
		VPN connection
	is contained in	Route table

Getting Started with AWS Config

After you sign up for an AWS account, you can get started with AWS Config with the AWS Management Console, AWS CLI, or the AWS SDKs. Use the console for a quick and streamlined process.

When you set up AWS Config, you can complete the following:

- Specify the resource types that you want AWS Config to record.
- Set up an Amazon S3 bucket to receive a configuration snapshot on request and configuration history.
- Set up an Amazon SNS topic to send configuration stream notifications.
- Grant AWS Config the permissions it needs to access the Amazon S3 bucket and the SNS topic.
- Specify the rules that you want AWS Config to use to evaluate compliance information for the recorded resource types.

For more information about using the AWS CLI, see [Setting up AWS Config with the AWS CLI \(p. 20\)](#).

For more information about using the AWS SDKs, see [AWS Software Development Kits for AWS Config \(p. 129\)](#).

Topics

- [Signing up for AWS \(p. 16\)](#)
- [Setting up AWS Config with the Console \(p. 17\)](#)
- [Setting up AWS Config with the AWS CLI \(p. 20\)](#)

Signing up for AWS

When you sign up for AWS, your account has access to all AWS services. You pay only for the services that you use.

If you do not have an AWS account, use the following procedure to create one.

To sign up for AWS

1. Open <https://aws.amazon.com/> and choose **Create an AWS Account**.
2. Follow the online instructions.

Setting up AWS Config with the Console

You can use the AWS Management Console to get started with AWS Config to do the following:

- Specify the resource types you want AWS Config to record.
- Set up Amazon SNS to notify you of configuration changes.
- Specify an Amazon S3 bucket to receive configuration information.
- Add AWS Config managed rules to evaluate the resource types.

If you are using AWS Config for the first time or configuring AWS Config for a new region, you can choose managed rules to evaluate resource configurations. For regions that support AWS Config and AWS Config Rules, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.

To set up AWS Config with the console

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. If this is the first time you are opening the AWS Config console or you are setting up AWS Config in a new region, the AWS Config console page looks like the following:



3. Choose **Get Started Now**.
4. On the **Settings** page, for **Resource types to record**, specify the AWS resource types you want AWS Config to record:
 - **All resources** – AWS Config records all supported resources with the following options:
 - **Record all resources supported in this region** – AWS Config records configuration changes for every supported type of regional resource. When AWS Config adds support for a new resource type, AWS Config automatically starts recording resources of that type.
 - **Include global resources** – AWS Config includes supported types of global resources with the resources that it records (for example, IAM resources). When AWS Config adds support for a new global resource type, AWS Config automatically starts recording resources of that type.
 - **Specific types** – AWS Config records configuration changes for only the AWS resource types that you specify.

For more information about these options, see [Selecting Which Resources AWS Config Records](#) (p. 109).

5. For **Amazon S3 Bucket**, choose the Amazon S3 bucket to which AWS Config sends configuration history and configuration snapshot files:

- **Create a new bucket** – For **Bucket Name**, type a name for your Amazon S3 bucket.

The name that you type must be unique across all existing bucket names in Amazon S3. One way to help ensure uniqueness is to include a prefix; for example, the name of your organization. You can't change the bucket name after it is created. For more information, see [Bucket Restrictions and Limitations](#) in the *Amazon Simple Storage Service Developer Guide*.

- **Choose a bucket from your account** – For **Bucket Name**, choose your preferred bucket.
- **Choose a bucket from another account** – For **Bucket Name**, type the bucket name.

If you choose a bucket from another account, that bucket must have policies that grant access permissions to AWS Config. For more information, see [Permissions for the Amazon S3 Bucket](#) (p. 116).

6. For **Amazon SNS Topic**, choose whether AWS Config streams information by selecting the **Stream configuration changes and notifications to an Amazon SNS topic**. AWS Config sends notifications such as configuration history delivery, configuration snapshot delivery, and compliance.
7. If you chose to have AWS Config stream to an Amazon SNS topic, choose the target topic:

- **Create a new topic** – For **Topic Name**, type a name for your SNS topic.
- **Choose a topic from your account** – For **Topic Name**, select your preferred topic.
- **Choose a topic from another account** – For **Topic ARN**, type the Amazon Resource Name (ARN) of the topic.

If you choose a topic from another account, the topic must have policies that grant access permissions to AWS Config. For more information, see [Permissions for the Amazon SNS Topic](#) (p. 117).

Note

The Amazon SNS topic must exist in the same region as the region in which you set up AWS Config.

8. For **AWS Config role**, choose the IAM role that grants AWS Config permission to record configuration information and send this information to Amazon S3 and Amazon SNS:
 - **Create a role** – AWS Config creates a role that has the required permissions. For **Role name**, you can customize the name that AWS Config creates.
 - **Choose a role from your account** – For **Role name**, select an IAM role in your account that grants the required permissions. For the required permissions, see [Permissions for the IAM Role Assigned to AWS Config](#) (p. 113).
9. If you are setting up AWS Config in a region that supports rules, choose **Next**. See [Setting Up AWS Config Rules with the Console](#) (p. 19).

Otherwise, choose **Save**. AWS Config displays the **Resource inventory** page.

For information about looking up the existing resources in your account and understanding the configurations of your resources, see [Viewing AWS Resource Configurations and History](#) (p. 71).

If you chose to have AWS Config stream information to an Amazon SNS topic, you can receive notifications by email. For more information, see [Monitoring AWS Config Resource Changes by Email](#) (p. 84). You

can also use Amazon Simple Queue Service to monitor AWS resources programmatically. For more information, see [Using Amazon SQS to Monitor AWS Resource Changes \(p. 101\)](#).

Setting Up AWS Config Rules with the Console

The **Rules** page provides initial AWS managed rules that you can add to your account. After set up, AWS Config evaluates your AWS resources against the rules that you choose. You can update the rules and create additional managed rules after set up.

To see the complete list of AWS managed rules, see [AWS Managed Config Rules \(p. 29\)](#).

For example, you can choose the **cloudtrail-enabled** rule, which evaluates whether your account has a CloudTrail trail. If your account doesn't have a trail, AWS Config flags the resource type and the rule as noncompliant.

Set up AWS Config

- Step 1: Settings
- Step 2: Rules**
- Step 3: Review

AWS Config rules

AWS Config can check the configuration of your resources against rules that you define. Choose one or more of the following rules to get started. After you've set up AWS Config, you can customize these rules, set up other rules provided by AWS Config, or create your own rules.

Learn more about [AWS Config rules](#) and [pricing details](#).

A Filter by rule name, label or description

B Select all 20 | Clear all

C acm-certificate-expiration-check

Checks whether ACM Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed.

ACM

D cloudtrail-enabled

Checks whether AWS CloudTrail is enabled in your AWS account.

CloudTrail . Periodic

db-instance-backup-enabled

Checks whether RDS DB instances have backups enabled. Optionally, you can specify the backup retention period and the backup window.

RDS

dynamodb-throughput-limit-check

Checks whether provisioned DynamoDB throughput is approaching the maximum limit for your account. By default, the rule checks if provisioned throughput exceeds a threshold of 100 MB/s.

DynamoDb . Periodic

ebs-optimized-instance

Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized.

EC2

ec2-instance-detailed-monitoring

Checks whether detailed monitoring is enabled for EC2 instances.

EC2

ec2-instances-in-vpc

Checks whether your EC2 instances belong to a virtual private cloud (VPC). Optionally, you can specify the VPC ID to associate with your instances.

EC2

ec2-volume-in-use-check

Checks whether EBS volumes are attached to EC2 instances. Optionally checks if EBS volumes are marked for deletion when an instance is terminated.

EC2

eip-attached

Checks whether all EIP addresses are attached to a VPC are attached to EC2 instances.

EC2

On the **Rules** page, you can do the following:

- Type in the search field to filter results by rule name, description, or label. For example, type **EC2** to return rules that evaluate EC2 resource types or type **periodic** to return rules that have a periodic trigger. For more information about trigger types, see [Specifying Triggers for AWS Config Rules \(p. 27\)](#).

- B. Choose **Select all** to add all rules or **Clear all** to remove all rules.
- C. Choose a rule to select it.
- D. See the labels to identify the service that the rule evaluates and if the rule has a periodic trigger.
- E. Choose the arrow icon to see the next page of rules.

To set up AWS Config rules

1. On the **Rules** page, choose the rules that you want. You can customize these rules and add other rules to your account after set up.
2. Choose **Next**.
3. On the **Review** page, verify your setup details, and then choose **Confirm**.

The **Rules** page shows your rules and their current compliance results in the table. The result for each rule is **Evaluating...** until AWS Config finishes evaluating your resources against the rule. You can update the results with the refresh button. When AWS Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see [Viewing Configuration Compliance](#) (p. 62).

Note

AWS Config evaluates only the resource types that it is recording. For example, if you add the **cloudtrail-enabled** rule but don't record the CloudTrail trail resource type, AWS Config can't evaluate whether the trails in your account are compliant or noncompliant. For more information, see [Selecting Which Resources AWS Config Records](#) (p. 109).

You can view, edit, and delete your existing rules. You can also create additional AWS managed rules or create your own. For more information, see [Managing your AWS Config Rules](#) (p. 64).

Setting up AWS Config with the AWS CLI

You can use the AWS Command Line Interface to control and automate the services from AWS.

For more information about the AWS CLI and for instructions on installing the AWS CLI tools, see the following in the *AWS Command Line Interface User Guide*.

- [AWS Command Line Interface User Guide](#)
- [Getting Set Up with the AWS Command Line Interface](#)

See the following topics to set up AWS Config with the AWS CLI. After you set up AWS Config, you can add rules to evaluate the resource types in your account. For more information about setting up rules with AWS Config, see [Using the AWS CLI](#) (p. 66).

Topics

- [Prerequisites](#) (p. 20)
- [Turning on AWS Config](#) (p. 23)
- [Verify that AWS Config Is On](#) (p. 24)

Prerequisites

Follow this procedure to create an Amazon S3 bucket, an Amazon SNS topic, and an IAM role with attached policies. You can then use the AWS CLI to specify the bucket, topic, and role for AWS Config.

Contents

- [Creating an Amazon S3 Bucket \(p. 21\)](#)
- [Creating an Amazon SNS Topic \(p. 21\)](#)
- [Creating an IAM Role \(p. 22\)](#)

Creating an Amazon S3 Bucket

If you already have an Amazon S3 bucket in your account and want to use it, skip this step and go to [Creating an Amazon SNS Topic \(p. 21\)](#).

To create an Amazon S3 bucket with the AWS CLI, use the [create-bucket](#) command.

To create an Amazon S3 bucket with the console

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose **Actions** and then choose **Create Bucket**.
3. For the **Bucket Name**:, type a name for your Amazon S3 bucket, such as *my-config-bucket*.

Note

Make sure the bucket name you choose is unique across all existing bucket names in Amazon S3. You cannot change the name of a bucket after it is created. For more information on bucket naming rules and conventions, see [Bucket restrictions and Limitations](#) in the *Amazon Simple Storage Service Developer Guide*.

4. Choose **Create**.

Note

You can also use an Amazon S3 bucket from a different account, but you may need to create a policy for the bucket that grants access permissions to AWS Config. For information on granting permissions to an Amazon S3 bucket, see [Permissions for the Amazon S3 Bucket \(p. 116\)](#), and then go to [Creating an Amazon SNS Topic \(p. 21\)](#).

Creating an Amazon SNS Topic

If you already have an Amazon SNS topic in your account and want to use it, skip this step and go to [Creating an IAM Role \(p. 22\)](#).

To create an Amazon SNS topic with the AWS CLI, use the [create-topic](#) command.

To create an Amazon SNS topic with the console

1. Sign in to the AWS Management Console and open the Amazon SNS console at <https://console.aws.amazon.com/sns/v2/home>.
2. Choose **Create New Topic**.
3. For **Topic Name**, type a name for your SNS topic, such as *my-config-notice*.
4. Choose **Create Topic**.

The new topic appears in the **Topic Details** page. Copy the **Topic ARN** for the next task.

For more information, see [ARN Format](#) in the *AWS General Reference*.

To receive notifications from AWS Config, you must subscribe an email address to the topic.

To subscribe an email address to the SNS topic

1. In the Amazon SNS console, choose **Subscriptions** in the navigation pane.
2. On the **Subscriptions** page, choose **Create Subscription**.
3. For **Topic ARN**, paste the topic ARN you copied in the previous task.
4. For **Protocol**, choose **Email**.
5. For **Endpoint**, type an email address that you can use to receive the notification and then choose **Subscribe**.
6. Go to your email application and open the message from **AWS Notifications**. Choose the link to confirm your subscription.

Your web browser displays a confirmation response from Amazon SNS. Amazon SNS is now configured to receive notifications and send the notification as an email to the specified email address.

Note

You can also use an Amazon SNS topic in a different account, but in that case you might need to create a policy for topic that grants access permissions to AWS Config. For information on granting permissions to an Amazon SNS topic, see [Permissions for the Amazon SNS Topic \(p. 117\)](#) and then go to [Creating an IAM Role \(p. 22\)](#).

Creating an IAM Role

You can use the IAM console to create an IAM role that grants AWS Config permissions to access your Amazon S3 bucket, access your Amazon SNS topic, and get configuration details for supported AWS resources. After you create the IAM role, you will create and attach policies to the role.

To create an IAM role with the AWS CLI, use the [create-role](#) command. You can then attach a policy to the role with the [attach-role-policy](#) command.

To create an IAM role with the console

1. Sign in to the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the IAM console, choose **Roles** in the navigation pane, and choose **Create New Role**.
3. For **Role Name**, type a name that describes the purpose of this role. Role names must be unique within your AWS account. Because various entities might reference the role, you cannot edit the name of the role after you create it.

Choose **Next Step**.

4. Choose **AWS Service Roles**, and then choose **Select** for **AWS Config**.
5. On the **Attach Policy** page, select **AWSServiceRole**. This AWS managed policy grants AWS Config permission to get configuration details for supported AWS resources. Then, choose **Next Step**.
6. On the **Review** page, review the details about your role, and choose **Create Role**.
7. On the **Roles** page, choose the role that you created to open its details page.

You will expand the permissions in the role by creating inline policies that allow AWS Config to access your Amazon S3 bucket and your Amazon SNS topic.

To create an inline policy that grants AWS Config permission to access your Amazon S3 bucket

1. In the **Permissions** section, expand the **Inline Policies** section, and choose **click here**.
2. Choose **Custom Policy**, and choose **Select**.
3. For **Policy Name**, type a name for your inline policy.

4. Copy the example Amazon S3 bucket policy in [IAM Role Policy for Amazon S3 Bucket \(p. 114\)](#) and paste it in the **Policy Document** editor.

Important

Before you proceed to the next step, replace the following values in the policy. If you do not replace the values, your policy will fail.

- *myBucketName* – Replace with the name of your Amazon S3 bucket.
- *prefix* – Replace with your own prefix or leave blank by removing the trailing '/'.
- *myAccountID-WithoutHyphens* – Replace with your AWS account ID.

5. Choose **Apply Policy**.

To create an inline policy that grants AWS Config permissions to deliver notifications to your Amazon SNS topic

1. In the **Permissions** section, expand the **Inline Policies** section, and choose **click here**.
2. Choose **Custom Policy**, and choose **Select**.
3. For **Policy Name**, type a name for your inline policy.
4. Copy the Amazon SNS topic example policy in [IAM Role Policy for Amazon SNS Topic \(p. 115\)](#) and paste it in the **Policy Document** editor.

Important

Before you proceed to the next step, replace *arn:aws:sns:region:account-id:myTopic* with the ARN you saved when you created your Amazon SNS topic.

5. Choose **Apply Policy**.

Turning on AWS Config

You can use the AWS CLI to turn on AWS Config with the `subscribe` command and a few parameters.

You can use the `subscribe` command to have AWS Config start recording configurations of all supported AWS resources in your account. The `subscribe` command creates a configuration recorder, a delivery channel using a specified Amazon S3 bucket and Amazon SNS topic, and starts recording the configuration items. You can have one configuration recorder and one delivery channel per region in your account.

To turn on AWS Config, use the `subscribe` with the following parameters:

The `subscribe` command uses the following options:

`--s3-bucket`

Specify the name of an Amazon S3 bucket existing in your account or existing in another account.

`--sns-topic`

Specify the Amazon Resource Name (ARN) of an SNS topic existing in your account or existing in another account.

`--iam-role`

Specify the Amazon Resource Name (ARN) of an existing IAM Role.

The specified IAM role must have policies attached that grant AWS Config permissions to deliver configuration items to the Amazon S3 bucket and the Amazon SNS topic, and the role must grant permissions to the `Describe` APIs of the supported AWS resources.

Your command should look like the following example:

```
$ aws configservice subscribe --s3-bucket my-config-bucket --sns-topic arn:aws:sns:us-east-1:012345678912:my-config-notice --iam-role arn:aws:iam::012345678912:role/myConfigRole
```

After you run the `subscribe` command, AWS Config records all supported resources that it finds in the region. If you don't want AWS Config to record supported resources, specify the types of resources to record by updating the configuration recorder to use a recording group. For more information, see [Selecting Resources \(AWS CLI\) \(p. 110\)](#).

Verify that AWS Config Is On

Once you have turned on AWS Config, you can use AWS CLI commands to verify that the AWS Config is running and that the `subscribe` command has created a configuration recorder and a delivery channel. You can also confirm that AWS Config has started recording and delivering configurations to the delivery channel.

Contents

- [Verify that the Delivery Channel Is Created \(p. 24\)](#)
- [Verify that the Configuration Recorder Is Created \(p. 24\)](#)
- [Verify that AWS Config has started recording \(p. 25\)](#)

Verify that the Delivery Channel Is Created

Use the `describe-delivery-channels` command to verify that your Amazon S3 bucket and Amazon SNS topic is configured.

```
$ aws configservice describe-delivery-channels
{
  "DeliveryChannels": [
    {
      "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
      "name": "my-delivery-channel",
      "s3BucketName": "my-config-bucket"
    }
  ]
}
```

When you use the CLI, the service API, or the SDKs to configure your delivery channel and do not specify a name, AWS Config automatically assigns the name "default".

Verify that the Configuration Recorder Is Created

Use the `describe-configuration-recorders` command to verify that a configuration recorder is created and that the configuration recorder has assumed an IAM role. For more information, see [Creating an IAM Role \(p. 22\)](#).

```
$ aws configservice describe-configuration-recorders
{
  "ConfigurationRecorders": [
    {
      "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
      "name": "default"
    }
  ]
}
```

Verify that AWS Config has started recording

Use the `describe-configuration-recorder-status` command to verify that the AWS Config has started recording the configurations of the supported AWS resources existing in your account. The recorded configurations are delivered to the specified delivery channel.

```
$ aws configservice describe-configuration-recorder-status
{
  "ConfigurationRecordersStatus": [
    {
      "name": "default",
      "lastStatus": "SUCCESS",
      "lastStopTime": 1414511624.914,
      "lastStartTime": 1414708460.276,
      "recording": true,
      "lastStatusChangeTime": 1414816537.148,
      "lastErrorMessage": "NA",
      "lastErrorCode": "400"
    }
  ]
}
```

The value `true` in the `recording` field confirms that the configuration recorder has started recording configurations of all your resources. AWS Config uses UTC format (GMT - 8:00) to record the time.

For information about looking up the resources existing in your account and understanding the configurations of your resources, see [Viewing AWS Resource Configurations and History \(p. 71\)](#).

Evaluating Resources With AWS Config Rules

Use AWS Config to evaluate the configuration settings of your AWS resources. You do this by creating AWS Config rules, which represent your ideal configuration settings. AWS Config provides customizable, predefined rules called managed rules to help you get started. You can also create your own custom rules. While AWS Config continuously tracks the configuration changes that occur among your resources, it checks whether these changes violate any of the conditions in your rules. If a resource violates a rule, AWS Config flags the resource and the rule as *noncompliant*.

For example, when an EC2 volume is created, AWS Config can evaluate the volume against a rule that requires volumes to be encrypted. If the volume is not encrypted, AWS Config flags the volume and the rule as noncompliant. AWS Config can also check all of your resources for account-wide requirements. For example, AWS Config can check whether the number of EC2 volumes in an account stays within a desired total, or whether an account uses AWS CloudTrail for logging.

The AWS Config console shows the compliance status of your rules and resources. You can see how your AWS resources comply overall with your desired configurations, and learn which specific resources are noncompliant. You can also use the AWS CLI, the AWS Config API, and AWS SDKs to make requests to the AWS Config service for compliance information.

By using AWS Config to evaluate your resource configurations, you can assess how well your resource configurations comply with internal practices, industry guidelines, and regulations.

For regions that support AWS Config rules, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.

You can create up to 50 AWS Config rules per region in your account. For more information, see [AWS Config Limits](#) in the *Amazon Web Services General Reference*.

You can also create custom rules to evaluate additional resources that AWS Config doesn't yet record. For more information, see [Evaluating Additional Resource Types \(p. 53\)](#).

Topics

- [Specifying Triggers for AWS Config Rules \(p. 27\)](#)
- [About AWS Managed Config Rules \(p. 28\)](#)
- [Developing Custom Rules for AWS Config \(p. 48\)](#)

- [Viewing Configuration Compliance \(p. 62\)](#)
- [Managing your AWS Config Rules \(p. 64\)](#)
- [Manually Evaluate your Resources \(p. 68\)](#)

Specifying Triggers for AWS Config Rules

When you add a rule to your account, you can specify when you want AWS Config to run the rule; this is called a *trigger*. AWS Config evaluates your resource configurations against the rule when the trigger occurs.

Contents

- [Trigger types \(p. 27\)](#)
- [Example rules with triggers \(p. 27\)](#)
- [Rule evaluations when the configuration recorder is turned off \(p. 28\)](#)

Trigger types

There are two types of triggers:

Configuration changes

AWS Config runs evaluations for the rule when certain types of resources are created, changed, or deleted.

You choose which resources trigger the evaluation by defining the rule's *scope*. The scope can include the following:

- One or more resource types
- A combination of a resource type and a resource ID
- A combination of a tag key and value
- When any recorded resource is created, updated, or deleted

AWS Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to constrain which resources trigger evaluations. Otherwise, evaluations are triggered when any recorded resource changes.

Periodic

AWS Config runs evaluations for the rule at a frequency that you choose (for example, every 24 hours).

If you choose configuration changes and periodic, AWS Config invokes your Lambda function when it detects a configuration change and also at the frequency that you specify.

Example rules with triggers

Example rule with configuration change trigger

1. You add the AWS Config managed rule, `S3_BUCKET_LOGGING_ENABLED`, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.

3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.

Example rule with periodic trigger

1. You add the AWS Config managed rule, `IAM_PASSWORD_POLICY`, to your account. The rule checks whether the password policy for your IAM users comply with your account policy, such as requiring a minimum length or requiring specific characters.
2. The trigger type for the rule is periodic. AWS Config runs evaluation for the rule at a frequency that you specify, such as every 24 hours.
3. Every 24 hours, the rule is triggered and AWS Config evaluates whether the passwords for your IAM users are compliant against the rule.

Example rule with configuration change and periodic triggers

1. You create a custom rule that evaluates whether CloudTrail trails in your account are turned on and logging for all regions.
2. You want AWS Config to run evaluations for the rule every time a trail is created, updated, or deleted. You also want AWS Config to run the rule every 12 hours.
3. For the trigger type, choose configuration changes and periodic.

Rule evaluations when the configuration recorder is turned off

If you turn off the configuration recorder, AWS Config stops recording changes to your resource configurations. This affects your rule evaluations in the following ways:

- Rules with a periodic trigger continue to run evaluations at the specified frequency.
- Rules with a configuration change trigger do not run evaluations.
- Rules with both trigger types run evaluations only at the specified frequency. The rules do not run evaluations for configuration changes.
- If you run an on-demand evaluation for a rule with a configuration change trigger, the rule evaluates the last known state of the resource, which is the last recorded configuration item. For more information about on-demand evaluations, see [Manually Evaluate your Resources \(p. 68\)](#).

