What Is AWS Config?

PDF | RSS

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 a complete list of AWS resources supported by AWS Config, see Supported Resource Types.

Considerations

- **AWS account**: You need an active AWS account. For more information, see Signing up for AWS.
- **Amazon S3 Bucket**: You need to an S3 bucket to receive data for your configuration snapshots and history. For more information, see Permissions for the Amazon S3 Bucket.
- **Amazon SNS Topic**: You need an Amazon SNS to receive notifications when there are changes to your configuration snapshots and history. For more information, see Permissions for the Amazon SNS Topic.
- **IAM Role**: You need an IAM role that has the necessary permissions to access AWS Config. For more information, see Permissions for the IAM Role.

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 quickly determine the last known good configuration of a problem resource.

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 a 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.

Partner Solutions

AWS partners with third-party specialists in logging and analysis to provide solutions that use AWS Config output. For more information, visit the AWS Config detail page at AWS Config.

Features

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

Resource management

- Specify the resource types you want AWS Config to record.
- Set up an Amazon S3 bucket to receive a configuration snapshot on request and configuration history.
- Set up Amazon SNS to send configuration stream notifications.
- Grant AWS Config the permissions it
For more information, see Viewing AWS Resource Configurations and
Rules and conformance packs

- Use conformance packs, or a collection of rules that can be deployed and monitored as a single entity in your AWS account.

  For more information, see Evaluating Resources with AWS Config Rules and Conformance Packs.

Remediation

- Remediate noncompliant resources that are evaluated by AWS Config Rules.

  For more information, see Remediation.

Aggregators

- Use an aggregator to get a centralized view of your resource inventory and compliance. An aggregator collects AWS Config configuration and compliance data from multiple AWS accounts and AWS Regions into a single account and Region.

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

Advanced queries

- Use one of the sample queries or write your own query by referring to the configuration schema of the AWS resource.

  For more information, see Querying the Current Configuration State of AWS Resources .

Did this page help you?

Yes

No

Provide feedback

Next topic: How AWS Config Works

Need help?

- Try AWS re:Post
- Connect