AWS Config

Understanding the basic components of AWS Config will help you track resource inventory and changes and evaluate configurations of your AWS resources.

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 Resource Types.

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.

For more information, see Viewing AWS Resource Configurations and History and Managing AWS Resource Configurations and History.

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 more information, see Components of a Configuration Item.

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.

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.

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 Types.

AWS Config Rules

An AWS Config rule represents your desired configuration settings for specific AWS resources or for an entire AWS account. If a resource does not pass a rule check, AWS Config flags the resource and the rule as *noncompliant*, and AWS Config notifies you through Amazon SNS. The following are the possible evaluation results for an AWS Config rule:

- `COMPLIANT` - the rule passes the conditions of the compliance check.
- `NON_COMPLIANT` - the rule fails the conditions of the compliance check.
- `ERROR` - the one of the required/optional parameters is not valid, not of the correct type, or is formatted incorrectly.
- `NOT_APPLICABLE` - used to filter out resources that the logic of the rule cannot be applied to. For example, the alb-desync-mode-check rule only checks Application Load Balancers, and ignores Network Load Balancers and Gateway Load Balancers.

There are two types of rules: AWS Config Managed Rules and AWS Config Custom Rules. For more information about the structure of rule definitions and rule metadata, see Components of an AWS Config Rule.

AWS Config Managed Rules

AWS Config Managed Rules are predefined, customizable rules created by AWS Config. For a list of managed rules, see List of AWS Config Managed Rules.

AWS Config Custom Rules

AWS Config Custom Rules are rules that you create from scratch. There are two ways to create AWS Config custom rules: with Lambda functions (AWS Lambda Developer Guide) and with Guard (Guard GitHub Repository), a policy-as-code language. AWS Config custom rules created

with AWS Lambda are called *AWS Config Custom Lambda Rules* and AWS Config custom rules created with Guard are called *AWS Config Custom Policy Rules*.

For a walkthrough showing how to create AWS Config Custom Policy Rules, see Creating AWS Config Custom Policy Rules. For a walkthrough showing how to create AWS Config Custom Lambda Rules, see Creating AWS Config Custom Lambda Rules.

Trigger Types

After you add a rule to your account, 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 runs evaluations for the rule when there is a resource that matches the rule's scope and there is a change in configuration of the resource. The evaluation runs after AWS Config sends a configuration item change notification.

You choose which resources initiate 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 define which resources initiate evaluations.

Periodic

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

Hybrid

Some rules have both configuration change and periodic triggers. For these rules, AWS Config evaluates your resources when it detects a configuration change and also at the frequency that you specify.

Evaluation modes

There are two evaluation modes for AWS Config rules:

Proactive

Use proactive evaluation to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an AWS resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

For more information, see Evaluation modes. For a list of managed rules that support proactive evaluation, see List of AWS Config Managed Rules by Evaluation Mode.

Note

Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

Detective

> Use detective evaluation to evaluate resources that have already been deployed. This allows you to evaluate the configuration settings of your existing resources.

Conformance Packs

A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations.

Conformance packs are created by authoring a YAML template that contains the list of AWS Config managed or custom rules and remediation actions. You can deploy the template by using the AWS Config console or the AWS CLI.

To quickly get started and to evaluate your AWS environment, use one of the sample conformance pack templates. You can also create a conformance pack YAML file from scratch based on Custom Conformance Pack. A custom conformance pack is a unique collection of AWS Config rules and remediation actions that you can deploy together in an account and an AWS Region, or across an organization in AWS Organizations.

Process checks is a type of AWS Config rule that allows you to track your external and internal tasks that require verification as part of the conformance packs. These checks can be added to an existing conformance pack or a new conformance pack. You can track all compliance that includes AWS Configurations and manual checks in a single location.

Multi-Account Multi-Region Data Aggregation

Multi-account multi-region data aggregation in AWS Config allows you to aggregate AWS Config configuration and compliance data from multiple accounts and regions into a single account. Multi-account multi-region data aggregation is useful for central IT administrators to monitor compliance for multiple AWS accounts in the enterprise.

Source Account

A source account is the AWS account from which you want to aggregate AWS Config resource configuration and compliance data. A source account can be an individual account or an organization in AWS Organizations. You can provide source accounts individually or you can retrieve them through AWS Organizations.

Source Region

A source region is the AWS Region from which you want to aggregate AWS Config configuration and compliance data.

Aggregator

An aggregator is a new resource type in AWS Config that collects AWS Config configuration and compliance data from multiple source accounts and regions. Create an aggregator in the region where you want to see the aggregated AWS Config configuration and compliance data.

Note

Aggregators provide a *read-only view* into the source accounts and regions that the aggregator is authorized to view. Aggregators do not provide mutating access into the source account or region. For example, this means that you cannot deploy rules through an aggregator or pull snapshot files from the source account or region through an aggregator.

Aggregator Account

An aggregator account is an account where you create an aggregator.

Authorization

As a source account owner, authorization refers to the permissions you grant to an aggregator account and region to collect your AWS Config configuration and compliance data.
Authorization is not required if you are aggregating source accounts that are part of AWS Organizations.

For more information, see topics in Multi-Account Multi-Region Data Aggregation section.

Managing AWS Config

AWS Config Console

You can manage the service using the AWS Config console. The console provides a user interface for performing many AWS Config tasks such as:

- Specifying the types of AWS resources for recording.
- Configuring resources to record, including:
    - Selecting an Amazon S3 bucket.

    - Selecting an Amazon SNS topic.
    - Creating AWS Config role.
- Creating managed rules and custom rules that represent desired configuration settings for specific AWS resources or for an entire AWS account.
- Creating and managing configuration aggregators to aggregate data across multiple accounts and regions.
- Viewing a snapshot of current configurations of the supported resources.
- Viewing relationships between AWS resources.

For more information about the AWS Management Console, see AWS Management Console.

AWS Config CLI

The AWS Command Line Interface is a unified tool that you can use to interact with AWS Config from the command line.

AWS Config APIs

In addition to the console and the CLI, you can also use the AWS Config RESTful APIs to program AWS Config directly.

AWS SDKs

As an alternative to using the AWS Config API, you can use one of the AWS SDKs. Each SDK consists of libraries and sample code for various programming languages and platforms. The SDKs provide a convenient way to create programmatic access to AWS Config. For example, you can use the SDKs to sign requests cryptographically, manage errors, and retry requests automatically. For more information, see the Tools for Amazon Web Services page.

Control Access to AWS Config

AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions.

To provide access, add permissions to your users, groups, or roles:

- Users and groups in AWS IAM Identity Center (successor to AWS Single Sign-On):
  Create a permission set. Follow the instructions in Create a permission set in the *AWS IAM Identity Center (successor to AWS Single Sign-On) User Guide*.
- Users managed in IAM through an identity provider:
  Create a role for identity federation. Follow the instructions in Creating a role for a third-party identity provider (federation) in the *IAM User Guide*.
- IAM users:
  - Create a role that your user can assume. Follow the instructions in Creating a role for an IAM user in the *IAM User Guide*.
  - (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in Adding permissions to a user (console) in the *IAM User Guide*.