AWS Config Rule Optimizer Solution Runbook

Contents

About this guide

This guide provides a comprehensive step-by-step walkthrough for deploying and utilizing the **AWS Config Rule Optimizer** solution offered by CloudMates. The guide is intended for AWS users who want to optimize their AWS Config rules by identifying and eliminating duplicate rules, thereby improving governance, reducing costs, and enhancing operational efficiency.

Who Should Use This Guide:

This guide is designed for:

- **Cloud administrators** responsible for managing AWS Config rules and optimizing AWS resources.
- **DevOps teams** aiming to reduce AWS Config rule evaluation costs and simplify cloud compliance.
- **IT professionals** looking to automate the deployment of a cost-saving solution through AWS CloudFormation.

What This Guide Covers:

- Detailed steps to deploy the AWS Config Rule Optimizer via CloudFormation.
- Instructions for configuring necessary AWS resources, such as IAM roles and CloudTrail access.
- Guidance on accessing and using the AWS Config Rule Optimizer interface to generate reports and recommendations for cost optimization.
- Best practices for securing your deployment and maximizing the operational benefits of the solution.

By following this guide, users will gain insights into their AWS Config rule usage and unlock the ability to reduce costs through a streamlined management process.

Solution Overview

The **CloudMates AWS Config Rule Optimizer** helps customers reduce costs by identifying duplicate rules within their AWS Config setup. The solution offers a user-friendly dashboard that provides insights into AWS Config rules across multiple accounts and regions. Users can also export detailed reports, which include recommendations for cost optimization and rule management.

Key Functionalities:

- **Dashboard**: A comprehensive view of all AWS Config rules, providing insights into rule usage and duplications.
- **PDF Export**: Generate detailed reports with rule information, including the number of rules, duplicates, and associated costs.
- **Duplicate Rule Identification**: Automatically detect and highlight duplicate rules to help optimize AWS costs by reducing unnecessary rule evaluations.
- **Recommendations**: Provides best practices and recommendations to remove duplicate or unnecessary rules, improving the efficiency of your AWS setup.

Deployment Options:

This solution can be deployed in two ways:

1. **Amazon EC2 Instance**: Deployed with an IAM role that provides read-only access to CloudTrail data for AWS Config rule analysis.
2. **CloudFormation Template**: Automatically launches an EC2 instance in an isolated VPC and subnet with all necessary resources, such as IAM roles and security groups, configured.

Cost

The **AWS Config Rule Optimizer** incurs costs based on the EC2 instance and AMI usage.

EC2 Instance Costs:

- Minimum required instance: **t3.micro**.
- Instance costs vary by region (e.g., $0.0104 per hour in **US East** as of Oct 2024).
- Larger instances (e.g., **t3.medium**) will incur higher costs.

AMI Charges:

- Additional charges apply for the AMI used in the analysis and reporting.

Total Cost Consideration:

- Costs will depend on the instance size and region selected. Monitor instance usage to control costs.

Architecture Overview

The AWS Config Rule Optimizer is deployed in an AWS environment using a CloudFormation template or an EC2 instance. The architecture consists of the following components:

- **VPC (Virtual Private Cloud)**: Provides a secure and isolated network environment for the EC2 instance.
- **Public Subnet**: Ensures the EC2 instance has public IP access for remote management and dashboard access.
- **Security Group**: Configures the necessary inbound and outbound rules to allow HTTP access on port 80.
- **IAM Role**: Grants the EC2 instance read-only permissions to CloudTrail to access AWS Config rule events.

Implementation Considerations

When deploying the **AWS Config Rule Optimizer**, consider the following:

1. **IAM Role Permissions**:
    a. The EC2 instance requires read-only access to CloudTrail. Ensure the IAM role has the necessary permissions to access CloudTrail logs.
2. **Network and Connectivity**:
    a. If using a **public subnet**, ensure the instance is accessible via public IP. For **private subnets**, configure VPN or Direct Connect to allow access.
    b. Use security groups to restrict access to trusted IP addresses.
3. **Cost Impact**:
    a. By eliminating duplicate AWS Config rules, you can reduce rule evaluation costs and improve operational efficiency.