About AWS Managed Config Rules

AWS Config provides *AWS managed rules*, which are predefined, customizable rules that AWS Config uses to evaluate whether your AWS resources comply with common best practices. For example, you could use a managed rule to quickly start assessing whether your Amazon Elastic Block Store (Amazon EBS) volumes are encrypted or whether specific tags are applied to your resources. You can set up and activate these rules without writing the code to create an AWS Lambda function, which is required if you want to create custom rules. The AWS Config console guides you through the process of configuring and activating a managed rule. You can also use the AWS Command Line Interface or AWS Config API to pass the JSON code that defines your configuration of a managed rule.

You can customize the behavior of a managed rule to suit your needs. For example, you can define the rule's scope to constrain which resources trigger an evaluation for the rule, such as EC2 instances or volumes. You can customize the rule's parameters to define attributes that your resources must have to comply with the rule. For example, you can customize a parameter to specify that your security group should block incoming traffic to a specific port number.

After you activate a rule, AWS Config compares your resources to the conditions of the rule. After this initial evaluation, AWS Config continues to run evaluations each time one is triggered. The evaluation triggers are defined as part of the rule, and they can include the following types:

- **Configuration changes** – AWS Config triggers the evaluation when any resource that matches the rule's scope changes in configuration. The evaluation runs after AWS Config sends a configuration item change notification.
- **Periodic** – AWS Config runs evaluations for the rule at a frequency that you choose (for example, every 24 hours).

The AWS Config console shows which resources comply with the rule and which rules are being followed. For more information, see [Viewing Configuration Compliance \(p. 62\)](#).

Topics

- [AWS Managed Config Rules \(p. 29\)](#)
- [Working with AWS Managed Rules \(p. 46\)](#)
- [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#)

AWS Managed Config Rules

AWS Config provides the following managed rules.

Compute

- [approved-amis-by-id \(p. 30\)](#)
- [approved-amis-by-tag \(p. 31\)](#)
- [desired-instance-tenancy \(p. 33\)](#)
- [desired-instance-type \(p. 33\)](#)
- [ebs-optimized-instance \(p. 34\)](#)
- [ec2-instance-detailed-monitoring-enabled \(p. 35\)](#)
- [ec2-instances-in-vpc \(p. 35\)](#)
- [ec2-managedinstance-applications-blacklisted \(p. 36\)](#)
- [ec2-managedinstance-applications-required \(p. 36\)](#)
- [ec2-managedinstance-inventory-blacklisted \(p. 37\)](#)
- [ec2-managedinstance-platform-check \(p. 37\)](#)
- [ec2-volume-inuse-check \(p. 38\)](#)
- [eip-attached \(p. 38\)](#)
- [encrypted-volumes \(p. 39\)](#)
- [restricted-common-ports \(p. 43\)](#)
- [restricted-ssh \(p. 44\)](#)

Database

- [db-instance-backup-enabled \(p. 32\)](#)
- [dynamodb-throughput-limit-check \(p. 34\)](#)
- [rds-multi-az-support \(p. 41\)](#)
- [rds-storage-encrypted \(p. 41\)](#)
- [redshift-cluster-configuration-check \(p. 42\)](#)

- [redshift-cluster-maintenancesettings-check](#) (p. 42)

Management Tools

- [cloudtrail-enabled](#) (p. 31)
- [required-tags](#) (p. 43)

Security, Identity & Compliance

- [acm-certificate-expiration-check](#) (p. 30)
- [iam-password-policy](#) (p. 39)
- [iam-user-group-membership-check](#) (p. 40)
- [iam-user-no-policies-check](#) (p. 40)
- [root-account-mfa-enabled](#) (p. 44)

Storage

- [s3-bucket-logging-enabled](#) (p. 45)
- [s3-bucket-ssl-requests-only](#) (p. 45)
- [s3-bucket-versioning-enabled](#) (p. 46)

acm-certificate-expiration-check

Checks whether ACM Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed. ACM does not automatically renew certificates that you import.

Identifier: ACM_CERTIFICATE_EXPIRATION_CHECK

Trigger type: Configuration changes and periodic


Parameters:

daysToExpiration

Specify the number of days before the rule flags the ACM Certificate as noncompliant.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates](#) (p. 47).

View	Launch
View	

approved-amis-by-id

Checks whether running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are noncompliant.

Identifier: APPROVED_AMIS_BY_ID

Trigger type: Configuration changes


Parameters:

amilds

The AMI IDs (comma-separated list of up to 10).

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

approved-amis-by-tag

Checks whether running instances are using specified AMIs. Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags are noncompliant.

Identifier: APPROVED_AMIS_BY_TAG

Trigger type: Configuration changes


Parameters:

amisByTagKeyAndValue

The AMIs by tag (comma-separated list up to 10; for example, "tag-key:tag-value").

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

cloudtrail-enabled

Checks whether AWS CloudTrail is enabled in your AWS account. Optionally, you can specify which S3 bucket, SNS topic, and Amazon CloudWatch Logs ARN to use.

Identifier: CLOUD_TRAIL_ENABLED

Trigger type: Periodic

Parameters:

s3BucketName

The name of the S3 bucket for AWS CloudTrail to deliver log files to.

snsTopicArn


The ARN of the SNS topic for AWS CloudTrail to use for notifications.

cloudWatchLogsLogGroupArn

The ARN of the Amazon CloudWatch log group for AWS CloudTrail to send data to.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

db-instance-backup-enabled

Checks whether RDS DB instances have backups enabled. Optionally, the rule checks the backup retention period and the backup window.

Identifier: DB_INSTANCE_BACKUP_ENABLED

Trigger type: Configuration changes

Parameters:

backupRetentionPeriod

Retention period for backups.

preferredBackupWindow


Time range in which backups are created.

checkReadReplicas

Checks whether RDS DB instances have backups enabled for read replicas.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

desired-instance-tenancy

Checks instances for specified tenancy. Specify AMI IDs to check instances that are launched from those AMIs or specify host IDs to check whether instances are launched on those Dedicated Hosts. Separate multiple ID values with commas.

Identifier: DESIRED_INSTANCE_TENANCY

Trigger type: Configuration changes

Parameters:

tenancy

The desired tenancy of the instances. Valid values are `DEDICATED`, `HOST`, and `DEFAULT`.

imageId


The rule evaluates instances launched only from the AMI with the specified ID. Separate multiple AMI IDs with commas.

hostId

The ID of the Amazon EC2 Dedicated Host on which the instances are meant to be launched. Separate multiple host IDs with commas.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

desired-instance-type

Checks whether your EC2 instances are of the specified instance types.

For a list of supported Amazon EC2 instance types, see [Instance Types](#) in the *Amazon EC2 User Guide for Linux Instances*.

Identifier: DESIRED_INSTANCE_TYPE

Trigger type: Configuration changes


Parameters:

instanceType

Comma-separated list of EC2 instance types (for example, "t2.small, m4.large, i2.xlarge").

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

dynamodb-throughput-limit-check

Checks whether provisioned DynamoDB throughput is approaching the maximum limit for your account. By default, the rule checks if provisioned throughput exceeds a threshold of 80% of your account limits.

Identifier: DYNAMODB_THROUGHPUT_LIMIT_CHECK

Trigger type: Periodic

Parameters:

accountRCUThresholdPercentage


Percentage of provisioned read capacity units for your account. When this value is reached, the rule is marked as noncompliant.

accountWCUThresholdPercentage

Percentage of provisioned write capacity units for your account. When this value is reached, the rule is marked as noncompliant.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

ebs-optimized-instance

Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized.

Identifier: EBS_OPTIMIZED_INSTANCE


Trigger type: Configuration changes

Parameters:

None

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

ec2-instance-detailed-monitoring-enabled

Checks whether detailed monitoring is enabled for EC2 instances.

Identifier: EC2_INSTANCE_DETAILED_MONITORING_ENABLED


Trigger type: Configuration changes

Parameters:

None

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

ec2-instances-in-vpc

Checks whether your EC2 instances belong to a virtual private cloud (VPC). Optionally, you can specify the VPC ID to associate with your instances.

Identifier: INSTANCES_IN_VPC

Trigger type: Configuration changes

Parameters:

vpclId

The ID of the VPC that contains these instances.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

ec2-managedinstance-applications-blacklisted

Checks that none of the specified applications are installed on the instance. Optionally, you can specify the platform to apply the rule only to instances running that platform.

Identifier: EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Trigger type: Configuration changes

Parameters:

applicationNames


Comma-separated list of applications.

platformType

The platform type (for example, "Linux" or "Windows").

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

ec2-managedinstance-applications-required

Checks whether all of the specified applications are installed on the instance. Optionally, you can specify the platform to apply the rule only to instances running that platform.

Identifier: EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

Trigger type: Configuration changes

Parameters:

applicationNames


Comma-separated list of applications.

platformType

The platform type (for example, "Linux" or "Windows").

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

ec2-managedinstance-inventory-blacklisted

Checks whether instances managed by Amazon EC2 Systems Manager are configured to collect blacklisted inventory types.

Identifier: EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

Trigger type: Configuration changes

Parameters:

inventoryNames


Comma-separated list of Systems Manager inventory types (for example, "AWS:Network, AWS:WindowsUpdate").

platformType

Platform type (for example, "Linux").

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

ec2-managedinstance-platform-check

Checks whether EC2 managed instances have the desired configurations.

Identifier: EC2_MANAGEDINSTANCE_PLATFORM_CHECK

Trigger type: Configuration changes

Parameters:

agentVersion

The version of the agent (for example, "2.0.433.0").

platformType


The platform type (for example, "Linux" or "Windows").

platformVersion

The version of the platform (for example, "2016.09").

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

ec2-volume-inuse-check

Checks whether EBS volumes are attached to EC2 instances. Optionally checks if EBS volumes are marked for deletion when an instance is terminated.

Identifier: EC2_VOLUME_INUSE_CHECK

Trigger type: Configuration changes

Parameters:

deleteOnTermination

EBS volumes are marked for deletion when an instance is terminated.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

eip-attached

Checks whether all Elastic IP addresses that are allocated to a VPC are attached to EC2 instances or in-use elastic network interfaces (ENIs).

Results might take up to 6 hours to become available after an evaluation occurs.

Identifier: EIP_ATTACHED


Trigger type: Configuration changes

Parameters:

None

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

encrypted-volumes

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.

For more information, see [Amazon EBS Encryption](#) in the *Amazon EC2 User Guide for Linux Instances*.

Identifier: ENCRYPTED_VOLUMES

Trigger type: Configuration changes


Parameters:

kmsId

ID or ARN of the KMS key that is used to encrypt the volume.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates](#) (p. 47).

View	Launch
View	

iam-password-policy

Checks whether the account password policy for IAM users meets the specified requirements.

Identifier: IAM_PASSWORD_POLICY

Trigger type: Periodic

Parameters:

RequireUppercaseCharacters

Require at least one uppercase character in password.

RequireLowercaseCharacters

Require at least one lowercase character in password.

RequireSymbols

Require at least one symbol in password.

RequireNumbers

Require at least one number in password.

MinimumPasswordLength

Password minimum length.

PasswordReusePrevention


Number of passwords before allowing reuse.

MaxPasswordAge

Number of days before password expiration.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

iam-user-group-membership-check

Checks whether IAM users are members of at least one IAM group.

Identifier: IAM_USER_GROUP_MEMBERSHIP_CHECK

Trigger type: Configuration changes


Parameters:

groupName

Comma-separated list of IAM groups in which IAM users must be members.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

iam-user-no-policies-check

Checks that none of your IAM users have policies attached. IAM users must inherit permissions from IAM groups or roles.

Identifier: IAM_USER_NO_POLICIES_CHECK


Trigger type: Configuration changes

Parameters:

None

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

rds-multi-az-support

Checks whether high availability is enabled for your RDS DB instances.

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. For more information, see [High Availability \(Multi-AZ\)](#) in the *Amazon Relational Database Service User Guide*.

Note

This rule does not evaluate Amazon Aurora databases.

Identifier: RDS_MULTI_AZ_SUPPORT

Trigger type: Configuration changes

Parameters:

None

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

rds-storage-encrypted

Checks whether storage encryption is enabled for your RDS DB instances.

Identifier: RDS_STORAGE_ENCRYPTED

Trigger type: Configuration changes

Parameters:

kmsKeyId

KMS key ID or ARN used to encrypt the storage.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

redshift-cluster-configuration-check

Checks whether Amazon Redshift clusters have the specified settings.

Identifier: REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Trigger type: Configuration changes

Parameters:

clusterDbEncrypted

Database encryption is enabled.

nodeTypes


Specify node type.

loggingEnabled

Audit logging is enabled.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

redshift-cluster-maintenancesettings-check

Checks whether Amazon Redshift clusters have the specified maintenance settings.

Identifier: REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

Trigger type: Configuration changes

Parameters:

allowVersionUpgrade

Allow version upgrade is enabled.

preferredMaintenanceWindow


Scheduled maintenance window for clusters (for example, Mon:09:30-Mon:10:00).

automatedSnapshotRetentionPeriod

Number of days to retain automated snapshots.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

required-tags

Checks whether your resources have the tags that you specify. For example, you can check whether your EC2 instances have the 'CostCenter' tag. Separate multiple values with commas.

Identifier: REQUIRED_TAGS

Trigger type: Configuration changes

Parameters:

tag1Key


Key of the required tag.

tag1Value

Optional value of the required tag. Separate multiple values with commas.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

restricted-common-ports

Checks whether security groups that are in use disallow unrestricted incoming TCP traffic to the specified ports.

Identifier: RESTRICTED_INCOMING_TRAFFIC

Trigger type: Configuration changes

Parameters:

blockedPort1

Blocked TCP port number.

blockedPort2

Blocked TCP port number.

blockedPort3

Blocked TCP port number.

blockedPort4

Blocked TCP port number.

blockedPort5

Blocked TCP port number.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

restricted-ssh

Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.

Identifier: INCOMING_SSH_DISABLED


Trigger type: Configuration changes

Parameters:

None

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

root-account-mfa-enabled

Checks whether users of your AWS account require a multi-factor authentication (MFA) device to sign in with root credentials.

Identifier: ROOT_ACCOUNT_MFA_ENABLED


Trigger type: Periodic

Parameters:

None

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

s3-bucket-logging-enabled

Checks whether logging is enabled for your S3 buckets.

Identifier: S3_BUCKET_LOGGING_ENABLED

Trigger type: Configuration changes

Parameters:

targetBucket


Target S3 bucket for storing server access logs.

targetPrefix

Prefix of the target S3 bucket for storing server access logs.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

s3-bucket-ssl-requests-only

Checks whether S3 buckets have policies that require requests to use Secure Socket Layer (SSL).

Identifier: S3_BUCKET_SSL_REQUESTS_ONLY

Trigger type: Configuration changes

Parameters:

None

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

s3-bucket-versioning-enabled

Checks whether versioning is enabled for your S3 buckets. Optionally, the rule checks if MFA delete is enabled for your S3 buckets.

Identifier: S3_BUCKET_VERSIONING_ENABLED

Trigger type: Configuration changes


Parameters:

isMfaDeleteEnabled

MFA delete is enabled for your S3 buckets.

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed rules with AWS CloudFormation templates \(p. 47\)](#).

View	Launch
View	

Working with AWS Managed Rules

You can set up and activate AWS managed rules from the AWS Management Console, AWS CLI, or AWS Config API.

To set up and activate an AWS managed rule (console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. On the **Rules** page, choose **Add rule**.
5. On the **Rules** page, you can do the following:
 - Type in the search field to filter results by rule name, description, and label. For example, type **EC2** to return rules that evaluate EC2 resource types or type **periodic** to return rules that are triggered periodically.

- Choose the arrow icon to see the next page of rules. Recently added rules are marked as **New**.
- 6. Choose a rule that you want to create.
- 7. On the **Configure rule** page, configure the rule by completing the following steps:
 - a. For **Name**, type a unique name for the rule.
 - b. If the trigger types for your rule include **Configuration changes**, specify one of the following options for **Scope of changes** with which AWS Config invokes your Lambda function:
 - **Resources** – When a resource that matches the specified resource type, or the type plus identifier, is created, changed, or deleted.
 - **Tags** – When a resource with the specified tag is created, changed, or deleted.
 - **All changes** – When a resource recorded by AWS Config is created, changed, or deleted.
 - c. If the trigger types for your rule include **Periodic**, specify the **Frequency** with which AWS Config invokes your Lambda function.
 - d. If your rule includes parameters in the **Rule parameters** section, you can customize the values for the provided keys. A parameter is an attribute that your resources must have before they are considered compliant with the rule.
- 8. Choose **Save**. Your new rule displays on the **Rules** page.

Compliance will display **Evaluating...** until AWS Config has evaluation results for your rule. A summary of the results appears after several minutes. You can update the results with the refresh button.

If the rule or function is not working as expected, you might see one of the following for **Compliance**:

- **No results reported** - AWS Config evaluated your resources against the rule. The rule did not apply to the AWS resources in its scope, the specified resources were deleted, or the evaluation results were deleted. To get evaluation results, update the rule, change its scope, or choose **Re-evaluate**.

This message may also appear if the rule didn't report evaluation results.

- **No resources in scope** - AWS Config cannot evaluate your recorded AWS resources against this rule because none of your resources are within the rule's scope. To get evaluation results, edit the rule and change its scope, or add resources for AWS Config to record by using the **Settings** page.
- **Evaluations failed** - For information that can help you determine the problem, choose the rule name to open its details page and see the error message.

To set up and activate an AWS managed rule (AWS CLI)

- Use the `put-config-rule` command.

To set up and activate an AWS managed rule (AWS Config API)

- Use the `PutConfigRule` action.

Creating AWS Config Managed rules with AWS CloudFormation templates

For supported AWS Config managed rules, you can use the AWS CloudFormation templates to create the rule for your account or update an existing AWS CloudFormation stack. A stack is a collection of related resources that you provision and update as a single unit. When you launch a stack with a template, the AWS Config managed rule is created for you. The templates create only the rule, and don't create additional AWS resources.

Note

When AWS Config managed rules are updated, the templates are updated for the latest changes. To save a specific version of a template for a rule, download the template, and upload it to your S3 bucket.

For more information about working with AWS CloudFormation templates, see [Getting Started with AWS CloudFormation](#) in the *AWS CloudFormation User Guide*.

To launch an AWS CloudFormation stack for an AWS Config managed rule

1. Choose a rule from the list of [AWS Managed Config Rules \(p. 29\)](#).
2. Choose **View** to download a template or choose **Launch Stack**. If you choose **Launch Stack**, skip to step 4.
3. Go to the [CloudFormation console](#) and create a new stack.
4. For **Select Template**:
 - If you downloaded the template, choose **Upload a template to Amazon S3**, and then choose **Browse** to upload the template.
 - If you chose the **Launch Stack** button, the template URL appears automatically in the **Specify an Amazon S3 template URL** field.
5. Choose **Next**.
6. For **Specify Details**, type a stack name and enter parameter values for the AWS Config rule. For example, if you are using the `DESIRED_INSTANCE_TYPE` managed rule template, you can specify the instance type such as "m4.large".
7. Choose **Next**.
8. For **Options**, you can create tags or configure other advanced options. These are not required.
9. Choose **Next**.
10. For **Review**, verify that the template, parameters, and other options are correct.
11. Choose **Create**. The stack is created in a few minutes. You can view the created rule in the [AWS Config console](#).

You can use the templates to create a single stack for AWS Config managed rules or update an existing stack in your account. If you delete a stack, the managed rules created from that stack are also deleted. For more information, see [Working with Stacks](#) in the *AWS CloudFormation User Guide*.

Developing Custom Rules for AWS Config

You can develop custom rules and add them to AWS Config. You associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.

You associate this function with your rule, and the rule invokes the function either in response to configuration changes or periodically. The function then evaluates whether your resources comply with your rule, and sends its evaluation results to AWS Config.

The exercise in [Getting Started with Custom Rules \(p. 49\)](#) guides you through creating a custom rule for the first time. It includes an example function that you can add to AWS Lambda with no modification.

To learn how AWS Lambda functions work and how to develop them, see the [AWS Lambda Developer Guide](#).

Topics

- [Getting Started with Custom Rules \(p. 49\)](#)

- [Developing a Custom Rule for AWS Config \(p. 51\)](#)
- [Example AWS Lambda Functions and Events for AWS Config Rules \(p. 54\)](#)

Getting Started with Custom Rules

This procedure guides you through the process of creating a custom rule that evaluates whether each of your EC2 instances is the t2.micro type. AWS Config will run event-based evaluations for this rule, meaning it will check your instance configurations each time AWS Config detects a configuration change in an instance. AWS Config will flag t2.micro instances as compliant and all other instances as noncompliant. The compliance status will appear in the AWS Config console.

To have the best outcome with this procedure, you should have one or more EC2 instances in your AWS account. Your instances should include a combination of at least one t2.micro instance and other types.

To create this rule, first, you will create an AWS Lambda function by customizing a blueprint in the AWS Lambda console. Then, you will create a custom rule in AWS Config, and you will associate the rule with the function.

To create the AWS Lambda function for your custom rule

1. Sign in to the AWS Management Console and open the AWS Lambda console at <https://console.aws.amazon.com/lambda/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. In the AWS Lambda console, choose **Create a Lambda function**.
4. On the **Select blueprint** page, for **filter**, type **config-rule-change-triggered**. Select the blueprint in the filter results.
5. On the **Configure triggers** page, choose **Next**.
6. On the **Configure function** page, complete the following steps:
 - a. For **Name**, type `InstanceTypeCheck`.
 - b. For **Runtime**, keep **Node.js**.
 - c. For **Code entry type**, keep **Edit code inline**. The Node.js code for your function is provided in the code editor. For this procedure, you do not need to change the code.
 - d. For **Handler**, keep `index.handler`.
 - e. For **Role**, choose **Create new role from template(s)**.
 - f. For **Role name**, type a name.
 - g. For **Policy templates**, choose **AWS Config Rules permission**.
 - h. On the **Configure function** page, choose **Next**.
 - i. On the **Review page**, verify the details about your function, and choose **Create function**. The AWS Lambda console displays your function.
7. To verify that your function is set up correctly, test it with the following steps:
 - a. Choose **Actions**, and then choose **Configure test event**.
 - b. In the **Input test event** window, for **Sample event template**, choose **AWS Config Change Triggered Rule**.
 - c. Choose **Save and test**. AWS Lambda tests your function with the example event. If your function is working as expected, an error message similar to the following appears under **Execution result**:

```
{
  "errorMessage": "Result Token provided is invalid",
```

```
"errorType": "InvalidResultTokenException",  
. . .
```

The `InvalidResultTokenException` is expected because your function runs successfully only when it receives a *result token* from AWS Config. The result token identifies the AWS Config rule and the event that caused the evaluation, and the result token associates an evaluation with a rule. This exception indicates that your function has the permission it needs to send results to AWS Config. Otherwise, the following error message appears: `not authorized to perform: config:PutEvaluations`. If this error occurs, update the role that you assigned to your function to allow the `config:PutEvaluations` action, and test your function again.

To add your custom rule to AWS Config

1. Open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to the same region in which you created the AWS Lambda function for your custom rule.
3. On the **Rules** page, choose **Add rule**.
4. On the **Add rule** page, choose **Add custom rule**.
5. On the **Configure rule** page, complete the following steps:
 - a. For **Name**, type `InstanceTypesAreT2micro`.
 - b. For **Description**, type `Evaluates whether EC2 instances are the t2.micro type`.
 - c. For **AWS Lambda function ARN**, specify the ARN that AWS Lambda assigned to your function.

Note

The ARN that you specify in this step must not include the `$LATEST` qualifier. You can specify an ARN without a version qualifier or with any qualifier besides `$LATEST`. AWS Lambda supports function versioning, and each version is assigned an ARN with a qualifier. AWS Lambda uses the `$LATEST` qualifier for the latest version.

- d. For **Trigger type**, choose **Configuration changes**.
 - e. For **Scope of changes**, choose **Resources**.
 - f. For **Resources**, choose **Instance**.
 - g. In the **Rule parameters** section, you must specify the rule parameter that your AWS Lambda function evaluates and the desired value. The function for this procedure evaluates the `desiredInstanceType` parameter.
- For **Key**, type `desiredInstanceType`. For **Value**, type `t2.micro`.
6. Choose **Save**. Your new rule displays on the **Rules** page.

Compliance will display **Evaluating...** until AWS Config receives evaluation results from your AWS Lambda function. If the rule and the function are working as expected, a summary of the results appears after several minutes. For example, a result of **2 noncompliant resource(s)** indicates that 2 of your instances are not `t2.micro` instances, and a result of **Compliant** indicates that all instances are `t2.micro`. You can update the results with the refresh button.

