Lesson 07 Demo 05

Setting Up AWS Config and Creating Rules in it

Objective: To configure AWS Config and create rules in it to enable compliance monitoring in the AWS environment

Tools required: AWS Management Console

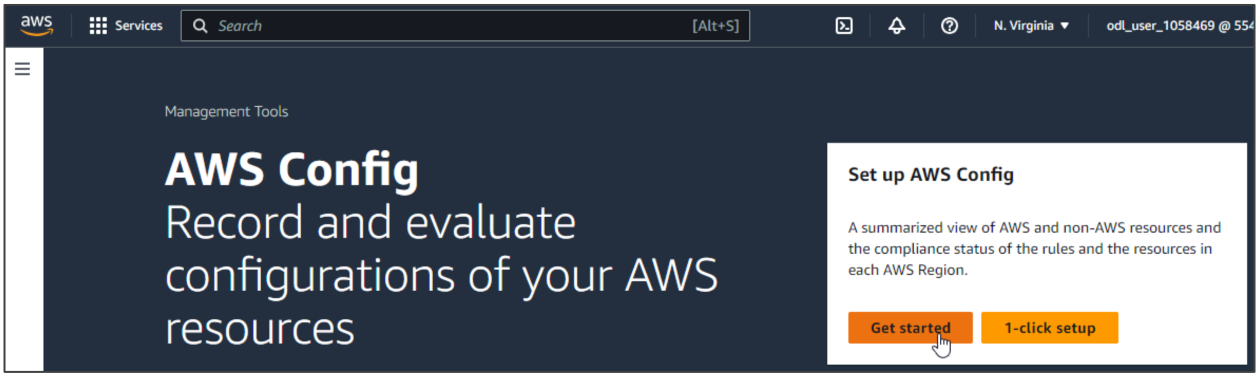
Prerequisites: None

Steps to be followed:

1. Set up AWS Config
2. Create rules in AWS Config

Step 1: Set up AWS Config

1.1 Sign in to the AWS Management Console, open the AWS Config at https://console.aws.amazon.com/config/, and click **Get started**



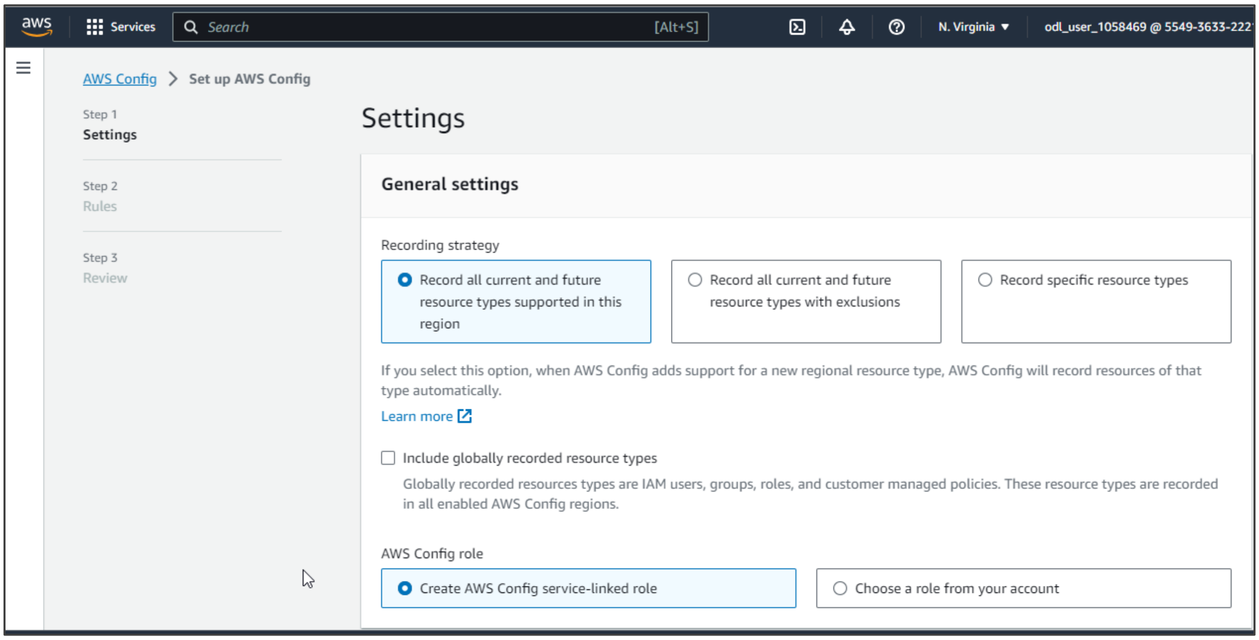
Management Tools

AWS Config
Record and evaluate configurations of your AWS resources

Set up AWS Config

A summarized view of AWS and non-AWS resources and the compliance status of the rules and the resources in each AWS Region.