Pre-requisites

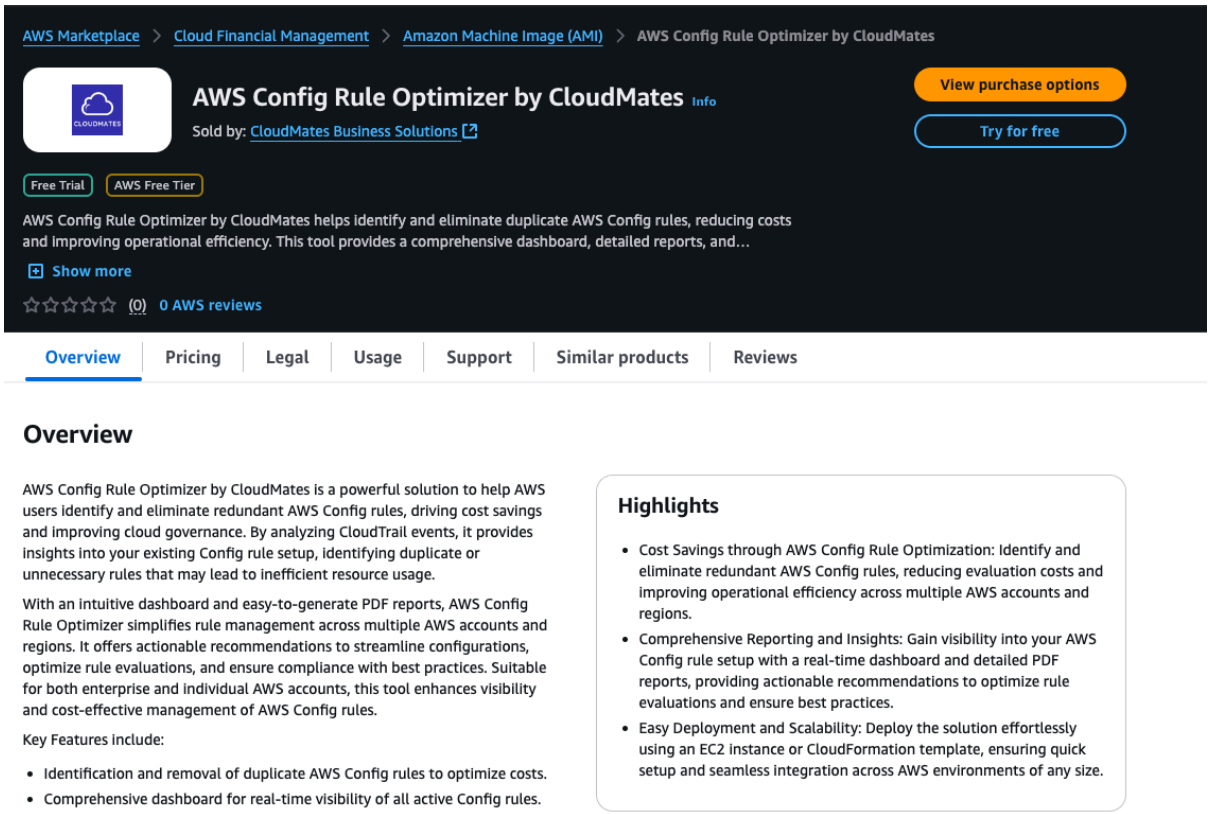
Before deploying the **AWS Config Rule Optimizer**, ensure the following:

1. **IAM Role or User with CloudTrail Read-Only Permissions**:
    a. Use an existing IAM role or create one with CloudTrail permissions (*cloudtrail:DescribeTrails*, *cloudtrail:GetTrailStatus*, *cloudtrail:LookupEvents)*.
    b. If using IAM user credentials, pre-configure **Access Key ID** and **Secret Access Key**.
2. **Network Connectivity**:
    a. Ensure the instance is accessible via public or private IP using VPN or Direct Connect.
3. **AWS CloudTrail**:
    a. Ensure **CloudTrail** is enabled in the AWS accounts where Config rules are to be analyzed.