If the rule or function is not working as expected, you might see one of the following for **Compliance**:

- **No results reported** - AWS Config evaluated your resources against the rule. The rule did not apply to the AWS resources in its scope, the specified resources were deleted, or the evaluation results were deleted. To get evaluation results, update the rule, change its scope, or choose **Re-evaluate**.

Verify that the scope includes **Instance** for **Resources**, and try again.

- **No resources in scope** - AWS Config cannot evaluate your recorded AWS resources against this rule because none of your resources are within the rule's scope. To get evaluation results, edit the rule and change its scope, or add resources for AWS Config to record by using the **Settings** page.

Verify that AWS Config is recording EC2 instances.

- **Evaluations failed** - For information that can help you determine the problem, choose the rule name to open its details page and see the error message.

If your rule works correctly and AWS Config provides evaluation results, you can learn which conditions affect the compliance status of your rule. You can learn which resources, if any, are noncompliant, and why. For more information, see [Viewing Configuration Compliance](#) (p. 62).

Developing a Custom Rule for AWS Config

Complete the following procedure to create a custom rule. To create a custom rule, you first create an AWS Lambda function, which contains the evaluation logic for the rule. Then you associate the function with a custom rule that you create in AWS Config.

Contents

- [Creating an AWS Lambda Function for a Custom Config Rule](#) (p. 51)
- [Creating a Custom Rule in AWS Config](#) (p. 52)
- [Evaluating Additional Resource Types](#) (p. 53)

Creating an AWS Lambda Function for a Custom Config Rule

A *Lambda function* is custom code that you upload to AWS Lambda, and it is invoked by events that are published to it by an event source. If the Lambda function is associated with a Config rule, AWS Config invokes it when the rule's trigger occurs. The Lambda function then evaluates the configuration information that is sent by AWS Config, and it returns the evaluation results. For more information about Lambda functions, see [Function and Event Sources](#) in the *AWS Lambda Developer Guide*.

You can use a programming language that is supported by AWS Lambda to create a Lambda function for a custom rule. To make this task easier, you can customize an AWS Lambda blueprint or reuse a sample function from the AWS Config Rules GitHub repository.

AWS Lambda blueprints

The AWS Lambda console provides sample functions, or *blueprints*, which you can customize by adding your own evaluation logic. When you create a function, you can choose one of the following blueprints:

- **config-rule-change-triggered** – Triggered when your AWS resource configurations change.
- **config-rule-periodic** – Triggered at a frequency that you choose (for example, every 24 hours).

AWS Config Rules GitHub repository

A public repository of sample functions for custom rules is available on GitHub, a web-based code hosting and sharing service. The sample functions are developed and contributed by the AWS community. If you want to use a sample, you can copy its code into a new AWS Lambda function. To view the repository, see <https://github.com/aws-labs/aws-config-rules/>.

To create the function for your custom rule

1. Sign in to the AWS Management Console and open the AWS Lambda console at <https://console.aws.amazon.com/lambda/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. Choose **Create a Lambda function**.

4. On the **Select blueprint** page, you can choose one of the blueprint functions for AWS Config rules as a starting point, or you can proceed without a blueprint by choosing **Skip**.
5. On the **Configure triggers** page, choose **Next**.
6. On the **Configure function** page, type a name and description.
7. For **Runtime**, choose the programming language in which your function is written.
8. For **Code entry type**, choose your preferred entry type. If you are using a blueprint, keep **Edit code inline**.
9. Provide your code using the method required by the code entry type that you selected. If you are using a blueprint, the function code is provided in the code editor, and you can customize it to include your own evaluation logic. Your code can evaluate the event data that AWS Config provides when it invokes your function:
 - For functions based on the **config-rule-change-triggered** blueprint, or for functions triggered by configuration changes, the event data is the configuration item or an oversized configuration item object for the AWS resource that changed.
 - For functions based on the **config-rule-periodic** blueprint, or for functions triggered at a frequency that you choose, the event data is a JSON object that includes information about when the evaluation was triggered.
 - For both types of functions, AWS Config passes rule parameters in JSON format. You can define which rule parameters are passed when you create the custom rule in AWS Config.
 - For example events that AWS Config publishes when it invokes your function, see [Example Events for AWS Config Rules \(p. 59\)](#).
10. For **Handler**, specify the handler for your function. If you are using a blueprint, keep the default value.
11. For **Role**, choose **Create new role from template(s)**.
12. For **Role name**, type a name.
13. For **Policy templates**, choose **AWS Config Rules permission**.
14. On the **Configure function** page, choose **Next**.
15. On the **Review page**, verify the details about your function, and choose **Create function**.

Creating a Custom Rule in AWS Config

Use AWS Config to create a custom rule and associate the rule with a Lambda function.

To create a custom rule

1. Open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to the same region in which you created the AWS Lambda function for your custom rule.
3. On the **Rules** page, choose **Add rule**.
4. On the **Add rule** page, choose **Add custom rule**.
5. On the **Configure rule** page, type a name and description.
6. For **AWS Lambda function ARN**, specify the ARN that AWS Lambda assigned to your function.

Note

The ARN that you specify in this step must not include the `$LATEST` qualifier. You can specify an ARN without a version qualifier or with any qualifier besides `$LATEST`. AWS Lambda supports function versioning, and each version is assigned an ARN with a qualifier. AWS Lambda uses the `$LATEST` qualifier for the latest version.

7. For **Trigger type**, choose one or both of the following:
 - **Configuration changes** – AWS Config invokes your Lambda function when it detects a configuration change.

- **Periodic** – AWS Config invokes your Lambda function at the frequency that you choose (for example, every 24 hours).
8. If the trigger types for your rule include **Configuration changes**, specify one of the following options for **Scope of changes** with which AWS Config invokes your Lambda function:
 - **Resources** – When a resource that matches the specified resource type, or the type plus identifier, is created, changed, or deleted.
 - **Tags** – When a resource with the specified tag is created, changed, or deleted.
 - **All changes** – When a resource recorded by AWS Config is created, changed, or deleted.
 9. If the trigger types for your rule include **Periodic**, specify the **Frequency** with which AWS Config invokes your Lambda function.
 10. In the **Rule parameters** section, specify any rule parameters that your AWS Lambda function evaluates and the desired value.
 11. Choose **Save**. Your new rule displays on the **Rules** page.

Compliance will display **Evaluating...** until AWS Config receives evaluation results from your AWS Lambda function. If the rule and the function are working as expected, a summary of results appears after several minutes. You can update the results with the refresh button.

If the rule or function is not working as expected, you might see one of the following for **Compliance**:

- **No results reported** - AWS Config evaluated your resources against the rule. The rule did not apply to the AWS resources in its scope, the specified resources were deleted, or the evaluation results were deleted. To get evaluation results, update the rule, change its scope, or choose **Re-evaluate**.

This message may also appear if the rule didn't report evaluation results.

- **No resources in scope** - AWS Config cannot evaluate your recorded AWS resources against this rule because none of your resources are within the rule's scope. You can choose which resources AWS Config records on the **Settings** page.
- **Evaluations failed** - For information that can help you determine the problem, choose the rule name to open its details page and see the error message.

Note

When you create a custom rule with the AWS Config console, the appropriate permissions are automatically created for you. If you create a custom rule with the AWS CLI, you need to give AWS Config permission to invoke your Lambda function, using the `aws lambda add-permission` command. For more information, see [Using Resource-Based Policies for AWS Lambda \(Lambda Function Policies\)](#) in the *AWS Lambda Developer Guide*.

Evaluating Additional Resource Types

You can create custom rules to run evaluations for resource types not yet recorded by AWS Config. This is useful if you want to evaluate compliance for additional resource types, such as Amazon Glacier vaults or Amazon SNS topics, that AWS Config doesn't currently record. For a list of additional resource types that you can evaluate with custom rules, see [AWS Resource Types Reference](#).

Example

1. You want to evaluate Amazon Glacier vaults in your account. Amazon Glacier vault resources are currently not recorded by AWS Config.
2. You create an AWS Lambda function that evaluates whether your Amazon Glacier vaults comply with your account requirements.
3. You create a custom rule named **evaluate-glacier-vaults** and then assign your AWS Lambda function to the rule.

4. AWS Config invokes your Lambda function and then evaluates the Amazon Glacier vaults against your rule.
5. AWS Config returns the evaluations and you can view the compliance results for your rule.

Note

You can view the configuration details in the AWS Config timeline and look up resources in the AWS Config console for resources that AWS Config supports. If you configured AWS Config to record all resource types, newly supported resources will automatically be recorded. For more information, see [Supported Resources, Configuration Items, and Relationships](#) (p. 6).

Example AWS Lambda Functions and Events for AWS Config Rules

Each custom Config rule is associated with an AWS Lambda *function*, which is custom code that contains the evaluation logic for the rule. When the trigger for a Config rule occurs (for example, when AWS Config detects a configuration change), AWS Config invokes the rule's Lambda function by publishing an *event*, which is a JSON object that provides the configuration data that the function evaluates.

For more information about functions and events in AWS Lambda, see [Function and Event Sources](#) in the *AWS Lambda Developer Guide*.

Topics

- [Example AWS Lambda Functions for AWS Config Rules \(Node.js\)](#) (p. 54)
- [Example Events for AWS Config Rules](#) (p. 59)

Example AWS Lambda Functions for AWS Config Rules (Node.js)

AWS Lambda executes functions in response to events that are published by AWS services. The function for a custom Config rule receives an event that is published by AWS Config, and the function then uses data that it receives from the event and that it retrieves from the AWS Config API to evaluate the compliance of the rule. The operations in a function for a Config rule differ depending on whether it performs an evaluation that is triggered by configuration changes or triggered periodically.

For information about common patterns within AWS Lambda functions, see [Programming Model](#) in the *AWS Lambda Developer Guide*.

Contents

- [Example Function for Evaluations Triggered by Configuration Changes](#) (p. 54)
- [Example Function for Periodic Evaluations](#) (p. 57)

Example Function for Evaluations Triggered by Configuration Changes

AWS Config will invoke a function like the following example when it detects a configuration change for a resource that is within a custom rule's scope.

If you use the AWS Config console to create a rule that is associated with a function like this example, choose **Configuration changes** as the trigger type. If you use the AWS Config API or AWS CLI to create the rule, set the `MessageType` attribute to `ConfigurationItemChangeNotification` and `OversizedConfigurationItemChangeNotification`. These settings enable your rule to be triggered whenever AWS Config generates a configuration item or an oversized configuration item as a result of a resource change.

This example evaluates your resources and checks whether the instances match the resource type, `AWS::EC2::Instance`. The rule is triggered when AWS Config generates a configuration item or an oversized configuration item notification.

```
'use strict';

const aws = require('aws-sdk');

const config = new aws.ConfigService();

// Helper function used to validate input
function checkDefined(reference, referenceName) {
  if (!reference) {
    throw new Error(`Error: ${referenceName} is not defined`);
  }
  return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
  checkDefined(messageType, 'messageType');
  return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory API.
function getConfiguration(resourceType, resourceId, configurationCaptureTime, callback) {
  config.getResourceConfigHistory({ resourceType, resourceId, laterTime: new
    Date(configurationCaptureTime), limit: 1 }, (err, data) => {
    if (err) {
      callback(err, null);
    }
    const configurationItem = data.configurationItems[0];
    callback(null, configurationItem);
  });
}

// Convert the oversized configuration item from the API model to the original invocation
// model.
function convertApiConfiguration(apiConfiguration) {
  apiConfiguration.awsAccountId = apiConfiguration.accountId;
  apiConfiguration.ARN = apiConfiguration.arn;
  apiConfiguration.configurationStateMd5Hash = apiConfiguration.configurationItemMD5Hash;
  apiConfiguration.configurationItemVersion = apiConfiguration.version;
  apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
  if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
    for (let i = 0; i < apiConfiguration.relationships.length; i++) {
      apiConfiguration.relationships[i].name =
        apiConfiguration.relationships[i].relationshipName;
    }
  }
  return apiConfiguration;
}

// Based on the message type, get the configuration item either from the configurationItem
// object in the invoking event or with the getResourceConfigHistory API in the
// getConfiguration function.
function getConfigurationItem(invokingEvent, callback) {
  checkDefined(invokingEvent, 'invokingEvent');
  if (isOverSizedChangeNotification(invokingEvent.messageType)) {
    const configurationItemSummary =
      checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
    getConfiguration(configurationItemSummary.resourceType,
      configurationItemSummary.resourceId,
      configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem) => {
```

```

        if (err) {
            callback(err);
        }
        const configurationItem = convertApiConfiguration(apiConfigurationItem);
        callback(null, configurationItem);
    });
} else {
    checkDefined(invokingEvent.configurationItem, 'configurationItem');
    callback(null, invokingEvent.configurationItem);
}
}

// Check whether the resource has been deleted. If the resource was deleted, then the
// evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope ===
    false;
}

// In this example, the resource is compliant if it is an instance and its type matches the
// type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration, 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
    configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
exports.handler = (event, context, callback) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    getConfigurationItem(invokingEvent, (err, configurationItem) => {
        if (err) {
            callback(err);
        }
        let compliance = 'NOT_APPLICABLE';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
            ruleParameters);
        }
        // Initializes the request that contains the evaluation results.
        putEvaluationsRequest.Evaluations = [
            {
                ComplianceResourceType: configurationItem.resourceType,
                ComplianceResourceId: configurationItem.resourceId,
                ComplianceType: compliance,
                OrderingTimestamp: configurationItem.configurationItemCaptureTime,
            },
        ];
        putEvaluationsRequest.ResultToken = event.resultToken;
    });
}

```

```
// Sends the evaluation results to AWS Config.
config.putEvaluations(putEvaluationsRequest, (error, data) => {
    if (error) {
        callback(error, null);
    } else if (data.FailedEvaluations.length > 0) {
        // Ends the function if evaluation results are not successfully reported to
        AWS Config.
        callback(JSON.stringify(data), null);
    } else {
        callback(null, data);
    }
});
});
};
```

Function Operations

The function performs the following operations at runtime:

1. The function runs when AWS Lambda passes the `event` object to the `handler` function. AWS Lambda also passes a `context` object, which contains information and methods that the function can use while it runs. In this example, the function accepts the optional `callback` parameter, which it uses to return information to the caller.
2. The function checks whether the `messageType` for the event is a configuration item or an oversized configuration item, and then returns the configuration item.
3. The handler calls the `isApplicable` function to determine whether the resource was deleted.
4. The handler calls the `evaluateChangeNotificationCompliance` function and passes the `configurationItem` and `ruleParameters` objects that AWS Config published in the event.

The function first evaluates whether the resource is an EC2 instance. If the resource is not an EC2 instance, the function returns a compliance value of `NOT_APPLICABLE`.

The function then evaluates whether the `instanceType` attribute in the configuration item is equal to the `desiredInstanceType` parameter value. If the values are equal, the function returns `COMPLIANT`. If the values are not equal, the function returns `NON_COMPLIANT`.

5. The handler prepares to send the evaluation results to AWS Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result, the resource type, and the ID of the resource that was evaluated. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for AWS Config.
6. The handler sends the evaluation results to AWS Config by passing the object to the `putEvaluations` method of the `config` client.

Example Function for Periodic Evaluations

AWS Config will invoke a function like the following example for periodic evaluations. Periodic evaluations occur at the frequency that you specify when you define the rule in AWS Config.

If you use the AWS Config console to create a rule that is associated with a function like this example, choose **Periodic** as the trigger type. If you use the AWS Config API or AWS CLI to create the rule, set the `MessageType` attribute to `ScheduledNotification`.

This example checks whether the total number of a specified resource exceeds a specified maximum.

```
var aws = require('aws-sdk'), // Loads the AWS SDK for JavaScript.
    config = new aws.ConfigService(), // Constructs a service object to use the
    aws.ConfigService class.
```

```
    COMPLIANCE_STATES = {
        COMPLIANT : 'COMPLIANT',
        NON_COMPLIANT : 'NON_COMPLIANT',
        NOT_APPLICABLE : 'NOT_APPLICABLE'
    };

// Receives the event and context from AWS Lambda.
exports.handler = function(event, context, callback) {
    // Parses the invokingEvent and ruleParameters values, which contain JSON objects
    // passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        noOfResources = 0;

    if (isScheduledNotification(invokingEvent)) {
        countResourceTypes(ruleParameters.applicableResourceType, "", noOfResources,
        function(err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                // Initializes the request that contains the evaluation results.
                putEvaluationsRequest = {
                    Evaluations : [ {
                        // Applies the evaluation result to the AWS account published in
                        // the event.
                        ComplianceResourceType : 'AWS:::Account',
                        ComplianceResourceId : event.accountId,
                        ComplianceType : evaluateCompliance(ruleParameters.maxCount,
                        count),
                        OrderingTimestamp : new Date()
                    } ],
                    ResultToken : event.resultToken
                };
                // Sends the evaluation results to AWS Config.
                config.putEvaluations(putEvaluationsRequest, function(err, data) {
                    if (err) {
                        callback(err, null);
                    } else {
                        if (data.FailedEvaluations.length > 0) {
                            // Ends the function execution if evaluation results are not
                            // successfully reported
                            callback(JSON.stringify(data));
                        }
                        callback(null, data);
                    }
                });
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
        Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return COMPLIANCE_STATES.NON_COMPLIANT;
    } else {
        return COMPLIANCE_STATES.COMPLIANT;
    }
}
```

```
    }  
  }  
  
  // Counts the applicable resources that belong to the AWS account.  
  function countResourceTypes(applicableResourceType, nextToken, count, callback) {  
    config.listDiscoveredResources({resourceType : applicableResourceType, nextToken :  
      nextToken}, function(err, data) {  
      if (err) {  
        callback(err, null);  
      } else {  
        count = count + data.resourceIdentifiers.length;  
        if (data.nextToken !== undefined && data.nextToken !== null) {  
          countResourceTypes(applicableResourceType, data.nextToken, count,  
            callback);  
        }  
        callback(null, count);  
      }  
    }  
  });  
  return count;  
}
```

Function Operations

The function performs the following operations at runtime:

1. The function runs when AWS Lambda passes the `event` object to the `handler` function. AWS Lambda also passes a `context` object, which contains information and methods that the function can use while it runs. In this example, the function accepts the optional `callback` parameter, which it uses to return information to the caller.
2. To count the resources of the specified type, the handler calls the `countResourceTypes` function, and it passes the `applicableResourceType` parameter that it received from the event. The `countResourceTypes` function calls the `listDiscoveredResources` method of the `config` client, which returns a list of identifiers for the applicable resources. The function uses the length of this list to determine the number of applicable resources, and it returns this count to the handler.
3. The handler prepares to send the evaluation results to AWS Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result and the AWS account that was published in the event. You can use the `Evaluations` parameter to apply the result to any resource type that is supported by AWS Config. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for AWS Config.
4. Within the `putEvaluationsRequest` object, the handler calls the `evaluateCompliance` function. This function tests whether the number of applicable resources exceeds the maximum assigned to the `maxCount` parameter, which was provided by the event. If the number of resources exceeds the maximum, the function returns `NON_COMPLIANT`. If the number of resources does not exceed the maximum, the function returns `COMPLIANT`.
5. The handler sends the evaluation results to AWS Config by passing the object to the `putEvaluations` method of the `config` client.

Example Events for AWS Config Rules

When the trigger for a rule occurs, AWS Config invokes the rule's AWS Lambda function by publishing an event. Then AWS Lambda executes the function by passing the event to the function's handler.

Example Event for Evaluations Triggered by Configuration Changes

AWS Config publishes an event when it detects a configuration change for a resource that is within a rule's scope. The following example event shows that the rule was triggered by a configuration change for an EC2 instance.


```
{
  "invokingEvent": "{\n\"configurationItem\":{\n\"configurationItemCaptureTime\":\n\"2016-02-17T01:36:34.043Z\", \n\"awsAccountId\": \"123456789012\", \n\"configurationItemStatus\":\n\"OK\", \n\"resourceId\": \"i-00000000\", \n\"ARN\": \"arn:aws:ec2:us-east-1:123456789012:instance/\ni-00000000\", \n\"awsRegion\": \"us-east-1\", \n\"availabilityZone\": \"us-east-1a\", \n\"resourceType\": \"AWS::EC2::Instance\", \n\"tags\": {\n\"Foo\": \"Bar\"}, \n\"relationships\":\n[{\n\"resourceId\": \"eipalloc-00000000\", \n\"resourceType\": \"AWS::EC2::EIP\", \n\"name\":\n\"Is attached to ElasticIp\"}], \n\"configuration\": {\n\"foo\": \"bar\"}, \n\"messageType\":\n\"ConfigurationItemChangeNotification\" }",
  "ruleParameters": "{\n\"myParameterKey\": \"myParameterValue\" }",
  "resultToken": "myResultToken",
  "eventLeftScope": false,
  "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
  "configRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/config-rule-0123456",
  "configRuleName": "change-triggered-config-rule",
  "configRuleId": "config-rule-0123456",
  "accountId": "123456789012",
  "version": "1.0"
}
```

Example Event for Evaluations Triggered by Oversized Configuration Changes

Some resource changes generate oversized configuration items. The following example event shows that the rule was triggered by an oversized configuration change for an EC2 instance.

```
{
  "invokingEvent": "{\n\"configurationItemSummary\": {\n\"changeType\": \"UPDATE\n\", \n\"configurationItemVersion\": \"1.2\", \n\"configurationItemCaptureTime\":\n\"2016-10-06T16:46:16.261Z\", \n\"configurationStateId\": 0, \n\"awsAccountId\": \"123456789012\", \n\"configurationItemStatus\": \"OK\", \n\"resourceType\": \"AWS::EC2::Instance\", \n\"resourceId\": \"i-00000000\", \n\"resourceName\": null, \n\"ARN\": \"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\", \n\"awsRegion\": \"us-west-2\", \n\"availabilityZone\": \"us-west-2a\", \n\"configurationStateMd5Hash\": \"8f1ee69b287895a0f8bc5753eca68e96\", \n\"resourceCreationTime\": \"2016-10-06T16:46:10.489Z\" }, \n\"messageType\":\n\"OversizedConfigurationItemChangeNotification\" }",
  "ruleParameters": "{\n\"myParameterKey\": \"myParameterValue\" }",
  "resultToken": "myResultToken",
  "eventLeftScope": false,
  "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
  "configRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/config-rule-ec2-managed-instance-inventory",
  "configRuleName": "change-triggered-config-rule",
  "configRuleId": "config-rule-0123456",
  "accountId": "123456789012",
  "version": "1.0"
}
```

Example Event for Evaluations Triggered by Periodic Frequency

AWS Config publishes an event when it evaluates your resources at a frequency that you specify (such as every 24 hours). The following example event shows that the rule was triggered by a periodic frequency.

```
{
  "invokingEvent": "{\n\"awsAccountId\": \"123456789012\", \n\"notificationCreationTime\":\n\"2016-07-13T21:50:00.373Z\", \n\"messageType\": \"ScheduledNotification\", \n\"recordVersion\":\n\"1.0\" }",
  "ruleParameters": "{\n\"myParameterKey\": \"myParameterValue\" }",
  "resultToken": "myResultToken",
  "eventLeftScope": false,
  "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
}
```

```
"configRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/config-rule-0123456",
"configRuleName": "periodic-config-rule",
"configRuleId": "config-rule-6543210",
"accountId": "123456789012",
"version": "1.0"
}
```

Event Attributes

The JSON object for an AWS Config event contains the following attributes:

invokingEvent

The event that triggers the evaluation for a rule. If the event is published in response to a resource configuration change, the value for this attribute is a string that contains a JSON `configurationItem` or a `configurationItemSummary` (for oversized configuration items). The configuration item represents the state of the resource at the moment that AWS Config detected the change. For an example of a configuration item, see the output produced by the `get-resource-config-history` AWS CLI command in [View Configuration History \(p. 74\)](#).

If the event is published for a periodic evaluation, the value is a string that contains a JSON object. The object includes information about the evaluation that was triggered.

For each type of event, a function must parse the string with a JSON parser to be able to evaluate its contents, as shown in the following Node.js example:

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

ruleParameters

Key/value pairs that the function processes as part of its evaluation logic. You define parameters when you use the AWS Config console to create a custom rule. You can also define parameters with the `InputParameters` attribute in the `PutConfigRule` AWS Config API request or the `put-config-rule` AWS CLI command.

