AWS Config

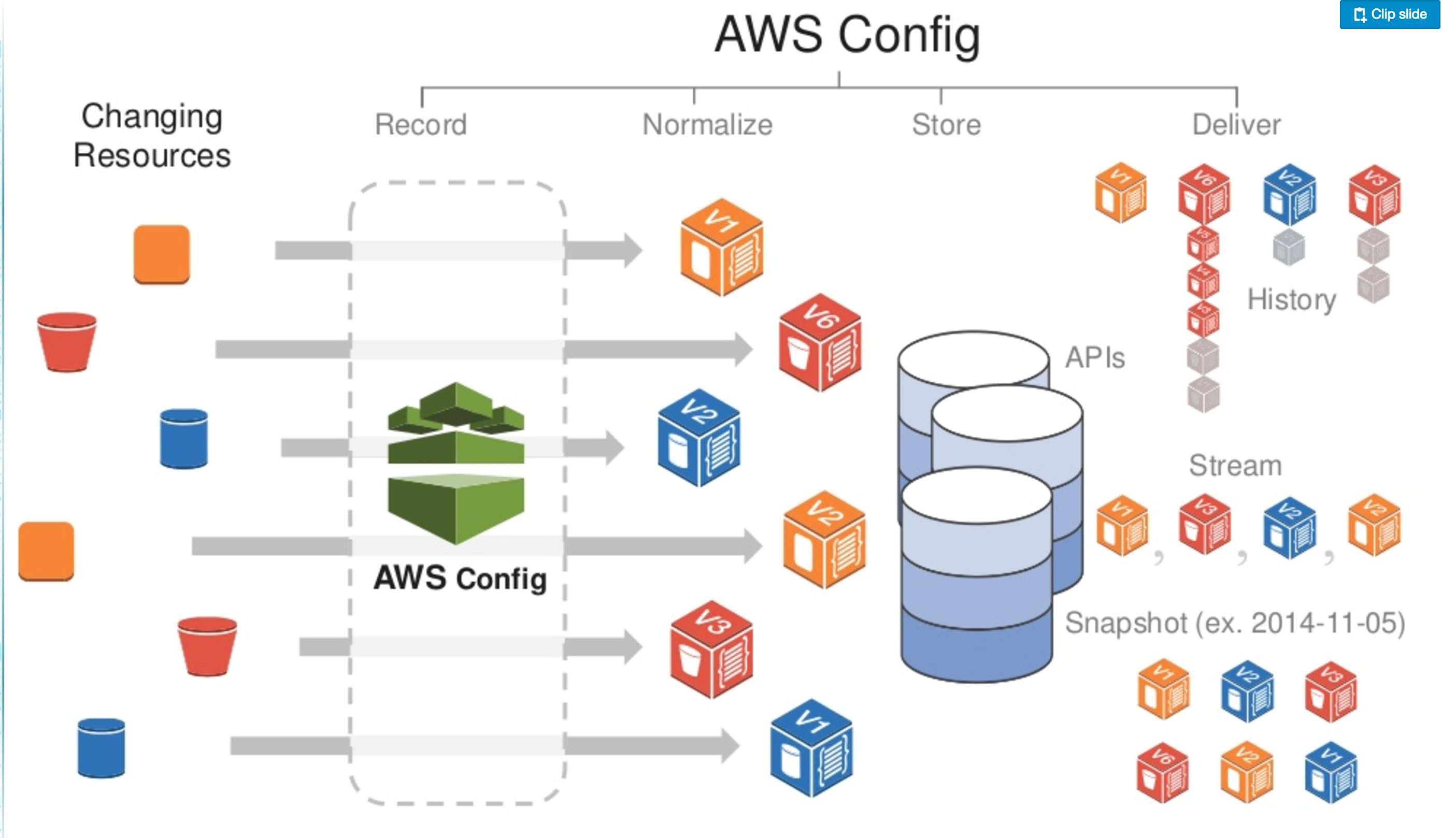
# AWS Config

* AWS Config is a fully managed service that provides AWS resource inventory, configuration history, and configuration change notifications to enable security and governance
* It provides a detailed view of the configuration of AWS resources in the AWS account.
* It gives point-in-time and historical states and allows user to see changes visually in a timeline
* In cases where several configuration changes are made to a resource in quick succession (i.e., within a span of few minutes), AWS Config will only record the latest configuration of that resource; this represents the cumulative impact of that entire set of changes
* AWS Config does not cover all the AWS services and for the services unsupported the configuration management process can be automated using API and code and used to compare current and past data