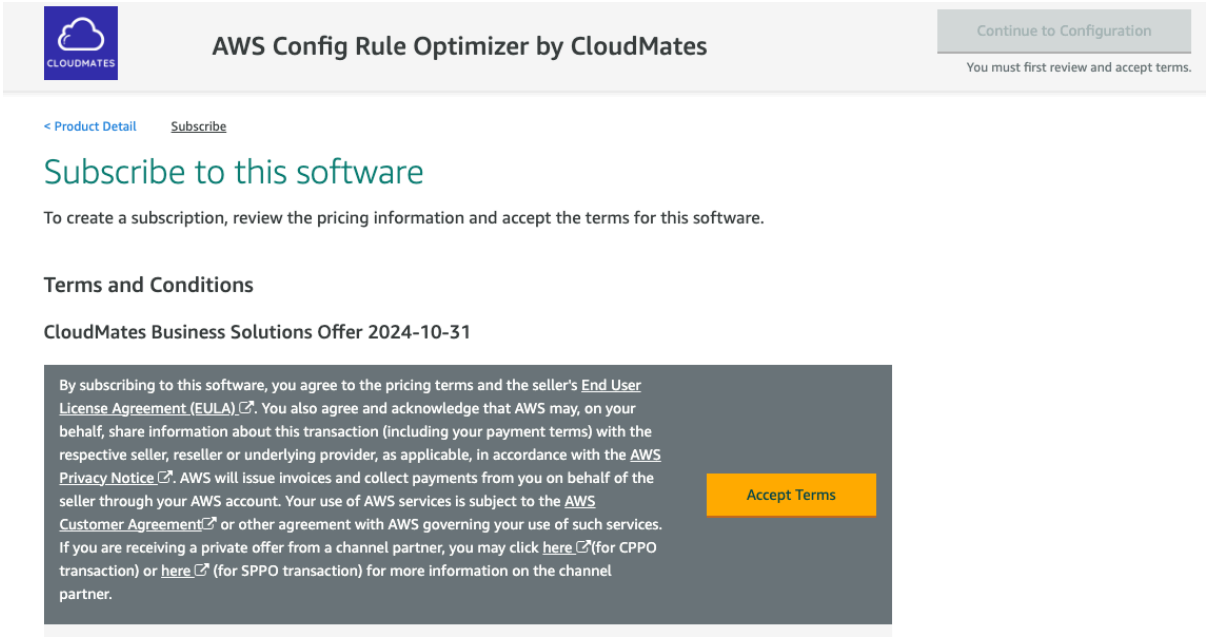
Steps to Deploy

Option 1: Launch EC2 Instance with IAM Role

1. **Subscribe to the Public AMI**:
    - Search for the public AMI **"CloudMatesAWSConfigRulesAnalyzer"** in the AWS Marketplace.



    - Subscribe to the AMI and proceed with the launch.



2. **Create IAM Role for EC2**:
   - Attach the **AWSCloudTrailReadOnlyAccess** and **AWSConfigUserAccess** managed policy to the IAM role.
   - Alternatively, create a custom policy with the following permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

