1. Overview

1. AWS Config as is **Compliance-as-Code** framework that allows us to manage change in your AWS accounts on a **per region basis**

2. AWS Config use cases:

    1. Inventory of your AWS resources.
    2. Audit Aws Resource change history
    3. Notifies when a resource gets changed.
    4. Auditing Compliances (NOTE: **Automatic Compliance Remediation** is done by AWS Cloud Trail)
    5. Have your own rule or AWS provided rules and tigger based on them
    6. Helps to find the relationship with other AWS resources based on a Tag

3. It's **NOT** Enabled by Default. You need to enable it per region based on your need

4. AWS Config can measure for configuration drift and alert you to changes.

5. However, **it can't prevent changes, nor can it change settings back**.

6. You can Turn it on for free per region and it will "**discover**" resources within the region and it will create a **Resource Inventory**.

7. Config Rules: You can use Config rules to audit your use of AWS resources for compliance with external compliance frameworks

    1. AWS Managed Rules - You can use AWS managed config rules (over 75)
    2. Custom Rules - Can make custom config rules (must be defined in AWS lambda)

8. A Config Rule is triggered when there is a **configuration change** or **periodic**

    1. Configuration Change: Evaluates when a resource is **created or updated or modified**
    2. Periodic Change: Evaluates on a defined interval. (at regular time interval 1hr , 3hr, 6hr, 12hr, 24hr)

       Pricing:

       No Free tier

       $2 USD per active rule per region per month (less after 10 rules)

9. AWS Config Triggered Rules:

    1. **Change-Triggered Rule:** A change-triggered rule is executed when AWS Config records a configuration changes for any of the resources specified

2. **Periodic Rule:** This rule triggered at a specific frequency. Available frequencies are **1hr, 3hr, 6hr, or 24 hr**

3. **Configuration Recorder**: AWS Config uses Configuration Recorder to detect and change for the resources. When the Configuration recorder is stopped or deleted, the configuration trigger doesn't run while the periodic trigger continue to run at a specific period

10. Resource Timelines - When you click into a resource its possible to see a timeline of changes

You can see 2 different kind of timelines

1. Configuration Timeline: when the changes have been made to the resource
2. Compliance Timeline: When a resource has become non compliant with a rule

11. Remediation: This is the act of reversing, stopping, or correcting something. To remedy a problem.

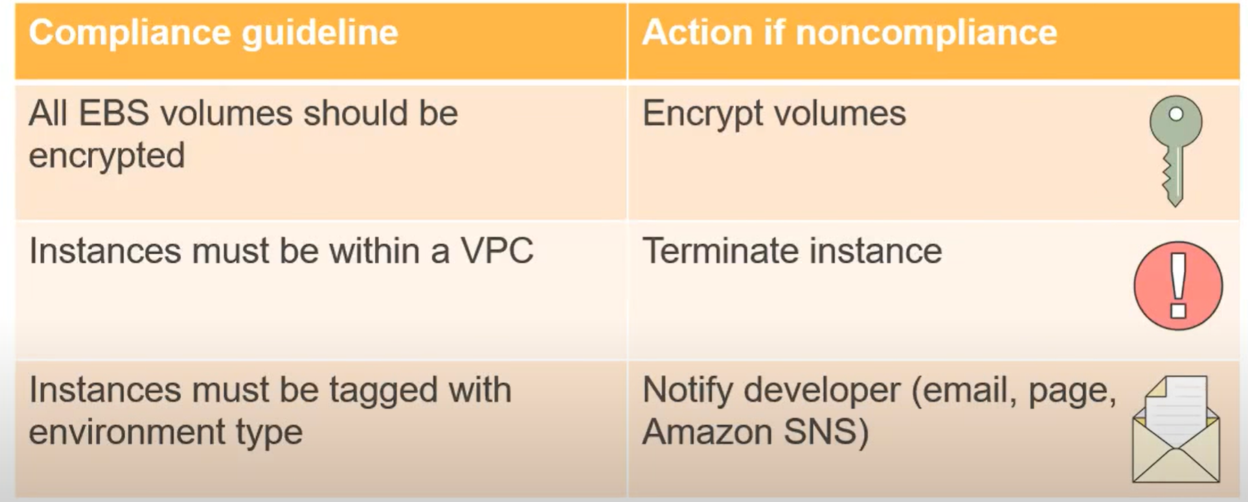
12. You can configure a rule to remediate:
    1. Remediate automatically
    2. Manually trigger remediation
    3. You can choose a remediation act that you want to occur (Ex: AWS-TerminateEC2Instance)