1.2 In the settings page, select **Record all current and future resource types supported in this region** under the **Recording strategy** section and **Create AWS Config service-linked role** under the **AWS Config role section**



AWS Config > Set up AWS Config

Step 1 Settings

Step 2 Rules

Step 3 Review

Settings

General settings

Recording strategy

● Record all current and future resource types supported in this region

○ Record all current and future resource types with exclusions

○ Record specific resource types

If you select this option, when AWS Config adds support for a new regional resource type, AWS Config will record resources of that type automatically.

Learn more

□ Include globally recorded resource types

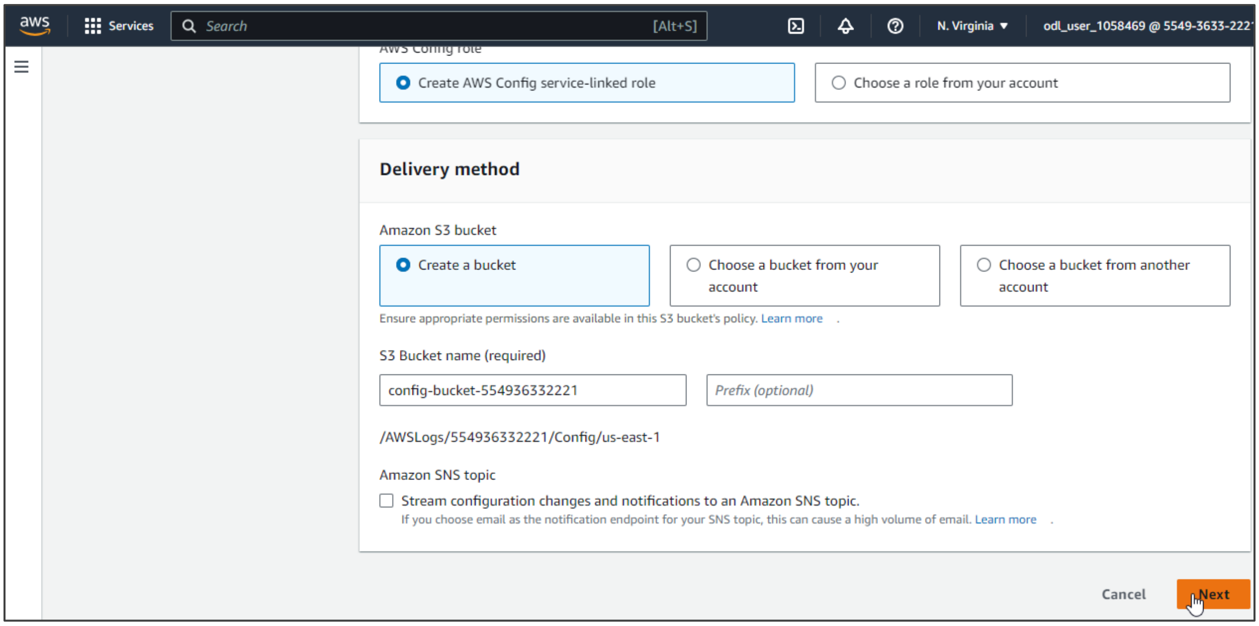
Globally recorded resources types are IAM users, groups, roles, and customer managed policies. These resource types are recorded in all enabled AWS Config regions.

AWS Config role

● Create AWS Config service-linked role

○ Choose a role from your account

1.3 In the **Delivery method** section, select **Create a bucket** under **Amazon S3 bucket** and then click **Next**



● Create AWS Config service-linked role

○ Choose a role from your account

Delivery method

Amazon S3 bucket

● Create a bucket

○ Choose a bucket from your account

○ Choose a bucket from another account

Ensure appropriate permissions are available in this S3 bucket's policy. Learn more

S3 Bucket name (required)

config-bucket-554936332221

Prefix (optional)