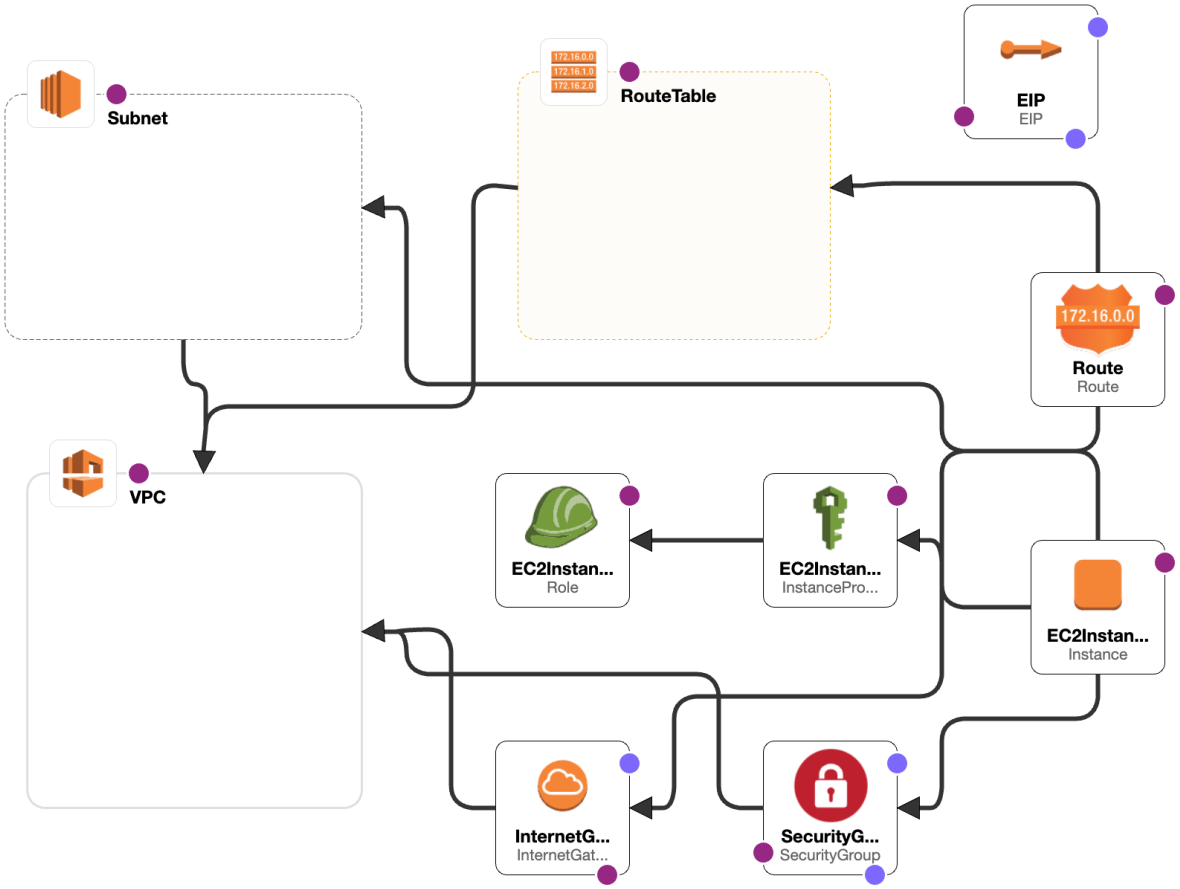
3. **Launch EC2 Instance**:
   - During the instance launch, provide the following parameters:

- **VPC ID**: Specify the VPC where the instance will be deployed.
- **Subnet**: Provide the subnet within the VPC.
- **Public IP**: Ensure the instance is assigned a public IP for external access or configure private connectivity if needed.
- Attach the IAM role created in the previous step to the EC2 instance.

  - Proceed with the instance creation using the subscribed AMI and provided parameters.

Option 2: Deploy via CloudFormation Template

Use the provided CloudFormation template to automatically launch the solution in an isolated VPC and subnet. This template will configure the EC2 instance, IAM role, and associated security group.



To deploy using the CloudFormation template:

1. **Access the CloudFormation Quick Create Link**:
   a. Use the following link to access the CloudFormation stack creation page:

   https://us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/quickcreate?stackName=ConfigAnalyzerStack&templateURL=https://cloudmates-solutions-artifacts.s3.us-west-2.amazonaws.com/configanalyzer.yml

You can also click the below button which takes you to the CloudFormation stack creation page.

