AWS Config

is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.

With AWS Config you can discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time.

These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

Allow you to assess, audit and evaluate configurations of your AWS resources.

Very useful for Configuration Management as part of an ITIL program.

Creates a baseline of various configuration settings and files and can then track variations against that baseline.

## **AWS Config vs CloudTrail**

[**AWS CloudTrail**](https://digitalcloud.training/aws-cloudtrail/) records user API activity on your account and allows you to access information about this activity.

AWS Config records point-in-time configuration details for your AWS resources as Configuration Items (CIs).

You can use an AWS Config CI to answer, “What did my AWS resource look like?” at a point in time.

You can use AWS CloudTrail to answer, “Who made an API call to modify this resource?”.

## **AWS Config Rules**

A Config Rule represents desired configurations for a resource and is evaluated against configuration changes on the relevant resources, as recorded by AWS Config.

[**AWS Config Rules**](https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html) can check resources for certain desired conditions and if violations are found the resources are flagged as “noncompliant”.

Examples of Config Rules:

* Is backup enabled on [**Amazon RDS**](https://digitalcloud.training/amazon-rds/)?
* Is CloudTrail enabled on the AWS account?
* Are [**Amazon EBS**](https://digitalcloud.training/amazon-ebs/) volumes encrypted.

## **Configuration Items**

A [**Configuration Item (CI)**](https://docs.aws.amazon.com/config/latest/developerguide/config-item-table.html) is the configuration of a resource at a given point-in-time. A CI consists of 5 sections:

1. Basic information about the resource that is common across different resource types (e.g., Amazon Resource Names, tags).
2. Configuration data specific to the resource (e.g., [**Amazon EC2**](https://digitalcloud.training/amazon-ec2/) instance type).
3. Map of relationships with other resources (e.g., EC2::Volume vol-3434df43 is “attached to instance” EC2 Instance i-3432ee3a).
4. AWS CloudTrail event IDs that are related to this state.
5. Metadata that helps you identify information about the CI, such as the version of this CI, and when this CI was captured.

## **Charges**

With AWS Config, you are charged based on the number configuration items (CIs) recorded for supported resources in your AWS account.

AWS Config creates a configuration item whenever it detects a change to a resource type that it is recording.

### **Related posts:**

* ****