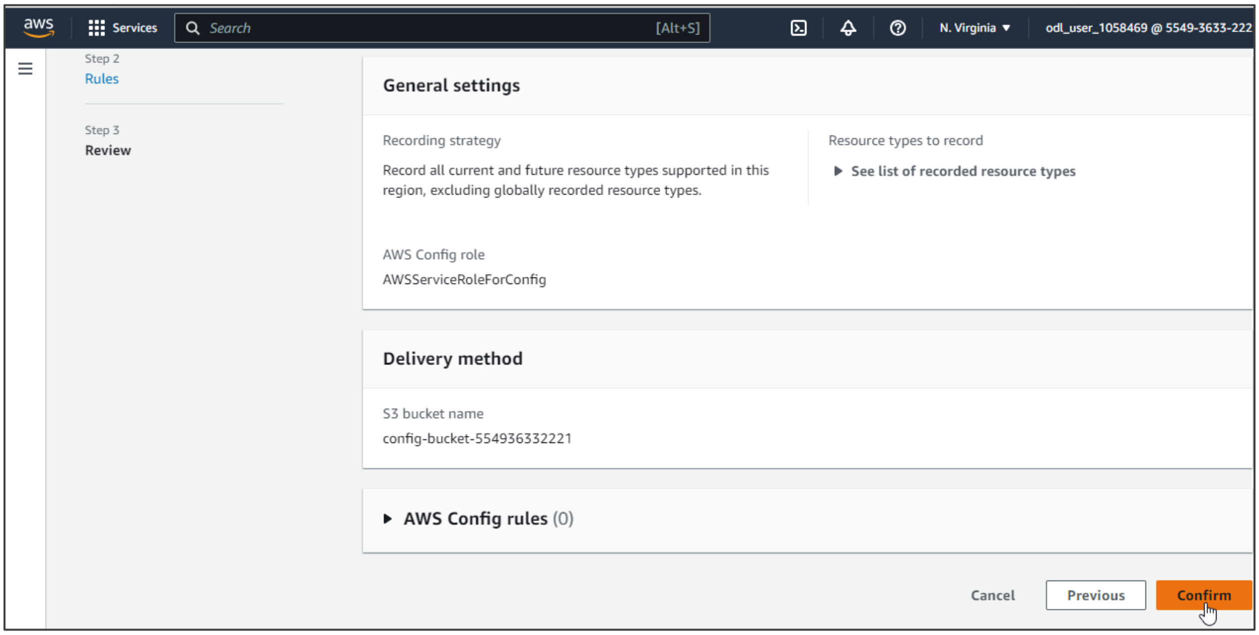
/AWSLogs/554936332221/Config/us-east-1

Amazon SNS topic

□ Stream configuration changes and notifications to an Amazon SNS topic.

If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. Learn more

1.4 Review the settings and click **Confirm**



General settings

Recording strategy
Record all current and future resource types supported in this region, excluding globally recorded resource types.

Resource types to record
See list of recorded resource types

AWS Config role
AWSServiceRoleForConfig

Delivery method

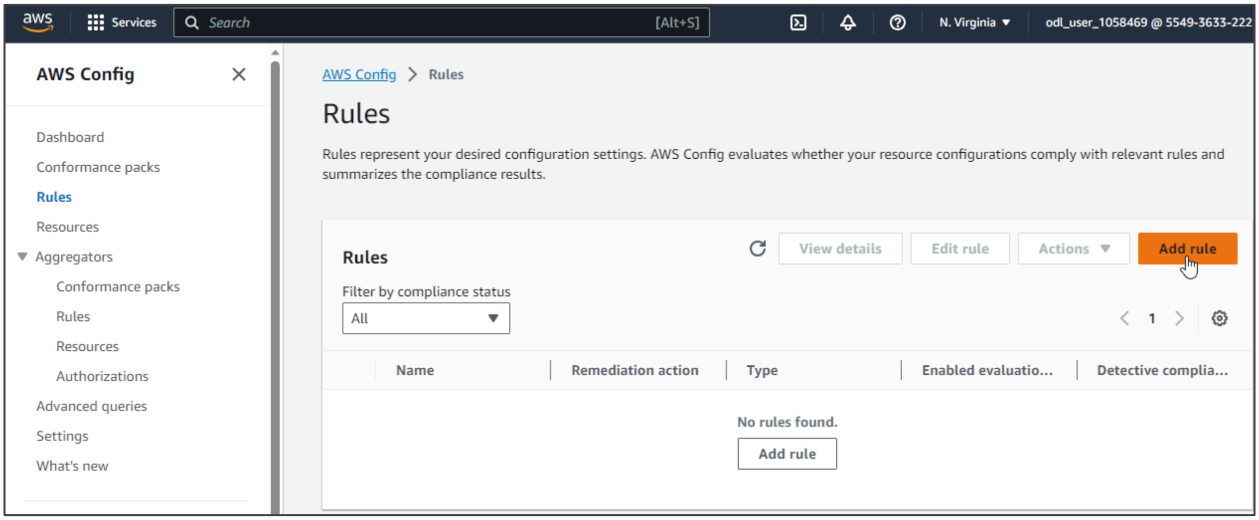
S3 bucket name
config-bucket-554936332221

AWS Config rules (0)

The set up for AWS Config is completed.

