AWS Config Overview

AWS Config is a service that allows you to assess, audit, and evaluate the configurations of your AWS resources. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.

Key Features:

1. **Continuous Monitoring**: AWS Config continuously records configuration changes of your AWS resources, capturing details like relationships between resources and their configurations over time.
2. **Resource Configuration History**: You can view the history of AWS resource configurations to see how the configurations have changed over time.
3. **Compliance Auditing**: AWS Config enables you to define rules based on your organizational policies. These rules automatically evaluate the configuration of your AWS resources for compliance.
4. **Change Management**: By recording all configuration changes, AWS Config helps in identifying and managing changes that could lead to non-compliance or security vulnerabilities.
5. **Automated Remediation**: AWS Config can be integrated with AWS Systems Manager Automation or Lambda functions to automatically remediate non-compliant resources, bringing them back into compliance.
6. **Integration with AWS Services**: AWS Config integrates with other AWS services like AWS CloudTrail, AWS CloudFormation, AWS Organizations, and Amazon SNS for comprehensive resource management and notification capabilities.

Key Concepts:

- **Configuration Item (CI)**: A record of the configuration of a resource at a specific point in time.
- **Configuration Recorder**: A component that records the configuration changes of the AWS resources.
- **Configuration Snapshot**: A collection of configuration items that AWS Config captures and stores at a specific point in time.
- **Compliance Rules**: These are custom rules that evaluate whether your AWS resources comply with your organization's guidelines.
- **Managed Rules**: Predefined rules provided by AWS to check resource compliance.

- **Custom Rules**: User-defined rules written in AWS Lambda that can evaluate the configurations of resources.

Common Use Cases:

1. **Security Analysis**: Monitoring security configurations, such as ensuring that security groups do not allow unrestricted access.
2. **Operational Troubleshooting**: Understanding changes in your infrastructure that may have led to operational issues.
3. **Resource Inventory**: Maintaining an inventory of all your AWS resources along with their configuration details.
4. **Compliance Audits**: Ensuring that your AWS resources are compliant with industry standards, such as PCI-DSS, HIPAA, or internal organizational policies.

Benefits:

- **Visibility**: Gain insight into the current and historical configurations of your resources.
- **Compliance**: Ensure continuous compliance with internal and external regulations.
- **Automation**: Automate the remediation of non-compliant resources to save time and reduce errors.
- **Security**: Enhance security by monitoring and enforcing security-related configurations.

AWS Config is particularly useful for organizations that need to manage large and complex AWS environments, ensuring that all resources comply with best practices and security standards.

AWS Config Setup: Step by Step Guide

Here's how you can set up AWS Config to start monitoring your AWS resources:

Step 1: Sign in to the AWS Management Console

1. Go to the AWS Management Console.
2. Log in with your AWS credentials.

Step 2: Navigate to AWS Config

1. In the AWS Management Console, search for “AWS Config” in the search bar.
2. Click on **AWS Config** under Services.

Step 3: Set Up AWS Config

1. On the AWS Config dashboard, click **Get Started**.

Step 4: Choose Resources to Record

1. **Record all resources supported in this region**: Select this option if you want AWS Config to track all the resource types in the selected region.
2. **Record specific types of resources**: Select this option if you want to monitor specific AWS resource types. Choose the resource types you want to record.

Step 5: Set Up an Amazon S3 Bucket for Configuration History

1. **Create a New S3 Bucket**:
   - If you don't already have an S3 bucket, select **Create a bucket**.
   - Provide a unique bucket name and select a region.
2. **Use an Existing S3 Bucket**:
   - If you already have an S3 bucket, select **Choose a bucket**.
   - Choose the bucket from the dropdown list.

AWS Config will store configuration history and snapshots in this bucket.

Step 6: Set Up an Amazon SNS Topic (Optional)

1. **Create a New SNS Topic**:
   - If you want to receive notifications, select **Create a topic**.
   - Provide a name for the SNS topic.
2. **Use an Existing SNS Topic**:
   - If you already have an SNS topic, select **Choose a topic**.
   - Choose the topic from the dropdown list.

This allows you to receive notifications about configuration changes and compliance events.

Step 7: Set Up AWS Config Rules (Optional)

1. **Add AWS Managed Rules**:
   - AWS Config provides predefined rules. Click on **Add rule** and select the rules you want to apply.
   - Customize the rule parameters if necessary.
2. **Create Custom Rules**:
   - If you have specific compliance requirements, you can create custom rules using AWS Lambda.

    - Select **Create rule** and follow the prompts to define your custom rule.

Step 8: Review and Confirm Settings

1. Review the settings you've configured, including the resources to record, the S3 bucket, SNS topic, and rules.
2. Click **Confirm** to enable AWS Config.

Step 9: Monitor and Review AWS Config Dashboard

1. Once AWS Config is enabled, you can monitor the configuration changes and compliance status from the AWS Config dashboard.
2. The dashboard will display:
    - **Resource Inventory**: List of resources being monitored.
    - **Configuration Changes**: Details of configuration changes.
    - **Compliance**: Status of resources in relation to the rules you've set up.

Step 10: Optional - Automate Remediation

1. To automatically remediate non-compliant resources, integrate AWS Config with AWS Systems Manager or use AWS Lambda functions.
2. This can be set up by creating a remediation action in the **Remediations** section.

Conclusion

With AWS Config set up, you now have continuous monitoring and visibility into your AWS resource configurations, which helps in maintaining compliance and enhancing security.