13 **AWS Config Aggregator:** This allows you to collect AWS Config data from **multiple accounts and regions.**

1. An Aggregator will replicate data from source account to aggregator account
2. The Aggregator has 3 sub categories on:
    a. Rules : All your resource are in one place
    b. Resources: All your resources are in one place
    c. Authorizations: Grant permission to the aggregator accounts and regions to collect AWS Config configuration and compliances data

14. **A Conformance Pack**: This is a collection of **AWS Config Rules and Remediation actions** that can be easily deployed as a single entity in an account in a Region or across an AWS organization

1. Packs are created by authorizing a YAML template



Compliance guideline	Action if noncompliance
All EBS volumes should be encrypted	Encrypt volumes
Instances must be within a VPC	Terminate instance
Instances must be tagged with environment type	Notify developer (email, page, Amazon SNS)

Possibility to store AWS Config Data into S3

2. Questions that can be solved using AWS Config?

1. Is there unrestricted SSH access to my Security Groups?
2. Do my buckets have any public access?
3. How has ALB configuration changed over time?

It’s a **PER-Region** Service but, there is a way to be aggregated across regions and accounts

You can get alerts for any changes

3. Notes based on the Question from WhizLab

Note 1: You are setting AWS Config via AWS CLI and you created an S3 bucket named “1234”. You’re not receiving any change configuration notification in this bucket. What could be the reason for this?

Step 1: AWS Config requires I**AM permission** to get the configuration details about your resources

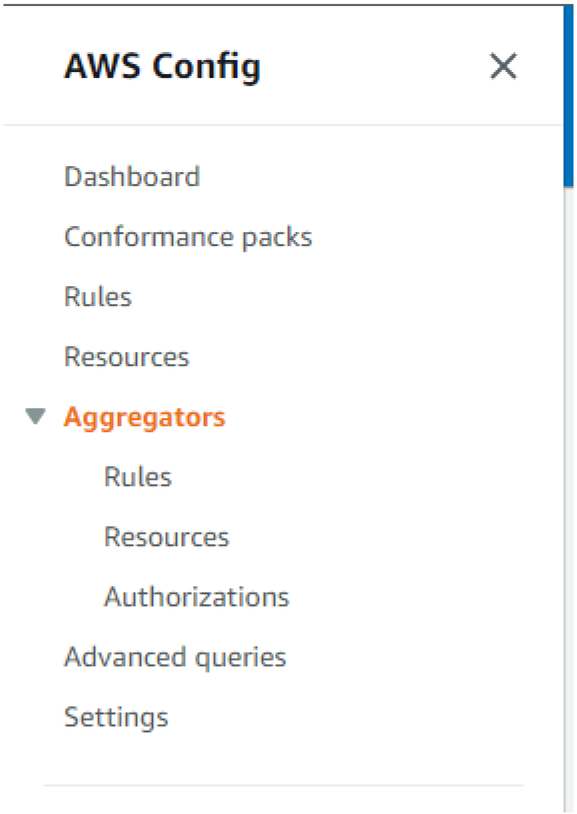
Step 2: Use the AWS Managed Policy **AWSConfigServiceRolePolicy** and attach it to the IAM role that you assign to AWS Config

Note 2: **AWS Config DOES NOT currently record Amazon S3 Glacier Vaults.**

Permissions needed for Config

4. Quick Recap:

Teva, tell each of the following components use cases?


AWS Config
Dashboard
Conformance packs
Rules
Resources
Aggregators
Rules
Resources
Authorizations
Advanced queries
Settings