Step 2: Create rules in AWS Config

2.1 In the AWS Config dashboard, select **Rules** and then click **Add rule**



Rules

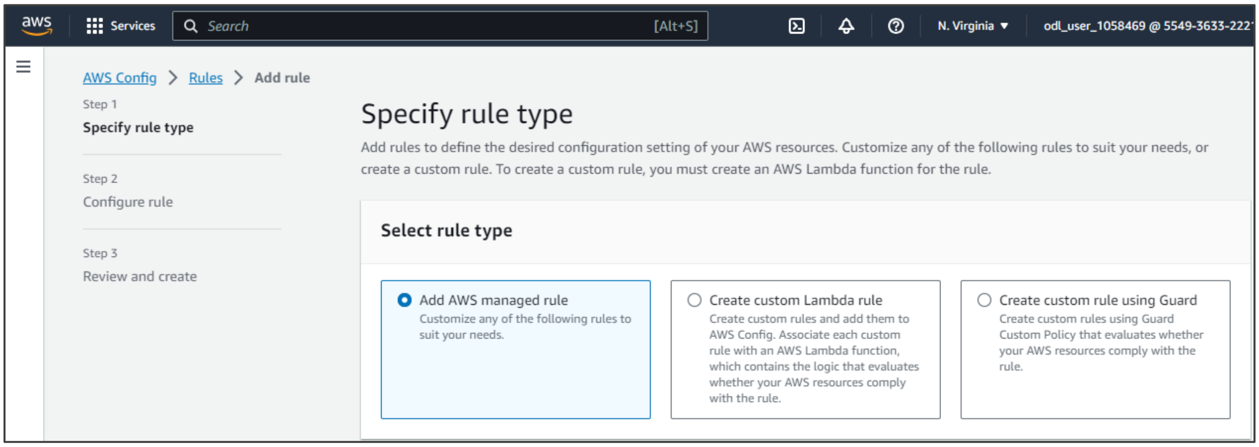
Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Rules

Name	Remediation action	Type	Enabled evaluatio...	Detective complia...

No rules found.

2.2 In the **Specify rule type** page, select **Add AWS managed rule** under the **Select rule type** section



Specify rule type

Add rules to define the desired configuration setting of your AWS resources. Customize any of the following rules to suit your needs, or create a custom rule. To create a custom rule, you must create an AWS Lambda function for the rule.

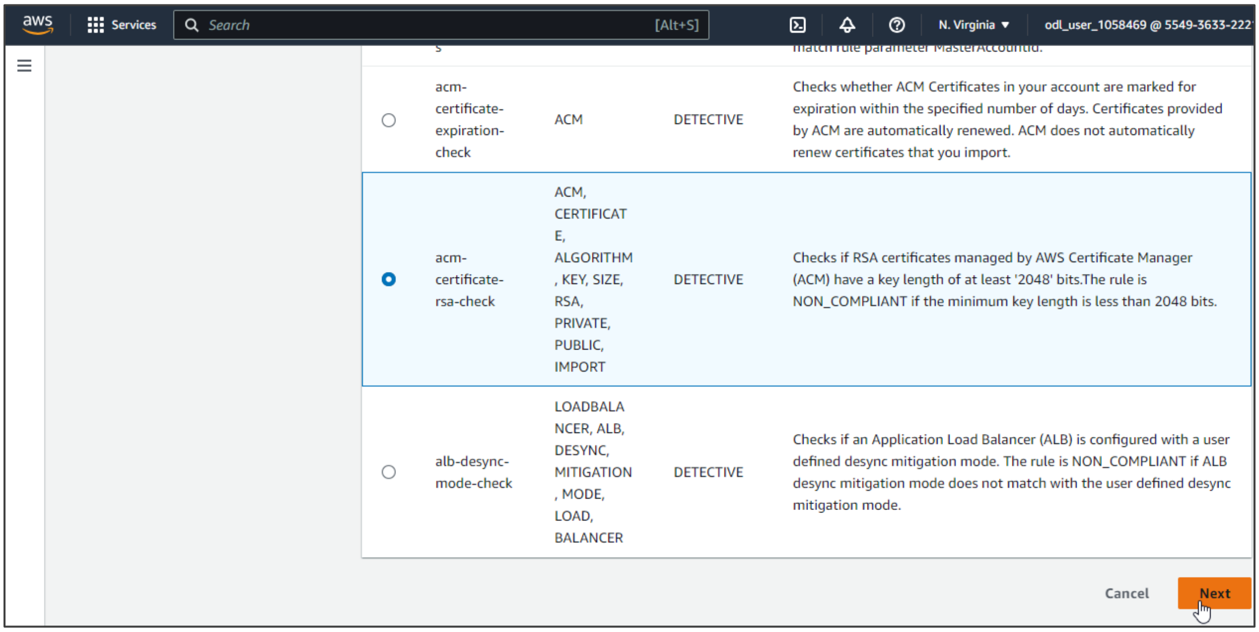
Select rule type

● Add AWS managed rule
Customize any of the following rules to suit your needs.