Launch Stack

2. **Change Region if Needed**:
    a. By default, this link opens the CloudFormation console in the **us-east-1** region. You can change the region by selecting your preferred region from the dropdown at the top right corner of the console.
3. **Review and Launch**:
    a. The template URL and stack name (ConfigAnalyzerStack) will be pre-filled.
    b. Review the details and parameters and click **Create Stack** to launch the solution.
4. **Monitor Stack Creation**:
    a. The CloudFormation console will display the status of the stack creation. Once the status shows CREATE_COMPLETE, the EC2 instance with the required configuration will be ready.

Accessing the Solution

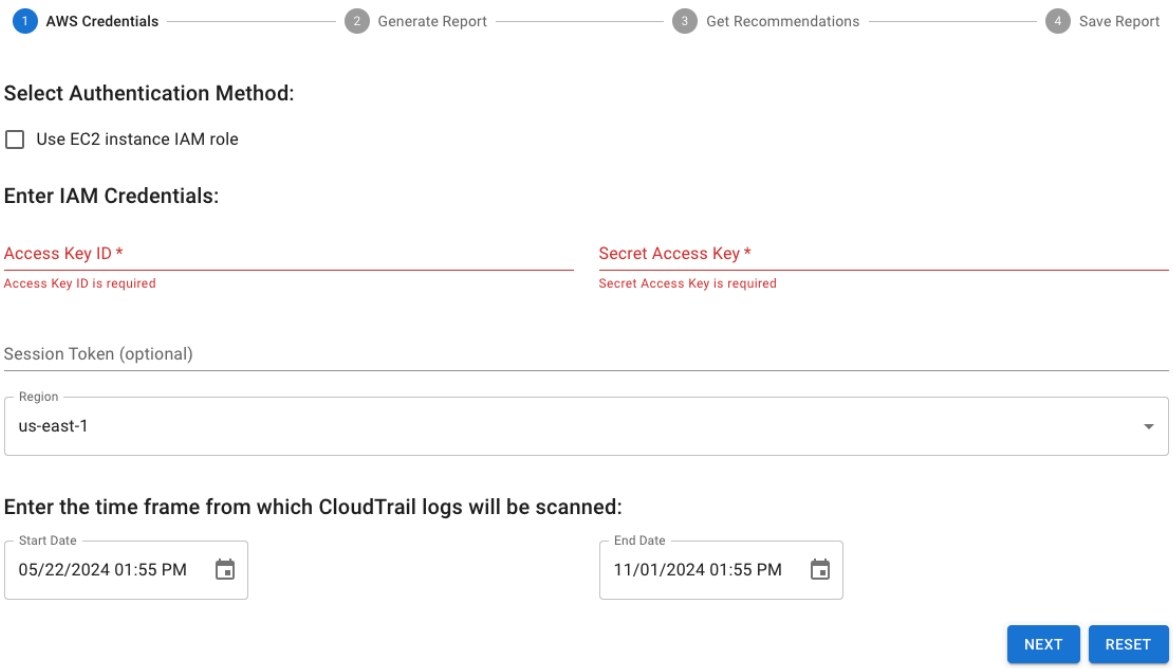
1. **Public IP Access**:
    a. Open your web browser and navigate to http://<public-ip-address> to access the solution's dashboard.
2. **Private IP Access**:
    a. If connected via VPN/Direct Connect, access the solution at http://<private-ip-address>.