The JSON code for the parameters is contained within a string, so a function must parse the string with a JSON parser to be able to evaluate its contents, as shown in the following Node.js example:

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

resultToken

A token that the function must pass to AWS Config with the `PutEvaluations` call.

eventLeftScope

A Boolean value that indicates whether the AWS resource to be evaluated has been removed from the rule's scope. If the value is `true`, the function indicates that the evaluation can be ignored by passing `NOT_APPLICABLE` as the value for the `ComplianceType` attribute in the `PutEvaluations` call.

executionRoleArn

The ARN of the IAM role that is assigned to AWS Config.

configRuleArn

The ARN that AWS Config assigned to the rule.

configRuleName

The name that you assigned to the rule that caused AWS Config to publish the event and invoke the function.

`configRuleId`

The ID that AWS Config assigned to the rule.

`accountId`

The ID of the AWS account that owns the rule.

`version`


A version number assigned by AWS. The version will increment if AWS adds attributes to AWS Config events. If a function requires an attribute that is only in events that match or exceed a specific version, then that function can check the value of this attribute.

The current version for AWS Config events is 1.0.

Viewing Configuration Compliance

You can use the AWS Config console, AWS CLI, or AWS Config API to view the compliance state of your rules and resources.

To view compliance (console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Rules**. The console shows the **Rules** page, which lists your rules and the compliance status of each.
4. Choose a rule to view its **Rule details** page. This page shows the rule's configuration, its status, and any AWS resources that do not comply with it.
5. If the **Rule details** shows any noncompliant resources, choose the **Config timeline** icon () for a resource to see its configuration timeline page. The page shows the configuration settings that AWS Config captured when it detected that the resource was noncompliant. This information can help you determine why the resource fails to comply with the rule. For more information, see [Viewing Configuration Details in the AWS Config Console \(p. 73\)](#).

You can also view the compliance of your resources by looking them up on the **Resource inventory** page. For more information, see [Looking Up Resources That Are Discovered by AWS Config \(p. 71\)](#).

To view compliance (AWS CLI)

To view compliance, use any of the following CLI commands:

- To see the compliance state of each of your rules, use the `describe-compliance-by-config-rule` command, as shown in the following example:

```
$ aws configservice describe-compliance-by-config-rule
{
  "ComplianceByConfigRules": [
    {
      "Compliance": {
        "ComplianceContributorCount": {
          "CappedCount": 2,
          "CapExceeded": false
        }
      }
    }
  ]
}
```

```
        },
        "ComplianceType": "NON_COMPLIANT"
      },
      "ConfigRuleName": "instances-in-vpc"
    },
    {
      "Compliance": {
        "ComplianceType": "COMPLIANT"
      },
      "ConfigRuleName": "restricted-common-ports"
    },
    ...
  ]
}
```

For each rule that has a compliance type of `NON_COMPLIANT`, AWS Config returns the number of noncompliant resources for the `CappedCount` parameter.

- To see the compliance state of each resource that AWS Config evaluates for a specific rule, use the `get-compliance-details-by-config-rule` command, as shown in the following example:

```
$ aws configservice get-compliance-details-by-config-rule --config-rule-
name ConfigRuleName {
  "EvaluationResults": [
    {
      "EvaluationResultIdentifier": {
        "OrderingTimestamp": 1443610576.349,
        "EvaluationResultQualifier": {
          "ResourceType": "AWS::EC2::Instance",
          "ResourceId": "i-nnnnnnnn",
          "ConfigRuleName": "ConfigRuleName"
        }
      },
      "ResultRecordedTime": 1443751424.969,
      "ConfigRuleInvokedTime": 1443751421.208,
      "ComplianceType": "COMPLIANT"
    },
    {
      "EvaluationResultIdentifier": {
        "OrderingTimestamp": 1443610576.349,
        "EvaluationResultQualifier": {
          "ResourceType": "AWS::EC2::Instance",
          "ResourceId": "i-nnnnnnnn",
          "ConfigRuleName": "ConfigRuleName"
        }
      },
      "ResultRecordedTime": 1443751425.083,
      "ConfigRuleInvokedTime": 1443751421.301,
      "ComplianceType": "NON_COMPLIANT"
    },
    ...
  ]
}
```

- To see the compliance state for each AWS resource of a specific type, use the `describe-compliance-by-resource` command, as shown in the following example:

```
$ aws configservice describe-compliance-by-resource --resource-type AWS::EC2::Instance
{
  "ComplianceByResources": [
    {
      "ResourceType": "AWS::EC2::Instance",
      "ResourceId": "i-nnnnnnnn",
      "Compliance": {
        "ComplianceContributorCount": {
          "CappedCount": 1,
          "CapExceeded": false
        }
      }
    },
    ...
  ]
}
```

```
        "ComplianceType": "NON_COMPLIANT"
      },
    ],
    {
      "ResourceType": "AWS::EC2::Instance",
      "ResourceId": "i-nnnnnnnnn",
      "Compliance": {
        "ComplianceType": "COMPLIANT"
      }
    },
    ...
  ]
}
```

- To see the compliance details of an individual AWS resource, use the `get-compliance-details-by-resource` command.

```
$ aws configservice get-compliance-details-by-resource --resource-type AWS::EC2::Instance
--resource-id i-nnnnnnnnn
{
  "EvaluationResults": [
    {
      "EvaluationResultIdentifier": {
        "OrderingTimestamp": 1443610576.349,
        "EvaluationResultQualifier": {
          "ResourceType": "AWS::EC2::Instance",
          "ResourceId": "i-nnnnnnnnn",
          "ConfigRuleName": "instances-in-vpc"
        }
      },
      "ResultRecordedTime": 1443751425.083,
      "ConfigRuleInvokedTime": 1443751421.301,
      "ComplianceType": "NON_COMPLIANT"
    }
  ]
}
```

To view compliance (AWS Config API)

To view compliance, use any of the following API actions:

- To see the compliance state of each of your rules, use the `DescribeComplianceByConfigRule` action.
- To see the compliance state of each resource that AWS Config evaluates for a specific rule, use the `GetComplianceDetailsByConfigRule` action.
- To see the compliance state for each AWS resource of a specific type, use the `DescribeComplianceByResource` action.
- To see the compliance details of an individual AWS resource, use the `GetComplianceDetailsByResource` action. The details include which AWS Config rules evaluated the resource, when each rule last evaluated it, and whether the resource complies with each rule.

Managing your AWS Config Rules

You can use the AWS Config console, AWS CLI, and AWS Config API to view, add, and delete your rules.

Contents

- [Using the Console \(p. 65\)](#)
- [Using the AWS CLI \(p. 66\)](#)
- [Using the AWS Config API \(p. 68\)](#)

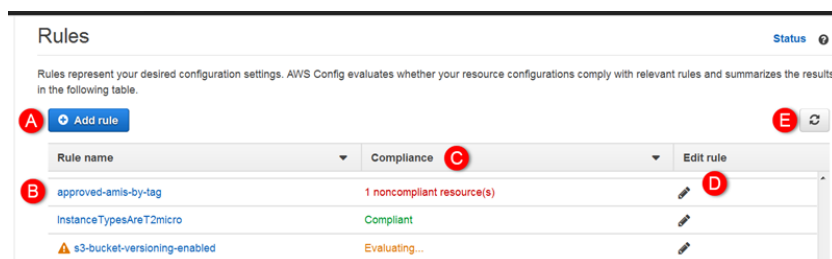
- [Deleting Evaluation Results \(p. 68\)](#)

Using the Console

On the **Rules** page, you can view the rules for the region in your account. You can also see the evaluation status for each rule.

To view your rules

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. Choose **Rules**. The **Rules** page shows your rules and the compliance status for each.



- A. Choose **Add rule** to get started with creating a rule.
- B. Choose a rule name to see its settings.
- C. See the compliance status of the rule when it evaluates your resources.
- D. Choose the **Edit rule** icon (✎) to edit the rule.
- E. Choose the refresh (↻) icon to reload compliance results.

To update a rule

1. Choose the **Edit rule** icon (✎) for the rule that you want to update.
2. Modify the settings on the **Configure rule** page to change your rule as needed.
3. Choose **Save**.

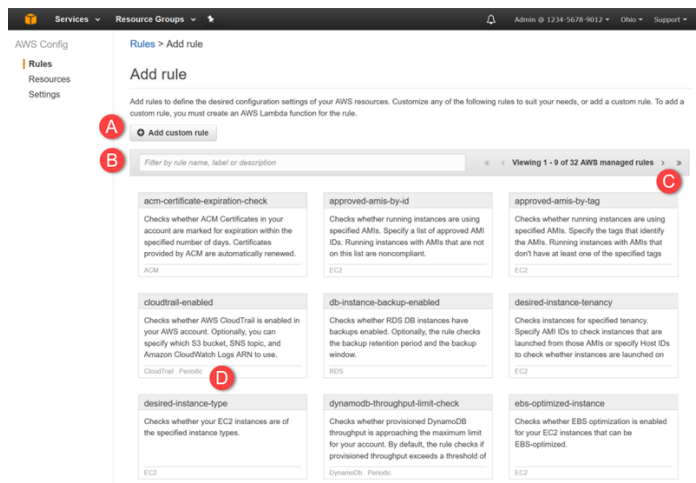
To delete a rule

1. Choose the **Edit rule** icon (✎) for the rule that you want to delete.
2. On the **Configure rule** page, choose **Delete rule**.
3. When prompted, choose **Delete**.

To add a rule

If you choose **Add rule**, you can see the available AWS managed rules on the **Add rule** page. You can also create your own custom rule.

1. If you want to create your own rule, choose **Add custom rule** and follow the procedure in [Developing a Custom Rule for AWS Config \(p. 51\)](#).
2. To add a managed rule, choose a rule on the page and follow the procedure in [Working with AWS Managed Rules \(p. 46\)](#).



On the **Add rule** page, you can do the following:

- A. Choose **Add custom rule** to create your own rule.
- B. Type in the search field to filter results by rule name, description, or label. For example, type **EC2** to return rules that evaluate EC2 resource types or type **periodic** to return rules with periodic triggers. For more information about trigger types, see [Specifying Triggers for AWS Config Rules \(p. 27\)](#).
- C. Choose the arrow icon to see the next page of rules.
- D. See the labels to identify the resource type that the rule evaluates and if the rule has a periodic trigger.

Note

Recently added rules are marked as **New**.

Using the AWS CLI

To view your rules

- Use the `describe-config-rules` command:

```
$ aws configservice describe-config-rules
```

AWS Config returns the details for all of your rules.

To update a rule

1. Use the `put-config-rule` command with the `--generate-cli-skeleton` parameter to create a local JSON file that has the parameters for your rule:

```
$ aws configservice put-config-rule --generate-cli-skeleton > putConfigRule.json
```

2. Open the JSON file in a text editor and remove any parameters that don't need updating, with the following exceptions:

- Include at least one of the following parameters to identify the rule:

`ConfigRuleName`, `ConfigRuleArn`, Or `ConfigRuleId`.

- If you are updating a custom rule, you must include the `Source` object and its parameters.
3. Fill in the values for the parameters that remain. To reference the details of your rule, use the **describe-config-rules** command.

For example, the following JSON code updates the resource types that are in the scope of a custom rule:

```
{
  "ConfigRule": {
    "ConfigRuleName": "ConfigRuleName",
    "Scope": {
      "ComplianceResourceTypes": [
        "AWS::EC2::Instance",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC"
      ]
    },
    "Source": {
      "Owner": "CUSTOM_LAMBDA",
      "SourceIdentifier": "arn:aws:lambda:us-east-1:123456789012:function:ConfigRuleName",
      "SourceDetails": [
        {
          "EventSource": "aws.config",
          "MessageType": "ConfigurationItemChangeNotification"
        }
      ]
    }
  }
}
```

4. Use the `put-config-rule` command with the `--cli-input-json` parameter to pass your JSON configuration to AWS Config:

```
$ aws configservice put-config-rule --cli-input-json file://putConfigRule.json
```

5. To verify that you successfully updated your rule, use the **describe-config-rules** command to view the rule's configuration:

```
$ aws configservice describe-config-rules --config-rule-name ConfigRuleName
{
  "ConfigRules": [
    {
      "ConfigRuleState": "ACTIVE",
      "ConfigRuleName": "ConfigRuleName",
      "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/config-rule-nnnnnn",
      "Source": {
        "Owner": "CUSTOM_LAMBDA",
        "SourceIdentifier": "arn:aws:lambda:us-east-1:123456789012:function:ConfigRuleName",
        "SourceDetails": [
          {
            "EventSource": "aws.config",
            "MessageType": "ConfigurationItemChangeNotification"
          }
        ]
      }
    }
  ]
}
```



```
    "Scope": {
      "ComplianceResourceTypes": [
        "AWS::EC2::Instance",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC"
      ]
    },
    "ConfigRuleId": "config-rule-nnnnnnn"
  }
}
```

To delete a rule

- Use the `delete-config-rule` command as shown in the following example:

```
$ aws configservice delete-config-rule --config-rule-name ConfigRuleName
```

Using the AWS Config API

To view your rules

Use the `DescribeConfigRules` action.

To update or add a rule

Use the `PutConfigRule` action.

To delete a rule

Use the `DeleteConfigRule` action.

Deleting Evaluation Results

If a rule is creating invalid evaluation results, you might want to delete these results before you fix the rule and run a new evaluation. For more information, see [Deleting Evaluation Results \(p. 69\)](#).

Manually Evaluate your Resources

You can use AWS Config to manually evaluate your resources against your AWS Config rules or to delete evaluation results.

Contents

- [Evaluating your Resources \(p. 68\)](#)
- [Deleting Evaluation Results \(p. 69\)](#)

Evaluating your Resources

When you create custom rules or use managed rules, AWS Config evaluates your resources against those rules. You can run on-demand evaluations for resources against your rules. For example, this is helpful when you create a custom rule and want to verify that AWS Config is correctly evaluating your resources or to identify if there is an issue with the evaluation logic of your AWS Lambda function.

Example

1. You create a custom rule that evaluates whether your IAM users have active access keys.
2. AWS Config evaluates the resources against your custom rule.
3. An IAM user who doesn't have an active access key exists in your account. Your rule doesn't correctly flag this resource as noncompliant.
4. You fix the rule and start the evaluation again.
5. Because you fixed your rule, the rule correctly evaluates your resources, and flags the IAM user resource as noncompliant.

To manually evaluate your resources (console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Rules**. The **Rules** page shows your rules and the compliance status for each.
4. Choose a rule from the list.
5. In the **Re-evaluate rule** section, choose **Re-evaluate**.
6. AWS Config starts evaluating the resources against your rule.

Note

You can re-evaluate a rule once per minute. You must wait for AWS Config to complete the evaluation for your rule before you start another evaluation. You can't run an evaluation if at the same time the rule is being updated or if the rule is being deleted.

To manually evaluate your resources (AWS CLI)

- Use the **start-config-rules-evaluation** command.

```
$ aws configservice start-config-rules-evaluation --config-rule-names ConfigRuleName
```

AWS Config starts evaluating the recorded resource configurations against your rule.

You can also specify multiple rules in your request.

```
aws configservice start-config-rules-evaluation --config-rule-names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

To manually evaluate your resources (AWS Config API)

- Use the [StartConfigRulesEvaluation](#) action.

Deleting Evaluation Results

After AWS Config evaluates your rule, you can see the evaluation results on the **Rules** page or the **Rules details** page for the rule. If the evaluation results are incorrect or if you want to evaluate again, you can delete the current evaluation results for the rule. For example, if your rule was incorrectly evaluating your

resources or you recently deleted resources from your account, you can delete the evaluation results and then run a new evaluation.

To manually delete evaluation results (console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Rules**. The **Rules** page shows your rules and the compliance status.
4. Choose a rule from the list.
5. In the **Delete evaluation results** section, choose **Delete results**. AWS Config deletes the evaluation results for this rule.
6. When prompted, choose **Delete**. Deleted evaluations can't be retrieved.
7. After the evaluation results are deleted, you can manually start a new evaluation.

To manually delete evaluation results (AWS CLI)

- Use the **delete-evaluation-results** command:

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

AWS Config deletes the evaluation results for the rule.

To manually delete evaluation results (AWS Config API)

- Use the [DeleteEvaluationResults](#) action.

Viewing AWS Resource Configurations and History

You can view all of the resources that AWS Config is recording in your account, the configuration changes that took place for a resource over a specified time period, and the relationships of the selected resource with all the related resources. You can follow the steps using either the AWS Config console or the AWS CLI.

Topics

- [Looking Up Resources That Are Discovered by AWS Config \(p. 71\)](#)
- [Viewing Configuration Details in the AWS Config Console \(p. 73\)](#)
- [View Configuration Details Using the CLI \(p. 74\)](#)
- [Example Amazon EBS Configuration History from AWS Config \(p. 77\)](#)
- [Example Configuration Snapshot from AWS Config \(p. 79\)](#)
- [Notifications that AWS Config sends \(p. 83\)](#)

Looking Up Resources That Are Discovered by AWS Config


You can use the AWS Config console, AWS CLI, and AWS Config API to look up the resources that AWS Config has taken an inventory of, or *discovered*, including deleted resources and resources that AWS Config is not currently recording. AWS Config discovers supported resource types only. For more information, see [Supported AWS Resource Types \(p. 7\)](#).

Looking Up Resources (AWS Config Console)

You can use resource types or tag information to look up resources in the AWS Config console.

To look up resources

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.

2. On the **Resource inventory** page, specify the search options for the resources that you want to look up:
 - Choose **Resources** and then choose one or more resource types in the list. This list includes resource types that AWS Config supports. To narrow results, type a resource ID or, if applicable, a resource name in the next box. You can also choose **Include deleted resources**.
 - Choose **Tag** and type a tag key that is applied to your resources, such as `CostCenter`. To narrow results, type a tag value in the next box.
3. After you specify the search options, choose **Look up**.
4. AWS Config lists the resources that match your search options. You can see the following information about the resources:
 - **Resource identifier** – The resource identifier might be a resource ID or a resource name, if applicable. Choose the resource identifier link to view that resource in the console for that service. For example, choosing the resource identifier for an EC2 instance takes you to the Amazon EC2 console.
 - **Compliance** – The status of the resource that AWS Config evaluated against your rule.
 - **Config timeline** – The Config timeline  displays the history of configuration details for the resource. Choose the icon to view the details page for that resource. For more information, see [Viewing Configuration Details in the AWS Config Console \(p. 73\)](#).

Looking Up Resources (AWS CLI)

You can use the AWS CLI to list resources that AWS Config has discovered.

To look up resources (AWS CLI)

- Use the `aws configservice list-discovered-resources` command:

Example

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
{
  "resourceIdentifiers": [
    {
      "resourceType": "AWS::EC2::Instance",
      "resourceId": "i-nnnnnnnnn"
    }
  ]
}
```

To view the configuration details of a resource that is listed in the response, use the `get-resource-config-history` command, and specify the resource type and ID. For an example of this command and the response from AWS Config, see [View Configuration History \(p. 74\)](#).

Looking up Resources (AWS Config API)

You specify a resource type, and AWS Config returns a list of resource identifiers for resources of that type. For more information, see `ResourceIdentifier` in the *AWS Config API Reference*.

To look up resources (AWS Config API)

- Use the `ListDiscoveredResources` action.

To get the configuration details of a resource that is listed in the response, use the [GetResourceConfigHistory](#) action, and specify the resource type and ID.

Viewing Configuration Details in the AWS Config Console

When you look up resources on the **Resource inventory** page, you can choose the Config timeline



to view the resource's details page. The details page provides information about the configuration, relationships, and number of changes made to that resource.

The blocks at the top of the page are collectively called the *timeline*. The timeline shows the date and the time that the recording was made.

Details page features

1. Click to scroll the timeline to an earlier point in the resource's configuration history.
2. Click a timeline block to select that time period. The descriptions in the **Configuration Details**, **Relationships**, and **Changes** sections comprise the configuration item of the selected resource at the selected time period.
3. Shows the latest configuration change.
4. Click to return the timeline to the current time.
5. Click to view a configuration item by specifying a date (and, if needed, time) and then choose **Apply**.
6. Click to navigate to the **Changes** section. The number that follows **Changes** is the number of configuration changes that occurred for the resource between the selected time period and the previous block.
7. Click to navigate to the **CloudTrail events** section. The number that follows **Events** is the number of API events that occurred for the resource between the selected time period and the previous block. You can see the API events that AWS CloudTrail logged for the last 7 days. CloudTrail events that occurred prior to the last 7 days can't be viewed in the timeline.

For more information, see [Viewing Events with CloudTrail API Activity History](#) in the *AWS CloudTrail User Guide*.

Note

CloudTrail events may not be available for the following reasons:

- Verify that you have sufficient read permissions for CloudTrail. For more information, see [Example read-only permission \(p. 119\)](#).
- There is a service issue and CloudTrail events can't be displayed at this time. Try refreshing the page.
- You don't have a CloudTrail trail in this region or your trail is not enabled for logging. For more information, see [Creating a Trail for the First Time](#) in the *AWS CloudTrail User Guide*.

To view information about the selected resource

1. Use the arrows at either end of the timeline to view the timeline blocks for configuration items that were recorded in other time periods.
2. Choose **Configuration Details** to view the description of the selected resource.

3. Choose **Relationships** to see a list of supported resources in the account that are related to the selected resource. If the **Relationships** section doesn't expand, the selected resource was not related to another resource that was in your account during the selected time period.

For more information, see [Resource Relationship \(p. 4\)](#).

4. If changes are indicated for the selected time period, choose **Changes** to view the configuration changes made to the resource. The **Changes** section also lists the relationship changes that occurred as a result of configuration changes.
5. Choose **CloudTrail events** to view information about API calls that involve the resource, such as the event time, the user name, and the event name. For example, if AWS Config is recording IAM resource types, and an IAM role is updated, you can view the event to see the `UpdateRole` in the **Event name** column.
 - In the **View event** column, you can also choose the **CloudTrail** link to view more information about the event in the CloudTrail console. You must create a trail and enable logging for CloudTrail to view the events in the AWS Config timeline.
6. (Optional) Choose **View Details** to view the configuration information in text or JSON format. Click the arrows in the details window to see additional details.

For more information about the entries in the details window, see [Components of a Configuration Item \(p. 6\)](#).

7. (Optional) Choose **Manage resources** to go to the console for the selected resource. If you make a change to the resource, go back to the AWS Config console and choose **Now** to see the changes. It can take up to 10 minutes to refresh the details page for the resource.

The console also provides details pages for supported resources that you do not include in the list of resources that AWS Config records. The information that is provided on these details pages is limited, and ongoing configuration changes are not shown.

View Configuration Details Using the CLI

The configuration items that AWS Config records are delivered to the specified delivery channel on demand as a configuration snapshot and as a configuration stream. AWS Config also delivers configuration items at regular intervals to the specified delivery channel as configuration history.

You can use the AWS CLI to view the history of configuration items for each resource and to deliver and view a configuration snapshot.