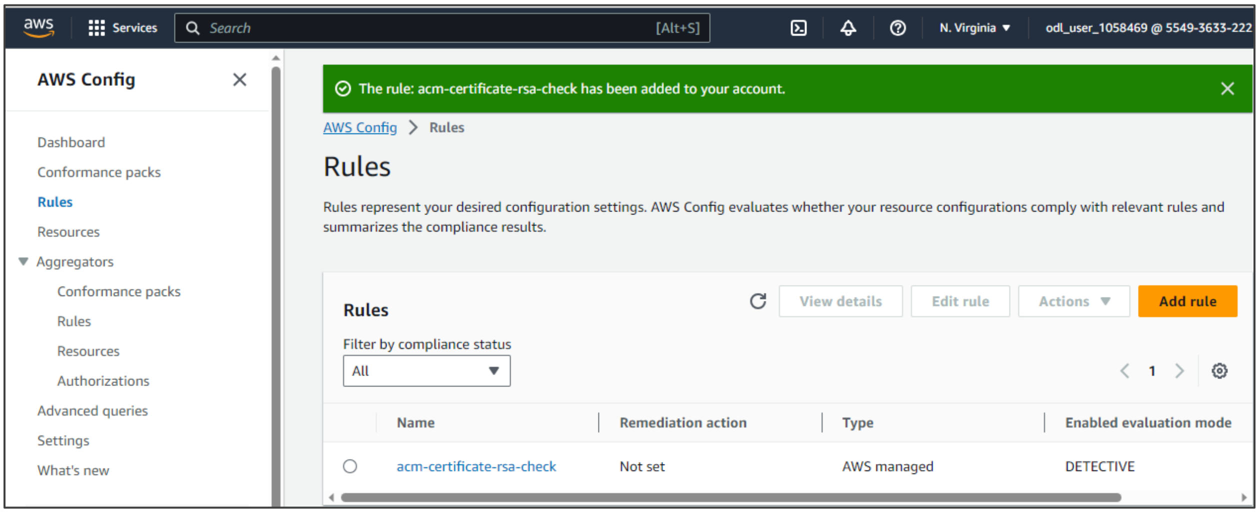
○ Create custom Lambda rule
Create custom rules and add them to AWS Config. Associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.

○ Create custom rule using Guard
Create custom rules using Guard Custom Policy that evaluates whether your AWS resources comply with the rule.

2.3 Select the rule as shown here and click **Next**



	s			match rule parameter MasterAccountId.
○	acm-certificate-expiration-check	ACM	DETECTIVE	Checks whether ACM Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed. ACM does not automatically renew certificates that you import.
●	acm-certificate-rsa-check	ACM, CERTIFICATE, ALGORITHM, KEY, SIZE, RSA, PRIVATE, PUBLIC, IMPORT	DETECTIVE	Checks if RSA certificates managed by AWS Certificate Manager (ACM) have a key length of at least '2048' bits.The rule is NON_COMPLIANT if the minimum key length is less than 2048 bits.
○	alb-desync-mode-check	LOADBALANCER, ALB, DESYNC, MITIGATION, MODE, LOAD, BALANCER	DETECTIVE	Checks if an Application Load Balancer (ALB) is configured with a user defined desync mitigation mode. The rule is NON_COMPLIANT if ALB desync mitigation mode does not match with the user defined desync mitigation mode.



The rule: acm-certificate-rsa-check has been added to your account.

Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

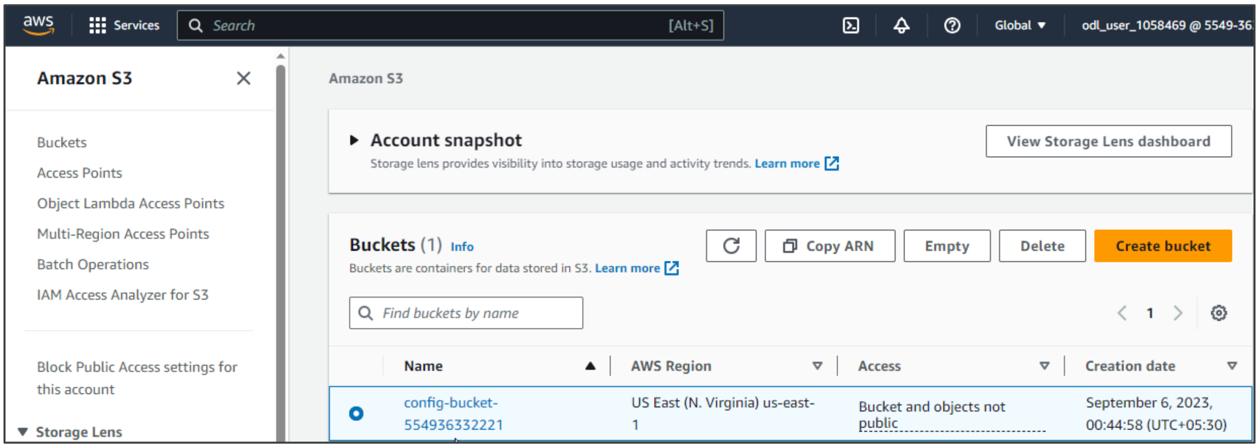
Rules

Filter by compliance status: All

	Name	Remediation action	Type	Enabled evaluation mode
○	acm-certificate-rsa-check	Not set	AWS managed	DETECTIVE

The rule is created successfully.