Insert Picture: Accessing the Solution via Public or Private IP

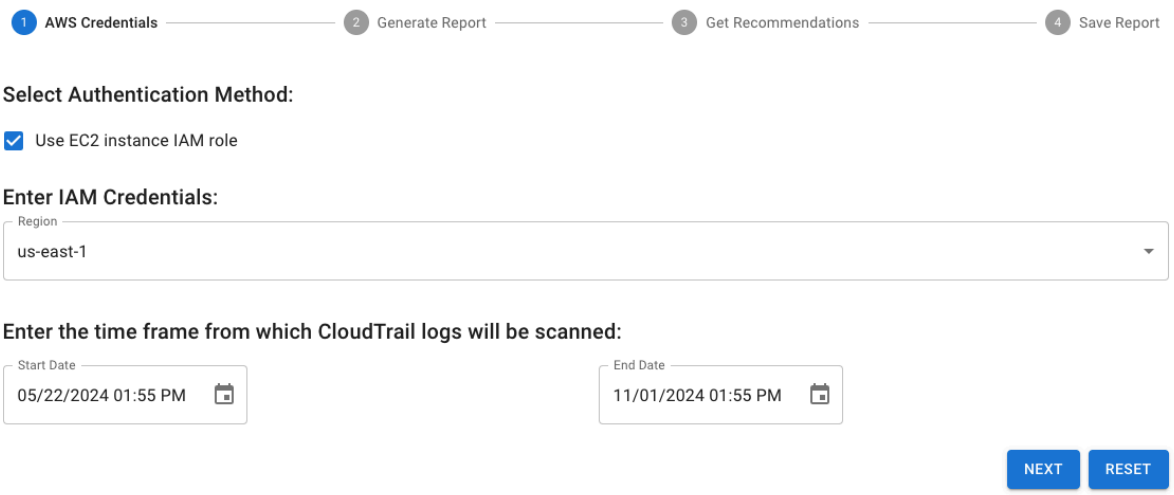
System Setup and Access

Once you've accessed the solution:

1. **Specify Authentication Method**:
    a. Provide either the IAM Access Key ID and Secret Access Key or allow the instance to use its IAM role permissions.



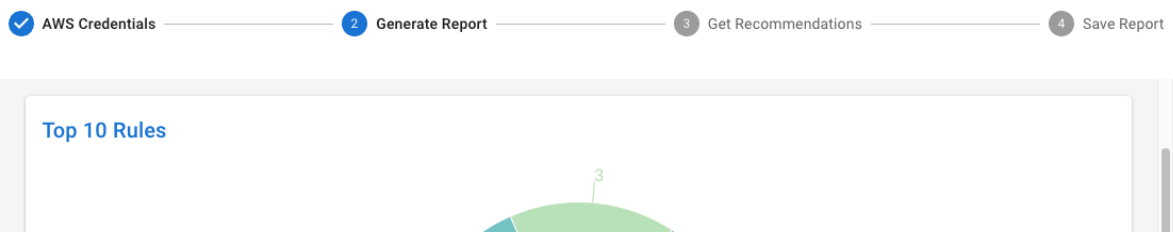
2. **Specify Time Range and Region**:
    a. Set the start and end timestamps for analysing CloudTrail events.
    b. Select the AWS region you want to analyse.



3. Click the **NEXT** button

Using the Dashboard

1. **Dashboard Overview**:
    a. The dashboard shows a summary of AWS Config rules configured in the selected region.
    b. The **pie chart** illustrates the top 10 rules by usage.