Topics

- [View Configuration History \(p. 74\)](#)
- [Deliver Configuration Snapshot \(p. 75\)](#)

View Configuration History

You can use the AWS CLI to view the history of a resource's various configurations. Use the `get-resource-config-history` command and specify the resource type and the resource ID; for example:

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup --resource-id sg-6fbb3807
{
  "configurationItems": [
    {
      "configurationItemCaptureTime": 1414708529.9219999,
      "relationships": [
```



```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
  "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3cla55"
}
```

The next step is to verify that configuration snapshot was delivered successfully to the delivery channel.

To verify delivery status

- Use the `describe-delivery-channel-status` command to verify that the AWS Config has started delivering the configurations to the specified delivery channel; for example:

```
$ aws configservice describe-delivery-channel-status
{
  "DeliveryChannelsStatus": [
    {
      "configStreamDeliveryInfo": {
        "lastStatusChangeTime": 1415138614.125,
        "lastStatus": "SUCCESS"
      },
      "configHistoryDeliveryInfo": {
        "lastSuccessfulTime": 1415148744.267,
        "lastStatus": "SUCCESS",
        "lastAttemptTime": 1415148744.267
      },
      "configSnapshotDeliveryInfo": {
        "lastSuccessfulTime": 1415333113.4159999,
        "lastStatus": "SUCCESS",
        "lastAttemptTime": 1415333113.4159999
      },
      "name": "default"
    }
  ]
}
```

The response lists the status of all the three delivery formats that AWS Config uses to deliver configurations to your bucket and topic.

Take a look at the `lastSuccessfulTime` field in `configSnapshotDeliveryInfo`. The time should match the time you last requested the delivery of the configuration snapshot.

Note

AWS Config uses the UTC format (GMT-08:00) to record the time.

To view the configuration snapshot in your Amazon S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the Amazon S3 console **All Buckets** list, click the name of your Amazon S3 bucket.
3. Click through the nested folders in your bucket until you see the `ConfigSnapshot` object with a snapshot ID that matches with the ID returned by the command. Download and open the object to view the configuration snapshot.

The S3 bucket also contains an empty file named `ConfigWritabilityCheckFile`. AWS Config creates this file to verify that the service can successfully write to the S3 bucket.

Example Amazon EBS Configuration History from AWS Config

AWS Config generates a set of files that each represent a resource type and lists all configuration changes for the resources of that type that AWS Config is recording. AWS Config exports this resource-centric configuration history as an object in the Amazon S3 bucket that you specified when you enabled AWS Config. The configuration history file for each resource type contains the changes that were detected for the resources of that type since the last history file was delivered. History files are typically delivered every six hours.

The following is an example of the contents of the Amazon S3 object that describes the configuration history of all the Amazon Elastic Block Store volumes in the current region for your AWS account. The volumes in this account include vol-ce676ccc and vol-cia007c . Volume vol-ce676ccc had two configuration changes since the previous history file was delivered while volume vol-cia007c had one.

```
{
  "fileVersion": "1.0",
  "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
  "configurationItems": [
    {
      "snapshotVersion": "1.0",
      "resourceId": "vol-ce676ccc",
      "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
      "accountId": "12345678910",
      "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
      "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
      "configurationItemStatus": "OK",
      "relatedEvents": [
        "06c12a39-eb35-11de-ae07-adb69edbb1e4",
        "c376e30d-71a2-4694-89b7-a5a04ad92281"
      ],
      "availabilityZone": "us-west-2b",
      "resourceType": "AWS::EC2::Volume",
      "resourceCreationTime": "2014-02-27T21:43:53.885Z",
      "tags": {},
      "relationships": [
        {
          "resourceId": "i-344c463d",
          "resourceType": "AWS::EC2::Instance",
          "name": "Attached to Instance"
        }
      ]
    },
    {
      "configuration": {
        "volumeId": "vol-ce676ccc",
        "size": 1,
        "snapshotId": "",
        "availabilityZone": "us-west-2b",
        "state": "in-use",
        "createTime": "2014-02-27T21:43:53.0885+0000",
        "attachments": [
          {
            "volumeId": "vol-ce676ccc",
            "instanceId": "i-344c463d",
            "device": "/dev/sdf",
            "state": "attached",
            "attachTime": "2014-03-07T23:46:28.0000+0000",
            "deleteOnTermination": false
          }
        ]
      },
      "tags": [
        {

```

```
        "tagName": "environment",
        "tagValue": "PROD"
    },
    {
        "tagName": "name",
        "tagValue": "DataVolume1"
    }
],
"volumeType": "standard"
}
},
{
    "configurationItemVersion": "1.0",
    "resourceId": "vol-ce676ccc",
    "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
    "accountId": "12345678910",
    "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
    "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
    "configurationItemStatus": "OK",
    "relatedEvents": [
        "06c12a39-eb35-11de-ae07-ad229edbb1e4",
        "c376e30d-71a2-4694-89b7-a5a04w292281"
    ],
    "availabilityZone": "us-west-2b",
    "resourceType": "AWS::EC2::Volume",
    "resourceCreationTime": "2014-02-27T21:43:53.885Z",
    "tags": {},
    "relationships": [
        {
            "resourceId": "i-344c463d",
            "resourceType": "AWS::EC2::Instance",
            "name": "Attached to Instance"
        }
    ],
    "configuration": {
        "volumeId": "vol-ce676ccc",
        "size": 1,
        "snapshotId": "",
        "availabilityZone": "us-west-2b",
        "state": "in-use",
        "createTime": "2014-02-27T21:43:53.0885+0000",
        "attachments": [
            {
                "volumeId": "vol-ce676ccc",
                "instanceId": "i-344c463d",
                "device": "/dev/sdf",
                "state": "attached",
                "attachTime": "2014-03-07T23:46:28.0000+0000",
                "deleteOnTermination": false
            }
        ],
        "tags": [
            {
                "tagName": "environment",
                "tagValue": "PROD"
            },
            {
                "tagName": "name",
                "tagValue": "DataVolume1"
            }
        ],
        "volumeType": "standard"
    }
},
{
    "configurationItemVersion": "1.0",
```

```
    "resourceId": "vol-cia007c",
    "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
    "accountId": "12345678910",
    "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
    "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
    "configurationItemStatus": "OK",
    "relatedEvents": [
      "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
      "c376e30d-71a2-4694-89b7-a5a67u292281"
    ],
    "availabilityZone": "us-west-2b",
    "resourceType": "AWS::EC2::Volume",
    "resourceCreationTime": "2014-02-27T20:43:53.885Z",
    "tags": {},
    "relationships": [
      {
        "resourceId": "i-344e563d",
        "resourceType": "AWS::EC2::Instance",
        "name": "Attached to Instance"
      }
    ],
    "configuration": {
      "volumeId": "vol-cia007c",
      "size": 1,
      "snapshotId": "",
      "availabilityZone": "us-west-2b",
      "state": "in-use",
      "createTime": "2014-02-27T20:43:53.0885+0000",
      "attachments": [
        {
          "volumeId": "vol-cia007c",
          "instanceId": "i-344e563d",
          "device": "/dev/sdf",
          "state": "attached",
          "attachTime": "2014-03-07T23:46:28.0000+0000",
          "deleteOnTermination": false
        }
      ],
      "tags": [
        {
          "tagName": "environment",
          "tagValue": "PROD"
        },
        {
          "tagName": "name",
          "tagValue": "DataVolume2"
        }
      ],
      "volumeType": "standard"
    }
  }
}
```

Example Configuration Snapshot from AWS Config

AWS Config generates configuration snapshots when you invoke the [DeliverConfigSnapshot](#) action or you run the AWS CLI `deliver-config-snapshot` command. AWS Config stores configuration snapshots in the Amazon S3 bucket that you specified when you enabled AWS Config.

The following is an example of the information that AWS Config includes in a configuration snapshot. The snapshot describes the configuration for the resources that AWS Config is recording in the current region for your AWS account, and it describes the relationships between these resources.

Note

The configuration snapshot can include references to resources types and resource IDs that are not supported.

```
{
  "fileVersion": "1.0",
  "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
  "configurationItems": [
    {
      "configurationItemVersion": "1.0",
      "resourceId": "vol-ce676ccc",
      "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
      "accountId": "12345678910",
      "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
      "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
      "configurationItemStatus": "OK",
      "relatedEvents": [
        "06c12a39-eb35-11de-ae07-adb69edbb1e4",
        "c376e30d-71a2-4694-89b7-a5a04ad92281"
      ],
      "availabilityZone": "us-west-2b",
      "resourceType": "AWS::EC2::Volume",
      "resourceCreationTime": "2014-02-27T21:43:53.885Z",
      "tags": {},
      "relationships": [
        {
          "resourceId": "i-344c463d",
          "resourceType": "AWS::EC2::Instance",
          "name": "Attached to Instance"
        }
      ],
      "configuration": {
        "volumeId": "vol-ce676ccc",
        "size": 1,
        "snapshotId": "",
        "availabilityZone": "us-west-2b",
        "state": "in-use",
        "createTime": "2014-02-27T21:43:53.0885+0000",
        "attachments": [
          {
            "volumeId": "vol-ce676ccc",
            "instanceId": "i-344c463d",
            "device": "/dev/sdf",
            "state": "attached",
            "attachTime": "2014-03-07T23:46:28.0000+0000",
            "deleteOnTermination": false
          }
        ],
        "tags": [
          {
            "tagName": "environment",
            "tagValue": "PROD"
          },
          {
            "tagName": "name",
            "tagValue": "DataVolume1"
          }
        ],
        "volumeType": "standard"
      }
    }
  ],
}
```

```
{
  "configurationItemVersion": "1.0",
  "resourceId": "i-344c463d",
  "accountId": "12345678910",
  "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
  "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
  "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
  "configurationItemStatus": "OK",
  "relatedEvents": [
    "06c12a39-eb35-11de-ae07-adb69edbb1e4",
    "c376e30d-71a2-4694-89b7-a5a04ad92281"
  ],
  "availabilityZone": "us-west-2b",
  "resourceType": "AWS::EC2::Instance",
  "resourceCreationTime": "2014-02-26T22:56:35.000Z",
  "tags": {
    "Name": "integ-test-1",
    "examplename": "examplevalue"
  },
  "relationships": [
    {
      "resourceId": "vol-ce676ccc",
      "resourceType": "AWS::EC2::Volume",
      "name": "Attached Volume"
    },
    {
      "resourceId": "vol-ef0e06ed",
      "resourceType": "AWS::EC2::Volume",
      "name": "Attached Volume",
      "direction": "OUT"
    },
    {
      "resourceId": "subnet-47b4cf2c",
      "resourceType": "AWS::EC2::SUBNET",
      "name": "Is contained in Subnet",
      "direction": "IN"
    }
  ],
  "configuration": {
    "instanceId": "i-344c463d",
    "imageId": "ami-ccf297fc",
    "state": {
      "code": 16,
      "name": "running"
    },
    "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
    "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
    "stateTransitionReason": "",
    "keyName": "configDemo",
    "amiLaunchIndex": 0,
    "productCodes": [],
    "instanceType": "t1.micro",
    "launchTime": "2014-02-26T22:56:35.0000+0000",
    "placement": {
      "availabilityZone": "us-west-2b",
      "groupName": "",
      "tenancy": "default"
    },
    "kernelId": "aki-fc8f11cc",
    "monitoring": {
      "state": "disabled"
    },
    "subnetId": "subnet-47b4cf2c",
    "vpcId": "vpc-41b4cf2a",
    "privateIpAddress": "172.31.21.63",
    "publicIpAddress": "54.218.4.189",
```

```
"architecture": "x86_64",
"rootDeviceType": "ebs",
"rootDeviceName": "/dev/sda1",
"blockDeviceMappings": [
  {
    "deviceName": "/dev/sda1",
    "ebs": {
      "volumeId": "vol-ef0e06ed",
      "status": "attached",
      "attachTime": "2014-02-26T22:56:38.0000+0000",
      "deleteOnTermination": true
    }
  },
  {
    "deviceName": "/dev/sdf",
    "ebs": {
      "volumeId": "vol-ce676ccc",
      "status": "attached",
      "attachTime": "2014-03-07T23:46:28.0000+0000",
      "deleteOnTermination": false
    }
  }
],
"virtualizationType": "paravirtual",
"clientToken": "aBCDe123456",
"tags": [
  {
    "key": "Name",
    "value": "integ-test-1"
  },
  {
    "key": "examplekey",
    "value": "examplevalue"
  }
],
"securityGroups": [
  {
    "groupName": "launch-wizard-2",
    "groupId": "sg-892adfec"
  }
],
"sourceDestCheck": true,
"hypervisor": "xen",
"networkInterfaces": [
  {
    "networkInterfaceId": "eni-55c03d22",
    "subnetId": "subnet-47b4cf2c",
    "vpcId": "vpc-41b4cf2a",
    "description": "",
    "ownerId": "12345678910",
    "status": "in-use",
    "privateIpAddress": "172.31.21.63",
    "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
    "sourceDestCheck": true,
    "groups": [
      {
        "groupName": "launch-wizard-2",
        "groupId": "sg-892adfec"
      }
    ]
  },
  {
    "attachment": {
      "attachmentId": "eni-attach-bf90c489",
      "deviceIndex": 0,
      "status": "attached",
      "attachTime": "2014-02-26T22:56:35.0000+0000",
      "deleteOnTermination": true
    }
  }
]
```

```
        },
        "association": {
            "publicIp": "54.218.4.189",
            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
            "ipOwnerId": "amazon"
        },
        "privateIpAddresses": [
            {
                "privateIpAddress": "172.31.21.63",
                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                "primary": true,
                "association": {
                    "publicIp": "54.218.4.189",
                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                    "ipOwnerId": "amazon"
                }
            }
        ]
    },
    "ebsOptimized": false
}
]
```

Notifications that AWS Config sends

You can configure AWS Config to stream configuration changes and notifications to an Amazon SNS topic. For example, when a resource is updated, you can get a notification sent to your email, so that you can view the changes. You can also be notified when AWS Config evaluates your custom or managed rules against your resources.

AWS Config sends notifications for the following events:

- Configuration item change for a resource.
- Configuration history for a resource was delivered for your account.
- Configuration snapshot for recorded resources was started and delivered for your account.
- Compliance state of your resources and whether they are compliant with your rules.
- Evaluation started for a rule against your resources.
- AWS Config failed to deliver the notification to your account.

Note

If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email.

Topics

- [Monitoring AWS Config Resource Changes by Email \(p. 84\)](#)
- [Example Configuration Item Change Notifications \(p. 87\)](#)
- [Example Configuration History Delivery Notification \(p. 95\)](#)
- [Example Configuration Snapshot Delivery Started Notification \(p. 95\)](#)
- [Example Configuration Snapshot Delivery Notification \(p. 96\)](#)

- [Example Compliance Change Notification \(p. 97\)](#)
- [Example Rules Evaluation Started Notification \(p. 98\)](#)
- [Example Oversized Configuration Item Change Notification \(p. 98\)](#)
- [Example Delivery Failed Notification \(p. 99\)](#)

Monitoring AWS Config Resource Changes by Email

If you have set up AWS Config to stream configuration changes and notifications to an Amazon SNS topic, you can monitor those changes by email. These emails can include configuration history, rule compliance, snapshot information, and change notifications. You can also set up email filters based on the subject line or message body to look for specific changes.

To monitor resource changes by email

1. If you haven't done so already, set up AWS Config to deliver notifications to an Amazon SNS topic. For more information, see [Setting up AWS Config with the Console \(p. 17\)](#) or [Setting up AWS Config with the AWS CLI \(p. 20\)](#).
2. Open the Amazon SNS console at <https://console.aws.amazon.com/sns/v2/home>.
3. In the navigation pane of the Amazon SNS console, choose **Topics**.
4. On the **Topics** page, open the Amazon SNS topic you specified when you set up AWS Config by choosing its name in the **ARN** column.
5. On the **Topic details** page, under **Subscriptions**, choose **Create subscription**.
6. In the **Create subscription** dialog box, for **Protocol**, choose **Email**.
7. For **Endpoint**, type the email address where you want the notifications sent.
8. Choose **Create subscription**.

Check your email for an email confirmation. In the meantime, the console displays **PendingConfirmation** in the **Subscription ID** column.

9. Open the email from "AWS Notifications" and choose **Confirm subscription**.

Tip

If you want to monitor specific resources or other important changes, you can set up email filters in your email application.

Example Email Format and Filters

If you created an email subscription to your Amazon SNS topic, you can filter the email you receive based on information in the subject line and message body. To create a subscription for an Amazon SNS topic, see [Monitoring AWS Config Resource Changes by Email \(p. 84\)](#).

The subject line of an email looks like the following example:

```
[AWS Config:us-west-2] AWS::EC2::Instance i-12abcd3e Created in Account 123456789012
```

In your email client application, you can set up email filters or rules to watch for specific changes or to organize your notifications. For example, you can organize email notifications by region, resource type, resource name, or AWS account. Email filters can help you manage notifications from multiple accounts or if you have many resources in your account.

The message body of an email subscription created with the **Email** protocol contains information about create, update, and delete events for your AWS resources. The following example shows an email

message body created with the **Email** protocol. The notification contains the configuration item change for the resource.

```
View the Timeline for this Resource in AWS Config Management Console:
https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/AWS::
EC2::Instance/i-12abcd3e
```

New State and Change Record:

```
-----
{
  "configurationItemDiff": {
    "changedProperties": {},
    "changeType": "CREATE"
  },
  "configurationItem": {
    "configurationItemVersion": "1.0",
    "configurationItemCaptureTime": "2015-03-19T21:20:35.737Z",
    "configurationStateId": 1,
    "relatedEvents": [
      "4f8abc4f-6def-4g42-hi03-46j3b48k0lmn"
    ],
    "awsAccountId": "123456789012",
    "configurationItemStatus": "ResourceDiscovered",
    "resourceId": "i-92aeda5b",
    "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/i-12abcd3e",
    "awsRegion": "us-west-2",
    "availabilityZone": "us-west-2c",
    "configurationStateMd5Hash": "123456789e0f930642026053208e",
    "resourceType": "AWS::EC2::Instance",
    "resourceCreationTime": "2015-03-19T21:13:05.000Z",
    "tags": {},
    "relationships": [
      {
        "resourceId": "abc-1234de56",
        "resourceType": "AWS::EC2::NetworkInterface",
        "name": "Contains NetworkInterface"
      },
      {
        "resourceId": "ab-c12defg3",
        "resourceType": "AWS::EC2::SecurityGroup",
        "name": "Is associated with SecurityGroup"
      },
      {
        "resourceId": "subnet-alb2c3d4",
        "resourceType": "AWS::EC2::Subnet",
        "name": "Is contained in Subnet"
      },
      {
        "resourceId": "vol-albc234d",
        "resourceType": "AWS::EC2::Volume",
        "name": "Is attached to Volume"
      },
      {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "name": "Is contained in Vpc"
      }
    ],
    "configuration": {
      "instanceId": "i-12abcd3e",
      "imageId": "ami-123a4567",
      "state": {
        "code": 16,
        "name": "running"
      }
    }
  }
}
```

```
    "privateDnsName": "ip-000-00-0-000.us-west-2.compute.internal",
    "publicDnsName":
"ec2-12-345-678-910.us-west-2.compute.amazonaws.com",
    "stateTransitionReason": "",
    "keyName": null,
    "amiLaunchIndex": 0,
    "productCodes": [],
    "instanceType": "t2.micro",
    "launchTime": "2015-03-19T21:13:05.000Z",
    "placement": {
      "availabilityZone": "us-west-2c",
      "groupName": "",
      "tenancy": "default"
    },
    "kernelId": null,
    "ramdiskId": null,
    "platform": null,
    "monitoring": {
      "state": "disabled"
    },
    "subnetId": "subnet-alb2c3d4",
    "vpcId": "vpc-al2bc345",
    "privateIpAddress": "000.00.0.000",
    "publicIpAddress": "00.000.000.000",
    "stateReason": null,
    "architecture": "x86_64",
    "rootDeviceType": "ebs",
    "rootDeviceName": "/dev/abcd",
    "blockDeviceMappings": [
      {
        "deviceName": "/dev/abcd",
        "ebs": {
          "volumeId": "vol-albc234d",
          "status": "attached",
          "attachTime": "2015-03-19T21:13:07.000Z",
          "deleteOnTermination": true
        }
      }
    ],
    "virtualizationType": "hvm",
    "instanceLifecycle": null,
    "spotInstanceRequestId": null,
    "clientToken": "ab1234c5-6d78-910-1112-13ef14g15hi16",
    "tags": [],
    "securityGroups": [
      {
        "groupName": "default",
        "groupId": "sg-al2bcde3"
      }
    ],
    "sourceDestCheck": true,
    "hypervisor": "xen",
    "networkInterfaces": [
      {
        "networkInterfaceId": "eni-1234ab56",
        "subnetId": "subnet-alb2c3d4",
        "vpcId": "vpc-al2bc345",
        "description": "",
        "ownerId": "123456789012",
        "status": "in-use",
        "macAddress": "1a:23:45:67:b8",
        "privateIpAddress": "000.00.0.000",
        "privateDnsName": "ip-000-00-0-000.us-west-2.compute.internal",
        "sourceDestCheck": true,
        "groups": [
          {
```

```
        "groupName": "default",
        "groupId": "sg-a12bcde3"
      },
    ],
    "attachment": {
      "attachmentId": "eni-attach-123a4b5c",
      "deviceIndex": 0,
      "status": "attached",
      "attachTime": "2015-03-19T21:13:05.000Z",
      "deleteOnTermination": true
    },
    "association": {
      "publicIp": "00.000.000.000",
      "publicDnsName":
"ec2-00-000-000-000.us-west-2.compute.amazonaws.com",
      "ipOwnerId": "amazon"
    },
    "privateIpAddresses": [
      {
        "privateIpAddress": "000.00.0.000",
        "privateDnsName":
"ip-000-00-0-000.us-west-2.compute.internal",
        "primary": true,
        "association": {
          "publicIp": "00.000.000.000",
          "publicDnsName":
"ec2-000-00-0-000.us-west-2.compute.amazonaws.com",
          "ipOwnerId": "amazon"
        }
      }
    ]
  },
  "iamInstanceProfile": null,
  "ebsOptimized": false,
  "sriovNetSupport": null
},
"notificationCreationTime": "2015-03-19T21:20:36.808Z",
"messageType": "ConfigurationItemChangeNotification",
"recordVersion": "1.2"
}
```

Example Configuration Item Change Notifications

AWS Config uses Amazon SNS to deliver notifications to subscription endpoints. These notifications provide the delivery status for configuration snapshots and configuration histories, and they provide each configuration item that AWS Config creates when the configurations of recorded AWS resources change. AWS Config also sends notifications that show whether your resources are compliant against your rules. If you choose to have notifications sent by email, you can use filters in your email client application based on the subject line and message body of the email.

The following is an example payload of an Amazon SNS notification that is generated when AWS Config detects that the Amazon Elastic Block Store volume `vol-ce676ccc` is attached to the instance with an ID of `i-344c463d`. The notification contains the configuration item change for the resource.

```
"Type": "Notification",
"MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
"TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
"Message": {
  "MessageVersion": "1.0",
```

```
"NotificationCreateTime": "2014-03-18T10:11:00Z",
"messageType": "ConfigurationItemChangeNotification",
"configurationItems": [
  {
    "configurationItemVersion": "1.0",
    "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
    "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
    "resourceId": "vol-ce676ccc",
    "accountId": "123456789012",
    "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
    "configurationItemStatus": "OK",
    "relatedEvents": [
      "06c12a39-eb35-11de-ae07-adb69edbble4",
      "c376e30d-71a2-4694-89b7-a5a04ad92281"
    ],
    "availabilityZone": "us-west-2b",
    "resourceType": "AWS::EC2::VOLUME",
    "resourceCreationTime": "2014-02-27T21:43:53.885Z",
    "tags": {},
    "relationships": [
      {
        "resourceId": "i-344c463d",
        "resourceType": "AWS::EC2::INSTANCE",
        "name": "Attached to Instance"
      }
    ],
    "configuration": {
      "volumeId": "vol-ce676ccc",
      "size": 1,
      "snapshotId": "",
      "availabilityZone": "us-west-2b",
      "state": "in-use",
      "createTime": "2014-02-27T21:43:53.0885+0000",
      "attachments": [
        {
          "volumeId": "vol-ce676ccc",
          "instanceId": "i-344c463d",
          "device": "/dev/sdf",
          "state": "attached",
          "attachTime": "2014-03-07T23:46:28.0000+0000",
          "deleteOnTermination": false
        }
      ]
    },
    "tags": [],
    "volumeType": "standard"
  }
],
"configurationItemDiff": {
  "changeType": "UPDATE",
  "changedProperties": {
    "Configuration.State": {
      "previousValue": "available",
      "updatedValue": "in-use",
      "changeType": "UPDATE"
    },
    "Configuration.Attachments.0": {
      "updatedValue": {
        "VolumeId": "vol-ce676ccc",
        "InstanceId": "i-344c463d",
        "Device": "/dev/sdf",
        "State": "attached",
        "AttachTime": "FriMar0723: 46: 28UTC2014",
        "DeleteOnTermination": "false"
      },
      "changeType": "CREATE"
    }
  }
}
```

```
    },
    },
  },
  "Timestamp": "2014-03-07T23:47:10.001Z",
  "SignatureVersion": "1",
  "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPAPk6HXRTBRLkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/
Ro9QTmiTNcEjQ5kB8wGsRWVrk/whAzT2lVtofC365En2TlNcd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTFXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kgapIo4CtC
+qZhMzEbHWpzFleZvF155KaZXDbznBDlZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
  "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
  "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```

Configuration Items for Resources with Relationships

If a resource is related to other resources, a change to that resource can result in multiple configuration items. The following example shows how AWS Config creates configuration items for resources with relationships.