2.4 Now, go to the S3 service, open the **Buckets** dashboard and select the **config bucket** that is created automatically after the AWS Config setup

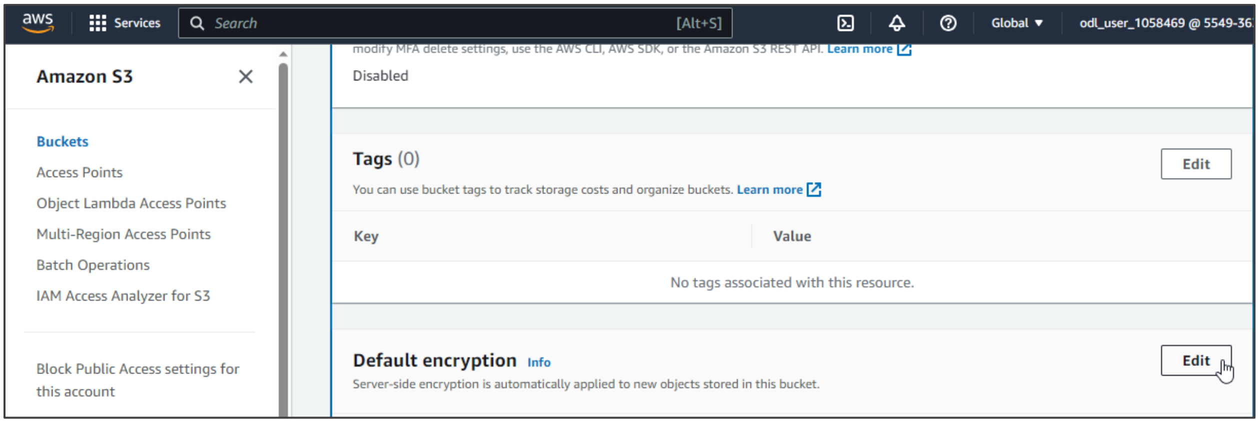


Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
●	config-bucket-554936332221	US East (N. Virginia) us-east-1	Bucket and objects not public	September 6, 2023, 00:44:58 (UTC+05:30)

2.5 Click **Edit** under the **Default encryption** section


aws
Services
Search
[Alt+S]
Global ▼
odl_user_1058469 @ 5549-36
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Tags (0)
Edit
Default encryption Info
Edit

modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more

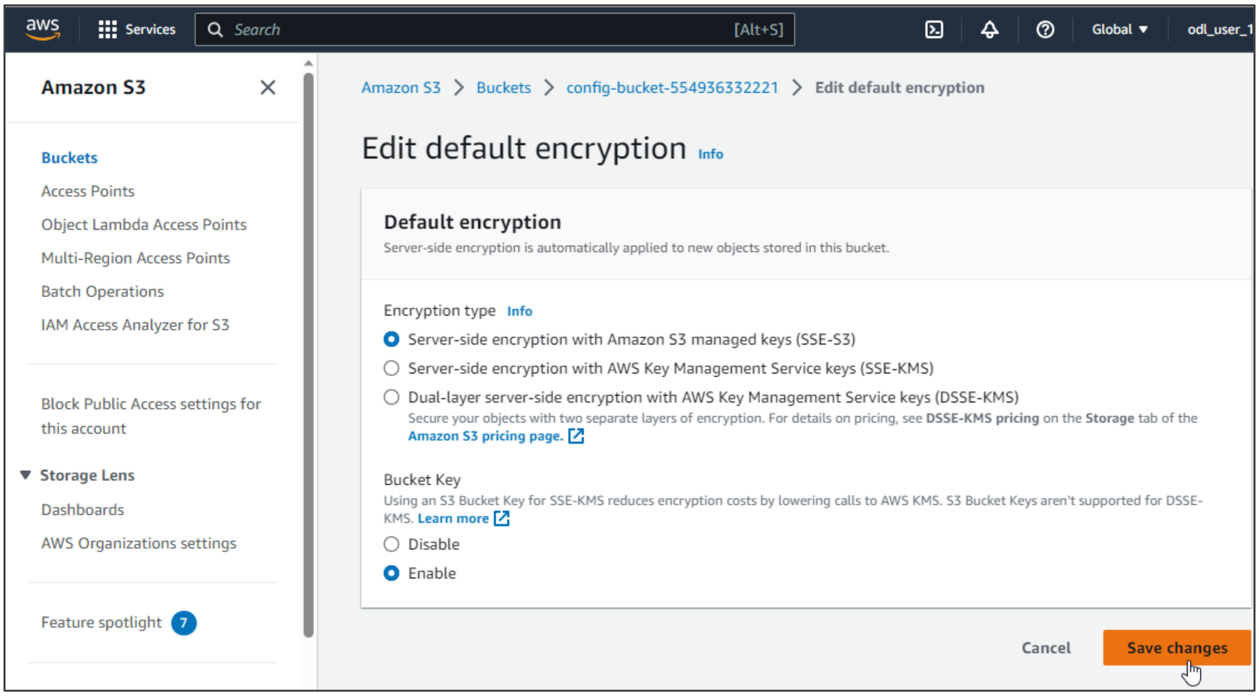
Disabled

You can use bucket tags to track storage costs and organize buckets. Learn more

Key	Value
No tags associated with this resource.	

