

Welcome to AWS Config.

What you'll learn

At the core of the lesson

You will learn how to:

- Describe the value of AWS Config
- Highlight the features of AWS Config

2

aws re/start



This module describes AWS Config and highlights its features.

Introduction to AWS Config

AWS Config is a fully managed service that enables you to assess, audit, and evaluate the configuration of your AWS resources.

- Nearly continuous monitoring
- Nearly continuous assessment
- Change management
- Operational troubleshooting

3


aws re/start

AWS Config is a fully managed service that enables you to assess, audit, and evaluate the configuration of your AWS resources. It provides nearly continuous monitoring, nearly continuous assessment, change management, and operational troubleshooting.

AWS Config

Track changes to resources

- Provides AWS resource inventory, configuration history, and configuration change notifications.
- Provides details on all configuration changes
- Combines with AWS CloudTrail
- Enables:
 - Compliance auditing
 - Security analysis
 - Resource change tracking
 - Troubleshooting



The illustration shows a cloud icon with a magnifying glass over it, a laptop displaying a list of resources, and a document icon with a checkmark, representing the monitoring and auditing capabilities of AWS Config.

4

aws re/start

AWS Config provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.

With AWS Config, you can:

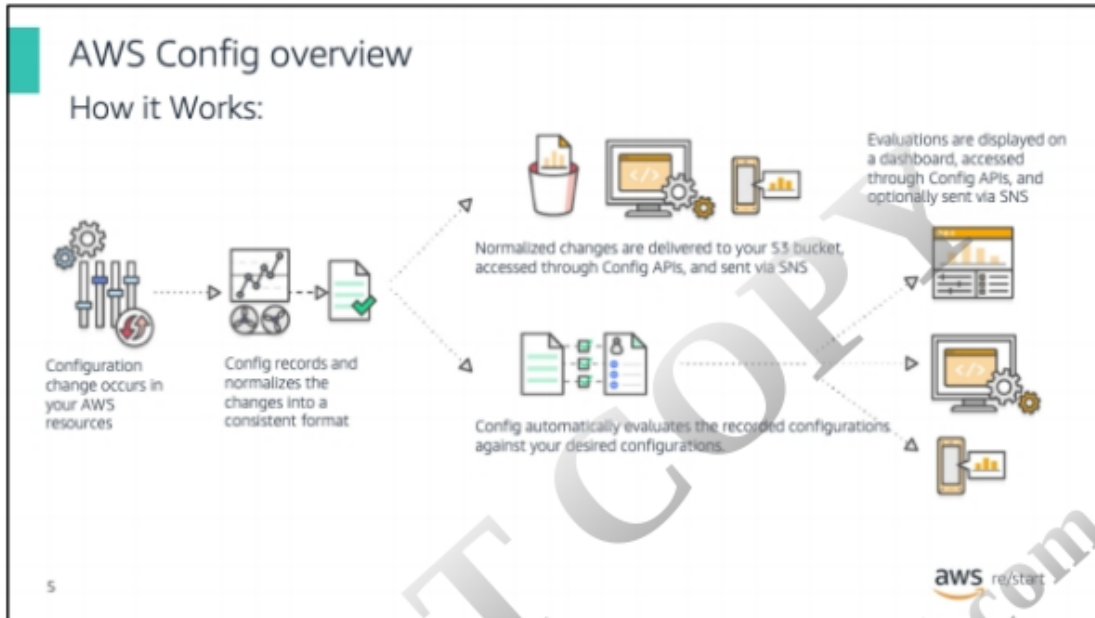
- Discover existing AWS resources
- Export a complete inventory of your AWS resources with all configuration details
- Determine how a resource was configured at any point in time

These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting. Of specific value are:

- DETECTION
 - Create detection controls and identify and analyze anomalies.
- COMPLIANCE
 - Create rules that assess resource compliance and assist with aligning with SOC certifications.
 - Review changes in configurations and relationships between

- AWS resources
- ACCESS CONTROL
 - Create IAM roles that grant AWS Config permissions to access resources like S3 buckets
 - Create service-link roles that are linked to AWS Config that include all permissions Config requires to call other services on the user's behalf.
- ENCRYPTION/DATA AT REST
 - AWS Config creates a configuration item whenever it detects a change to a resource type that it is recording. The components of a configuration item include metadata, attributes, relationships, current configuration, and related events.

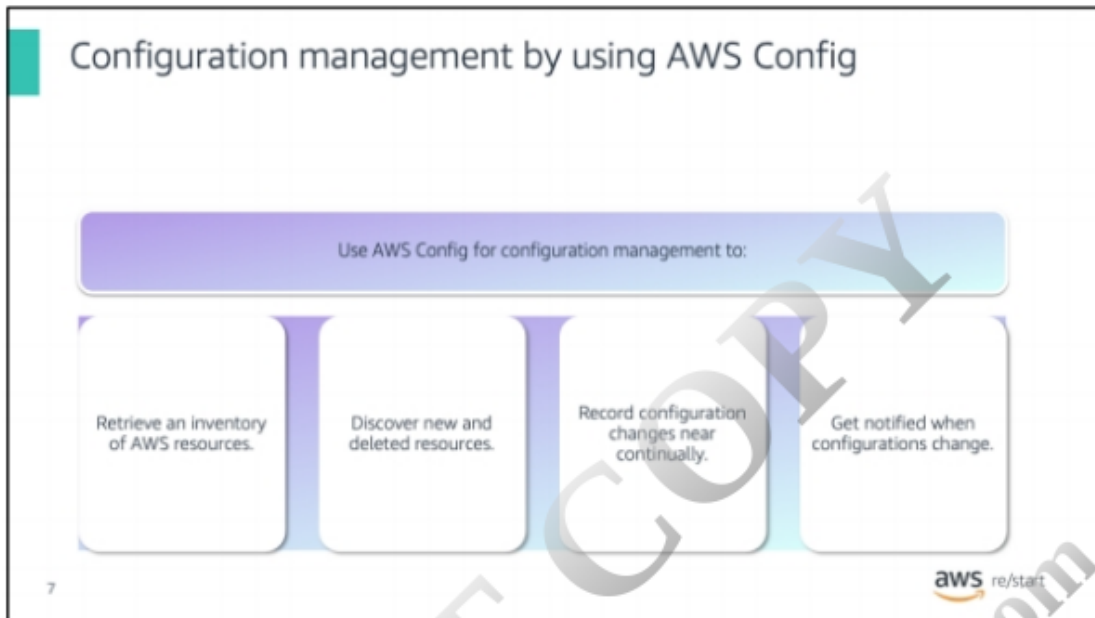
AWS Config enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.



