AWS Config

Week 6.1

What you will Learn

- Describe the value of AWS Config.
- Highlight the features of AWS Config.
- Understand AWS Config rules.
- Differentiate different concepts associated with AWS Config.

Introduction to AWS Config

- When working with AWS, we frequently build, delete, and manage resources.
- It is very important we carefully track all of these resources.
- This helps in evaluating these configurations and changes for compliance with ideal configurations.
- AWS Config is a fully managed service that enables you to assess, audit, and evaluate the configuration of your AWS resources.
- It provides a detailed inventory of the AWS resources and their current configuration while continuously recording changes.
- It provides:
  - Nearly continuous monitoring
  - Nearly continuous assessment
  - Change management
  - Operational troubleshooting

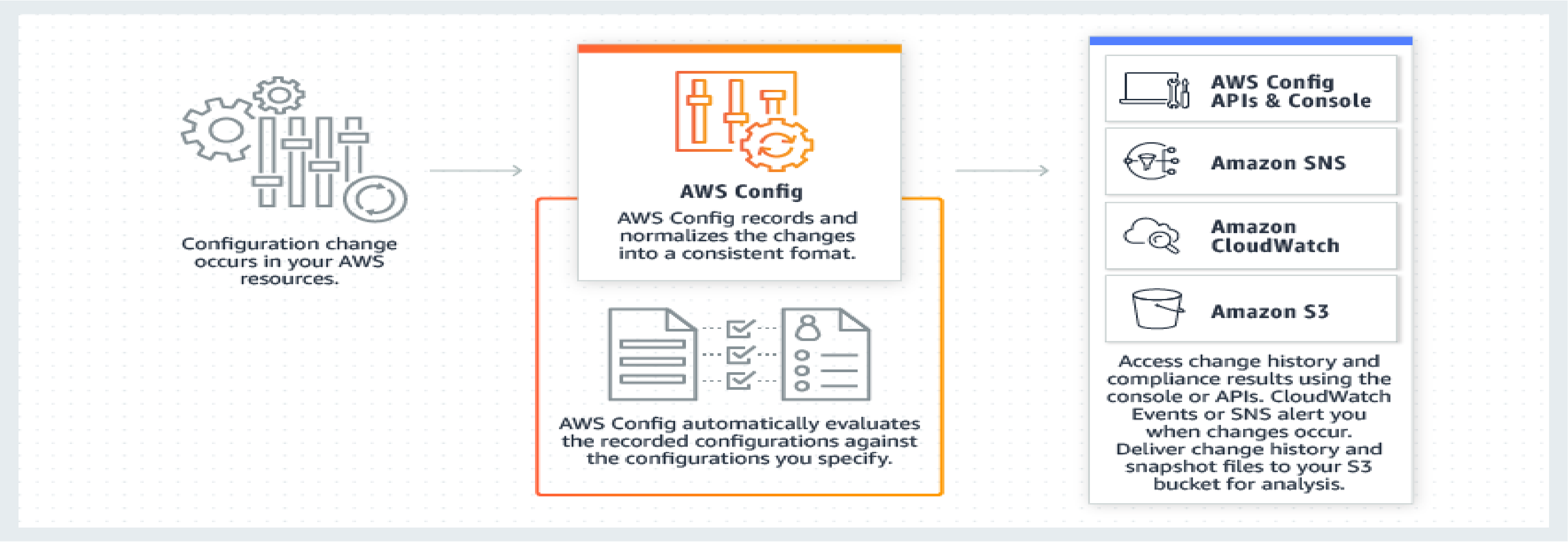
Introduction to AWS Config

- 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.

Introduction to AWS Config

- These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting. Of specific value are:
  - 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.
- For more information, check AWS Config documentation, AWS Config pricing

How AWS Config works


Configuration change occurs in your AWS resources.
AWS Config
AWS Config records and normalizes the changes into a consistent fomat.
AWS Config automatically evaluates the recorded configurations against the configurations you specify.
AWS Config APIs & Console
Amazon SNS
Amazon CloudWatch
Amazon S3
Access change history and compliance results using the console or APIs. CloudWatch Events or SNS alert you when changes occur. Deliver change history and snapshot files to your S3 bucket for analysis.

- A change occurs in one of your AWS resources.
- The AWS Config engine records and normalizes that change in a consistent format.

How AWS Config works

- 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).
- 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.

Configuration Management using AWS Config

- 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 continuously.
  - 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.

Configuration Items

- The attributes of a supported AWS resource such as metadata, attributes, relationships, current configuration, and related events at a certain point in time.
- AWS Config creates configuration items for every supported resource in the region.
- You can specify the resource types that you want it to track. For example, a security group inbound rules e.g. ssh on port 22 for the instances to access remotely.

Configuration Snapshot

- A collection of the configuration items for the supported resources, and is a very useful tool for validating the 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.
- 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

- Every time a resource is created, modified, or deleted, AWS Config creates a configuration item and adds it to the configuration stream that AWS Config is recording.
- The stream is created by using an Amazon Simple Notification Service (Amazon SNS) topic.
- It helps observe configuration changes as they occur so that you can spot potential problems in real-time.
- It generates notifications when specific resources are changed, and Configuration Stream will notify the owner.

Configuration History

- This is a collection of the configuration items for a given resource over any period, such as when an instance is created, modified or deleted.
- Configuration History logs the trail of actions taken on configuration items.
- AWS Config automatically delivers a configuration history file for each resource type that is being recorded to an Amazon S3 bucket that you specify.

Configuration Recorder

- Records and stores the configurations of all supported resources in the region where AWS Config is running.
- Users must first create and start the configuration recorder before recording begins.

AWS Config Rules

- An AWS Config rule represents customizable, predefined rules, and configuration settings for specific AWS resources (or for an entire AWS account).
- You can also define your own custom rules by using AWS Lambda - which is a web service that enables you to run code without provisioning or managing servers.
- AWS Config flags non-compliance and notifies owners when a resource change deviates from the defined rule.
- 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 periodically (hourly, daily, and so forth)

AWS Config Rules

- When users set AWS Config rules, AWS Config evaluates the resources periodically, or in response to configuration changes.
- Each rule is associated with an AWS Lambda function that contains the evaluation logic for the rule.
- When AWS Config evaluates the supported 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 NON-COMPLIANT.
- When the compliance status of the resource changes, AWS Config sends a notification to the owner’s Amazon SNS topic.
- 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 Rules

- You can 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.
  - Resources are properly tagged.
  - S3 Bucket is private

Key Takeaways

- By using AWS Config, you can track resource configuration changes and answer questions about them, demonstrate compliance, and detect and troubleshoot security vulnerabilities.
- You can define AWS Config rules to implement best practices for configuring resources and enforcing security and governance policies.
- AWS Config also enables you to receive a notification whenever a resource is created, modified, or deleted, and view relationships between resources.