Server-side encryption is automatically applied to new objects stored in this bucket.

2.6 In the **Edit default encryption** page, select **Server-side encryption with Amazon S3 managed keys (SSE-S3)** option under **Encryption type** section, choose **Enable** option under the **Bucket Key** section and click **Save changes**


aws
Services
Search
[Alt+S]
Global ▾
odl_user_1
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
▼ Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 7
Amazon S3 > Buckets > config-bucket-554936332221 > Edit default encryption
Cancel
Save changes

Edit default encryption Info

Default encryption

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

● Server-side encryption with Amazon S3 managed keys (SSE-S3)

○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the **Amazon S3 pricing page.**

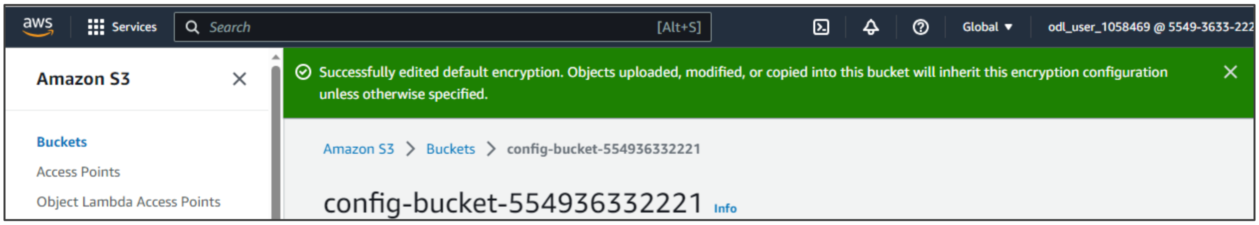
Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. **Learn more**

○ Disable

● Enable

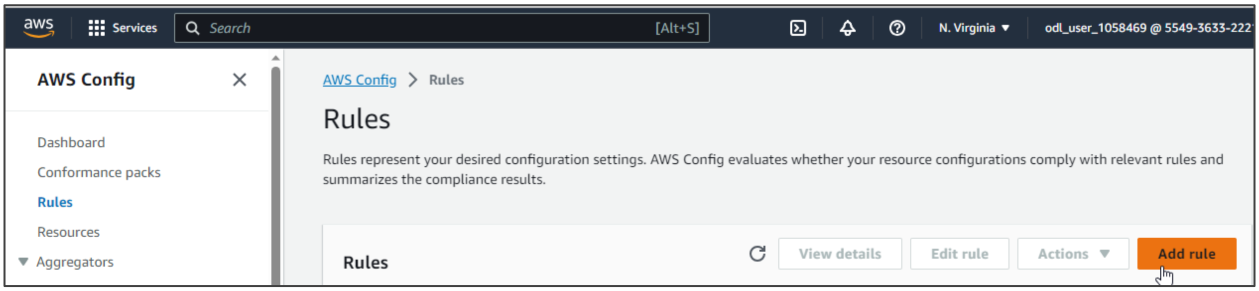
The default encryption is updated successfully.


aws
Services
Search
[Alt+S]
Global ▾
odl_user_1058469 @ 5549-3633-222
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Amazon S3 > Buckets > config-bucket-554936332221

Successfully edited default encryption. Objects uploaded, modified, or copied into this bucket will inherit this encryption configuration unless otherwise specified.