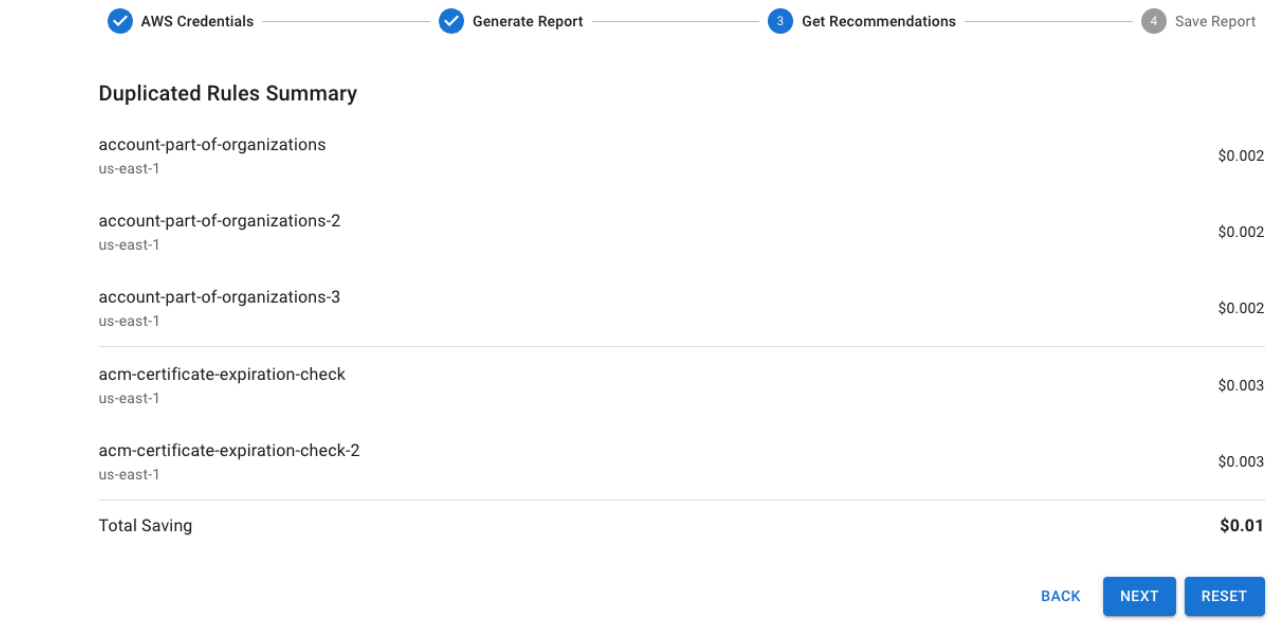
c. The table with **Rule Details** lists rule details including Rule Name, Count, Conformance Pack, and any identified duplicate rules.

Rule Details

Rule Name	Count	Conformance Pack	Duplicate Rule(s)
access-keys-rotated	3	None	
acm-certificate-expiration-check-2	3	None	1. acm-certificate-expiration-check
acm-certificate-expiration-check	3	None	1. acm-certificate-expiration-check-2
account-part-of-organizations	2	None	1. account-part-of-organizations-2 2. account-part-of-organizations-3
account-part-of-organizations-2	2	None	1. account-part-of-organizations 2. account-part-of-organizations-3
account-part-of-organizations-3	2	None	1. account-part-of-organizations 2. account-part-of-organizations-2
cloudtrail-enabled	2	None	
s3-bucket-cross-region-replication-enabled	2	None	

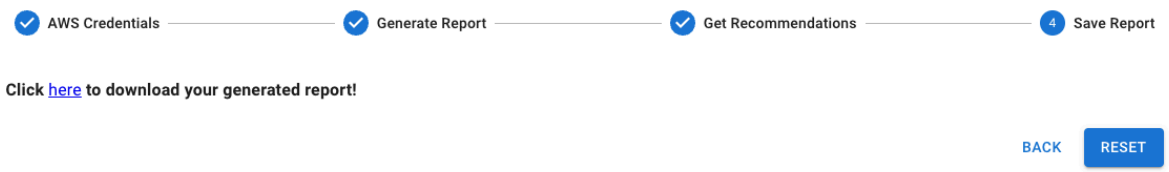
Get Recommendations

- Click **NEXT** to get recommendations about duplicate rules and best practices for rule management.



Generate Report

- Once analysed, generate a **PDF report** containing:
  - Rule names.
  - Count and details of duplicate rules.
  - Conformance Pack information.



- This report can be used to take actions such as removing redundant AWS Config rules to optimize costs.

Cost Optimization Benefits

- **Reduce AWS Config Rule Evaluations**: By deleting duplicate rules, customers can minimize the number of rule evaluations.
  - First 100,000 rule evaluations: **$0.001 per rule evaluation** per region.
- **Conformance Pack Evaluation Costs**:
  - First 100,000 evaluations: **$0.001 per evaluation** per region.
- **Overall Savings**: Deleting redundant or duplicate rules will result in fewer evaluations, directly reducing AWS Config service costs.
  - This also improves the efficiency of your AWS environment, ensuring that only necessary rules are in place, reducing the operational complexity.

Outcome Summary

The CloudMates AWS Config Rule Optimizer solution offers a simple and effective way to identify and manage duplicate AWS Config rules, enabling customers to save on evaluation costs and improve their cloud governance.