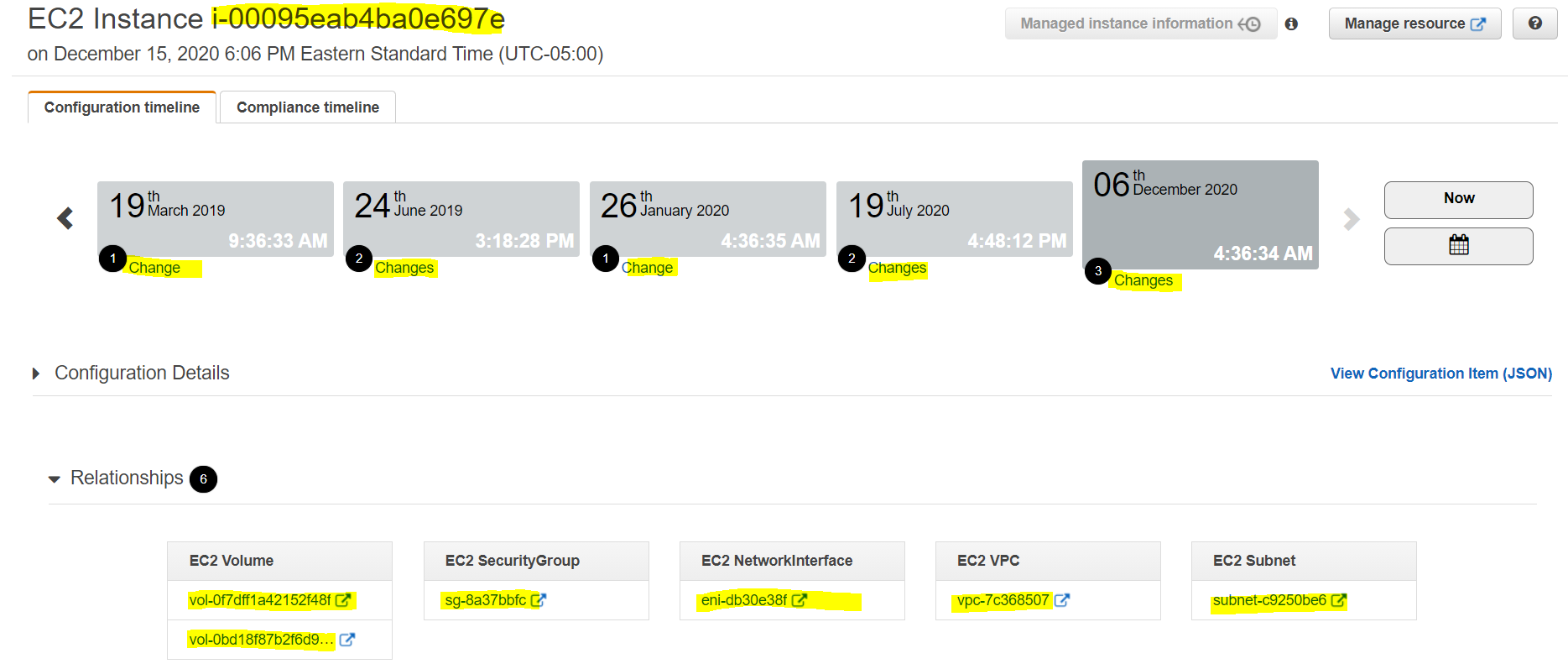
## AWS Config Use Case

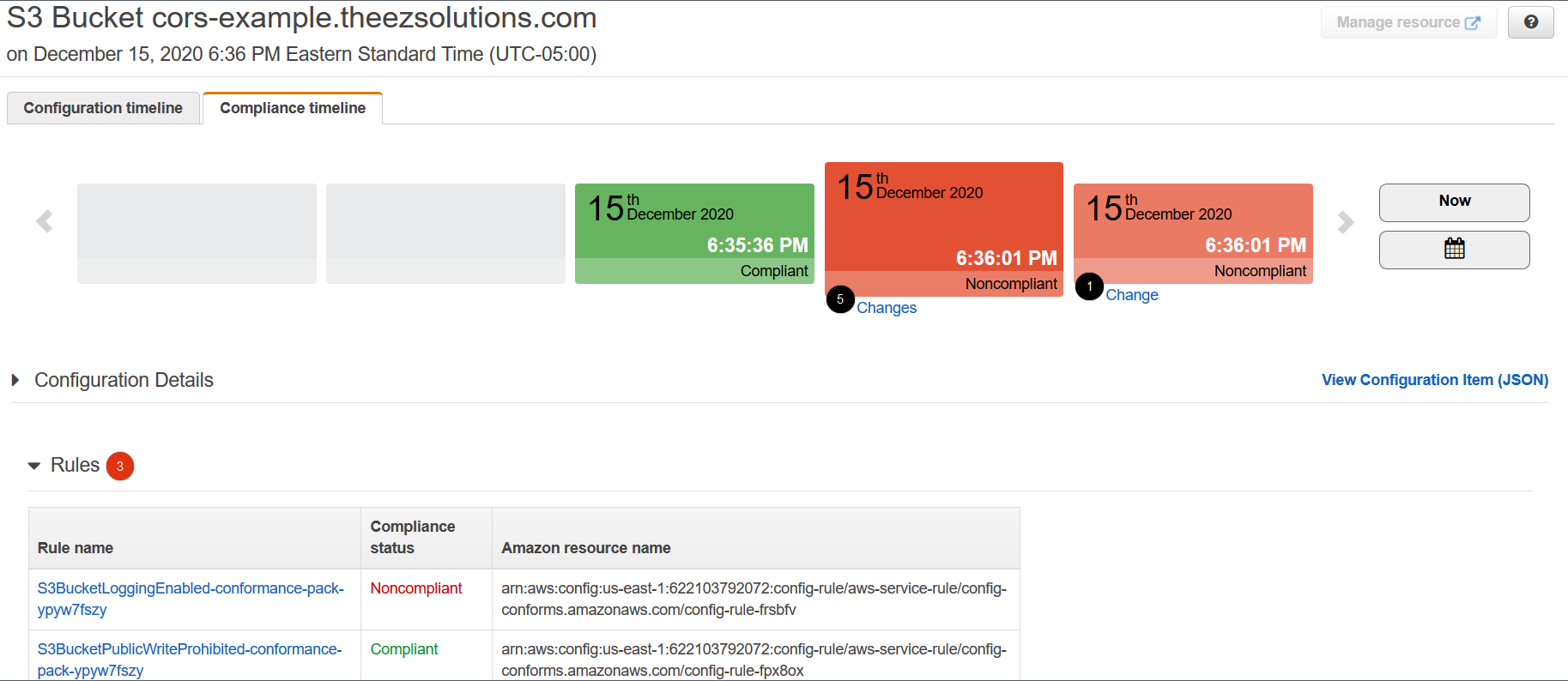
* **Security Analysis & Resource Administration**
  + AWS Config enables continuous monitoring and governance over resource configurations and help evaluate them for any misconfigurations leading to security gaps or weakness
* **Auditing & Compliance**
  + AWS Config help maintain a complete inventory of all resources and their configurations attributes as well as point in time history
  + Ability to retrieve historical configurations can be very useful to ensure compliance with internal policies and best practices and for audits
* **Change Management**
  + AWS Config helps understand relationships between resources so that the impact of the change can be proactively assessed
  + It can be configured to notify whenever resources are created, modified, or deleted without having to monitor these changes by polling the calls made to each resource
* **Troubleshooting**
  + AWS Config can help quickly identify and troubleshoot issues, by being able to use the historical configurations and compare the last working configuration to the one recent changed causing issues
* **Discovery**
  + AWS Config help discover resources that exist within an account leading to better inventory and asset management
  + Get a snapshot of the current configurations of the supported resources that are associated with the AWS account