config-bucket-554936332221 Info

2.7 Now, navigate back to the **Rules** tab in the AWS Config dashboard and click **Add rule** to create another rule

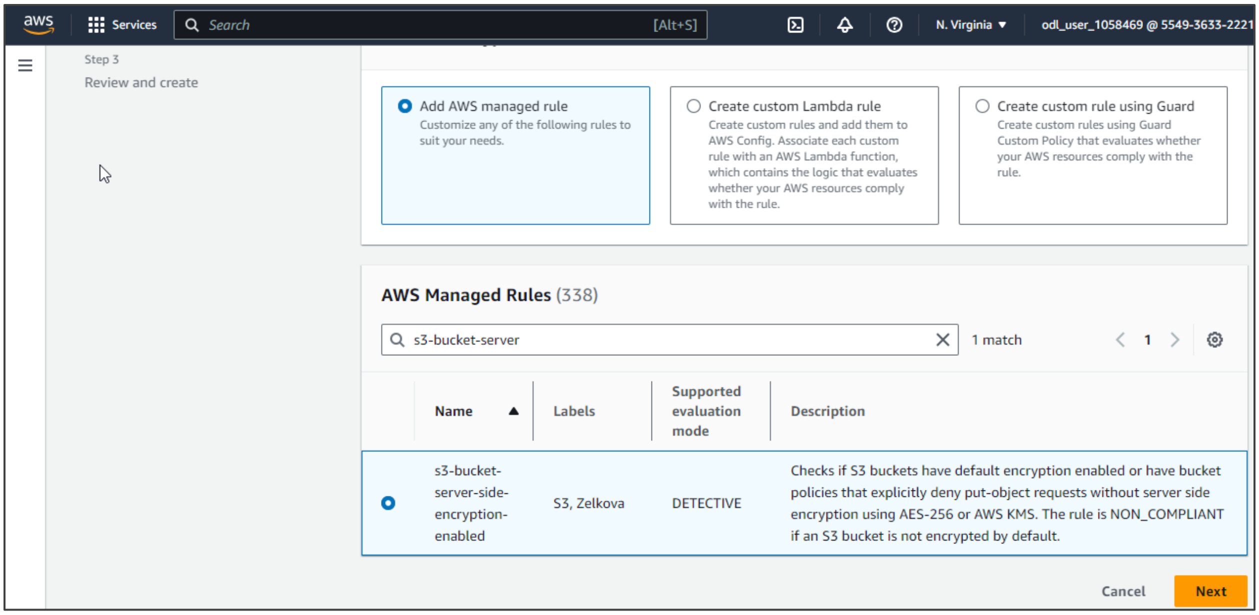


Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Rules

2.8 Choose **s3-bucket-server-side-encryption-enabled** rule from the AWS Managed rule list and click **Next**



● Add AWS managed rule
Customize any of the following rules to suit your needs.

○ Create custom Lambda rule
Create custom rules and add them to AWS Config. Associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.

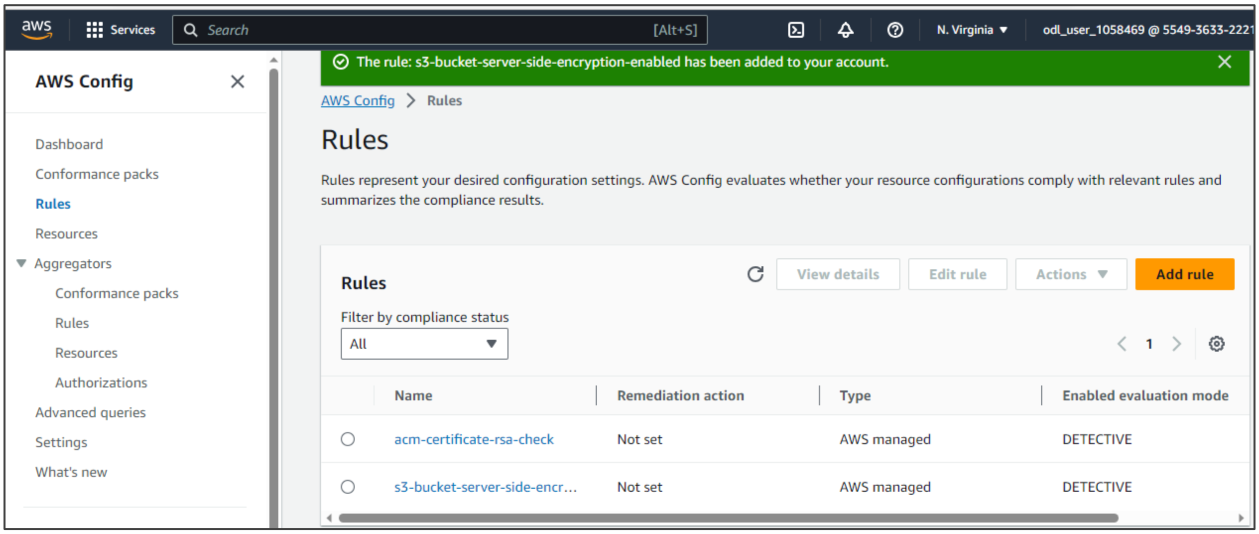
○ Create custom rule using Guard
Create custom rules using Guard Custom Policy that evaluates whether your AWS resources comply with the rule.

AWS Managed Rules (338)

s3-bucket-server — 1 match — 1

	Name	Labels	Supported evaluation mode	Description
●	s3-bucket-server-side-encryption-enabled	S3, Zelkova	DETECTIVE	Checks if S3 buckets have default encryption enabled or have bucket policies that explicitly deny put-object requests without server side encryption using AES-256 or AWS KMS. The rule is NON_COMPLIANT if an S3 bucket is not encrypted by default.

The rule is created successfully.



The rule: s3-bucket-server-side-encryption-enabled has been added to your account.

AWS Config > Rules

Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Rules

Filter by compliance status: All

	Name	Remediation action	Type	Enabled evaluation mode
○	acm-certificate-rsa-check	Not set	AWS managed	DETECTIVE
○	s3-bucket-server-side-encr...	Not set	AWS managed	DETECTIVE

By following these steps, you have successfully demonstrated the process of setting up AWS Config, configuring it, and creating rules in it.