1. You have an Amazon EC2 instance with an ID of `i-007d374c8912e3e90`, and the instance is associated with an Amazon EC2 security group, `sg-c8b141b4`.
2. You update your EC2 instance to change the security group to another security group, `sg-3f1fef43`.
3. Because the EC2 instance is related to another resource, AWS Config creates multiple configuration items like the following examples:

This notification contains the configuration item change for the EC2 instance when the security group is replaced.

```
{
  "Type": "Notification",
  "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
  "TopicArn": "arn:aws:sns:us-east-1:123456789012:config-topic-virginia",
  "Subject": "[AWS Config:us-east-1] AWS::EC2::Instance i-007d374c8912e3e90 Updated in Account 123456789012",
  "Message": {
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.NetworkInterfaces.0": {
          "previousValue": {
            "networkInterfaceId": "eni-fde9493f",
            "subnetId": "subnet-2372be7b",
            "vpcId": "vpc-14400670",
            "description": "",
            "ownerId": "123456789012",
            "status": "in-use",
            "macAddress": "0e:36:a2:d:c5:e0",
            "privateIpAddress": "172.31.16.84",
            "privateDnsName": "ip-172-31-16-84.ec2.internal",
            "sourceDestCheck": true,
            "groups": [{
              "groupName": "example-security-group-1",
              "groupId": "sg-c8b141b4"
            }],
          },
          "attachment": {
            "attachmentId": "eni-attach-85bd89d9",
            "deviceIndex": 0,

```

```
        "status": "attached",
        "attachTime": "2017-01-09T19:36:02.000Z",
        "deleteOnTermination": true
    },
    "association": {
        "publicIp": "54.175.43.43",
        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
        "ipOwnerId": "amazon"
    },
    "privateIpAddresses": [{
        "privateIpAddress": "172.31.16.84",
        "privateDnsName": "ip-172-31-16-84.ec2.internal",
        "primary": true,
        "association": {
            "publicIp": "54.175.43.43",
            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
            "ipOwnerId": "amazon"
        }
    }]
},
"updatedValue": null,
"changeType": "DELETE"
},
"Relationships.0": {
    "previousValue": {
        "resourceId": "sg-c8b141b4",
        "resourceName": null,
        "resourceType": "AWS::EC2::SecurityGroup",
        "name": "Is associated with SecurityGroup"
    },
    "updatedValue": null,
    "changeType": "DELETE"
},
"Configuration.NetworkInterfaces.1": {
    "previousValue": null,
    "updatedValue": {
        "networkInterfaceId": "eni-fde9493f",
        "subnetId": "subnet-2372be7b",
        "vpcId": "vpc-14400670",
        "description": "",
        "ownerId": "123456789012",
        "status": "in-use",
        "macAddress": "0e:36:a2:2d:c5:e0",
        "privateIpAddress": "172.31.16.84",
        "privateDnsName": "ip-172-31-16-84.ec2.internal",
        "sourceDestCheck": true,
        "groups": [{
            "groupName": "example-security-group-2",
            "groupId": "sg-3flfef43"
        }]
    },
    "attachment": {
        "attachmentId": "eni-attach-85bd89d9",
        "deviceIndex": 0,
        "status": "attached",
        "attachTime": "2017-01-09T19:36:02.000Z",
        "deleteOnTermination": true
    },
    "association": {
        "publicIp": "54.175.43.43",
        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
        "ipOwnerId": "amazon"
    },
    "privateIpAddresses": [{
        "privateIpAddress": "172.31.16.84",
        "privateDnsName": "ip-172-31-16-84.ec2.internal",
```

```
        "primary": true,
        "association": {
            "publicIp": "54.175.43.43",
            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
            "ipOwnerId": "amazon"
        }
    }
}
},
"changeType": "CREATE"
},
"Relationships.1": {
    "previousValue": null,
    "updatedAt": {
        "resourceId": "sg-3f1fef43",
        "resourceName": null,
        "resourceType": "AWS::EC2::SecurityGroup",
        "name": "Is associated with SecurityGroup"
    },
    "changeType": "CREATE"
},
"Configuration.SecurityGroups.1": {
    "previousValue": null,
    "updatedAt": {
        "groupName": "example-security-group-2",
        "groupId": "sg-3f1fef43"
    },
    "changeType": "CREATE"
},
"Configuration.SecurityGroups.0": {
    "previousValue": {
        "groupName": "example-security-group-1",
        "groupId": "sg-c8b141b4"
    },
    "updatedAt": null,
    "changeType": "DELETE"
},
},
"changeType": "UPDATE"
},
"configurationItem": {
    "relatedEvents": ["e61e1419-7cb0-477f-8dde-bbfe27467a96"],
    "relationships": [
        {
            "resourceId": "eni-fde9493f",
            "resourceName": null,
            "resourceType": "AWS::EC2::NetworkInterface",
            "name": "Contains NetworkInterface"
        },
        {
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "resourceType": "AWS::EC2::SecurityGroup",
            "name": "Is associated with SecurityGroup"
        },
        {
            "resourceId": "subnet-2372be7b",
            "resourceName": null,
            "resourceType": "AWS::EC2::Subnet",
            "name": "Is contained in Subnet"
        },
        {
            "resourceId": "vol-0a2d63a256bce35c5",
            "resourceName": null,
            "resourceType": "AWS::EC2::Volume",
            "name": "Is attached to Volume"
        }
    ]
}
```



```
    },
    {
      "resourceId": "vpc-14400670",
      "resourceName": null,
      "resourceType": "AWS::EC2::VPC",
      "name": "Is contained in Vpc"
    }
  ],
  "configuration": {
    "instanceId": "i-007d374c8912e3e90",
    "imageId": "ami-9be6f38c",
    "state": {
      "code": 16,
      "name": "running"
    },
    "privateDnsName": "ip-172-31-16-84.ec2.internal",
    "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
    "stateTransitionReason": "",
    "keyName": "ec2-micro",
    "amiLaunchIndex": 0,
    "productCodes": [],
    "instanceType": "t2.micro",
    "launchTime": "2017-01-09T20:13:28.000Z",
    "placement": {
      "availabilityZone": "us-east-1c",
      "groupName": "",
      "tenancy": "default",
      "hostId": null,
      "affinity": null
    },
    "kernelId": null,
    "ramdiskId": null,
    "platform": null,
    "monitoring": {"state": "disabled"},
    "subnetId": "subnet-2372be7b",
    "vpcId": "vpc-14400670",
    "privateIpAddress": "172.31.16.84",
    "publicIpAddress": "54.175.43.43",
    "stateReason": null,
    "architecture": "x86_64",
    "rootDeviceType": "ebs",
    "rootDeviceName": "/dev/xvda",
    "blockDeviceMappings": [{
      "deviceName": "/dev/xvda",
      "ebs": {
        "volumeId": "vol-0a2d63a256bce35c5",
        "status": "attached",
        "attachTime": "2017-01-09T19:36:03.000Z",
        "deleteOnTermination": true
      }
    }
  ],
    "virtualizationType": "hvm",
    "instanceLifecycle": null,
    "spotInstanceRequestId": null,
    "clientToken": "bIYqA1483990561516",
    "tags": [{
      "key": "Name",
      "value": "value"
    }
  ],
    "securityGroups": [{
      "groupName": "example-security-group-2",
      "groupId": "sg-3flfef43"
    }
  ],
    "sourceDestCheck": true,
    "hypervisor": "xen",
    "networkInterfaces": [{
```

```
"networkInterfaceId": "eni-fde9493f",
"subnetId": "subnet-2372be7b",
"vpcId": "vpc-14400670",
"description": "",
"ownerId": "123456789012",
"status": "in-use",
"macAddress": "0e:36:a2:2d:c5:e0",
"privateIpAddress": "172.31.16.84",
"privateDnsName": "ip-172-31-16-84.ec2.internal",
"sourceDestCheck": true,
"groups": [{
  "groupName": "example-security-group-2",
  "groupId": "sg-3f1fef43"
}],
"attachment": {
  "attachmentId": "eni-attach-85bd89d9",
  "deviceIndex": 0,
  "status": "attached",
  "attachTime": "2017-01-09T19:36:02.000Z",
  "deleteOnTermination": true
},
"association": {
  "publicIp": "54.175.43.43",
  "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
  "ipOwnerId": "amazon"
},
"privateIpAddresses": [{
  "privateIpAddress": "172.31.16.84",
  "privateDnsName": "ip-172-31-16-84.ec2.internal",
  "primary": true,
  "association": {
    "publicIp": "54.175.43.43",
    "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
    "ipOwnerId": "amazon"
  }
}]
}],
"iamInstanceProfile": null,
"ebsOptimized": false,
"sriovNetSupport": null,
"enaSupport": true
},
"supplementaryConfiguration": {},
"tags": {"Name": "value"},
"configurationItemVersion": "1.2",
"configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
"configurationStateId": 1484002214328,
"awsAccountId": "123456789012",
"configurationItemStatus": "OK",
"resourceType": "AWS::EC2::Instance",
"resourceId": "i-007d374c8912e3e90",
"resourceName": null,
"ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-007d374c8912e3e90",
"awsRegion": "us-east-1",
"availabilityZone": "us-east-1c",
"configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
"resourceCreationTime": "2017-01-09T20:13:28.000Z"
},
"notificationCreationTime": "2017-01-09T22:50:15.928Z",
"messageType": "ConfigurationItemChangeNotification",
"recordVersion": "1.2"
},
"Timestamp": "2017-01-09T22:50:16.358Z",
"SignatureVersion": "1",
"Signature": "lpJTEYOSr8fUbiaARNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHL1C
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUGTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
```

```
+gVTNT009xtNIH8aMlvqyvUSXuh278xayExC5yTRXEG+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/  
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4S132bGqdeDULY4dFGukuzPYoHuEtDPH  
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w=",  
  "SigningCertURL": "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-  
b95095beb82e8f6a046b3aafc7f4149a.pem",  
  "UnsubscribeURL": "https://sns.us-east-1.amazonaws.com/?  
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-1:123456789012:config-topic-  
virginia:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"  
}
```

This notification contains the configuration item change for the EC2 security group, `sg-3flfef43`, which is associated with the instance.

```
{  
  "Type": "Notification",  
  "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",  
  "TopicArn": "arn:aws:sns:us-east-1:123456789012:config-topic-virginia",  
  "Subject": "[AWS Config:us-east-1] AWS::EC2::SecurityGroup sg-3flfef43 Created in  
Account 123456789012",  
  "Message": {  
    "configurationItemDiff": {  
      "changedProperties": {},  
      "changeType": "CREATE"  
    },  
    "configurationItem": {  
      "relatedEvents": ["e61e1419-7cb0-477f-8dde-bbfe27467a96"],  
      "relationships": [{  
        "resourceId": "vpc-14400670",  
        "resourceName": null,  
        "resourceType": "AWS::EC2::VPC",  
        "name": "Is contained in Vpc"  
      }],  
      "configuration": {  
        "ownerId": "123456789012",  
        "groupName": "example-security-group-2",  
        "groupId": "sg-3flfef43",  
        "description": "This is an example security group.",  
        "ipPermissions": [],  
        "ipPermissionsEgress": [{  
          "ipProtocol": "-1",  
          "fromPort": null,  
          "toPort": null,  
          "userIdGroupPairs": [],  
          "ipRanges": ["0.0.0.0/0"],  
          "prefixListIds": []  
        }],  
        "vpcId": "vpc-14400670",  
        "tags": []  
      },  
      "supplementaryConfiguration": {},  
      "tags": {},  
      "configurationItemVersion": "1.2",  
      "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",  
      "configurationStateId": "1484002215156",  
      "awsAccountId": "123456789012",  
      "configurationItemStatus": "ResourceDiscovered",  
      "resourceType": "AWS::EC2::SecurityGroup",  
      "resourceId": "sg-3flfef43",  
      "resourceName": null,  
      "ARN": "arn:aws:ec2:us-east-1:123456789012:security-group/sg-3flfef43",  
      "awsRegion": "us-east-1",  
      "availabilityZone": "Not Applicable",  
      "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",  
      "resourceCreationTime": null  
    }  
  }  
}
```

```
{
  "notificationCreationTime": "2017-01-09T22:50:16.021Z",
  "messageType": "ConfigurationItemChangeNotification",
  "recordVersion": "1.2"
},
{
  "Timestamp": "2017-01-09T22:50:16.413Z",
  "SignatureVersion": "1",
  "Signature": "GocX3lUu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibY00sT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN900okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxalh/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVxNBQEI4k8
"SigningCertURL": "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
  "UnsubscribeURL": "https://sns.us-east-1.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-1:123456789012:config-topic-
virginia:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Example Configuration History Delivery Notification

The configuration history is a collection of the configuration items for a resource type over a time period. The following is an example notification that AWS Config sends when the configuration history for a CloudTrail trail resource is delivered for your account.

```
{
  "Type": "Notification",
  "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
  "TopicArn": "arn:aws:sns:us-east-1:123456789012:config-topic-virginia",
  "Subject": "[AWS Config:us-east-1] Configuration History Delivery Completed for Account
123456789012",
  "Message": {
    "s3ObjectKey": "AWSLogs/123456789012/Config/us-
east-1/2016/9/27/ConfigHistory/123456789012_Config_us-
east-1_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
    "s3Bucket": "config-bucket-123456789012-virginia",
    "notificationCreationTime": "2016-09-27T20:37:05.217Z",
    "messageType": "ConfigurationHistoryDeliveryCompleted",
    "recordVersion": "1.1"
  },
  "Timestamp": "2016-09-27T20:37:05.315Z",
  "SignatureVersion": "1",
  "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RjQiCPsCNfG0J0rUZlrfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EB0oGmxcTliUnlAie/
yeGFduc6P3EotP3zt02rhmxjezjf3c1lursthZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhrbCBgX5ma
"SigningCertURL": "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
  "UnsubscribeURL": "https://sns.us-east-1.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-1:123456789012:config-topic-
virginia:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Example Configuration Snapshot Delivery Started Notification

The following is an example notification that AWS Config sends when AWS Config starts delivering the configuration snapshot for your account.

```
{
  "Type": "Notification",
```

```
"MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
"TopicArn": "arn:aws:sns:us-east-1:123456789012:config-topic-virginia",
"Subject": "[AWS Config:us-east-1] Configuration Snapshot Delivery Started for Account
123456789012",
"Message": {
  "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
  "notificationCreationTime": "2016-10-18T17:26:09.572Z",
  "messageType": "ConfigurationSnapshotDeliveryStarted",
  "recordVersion": "1.1"
},
"Timestamp": "2016-10-18T17:26:09.840Z",
"SignatureVersion": "1",
"Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQqZBh6oKE0h0rxcazbyGf5KF5W5rlzKKlEnS9xugFzALPUx//
olSJ4neWallBKNIqlxvAQgu9qHfDR7dS2aCwe4scQfqOjnlEv7PlZqxmT+ux3SR/
C54cbfcdudPsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJ0/EnjduQ08/zd4SYXhm+H9wavcwXB9XECelHhRW70Y
+wHQixfx40SlSaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO+8lceAXIg2Elm7hZ7lZ4PA==",
"SigningCertURL": "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
"UnsubscribeURL": "https://sns.us-east-1.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-1:123456789012:config-topic-
virginia:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Example Configuration Snapshot Delivery Notification

The configuration snapshot is a collection of configuration items for all recorded resources and their configurations in your account. The following is an example notification that AWS Config sends when the configuration snapshot is delivered for your account.

```
{
  "Type": "Notification",
  "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
  "TopicArn": "arn:aws:sns:us-east-1:123456789012:config-topic-virginia",
  "Subject": "[AWS Config:us-east-1] Configuration Snapshot Delivery Completed for
Account 123456789012",
  "Message": {
    "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
    "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-1/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-1_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
    "s3Bucket": "config-bucket-123456789012-virginia",
    "notificationCreationTime": "2016-09-27T18:39:39.853Z",
    "messageType": "ConfigurationSnapshotDeliveryCompleted",
    "recordVersion": "1.1"
  },
  "Timestamp": "2016-09-27T18:39:40.062Z",
  "SignatureVersion": "1",
  "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKzi+RJQRnDJKL2qb+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y
+tRvmMLY5CI1cYrnuPRhTldUk+ROsshg5G+JMtSLVG/TvWbjz44CKXJprjIQg==",
  "SigningCertURL": "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
  "UnsubscribeURL": "https://sns.us-east-1.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-1:123456789012:config-topic-
virginia:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Example Compliance Change Notification

When AWS Config evaluates your resources against a custom or managed rule, AWS Config sends a notification that shows whether the resources are compliant against the rule.

The following is an example notification where the CloudTrail trail resource is compliant against the `cloudtrail-enabled` managed rule.

```
{
  "Type": "Notification",
  "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
  "TopicArn": "arn:aws:sns:us-east-1:123456789012:config-topic-virginia",
  "Subject": "[AWS Config:us-east-1] AWS:::Account 123456789012 is COMPLIANT with cloudtrail-enabled in Accoun...",
  "Message": {
    "awsAccountId": "123456789012",
    "configRuleName": "cloudtrail-enabled",
    "configRuleARN": "arn:aws:config:us-east-1:123456789012:config-rule/config-rule-9rpvxc",
    "resourceType": "AWS:::Account",
    "resourceId": "123456789012",
    "awsRegion": "us-east-1",
    "newEvaluationResult": {
      "evaluationResultIdentifier": {
        "evaluationResultQualifier": {
          "configRuleName": "cloudtrail-enabled",
          "resourceType": "AWS:::Account",
          "resourceId": "123456789012"
        },
        "orderingTimestamp": "2016-09-27T19:48:40.619Z"
      },
      "complianceType": "COMPLIANT",
      "resultRecordedTime": "2016-09-27T19:48:41.405Z",
      "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
      "annotation": null,
      "resultToken": null
    },
    "oldEvaluationResult": {
      "evaluationResultIdentifier": {
        "evaluationResultQualifier": {
          "configRuleName": "cloudtrail-enabled",
          "resourceType": "AWS:::Account",
          "resourceId": "123456789012"
        },
        "orderingTimestamp": "2016-09-27T16:30:49.531Z"
      },
      "complianceType": "NON_COMPLIANT",
      "resultRecordedTime": "2016-09-27T16:30:50.717Z",
      "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
      "annotation": null,
      "resultToken": null
    },
    "notificationCreationTime": "2016-09-27T19:48:42.620Z",
    "messageType": "ComplianceChangeNotification",
    "recordVersion": "1.0"
  },
  "Timestamp": "2016-09-27T19:48:42.749Z",
  "SignatureVersion": "1",
  "Signature": "XZ9FfLb2ywkW9y0yBkNtIP5q7Cry6JtCEyUiHmG9gpOzi3seQ41udhtAqCZoiNiizAEi+6gcttHCRVlhNemzp/YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/y4/6ez8rDyi545FDSLgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqslDHbgWYnp3c80mVL17ohP4hilcxdyWAgXrbsN32ekYr15gdHozx+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ=="
}
```

```
"SigningCertURL": "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
"UnsubscribeURL": "https://sns.us-east-1.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-1:123456789012:config-topic-
virginia:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Example Rules Evaluation Started Notification

AWS Config sends a notification when it starts to evaluate your custom or managed rule against your resources. The following is an example notification when AWS Config starts to evaluate the `iam-password-policy` managed rule.

```
{
  "Type": "Notification",
  "MessageId": "358c8e65-e27a-594e-82d0-delfe77393d7",
  "TopicArn": "arn:aws:sns:us-east-1:123456789012:config-topic-virginia",
  "Subject": "[AWS Config:us-east-1] Config Rules Evaluation Started for Account
123456789012",
  "Message": {
    "awsAccountId": "123456789012",
    "awsRegion": "us-east-1",
    "configRuleNames": ["iam-password-policy"],
    "notificationCreationTime": "2016-10-13T21:55:21.339Z",
    "messageType": "ConfigRulesEvaluationStarted",
    "recordVersion": "1.0"
  },
  "Timestamp": "2016-10-13T21:55:21.575Z",
  "SignatureVersion": "1",
  "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSB13sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPDOM+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGwPHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDvVzd15iMrAzQ==",
  "SigningCertURL": "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
  "UnsubscribeURL": "https://sns.us-east-1.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-1:123456789012:config-topic-
virginia:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Example Oversized Configuration Item Change Notification

When AWS Config detects a configuration change for a resource, it sends a configuration item notification. If the notification exceeds the maximum size allowed by Amazon Simple Notification Service (Amazon SNS), the notification includes a brief summary of the configuration item. You can view the complete notification in the Amazon S3 bucket location specified in the `s3BucketLocation` field.

The following example notification shows a configuration item for an Amazon EC2 instance. The notification includes a summary of the changes and the location of the notification in the Amazon S3 bucket.

```
View the Timeline for this Resource in AWS Config Management Console:
https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z
```

The full configuration item change notification for this resource exceeded the maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the configuration

item is provided here. You can view the complete notification in the specified Amazon S3 bucket location.

New State Record Summary:

```
-----
{
  "configurationItemSummary": {
    "changeType": "UPDATE",
    "configurationItemVersion": "1.2",
    "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
    "configurationStateId": 0,
    "awsAccountId": "123456789012",
    "configurationItemStatus": "OK",
    "resourceType": "AWS::EC2::Instance",
    "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
    "resourceName": null,
    "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
    "awsRegion": "us-west-2",
    "availabilityZone": null,
    "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
    "resourceCreationTime": "2016-10-06T16:46:10.489Z"
  },
  "s3DeliverySummary": {
    "s3BucketLocation": "my-bucket/AWSLogs/123456789012/Config/us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-a31942b02e80_20161006T164616Z_0.json.gz",
    "errorCode": null,
    "errorMessage": null
  },
  "notificationCreationTime": "2016-10-06T16:46:16.261Z",
  "messageType": "OversizedConfigurationItemChangeNotification",
  "recordVersion": "1.0"
}
```

Example Delivery Failed Notification

AWS Config sends a delivery failed notification if AWS Config can't deliver the configuration snapshot or an oversized configuration item change notification to your Amazon S3 bucket. Verify that you specified a valid Amazon S3 bucket.

View the Timeline for this Resource in AWS Config Management Console:
https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?time=2016-10-06T16:46:13.749Z

The full configuration item change notification for this resource exceeded the maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the configuration item is provided here. You can view the complete notification in the specified Amazon S3 bucket location.

New State Record Summary:

```
-----
{
  "configurationItemSummary": {
    "changeType": "UPDATE",
    "configurationItemVersion": "1.2",
    "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
    "configurationStateId": 0,
    "awsAccountId": "123456789012",
    "configurationItemStatus": "OK",
```



```
    "resourceType": "AWS::EC2::Instance",
    "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
    "resourceName": null,
    "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
    "awsRegion": "us-west-2",
    "availabilityZone": null,
    "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
    "resourceCreationTime": "2016-10-06T16:46:10.489Z"
  },
  "s3DeliverySummary": {
    "s3BucketLocation": null,
    "errorCode": "NoSuchBucket",
    "errorMessage": "Failed to deliver notification to bucket: bucket-example for
account 123456789012 in region us-west-2."
  },
  "notificationCreationTime": "2016-10-06T16:46:13.749Z",
  "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
  "recordVersion": "1.0"
}
```

Using Amazon SQS to Monitor AWS Resource Changes

AWS Config uses Amazon Simple Notification Service (SNS) to send you notifications every time a supported AWS resource is created, updated, or otherwise modified as a result of user API activity. However, you might be interested in only certain resource configuration changes. For example, you might consider it critical to know when someone modifies the configuration of a security group, but not need to know every time there is a change to tags on your Amazon EC2 instances. Or, you might want to write a program that performs specific actions when specific resources are updated. For example, you might want to start a certain workflow when a security group configuration is changed. If you want to programmatically consume the data from AWS Config in these or other ways, use an Amazon Simple Queue Service queue as the notification endpoint for Amazon SNS.

Note

Notifications can also come from Amazon SNS in the form of an email, a Short Message Service (SMS) message to SMS-enabled mobile phones and smartphones, a notification message to an application on a mobile device, or a notification message to one or more HTTP or HTTPS endpoints.