## AWS Config Concepts



* AWS Resources
  + AWS Resources are entities created and managed for e.g. EC2 instances, Security groups
* AWS Config Rules
  + AWS Config Rules helps define desired configuration settings for the resources or for the entire account
  + AWS Config continuously tracks the resource configuration changes against the rules and if violated marks the resource as noncompliant
* Resource Relationship
  + AWS Config discovers AWS resources in the account and then creates a map of relationships between AWS resources for e.g. EBS volume linked to an EC2 instance
* Configuration Items
  + A configuration item represents a point-in-time view of the supported AWS resource
  + Components of a configuration item include metadata, attributes, relationships, current configuration, and related events.
* Configuration Snapshot
  + A configuration snapshot is a collection of the configuration items for the supported resources that exist in your account
* Configuration History
  + A configuration history is a collection of the configuration items for a given resource over any time period
* Configuration Stream
  + Configuration stream is an automatically updated list of all configuration items for the resources that AWS Config is recording
* Configuration Recorder
  + Configuration recorder stores the configurations of the supported resources in your account as configuration items
  + A configuration recorder needs to created and started for recording and by default records all supported services in the region





## AWS Config Flow

* When AWS Config is turned on, it first discovers the supported AWS resources that exist in the account and generates a configuration item for each resource.
* AWS Config also generates configuration items when the configuration of a resource changes, and it maintains historical records of the configuration items of the resources from the time the configuration recorder is started.
* By default, AWS Config creates configuration items for every supported resource in the region, but can be customized to limited resource types.
* AWS Config keeps track of all changes to the resources by invoking the Describe or the List API call for each resource as well as related resources in the account
* Configuration items are delivered in a configuration stream to a S3 bucket
* AWS Config also tracks the configuration changes that were not initiated by the API. AWS Config examines the resource configurations periodically and generates configuration items for the configurations that have changed.
* AWS Config rules, if configured,
  + are evaluated continuously for resource configurations for desired settings.
  + Depending on the rule, resources are evaluated either in response to configuration changes or periodically.
  + When AWS Config evaluates the resources, it invokes the rule’s AWS Lambda function, which contains the evaluation logic for the rule.
  + Function returns the compliance status of the evaluated resources.
  + If a resource violates the conditions of a rule, the resource and the rule are flagged as noncompliant and a notification sent to SNS topic

## AWS Config vs CloudTrail

* AWS Config reports on **WHAT** has changed, whereas CloudTrail reports on **WHO** made the change, **WHEN**, and from **WHICH** location.
* AWS Config focuses on the configuration of the AWS resources and reports with detailed snapshots on **HOW** the resources have changed, whereas CloudTrail focuses on the events, or API calls, that drive those changes. It focuses on the user, application, and activity performed on the system.

## AWS Certification Exam Practice Questions

1. One of the challenges in managing AWS resources is to keep track of changes in the resource configuration over time. Which one of the following statements provide the best solution?
   1. Use strict syntax tagging on the resources
   2. Create a custom application to automate the configuration management process
   3. **Use AWS Config for supported services and use an automated process via APIs for unsupported services**
   4. Use resource groups and tagging along with CloudTrail so that you can audit changes using the logs
2. Fill the blanks: \_\_\_\_ helps us track AWS API calls and transitions, \_\_\_\_ helps to understand what resources we have now, and \_\_\_\_ allows auditing credentials and logins.
   1. AWS Config, CloudTrail, IAM Credential Reports
   2. CloudTrail, IAM Credential Reports, AWS Config
   3. **CloudTrail, AWS Config, IAM Credential Reports**
   4. AWS Config, IAM Credential Reports, CloudTrail