This diagram illustrates how AWS Config works:

1. A change occurs in one of your AWS resources.
2. The AWS Config engine records and normalizes that change in a consistent format.
3. The record of the change is then delivered to an Amazon Simple Storage Service (Amazon S3) bucket, where it can be accessed through the AWS Config application programming interfaces (APIs). The change can also be sent through a notification service such as Amazon Simple Notification Service (Amazon SNS).
4. If an **AWS Config rule** was defined for the affected resource, AWS Config verifies that the change does not violate the rule. AWS Config displays the result of the evaluation on a dashboard. The result can also be sent to Amazon SNS.

You might know what the current configuration of deployed resources should be. However, do you have visibility into possible configuration errors, and do you have a system for managing and tracking configuration changes?

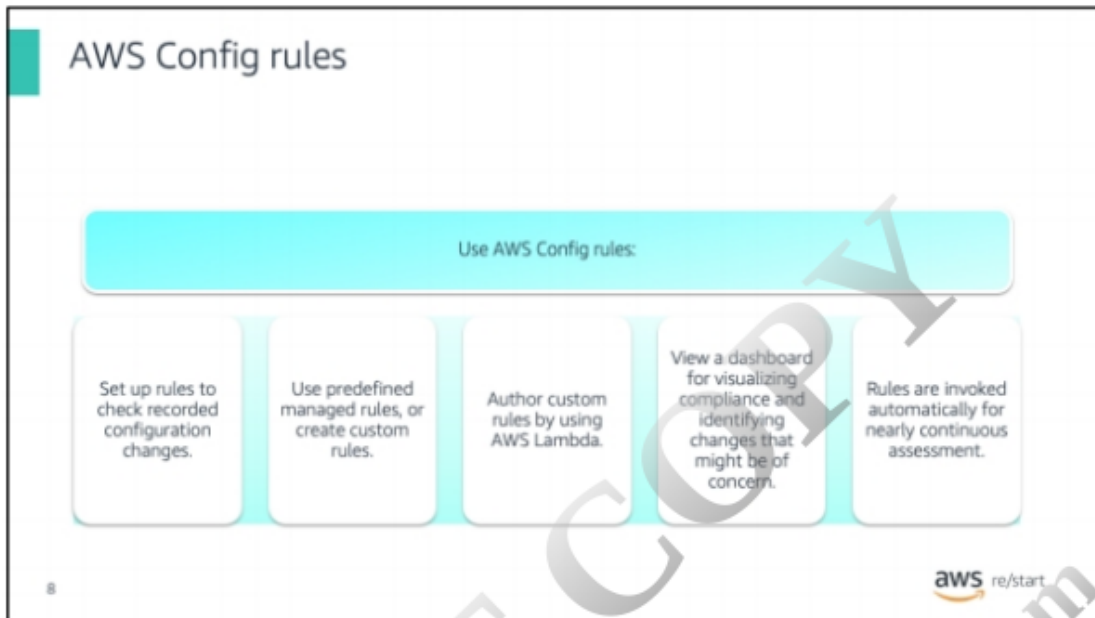


AWS Config monitors and records your AWS resource configurations near continuously. You can automate the evaluation of recorded configurations against desired configurations.

With AWS Config, you can perform the following tasks:

- Retrieve an inventory of AWS resources.
- Discover new and deleted resources.
- Record configuration changes near continually. Determine overall compliance against the configurations that are specified by your internal guidelines.
- Get notified when configurations change and analyze detailed resource configuration histories.

All these features enable you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.



AWS Config provides a rule system. You can use existing rules from AWS and from AWS Partners. You can also define your own custom rules by using AWS Lambda. AWS Lambda is a web service that enables you to run code without provisioning or managing servers.

You can target rules at specific resources, specific types of resources, or at resources that are tagged in a particular way. Rules are run when those resources are created or changed, and they can also be evaluated on a periodic basis (hourly, daily, and so forth).

You can set up rules to verify that configuration changes are recorded. After you set up AWS Config, it provides a dashboard for visualizing compliance. You can also use the dashboard to identify changes to your resources that might be of concern.

AWS Config is invoked automatically so that configurations are being assessed near continuously.

Example: AWS Config rules

- Amazon EBS volumes are encrypted.
- Instances are using approved Amazon Machine Images (AMIs).
- Elastic IP addresses are attached to instances.
- Amazon EC2 instances are properly tagged.

9

aws re/start

Rules can look for any desirable or undesirable condition.

For example, you could define rules that ensure the following:

- Amazon Elastic Block Store (Amazon EBS) volumes are encrypted.
- Instances are being created only from approved Amazon Machine Images (AMIs).
- Elastic IP addresses are attached to instances.
- Amazon EC2 instances are being properly tagged.