You can have a single SQS queue subscribe to multiple topics, whether you have one topic per region or one topic per account per region. You must subscribe the queue to your desired SNS topic. (You can subscribe multiple queues to one SNS topic.) For more information, see [Sending Amazon SNS Messages to Amazon SQS Queues](#).

Permissions for Amazon SQS

To use Amazon SQS with AWS Config, you must configure a policy that grants permissions to your account to perform all actions that are allowed on an SQS queue. The following example policy grants the account number 111122223333 and account number 444455556666 permission to send messages pertaining to each configuration change to the queue named `arn:aws:sqs:us-east-1:444455556666:queue1`.

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
  {
    "Sid": "Queue1_SendMessage",
```

```
    "Effect": "Allow",
    "Principal": {
      "AWS": ["111122223333", "444455556666"]
    },
    "Action": "sqs:SendMessage",
    "Resource": "arn:aws:sqs:us-east-1:444455556666:queue1"
  }
}
```

You must also create a policy that grants permissions for connections between an SNS topic and the SQS queue that subscribes to that topic. The following is an example policy that permits the SNS topic with the Amazon Resource Name (ARN) `arn:aws:sns:us-east-1:111122223333:test-topic` to perform any actions on the queue named `arn:aws:sqs:us-east-1:111122223333:test-topic-queue`.

Note

The account for the SNS topic and the SQS queue must be in the same region.

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement": [
    {
      "Sid": "rule1",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "sqs:*",
      "Resource": "arn:aws:sqs:us-east-1:111122223333:test-topic-queue",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "arn:aws:sns:us-east-1:111122223333:test-topic"
        }
      }
    }
  ]
}
```

Each policy can include statements that cover only a single queue, not multiple queues. For information about other restrictions on Amazon SQS policies, see [Special Information for Amazon SQS Policies](#).

Managing AWS Config

At any time, you can change the settings for your IAM role and modify or delete your delivery channel (that is, the Amazon Simple Storage Service bucket and the Amazon Simple Notification Service topic). You can start or stop the configuration recorder associated with your account, and you can customize which types of resources are recorded.

Topics

- [Managing the Delivery Channel \(p. 103\)](#)
- [Updating the IAM Role Assigned to AWS Config \(p. 106\)](#)
- [Managing the Configuration Recorder \(p. 107\)](#)
- [Selecting Which Resources AWS Config Records \(p. 109\)](#)

Managing the Delivery Channel

As AWS Config continually records the changes that occur to your AWS resources, it sends notifications and updated configuration states through the *delivery channel*. You can manage the delivery channel to control where AWS Config sends configuration updates.

You can have only one delivery channel per AWS account, and the delivery channel is required to use AWS Config.

Updating the Delivery Channel

When you update the delivery channel, you can set the following options:

- The Amazon S3 bucket to which AWS Config sends configuration snapshots and configuration history files.
- How often AWS Config delivers configuration snapshots to your Amazon S3 bucket.
- The Amazon SNS topic to which AWS Config sends notifications about configuration changes.

To update the delivery channel (console)

- You can use the AWS Config console to set the Amazon S3 bucket and the Amazon SNS topic for your delivery channel. For steps to manage these settings, see [Setting up AWS Config with the Console \(p. 17\)](#).

The console does not provide options to rename the delivery channel, set the frequency for configuration snapshots, or delete the delivery channel. To do these tasks, you must use the AWS CLI, the AWS Config API, or one of the AWS SDKs.

To update the delivery channel (AWS CLI)

1. Use the `put-delivery-channel` command:

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

The `deliveryChannel.json` file specifies the delivery channel attributes:

```
{
  "name": "default",
  "s3BucketName": "config-bucket-123456789012",
  "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
  "configSnapshotDeliveryProperties": {
    "deliveryFrequency": "Twelve_Hours"
  }
}
```

This example sets the following attributes:

- `name` – The name of the delivery channel. By default, AWS Config assigns the name `default` to a new delivery channel.

You cannot update the delivery channel name with the `put-delivery-channel` command. For the steps to change the name, see [Renaming the Delivery Channel \(p. 105\)](#).

- `s3BucketName` – The name of the Amazon S3 bucket to which AWS Config delivers configuration snapshots and configuration history files.

If you specify a bucket that belongs to another AWS account, that bucket must have policies that grant access permissions to AWS Config. For more information, see [Permissions for the Amazon S3 Bucket \(p. 116\)](#).

- `snsTopicARN` – The Amazon Resource Name (ARN) of the Amazon SNS topic to which AWS Config sends notifications about configuration changes.

If you choose a topic from another account, that topic must have policies that grant access permissions to AWS Config. For more information, see [Permissions for the Amazon SNS Topic \(p. 117\)](#).

- `configSnapshotDeliveryProperties` – Contains the `deliveryFrequency` attribute, which sets how often AWS Config delivers configuration snapshots.

2. (Optional) You can use the `describe-delivery-channels` command to verify that the delivery channel settings are updated:

```
$ aws configservice describe-delivery-channels
{
  "DeliveryChannels": [
    {
      "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
      },
      "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
      "name": "default",
      "s3BucketName": "config-bucket-123456789012"
    }
  ]
}
```

```
]
}
```

Renaming the Delivery Channel

To change the delivery channel name, you must delete it and create a new delivery channel with the desired name. Before you can delete the delivery channel, you must temporarily stop the configuration recorder.

The AWS Config console does not provide the option to delete the delivery channel, so you must use the AWS CLI, the AWS Config API, or one of the AWS SDKs.

To rename the delivery channel (AWS CLI)

1. Use the `stop-configuration-recorder` command to stop the configuration recorder:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-  
name configRecorderName
```

2. Use the `describe-delivery-channels` command, and take note of your delivery channel's attributes:

```
$ aws configservice describe-delivery-channels  
{  
  "DeliveryChannels": [  
    {  
      "configSnapshotDeliveryProperties": {  
        "deliveryFrequency": "Twelve_Hours"  
      },  
      "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",  
      "name": "default",  
      "s3BucketName": "config-bucket-123456789012"  
    }  
  ]  
}
```

3. Use the `delete-delivery-channel` command to delete the delivery channel:

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. Use the `put-delivery-channel` command to create a delivery channel with the desired name:

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

The `deliveryChannel.json` file specifies the delivery channel attributes:

```
{  
  "name": "myCustomDeliveryChannelName",  
  "s3BucketName": "config-bucket-123456789012",  
  "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",  
  "configSnapshotDeliveryProperties": {  
    "deliveryFrequency": "Twelve_Hours"  
  }  
}
```

5. Use the `start-configuration-recorder` command to resume recording:

```
$ aws configservice start-configuration-recorder --configuration-recorder-  
name configRecorderName
```

Updating the IAM Role Assigned to AWS Config

You can update the IAM role assumed by AWS Config any time. Before you update the IAM role, ensure that you have created a new role to replace the old one. You must attach policies to the new role that grant permissions to AWS Config to record configurations and deliver them to your delivery channel. In addition, make sure to copy the Amazon Resource Name (ARN) of your new IAM role. You will need it to update the IAM role. For information about creating an IAM role and attaching the required policies to the IAM role, see [Creating an IAM Role \(p. 22\)](#).

Tip

To find the ARN of an existing IAM role, go to the IAM console at <https://console.aws.amazon.com/iam/>. Choose **Roles** in the navigation pane. Then choose the name of the desired role and find the ARN at the top of the **Summary** page.

Updating the IAM Role

You can update your IAM role using the AWS Management Console or the AWS CLI.

To update the IAM role in a region where rules are supported (console)

If you are using AWS Config in a region that supports AWS Config rules, complete the following steps. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Settings** in the navigation pane.
3. In the **AWS Config role**, section, choose the IAM role:
 - **Create a role** – AWS Config creates a role that has the required permissions. For **Role name**, you can customize the name that AWS Config creates.
 - **Choose a role from your account** – For **Role name**, choose an IAM role in your account that grants the required permissions. For the required permissions, see [Permissions for the IAM Role Assigned to AWS Config \(p. 113\)](#).
4. Choose **Save**.

To update the IAM role in a region where rules are not supported (console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. On the **Resource inventory** page, choose the settings icon (⚙️).
3. Choose **Continue**.
4. In the **AWS Config is requesting permissions to read your resources' configuration** page, choose **View Details**.
5. In the **Role Summary** section, choose the IAM role:
 - If you want to create a role, for **IAM Role**, choose **Create a new IAM Role**. Then type a name for **Role Name**.

- If you want to use an existing role, select it for **IAM Role**. Then, for **Policy Name**, select an available policy or create one by selecting **Create a new Role Policy**.
6. Choose **Allow**.

To update the IAM role (AWS CLI)

- Use the `put-configuration-recorder` command and specify the Amazon Resource Name (ARN) of the new role:

```
$ aws configservice put-configuration-recorder --configuration-recorder
name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

Managing the Configuration Recorder

AWS Config uses the *configuration recorder* to detect changes in your resource configurations and capture these changes as configuration items. You must create a configuration recorder before AWS Config can track your resource configurations.

If you set up AWS Config by using the console or the AWS CLI, AWS Config automatically creates and then starts the configuration recorder for you. For more information, see [Getting Started with AWS Config \(p. 16\)](#).

By default, the configuration recorder records all supported resources in the region where AWS Config is running. You can create a customized configuration recorder that records only the resource types that you specify. For more information, see [Selecting Which Resources AWS Config Records \(p. 109\)](#).

You are charged service usage fees when AWS Config starts recording configurations. For pricing information, see [AWS Config Pricing](#). To control costs, you can stop recording by stopping the configuration recorder. After you stop recording, you can continue to access the configuration information that was already recorded. You will not be charged AWS Config usage fees until you resume recording.

When you start the configuration recorder, AWS Config takes an inventory of all AWS resources in your account.

Managing the Configuration Recorder (Console)

You can use the AWS Config console to stop or start the configuration recorder.

To stop or start the configuration recorder

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Settings** in the navigation pane.
3. Stop or start the configuration recorder:
 - If you want to stop recording, under **Recording is on**, choose **Turn off**. When prompted, choose **Continue**.
 - If you want to start recording, under **Recording is off**, choose **Turn on**. When prompted, choose **Continue**.

Managing the Configuration Recorder (AWS CLI)

You can use the AWS CLI to stop or start the configuration recorder. You can also rename or delete the configuration recorder using the AWS CLI, the AWS Config API, or one of the AWS SDKs. The following steps help you use the AWS CLI.

To stop the configuration recorder

- Use the `stop-configuration-recorder` command:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-name configRecorderName
```

To start the configuration recorder

- Use the `start-configuration-recorder` command:

```
$ aws configservice start-configuration-recorder --configuration-recorder-name configRecorderName
```

To rename the configuration recorder

To change the configuration recorder name, you must delete it and create a new configuration recorder with the desired name.

- Use the `describe-configuration-recorders` command to look up the name of your current configuration recorder:

```
$ aws configservice describe-configuration-recorders
{
  "ConfigurationRecorders": [
    {
      "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
      "name": "default"
    }
  ]
}
```

- Use the `delete-configuration-recorder` command to delete your current configuration recorder:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-name default
```

- Use the `put-configuration-recorder` command to create a configuration recorder with the desired name:

```
$ aws configservice put-configuration-recorder --configuration-recorder-name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

- Use the `start-configuration-recorder` command to resume recording:

```
$ aws configservice start-configuration-recorder --configuration-recorder-name configRecorderName
```

To delete the configuration recorder

- Use the `delete-configuration-recorder` command:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-name default
```

Selecting Which Resources AWS Config Records

AWS Config continuously detects when any resource of a supported type is created, changed, or deleted. AWS Config records these events as configuration items. You can customize AWS Config to record changes for all supported types of resources or for only those types that are relevant to you. To learn which types of resources AWS Config can record, see [Supported AWS Resource Types \(p. 7\)](#).

Recording All Supported Resource Types

By default, AWS Config records the configuration changes for all supported types of *regional resources* that AWS Config discovers in the region in which it is running. Regional resources are tied to a region and can be used only in that region. Examples of regional resources are EC2 instances and EBS volumes.

You can also have AWS Config record supported types of *global resources*. Global resources are not tied to a specific region and can be used in all regions. The global resource types that AWS Config supports are IAM users, groups, roles, and customer managed policies.

Important

The configuration details for a specific global resource are the same in all regions. If you customize AWS Config in multiple regions to record global resources, AWS Config creates multiple configuration items each time a global resource changes: one configuration item for each region. These configuration items will contain identical data. To prevent duplicate configuration items, you should consider customizing AWS Config in only one region to record global resources, unless you want the configuration items to be available in multiple regions.

Recording Specific Resource Types

If you don't want AWS Config to record the changes for all supported resources, you can customize it to record changes for only specific types. AWS Config records configuration changes for the types of resources that you specify, including the creation and deletion of such resources.

If a resource is not recorded, AWS Config captures only the creation and deletion of that resource, and no other details, at no cost to you. When a nonrecorded resource is created or deleted, AWS Config sends a notification, and it displays the event on the resource details page. The details page for a nonrecorded resource provides null values for most configuration details, and it does not provide information about relationships and configuration changes.

The relationship information that AWS Config provides for recorded resources is not limited because of missing data for nonrecorded resources. If a recorded resource is related to a nonrecorded resource, that relationship is provided in the details page of the recorded resource.

You can stop AWS Config from recording a type of resource any time. After AWS Config stops recording a resource, it retains the configuration information that was previously captured, and you can continue to access this information.

AWS Config rules can be used to evaluate compliance for only those resources that AWS Config records.

Selecting Resources (Console)

You can use the AWS Config console to select the types of resources that AWS Config records.

To select resources

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Open the **Settings** page:
 - If you are using AWS Config in a region that supports AWS Config rules, choose **Settings** in the navigation pane. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
 - Otherwise, choose the settings icon (⚙️) on the **Resource inventory** page.
3. In the **Resource types to record** section, specify which types of AWS resources you want AWS Config to record:
 - **All resources** – AWS Config records all supported resources with the following options:
 - **Record all resources supported in this region** – AWS Config records configuration changes for every supported type of regional resource. When AWS Config adds support for a new type of regional resource, it automatically starts recording resources of that type.
 - **Include global resources** – AWS Config includes supported types of global resources with the resources that it records (for example, IAM resources). When AWS Config adds support for a new type of global resource, it automatically starts recording resources of that type.
 - **Specific types** – AWS Config records configuration changes for only those types of AWS resources that you specify.
4. Save your changes:
 - If you are using AWS Config in a region that supports AWS Config rules, choose **Save**.
 - Otherwise, choose **Continue**. In the **AWS Config is requesting permissions to read your resources' configuration** page, choose **Allow**.

Selecting Resources (AWS CLI)

You can use the AWS CLI to select the types of resources that you want AWS Config to record. You do this by creating a configuration recorder, which records the types of resources that you specify in a recording group. In the recording group, you specify whether all supported types or specific types of resources are recorded.

To select all supported resources

1. Use the following `put-configuration-recorder` command:

```
$ aws configservice put-configuration-recorder --configuration-recorder
name=default,roleARN=arn:aws:iam::123456789012:role/config-role --recording-group
allSupported=true,includeGlobalResourceTypes=true
```

This command uses the following options for the `--recording-group` parameter:

- `allSupported=true` – AWS Config records configuration changes for every supported type of *regional resource*. When AWS Config adds support for a new type of regional resource, it automatically starts recording resources of that type.
- `includeGlobalResourceTypes=true` – AWS Config includes supported types of global resources with the resources that it records. When AWS Config adds support for a new type of global resource, it automatically starts recording resources of that type.

Before you can set this option to `true`, you must set the `allSupported` option to `true`.

If you do not want to include global resources, set this option to `false`, or omit it.

2. (Optional) To verify that your configuration recorder has the settings that you want, use the following `describe-configuration-recorders` command:

```
$ aws configservice describe-configuration-recorders
```

The following is an example response:

```
{
  "ConfigurationRecorders": [
    {
      "recordingGroup": {
        "allSupported": true,
        "resourceTypes": [],
        "includeGlobalResourceTypes": true
      },
      "roleARN": "arn:aws:iam::123456789012:role/config-role",
      "name": "default"
    }
  ]
}
```

To select specific types of resources

1. Use the `aws configservice put-configuration-recorder` command, and pass one or more resource types through the `--recording-group` option, as shown in the following example:

```
$ aws configservice put-configuration-recorder --configuration-recorder
name=default,roleARN=arn:aws:iam::012345678912:role/myConfigRole --recording-
group file://recordingGroup.json
```

The `recordingGroup.json` file specifies which types of resources AWS Config will record:

```
{
  "allSupported": false,
  "includeGlobalResourceTypes": false,
  "resourceTypes": [
    "AWS::EC2::EIP",
    "AWS::EC2::Instance",
    "AWS::EC2::NetworkAcl",
    "AWS::EC2::SecurityGroup",
    "AWS::CloudTrail::Trail",
    "AWS::EC2::Volume",
    "AWS::EC2::VPC",
    "AWS::IAM::User",
    "AWS::IAM::Policy"
  ]
}
```

Before you can specify resource types for the `resourceTypes` key, you must set the `allSupported` and `includeGlobalResourceTypes` options to `false` or omit them.

2. (Optional) To verify that your configuration recorder has the settings that you want, use the following `describe-configuration-recorders` command:

```
$ aws configservice describe-configuration-recorders
```

The following is an example response:

```
{
  "ConfigurationRecorders": [
    {
      "recordingGroup": {
        "allSupported": false,
        "resourceTypes": [
          "AWS::EC2::EIP",
          "AWS::EC2::Instance",
          "AWS::EC2::NetworkAcl",
          "AWS::EC2::SecurityGroup",
          "AWS::CloudTrail::Trail",
          "AWS::EC2::Volume",
          "AWS::EC2::VPC",
          "AWS::IAM::User",
          "AWS::IAM::Policy"
        ],
        "includeGlobalResourceTypes": false
      },
      "roleARN": "arn:aws:iam::123456789012:role/config-role",
      "name": "default"
    }
  ]
}
```

Permissions for AWS Config

To get the most out of AWS Config, you need to create permissions [policies](#) to attach to your IAM role, your Amazon Simple Storage Service (S3) bucket, and your Amazon Simple Notification Service (SNS) topic. A policy is a set of statements that grants AWS Config permissions. The following topics provide examples of recommended IAM policies to use with the AWS Config console and the AWS Command Line Interface.

Topics

- [Permissions for the IAM Role Assigned to AWS Config \(p. 113\)](#)
- [Permissions for the Amazon S3 Bucket \(p. 116\)](#)
- [Permissions for the Amazon SNS Topic \(p. 117\)](#)
- [Permissions for Accessing AWS Config \(p. 118\)](#)

Permissions for the IAM Role Assigned to AWS Config

An AWS Identity and Access Management (IAM) role lets you define a set of permissions. AWS Config assumes the role that you assign to it to write to your S3 bucket, publish to your SNS topic, and to make [Describe](#) or [List](#) API requests to get configuration details for your AWS resources. For more information on IAM roles, see [IAM Roles](#) in the *IAM User Guide*.

When you use the AWS Config console to create or update an IAM role, AWS Config automatically attaches the required permissions for you. For more information, see [Setting up AWS Config with the Console \(p. 17\)](#).

Contents

- [Creating IAM Role Policies \(p. 113\)](#)
 - [Adding an IAM Trust Policy to your Role \(p. 114\)](#)
 - [IAM Role Policy for Amazon S3 Bucket \(p. 114\)](#)
 - [IAM Role Policy for Amazon SNS Topic \(p. 115\)](#)
 - [IAM Role Policy for Getting Configuration Details \(p. 115\)](#)

- [Troubleshooting for recording S3 buckets \(p. 115\)](#)

Creating IAM Role Policies

When you use the AWS Config console to create an IAM role, AWS Config automatically attaches the required permissions to the role for you.

If you are using the AWS CLI to set up AWS Config or you are updating an existing IAM role, you must manually update the policy to allow AWS Config to access your S3 bucket, publish to your SNS topic, and get configuration details about your resources.

Adding an IAM Trust Policy to your Role

You can create an IAM trust policy that enables AWS Config to assume a role and use it to track your resources. For more information about trust policies, see [Assuming a Role](#) in the *IAM User Guide*.

The following is an example trust policy for AWS Config roles:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

IAM Role Policy for Amazon S3 Bucket

The following example policy grants AWS Config permissions to access your Amazon S3 bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:PutObject"],
      "Resource": ["arn:aws:s3::: myBucketName/prefix/AWSLogs/myAccountID/*"],
      "Condition": {
        "StringLike": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetBucketAcl"],
      "Resource": "arn:aws:s3::: myBucketName "
    }
  ]
}
```

```
]
}
```

IAM Role Policy for Amazon SNS Topic

The following example policy grants AWS Config permissions to access your SNS topic:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sns:Publish",
      "Resource": "mySNSTopicARN"
    }
  ]
}
```

IAM Role Policy for Getting Configuration Details

To record your AWS resource configurations, AWS Config requires IAM permissions to get the configuration details about your resources.

Use the AWS managed policy **AWSConfigRole** and attach it to the IAM role that you assign to AWS Config. AWS updates this policy each time AWS Config adds support for an AWS resource type, which means AWS Config will continue to have the required permissions to get configuration details as long as the role has this managed policy attached.

If you create or update a role with the console, AWS Config attaches the **AWSConfigRole** for you.

If you use the AWS CLI, use the `attach-role-policy` command and specify the Amazon Resource Name (ARN) for **AWSConfigRole**:

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn arn:aws:iam::aws:policy/
service-role/AWSConfigRole
```

Troubleshooting for recording S3 buckets

If you configured AWS Config to record S3 buckets for your account, AWS Config records and delivers notifications when an S3 bucket is created, updated, or deleted.

If you configured AWS Config to record S3 buckets, and are not receiving configuration change notifications:

- Verify that the IAM role assigned to AWS Config has the **AWSConfigRole** managed policy.
- If you have S3 bucket policies attached to your buckets, verify that they allow AWS Config permission to record changes to your buckets.

If you have a custom policy for your S3 bucket, you can add the following policy to your existing bucket policy. This policy grants AWS Config permission to record the S3 bucket.

```
{
  "Sid": "AWSConfig_ReadConfiguration_Access",
  "Effect": "Allow",
```



```
"Principal": {"AWS": "arn:aws:iam::myAccountID::role/config-role"},
"Action": [
    "s3:GetAccelerateConfiguration",
    "s3:GetBucketAcl",
    "s3:GetBucketCORS",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketNotification",
    "s3:GetBucketPolicy",
    "s3:GetBucketRequestPayment",
    "s3:GetBucketTagging",
    "s3:GetBucketVersioning",
    "s3:GetBucketWebsite",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration"
],
"Resource": "arn:aws:s3:::myBucketName/*"
}
```

Permissions for the Amazon S3 Bucket

By default, all Amazon S3 buckets and objects are private. Only the resource owner and the AWS account that created the bucket can access that bucket and any objects it contains. The resource owner can, however, choose to grant access permissions to other resources and users. One way to do this is to write an access policy.

If AWS Config creates an S3 bucket for you automatically (for example, if you use the AWS Config console or use the `aws config subscribe` command to set up your delivery channel) or you choose an existing S3 bucket already existing in your account, these permissions are automatically added to the S3 bucket. However, if you specify an existing S3 bucket from another account, you must ensure that the S3 bucket has the correct permissions.

Required permissions for an Amazon S3 bucket in another account

When AWS Config sends configuration information (history files and snapshots) to the Amazon S3 bucket in your account, it assumes the IAM role that you assigned when you set up AWS Config. When AWS Config sends to an S3 bucket in another account, it first attempts to use the IAM role, but this attempt fails if the access policy for the bucket does not grant `WRITE` access to the IAM role. In this event, AWS Config sends the information again, this time as the AWS Config service principal. Before the delivery can succeed, the access policy must grant `WRITE` access to the `config.amazonaws.com` principal name. AWS Config is then the owner of the objects it delivers to the S3 bucket.

Granting AWS Config access to an Amazon S3 bucket in another account

Follow these steps to add an access policy to an Amazon S3 bucket in another account. The access policy allows AWS Config to send configuration information to the bucket.

1. Sign in to the AWS Management Console using the account that has the S3 bucket.
2. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
3. Select the bucket that you want AWS Config to use to deliver configuration items, and then choose **Properties**.

4. Choose **Permissions**.
5. Choose **Edit Bucket Policy**.
6. Copy the following policy into the **Bucket Policy Editor** window:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "config.amazonaws.com"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::targetBucketName"
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "config.amazonaws.com"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::targetBucketName/[optional] prefix/
AWSLogs/sourceAccountID-WithoutHyphens/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

7. Substitute the following values in the bucket policy:
 - *targetBucketName* – The name of the Amazon S3 bucket to which AWS Config will deliver configuration items.
 - *[optional] prefix* – An optional addition to the Amazon S3 object key that helps create a folder-like organization in the bucket.
 - *sourceAccountID-WithoutHyphens* – The ID of the account for which AWS Config will deliver configuration items to the target bucket.
8. Choose **Save** and then **Close**.

Permissions for the Amazon SNS Topic

AWS Config must have permissions to send notifications to an SNS topic. If you use the AWS Config console to set up your delivery channel with a new SNS topic or you choose an SNS topic that already exists in your account, these permissions are automatically added to the SNS topic. However, if you specify an existing topic from another account or you set up your delivery channel using the API, you must make sure that the topic has the correct permissions.

The following example shows the permissions that are automatically created by AWS Config for a new topic. This policy statement allows AWS Config to publish to a specified Amazon SNS topic.

If you want to use an existing SNS topic from another account or you set up your delivery channel using the API, make sure to attach the following policy to the SNS topic.

```
{
  "Id": "Policy1415489375392",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy20150201",
      "Action": [
        "SNS:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "Service": [
          "config.amazonaws.com"
        ]
      }
    }
  ]
}
```

For the `Resource` key, `account-id` is the account number of the topic owner; in topics that you create, this will be your account number. You must substitute appropriate values for `region` and `myTopic`.

Permissions for Accessing AWS Config

When you give permissions to IAM users to use the AWS Config console or the AWS CLI, you can (and should) restrict their permissions to the least amount of access that they need.

In most cases, permissions should cover these common uses:

- Setting up and managing AWS Config (full-access permissions)
- Using AWS Config (read-only permissions)

Users who set up and manage AWS Config must have full-access permissions. With full-access permissions, you can perform essential setup tasks such as:

- Provide Amazon S3 and Amazon SNS endpoints that AWS Config delivers data to
- Create the role that gets provided to AWS Config
- Turn recording on and off

Users who use AWS Config but don't need to set it up should have read-only permissions. These permissions are useful for users who look up the configurations of resources or who search for resources by tags.

To give read-only permission for AWS Config access

1. Sign in to the AWS Identity and Access Management (IAM) console at <https://console.aws.amazon.com/iam>.
2. In the navigation pane, choose **Policies**.
3. In the list of policies, select the `AWSConfigUserAccess` policy. You can use the **Filter** menu and the **Search** box to find the policy.
4. Choose **Policy Actions**, and then choose **Attach**.

5. Select the users, groups, or roles and then choose **Attach Policy**. You can use the **Filter** menu and the **Search** box to filter the list.
6. Choose **Apply Policy**.

To give full-access permission for AWS Config access

1. Sign in to the AWS Identity and Access Management (IAM) console at <https://console.aws.amazon.com/iam>.
2. In the navigation pane, choose **Policies**, and then choose **Create Policy**.
3. For **Create Your Own Policy**, choose **Select**.
4. Type a policy name and description. For example: `AWSConfigFullAccess`.
5. For **Policy Document**, type or paste the full-access policy into the editor. You can use the [Example full-access permission](#) (p. 120).
6. Choose **Validate Policy** and ensure that no errors display in a red box at the top of the screen. Correct any errors that are reported.
7. Choose **Create Policy** to save your new policy.
8. In the list of policies, select the policy that you created. You can use the **Filter** menu and the **Search** box to find the policy.
9. Choose **Policy Actions**, and then choose **Attach**.
10. Select the users, groups, or roles, and then choose **Attach Policy**. You can use the **Filter** menu and the **Search** box to filter the list.
11. Choose **Apply Policy**.

Note

Instead of creating a managed policy, you can also create an inline policy from the IAM console and attach it to an IAM user, group, or role. For more information, see [Working with Inline Policies](#) in the *IAM User Guide*.

Example policies

Example read-only permission

The following AWS managed policy, `AWSConfigUserAccess`, grants read-only permissions for AWS Config.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

Example full-access permission

The following example policy grants full-access permissions for AWS Config.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns>DeleteTopic",
        "sns:GetTopicAttributes",
        "sns:ListPlatformApplications",
        "sns:ListTopics",
        "sns:SetTopicAttributes"
      ],
      "Resource": "arn:aws:sns:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListBucketVersions",
        "s3:PutBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:PassRole",
        "iam:PutRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:CreatePolicyVersion",
        "iam>DeletePolicyVersion"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ]
    }
  ]
}
```

```
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
          "config:*",
          "tag:Get*"
        ],
        "Resource": "*"
      }
    ]
  }
```

Logging AWS Config API Calls with AWS CloudTrail

AWS Config is integrated with AWS CloudTrail, a service that captures API calls made by or on behalf of AWS services in your AWS account and delivers the log files to an Amazon Simple Storage Service (S3) bucket that you specify. CloudTrail captures all API calls from the AWS Config console or from the AWS Config API. Using the information collected by CloudTrail, you can determine what request was made to AWS Config, the source IP address from which the request was made, who made the request, when it was made, and so on. To learn more about CloudTrail, including how to configure and enable it, see the [AWS CloudTrail User Guide](#).

AWS Config Information in CloudTrail

When enabled in your AWS account, CloudTrail tracks API calls made to AWS Config. AWS Config records are written together with other AWS service records in a log file. CloudTrail determines when to create and write to a new file based on a time period and file size.

All of the AWS Config actions are logged and are documented in the [Actions](#) topic in the [AWS Config API Reference](#). For example, calls to the [DeliverConfigSnapshot](#), [DeleteDeliveryChannel](#), and [DescribeDeliveryChannels](#) actions generate entries in the CloudTrail log files.

Every log entry contains information about who generated the request. The user identity information in the log helps you determine whether the request was made with root or IAM user credentials, with temporary security credentials for a role or federated user, or by another AWS service. For more information, see the **userIdentity** field in the [CloudTrail Event Reference](#).

By default, your log files are encrypted by using Amazon S3 server-side encryption (SSE). You can store your log files in your bucket for as long as you want, but you can also define Amazon S3 lifecycle rules to archive or delete log files automatically. For information on setting up lifecycle rules, see [Managing Lifecycle Configuration](#) in the *Amazon Simple Storage Service Console User Guide*.

If you want to take quick action upon log file delivery, you can choose to have CloudTrail publish Amazon SNS notifications when new log files are delivered. For more information, see [Configuring Amazon SNS Notifications](#).

You can also aggregate AWS Config log files from multiple AWS regions and multiple AWS accounts into a single S3 bucket. For more information, see [Aggregating CloudTrail Log Files to a Single Amazon S3 Bucket](#).

Understanding AWS Config Log File Entries

CloudTrail log files can contain one or more log entries where each entry is made up of multiple JSON-formatted events. A log entry represents a single request from any source and includes information about the requested action, any parameters, the date and time of the action, and so on. The log entries are not guaranteed to be in any particular order. That is, they are not an ordered stack trace of the public API calls.

Following are examples of CloudTrail log files for all AWS Config actions.

DeleteDeliveryChannel

Following is an example CloudTrail log file for the `DeleteDeliveryChannel` action.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:32:57Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "DeleteDeliveryChannel",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "10.24.34.0",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "deliveryChannelName": "default"
  },
  "responseElements": null,
  "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```

DeliverConfigSnapshot

Following is an example CloudTrail log file for the `DeliverConfigSnapshot` action.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDAABCDEFGHJKLMNPQ:Config-API-Test",
    "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2014-12-11T00:58:42Z"
      }
    }
  },
  "eventTime": "2014-12-11T00:58:42Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "DeliverConfigSnapshot",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "10.24.34.0",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "deliveryChannelName": "default"
  },
  "responseElements": null,
  "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```



```
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AIDAABCDEFGHijklmnopq",
      "arn": "arn:aws:iam::111111111111:role/JaneDoe",
      "accountId": "111111111111",
      "userName": "JaneDoe"
    }
  },
  "eventTime": "2014-12-11T00:58:53Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "DeliverConfigSnapshot",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "10.24.34.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": {
    "deliveryChannelName": "default"
  },
  "responseElements": {
    "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
  },
  "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
  "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

DescribeConfigurationRecorderStatus

Following is an example CloudTrail log file for the [DescribeConfigurationRecorderStatus](#) action.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:35:44Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "DescribeConfigurationRecorderStatus",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```

DescribeConfigurationRecorders

Following is an example CloudTrail log file for the [DescribeConfigurationRecorders](#) action.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:34:52Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "DescribeConfigurationRecorders",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```

DescribeDeliveryChannels

Following is an example CloudTrail log file for the [DescribeDeliveryChannels](#) action.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:35:02Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "DescribeDeliveryChannels",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```

GetResourceConfigHistory

Following is an example CloudTrail log file for the [GetResourceConfigHistory](#) action.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDAABCDEFGHJKLMNOPQ:Config-API-Test",
    "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2014-12-11T00:58:42Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAABCDEFGHJKLMNOPQ",
        "arn": "arn:aws:iam::111111111111:role/JaneDoe",
        "accountId": "111111111111",
        "userName": "JaneDoe"
      }
    }
  },
  "eventTime": "2014-12-11T00:58:42Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "GetResourceConfigHistory",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "10.24.34.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": {
    "resourceId": "vpc-a12bc345",
    "resourceType": "AWS::EC2::VPC",
    "limit": 0,
    "laterTime": "Dec 11, 2014 12:58:42 AM",
    "earlierTime": "Dec 10, 2014 4:58:42 PM"
  },
  "responseElements": null,
  "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
  "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

PutConfigurationRecorder

Following is an example CloudTrail log file for the [PutConfigurationRecorder](#) action.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:35:23Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "PutConfigurationRecorder",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",

```

```
"userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
"requestParameters": {
  "configurationRecorder": {
    "name": "default",
    "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
  }
},
"responseElements": null,
"requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
"eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
"eventType": "AwsApiCall",
"recipientAccountId": "222222222222"
}
```

PutDeliveryChannel

Following is an example CloudTrail log file for the [PutDeliveryChannel](#) action.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:33:08Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "PutDeliveryChannel",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": {
    "deliveryChannel": {
      "name": "default",
      "s3BucketName": "config-api-test-pdx",
      "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
    }
  },
  "responseElements": null,
  "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```

StartConfigurationRecorder

Following is an example CloudTrail log file for the [StartConfigurationRecorder](#) action.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:35:34Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "StartConfigurationRecorder",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": {
    "configurationRecorderName": "default"
  },
  "responseElements": null,
  "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```

StopConfigurationRecorder

Following is an example CloudTrail log file for the `StopConfigurationRecorder` action.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:35:13Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "StopConfigurationRecorder",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": {
    "configurationRecorderName": "default"
  },
  "responseElements": null,
  "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```

AWS Config Resources

The following related resources can help you as you work with this service.

- [AWS Config](#) – The primary web page for information about AWS Config.
- [AWS Config Pricing](#)
- [Technical FAQ](#)
- [Partners](#) – Links to partner products that are fully integrated with AWS Config to help you visualize, monitor, and manage the data from your configuration stream, configuration snapshots, or configuration history.
- [Classes & Workshops](#) – Links to role-based and specialty courses as well as self-paced labs to help sharpen your AWS skills and gain practical experience.
- [AWS Developer Tools](#) – Links to developer tools, SDKs, IDE toolkits, and command line tools for developing and managing AWS applications.
- [AWS Whitepapers](#) – Links to a comprehensive list of technical AWS whitepapers, covering topics such as architecture, security, and economics and authored by AWS Solutions Architects or other technical experts.
- [AWS Support Center](#) – The hub for creating and managing your AWS Support cases. Also includes links to other helpful resources, such as forums, technical FAQs, service health status, and AWS Trusted Advisor.
- [AWS Support](#) – The primary web page for information about AWS Support, a one-on-one, fast-response support channel to help you build and run applications in the cloud.
- [Contact Us](#) – A central contact point for inquiries concerning AWS billing, account, events, abuse, and other issues.
- [AWS Site Terms](#) – Detailed information about our copyright and trademark; your account, license, and site access; and other topics.

AWS Software Development Kits for AWS Config

An AWS software development kit (SDK) makes it easier to build applications that access cost-effective, scalable, and reliable AWS infrastructure services. With AWS SDKs, you can get started in minutes with a single, downloadable package that includes the library, code samples, and reference documentation. The following table lists the available SDKs and third-party libraries you can use to access AWS Config programmatically.

Type of Access	Description
AWS SDKs	<p>AWS provides the following SDKs:</p> <ul style="list-style-type: none">• AWS SDK for C++ Documentation• AWS Mobile SDK for iOS Documentation• AWS SDK for Go Documentation• AWS SDK for Java Documentation• AWS SDK for JavaScript Documentation• AWS SDK for .NET Documentation• AWS SDK for PHP Documentation• AWS SDK for Python (Boto) Documentation• AWS SDK for Ruby Documentation
Third-party libraries	<p>Developers in the AWS developer community also provide their own libraries, which you can find at the following AWS developer centers:</p> <ul style="list-style-type: none">• AWS Java Developer Center• AWS JavaScript Developer Center• AWS PHP Developer Center• AWS Python Developer Center• AWS Ruby Developer Center• AWS Windows and .NET Developer Center

Document History

The following table describes the documentation release history of AWS Config.

- **API version:** 2014-11-12
- **Latest documentation update:** April 5, 2017

Feature	Description	Release Date
New and updated content	<p>This release supports an updated console experience for adding AWS Config managed rules to your account for the first time.</p> <p>When you set up AWS Config rules for the first time or in a new region, you can search for AWS managed rules by name, description, or label. You can choose Select all to select all rules or choose Clear all to clear all rules.</p> <p>For more information, see Setting Up AWS Config Rules with the Console (p. 19).</p>	April 5, 2017
AWS Config supports new managed rules	<p>This release supports the following seven new managed rules:</p> <ul style="list-style-type: none">• acm-certificate-expiration-check (p. 30)• ec2-instance-detailed-monitoring-enabled (p. 35)• ec2-managedinstance-inventory-blacklisted (p. 37)• ec2-volume-inuse-check (p. 38)• iam-user-group-membership-check (p. 40)• iam-user-no-policies-check (p. 40)• s3-bucket-ssl-requests-only (p. 45)	February 21, 2017

Feature	Description	Release Date
	For more information, see AWS Managed Config Rules (p. 29).	
New and updated content	This release adds support for AWS Config rules in the EU (London) Region. For more information, see AWS Regions and Endpoints in the <i>AWS General Reference</i> .	February 21, 2017
New and updated content	This release adds AWS CloudFormation templates for AWS Config managed rules. You can use the templates to create managed rules for your account. For more information, see Creating AWS Config Managed rules with AWS CloudFormation templates (p. 47).	February 16, 2017
New and updated content	This release adds support for a new test mode for the <code>PutEvaluations</code> API. Set the <code>TestMode</code> parameter to true in your custom rule to verify whether your AWS Lambda function will deliver evaluation results to AWS Config. No updates occur to your existing evaluations, and evaluation results are not sent to AWS Config. For more information, see PutEvaluations in the <i>AWS Config API Reference</i> .	February 16, 2017
New and updated content	This release adds support for AWS Config rules in the Asia Pacific (Seoul), and US West (N. California) Regions. For more information, see AWS Regions and Endpoints in the <i>AWS General Reference</i> .	December 21, 2016
New and updated content	This release adds support for AWS Config in the EU (London) Region. For more information, see AWS Regions and Endpoints in the <i>AWS General Reference</i> .	December 13, 2016
New and updated content	This release adds support for AWS Config in the Canada (Central) Region. For more information, see AWS Regions and Endpoints in the <i>AWS General Reference</i> .	December 8, 2016

Feature	Description	Release Date
AWS Config supports Amazon Redshift resource types and two new managed rules	<p>With this release, you can use AWS Config to record configuration changes to your Amazon Redshift clusters, cluster parameter groups, cluster security groups, cluster snapshots, cluster subnet groups, and event subscriptions.</p> <p>For more information, see Supported Resources, Configuration Items, and Relationships (p. 6).</p> <p>This release supports two new managed rules:</p> <ul style="list-style-type: none">• redshift-cluster-configuration-check• redshift-cluster-maintenancesettings-check <p>For more information, see AWS Managed Config Rules (p. 29).</p>	December 7, 2016
New and updated content	<p>This release adds support for a new managed rule:</p> <ul style="list-style-type: none">• dynamodb-throughput-limit-check <p>For more information, see AWS Managed Config Rules (p. 29).</p>	December 7, 2016
New and updated content	<p>This release adds support for creating up to 50 rules per region in an account. For more information, see AWS Config Limits in the <i>AWS General Reference</i>.</p>	December 7, 2016

Feature	Description	Release Date
AWS Config supports the managed instance inventory resource type for Amazon EC2 Systems Manager and three new managed rules	<p>With this release, you can use AWS Config to record software configuration changes on your managed instances with support for managed instance inventory. For more information, see Recording software configuration for managed instances (p. 8).</p> <p>This release supports three new managed rules:</p> <ul style="list-style-type: none">• ec2-managedinstance-inventory-blacklisted• ec2-managedinstance-applications-required• ec2-managedinstance-platform-check <p>For more information, see AWS Managed Config Rules (p. 29).</p>	December 1, 2016
AWS Config supports the Amazon S3 bucket resource and two new managed rules	<p>With this release, you can use AWS Config to record configuration changes to your Amazon S3 buckets. For more information, see Supported Resources, Configuration Items, and Relationships (p. 6).</p> <p>This release supports two new managed rules:</p> <ul style="list-style-type: none">• s3-bucket-logging-enabled• s3-bucket-versioning-enabled <p>For more information, see About AWS Managed Config Rules (p. 28).</p>	October 18, 2016
New and updated content	<p>This release adds support for AWS Config and AWS Config rules in the US East (Ohio) Region. For more information, see AWS Regions and Endpoints in the <i>AWS General Reference</i>.</p>	October 17, 2016

Feature	Description	Release Date
New and updated managed rules	<p>This update adds support for eight new managed rules:</p> <ul style="list-style-type: none">• approved-amis-by-id• approved-amis-by-tag• db-instance-backup-enabled• desired-instance-type• ebs-optimized-instance• iam-password-policy• rds-multi-az-support• rds-storage-encrypted <p>You can specify multiple parameter values for the desired-instance-tenancy and required-tags rules.</p> <p>For more information, see AWS Managed Config Rules (p. 29).</p>	October 4, 2016
New and updated content for the AWS Config console	<p>This update adds support for viewing AWS CloudTrail API activity in the AWS Config timeline. If CloudTrail is logging for your account, you can view create, update, and delete API events for configuration changes to your resources. For more information, see Viewing Configuration Details in the AWS Config Console (p. 73).</p>	September 06, 2016
AWS Config supports Elastic Load Balancing resource type	<p>With this release, you can use AWS Config to record configuration changes to your Elastic Load Balancing application load balancers. For more information, see Supported Resources, Configuration Items, and Relationships (p. 6).</p>	August 31, 2016
New and updated content	<p>This release adds support for AWS Config rules in the Asia Pacific (Singapore), and Asia Pacific (Sydney) Regions. For more information, see AWS Regions and Endpoints in the <i>AWS General Reference</i>.</p>	August 18, 2016

Feature	Description	Release Date
New and updated content for AWS Config rules	<p>This update adds support for creating a rule that can be triggered by both configuration changes and at a periodic frequency that you choose. For more information, see Specifying Triggers for AWS Config Rules (p. 27).</p> <p>This update also adds support for manually evaluating your resources against your rule and deleting evaluation results. For more information, see Manually Evaluate your Resources (p. 68).</p> <p>This update also adds support for evaluating additional resource types using custom rules. For more information, see Evaluating Additional Resource Types (p. 53).</p>	July 25, 2016
AWS Config supports Amazon RDS and AWS Certificate Manager (ACM) resource types	With this release, you can use AWS Config to record configuration changes to your Amazon Relational Database Service (Amazon RDS) DB instances, DB security groups, DB snapshots, DB subnet groups, and event subscriptions. You can also use AWS Config to record configuration changes to certificates provided by ACM. For more information, see Supported Resources, Configuration Items, and Relationships (p. 6).	July 21, 2016
Updated information about managing the configuration recorder	This update adds steps for renaming and deleting the configuration recorder to Managing the Configuration Recorder (p. 107).	July 07, 2016
Simplified role creation and updated policies	With this update, creating an IAM role for AWS Config is simplified. This enhancement is available in regions that support Config rules. To support this enhancement, the steps in Setting up AWS Config with the Console (p. 17) are updated, the example policy in Permissions for the Amazon S3 Bucket (p. 116) is updated, and the example policy in Permissions for Accessing AWS Config (p. 118) is updated.	March 31, 2016

Feature	Description	Release Date
Example functions and events for Config rules	This update provides updated example functions in Example AWS Lambda Functions for AWS Config Rules (Node.js) (p. 54), and this update adds example events in Example Events for AWS Config Rules (p. 59).	March 29, 2016
AWS Config Rules GitHub repository	This update adds information about the AWS Config Rules GitHub repository to Evaluating Resources With AWS Config Rules (p. 26). This repository provides sample functions for custom rules that are developed and contributed by AWS Config users.	March 1, 2016
AWS Config rules	This release introduces AWS Config rules. With rules, you can use AWS Config to evaluate whether your AWS resources comply with your desired configurations. For more information, see Evaluating Resources With AWS Config Rules (p. 26).	December 18, 2015
AWS Config supports IAM resource types	With this release, you can use AWS Config to record configuration changes to your IAM users, groups, roles, and customer managed policies. For more information, see Supported Resources, Configuration Items, and Relationships (p. 6).	December 10, 2015
AWS Config supports EC2 Dedicated host	With this release, you can use AWS Config to record configuration changes to your EC2 Dedicated hosts. For more information, see Supported Resources, Configuration Items, and Relationships (p. 6).	November 23, 2015
Updated permissions information	This update adds information about the following AWS managed policies for AWS Config: <ul style="list-style-type: none"> <code>AWSConfigRole</code> – Grants AWS Config permission to get configuration details about your resources. For more information, see IAM Role Policy for Getting Configuration Details (p. 115). <code>AWSConfigUserAccess</code> – Grants read-only access to an AWS Config user. For more information, see Permissions for Accessing AWS Config (p. 118). 	October 19, 2015

Feature	Description	Release Date
AWS Config rules preview	This release introduces the AWS Config rules preview. With rules, you can use AWS Config to evaluate whether your AWS resources comply with your desired configurations. For more information, see Evaluating Resources With AWS Config Rules (p. 26).	October 7, 2015
New and updated content	This release adds the ability to look up resources that AWS Config has discovered. For more information, see Looking Up Resources That Are Discovered by AWS Config (p. 71).	August 27, 2015
New and updated content	This release adds the ability to select which resource types AWS Config records. For more information, see Selecting Which Resources AWS Config Records (p. 109).	June 23, 2015
New and updated content	This release adds support for the following regions: Asia Pacific (Tokyo), Asia Pacific (Singapore), EU (Frankfurt), South America (São Paulo), and US West (N. California). For more information, see AWS Regions and Endpoints .	April 6, 2015
New and updated content	This release adds support for creating an optional email subscription to your Amazon SNS topic. You can also use email filters to monitor specific resource changes. For more information, see Monitoring AWS Config Resource Changes by Email (p. 84).	March 27, 2015
New and updated content	<p>This release supports integration with AWS CloudTrail for logging all AWS Config API activity. For more information, see Logging AWS Config API Calls with AWS CloudTrail (p. 122).</p> <p>This release adds support for the US West (Oregon), EU (Ireland), and Asia Pacific (Sydney) regions.</p> <p>This release also includes the following updates to the documentation:</p> <ul style="list-style-type: none"> • Information about monitoring AWS Config configurations • Various corrections throughout the document 	February 10, 2015
New guide	This release introduces AWS Config.	November 12, 2014

AWS Glossary

For the latest AWS terminology, see the [AWS Glossary](#) in the *AWS General Reference*.