

## 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

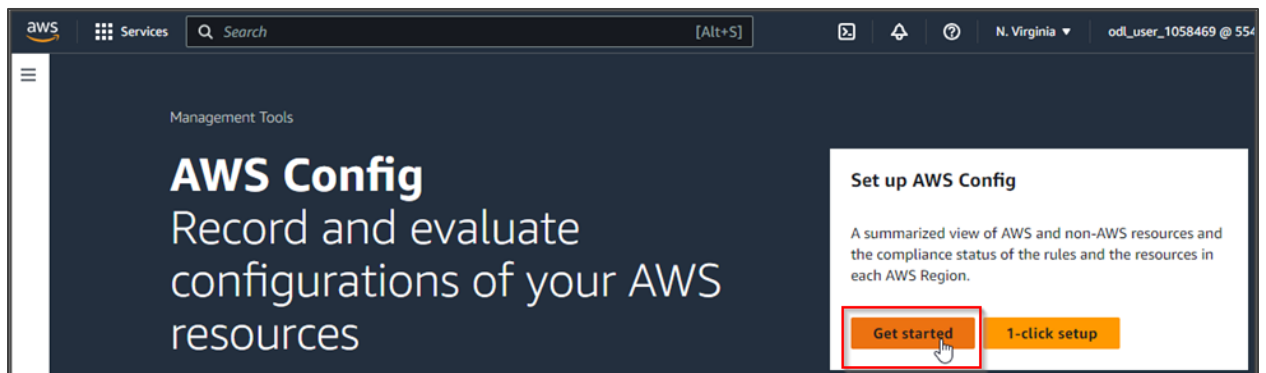
**Prerequisites:** None

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**



1.2 In the settings page, select **All resource types with customizable overrides** under the **Recording strategy** section

**Settings**

**Recording method**

**Recording strategy**  
Customize AWS Config to record configuration changes for all supported resource types, or for only the supported resource types that are relevant to you. Globally recorded resources (RDS global clusters and IAM users, groups, roles, and customer managed policies) may be recorded in more than this Region. [Learn more](#) You are charged based on the number of configuration items recorded. [Pricing details](#)

☒ **All resource types with customizable overrides**  
AWS Config will record all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording.

☐ **Specific resource types**  
AWS Config will only record the resource types that you specify.

1.3 In the **Data governance** section, select **Create AWS Config service-linked role** under **IAM role for AWS config**

**Data governance**

**IAM role for AWS Config**

☒ **Create AWS Config service-linked role**  
AWS Config will create a new IAM role for you to use for recording configuration changes.

☐ **Choose a role from your account**  
Choose an IAM role from one of your pre-existing roles and permission policies.

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

**Delivery method**

**Amazon S3 bucket**

☒ **Create a bucket**  
Ensure appropriate permissions are available in this S3 bucket's policy. [Learn more](#)

☐ **Choose a bucket from your account**

☐ **Choose a bucket from another account**

**S3 Bucket name (required)**  
config-bucket-808865497406 Prefix (optional) /AWSLogs/808865497406/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](#)

Cancel **Next**

### 1.5 Review the settings and click **Confirm**

The screenshot shows the AWS Config console during the 'Review' step of a configuration rule setup. The left sidebar indicates 'Step 3 Review' is the current step. The main content area is divided into sections: 'General settings' and 'Delivery method'. Under 'General settings', the 'Recording strategy' is set to 'Record all current and future resource types supported in this region, excluding globally recorded resource types.' The 'Resource types to record' section has a link to 'See list of recorded resource types'. The 'AWS Config role' is set to 'AWSServiceRoleForConfig'. Under 'Delivery method', the 'S3 bucket name' is 'config-bucket-554936332221'. At the bottom, there is a section for 'AWS Config rules (0)'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Confirm'. The 'Confirm' button is highlighted with a red box and a mouse cursor is clicking on it.

aws Services Search [Alt+S] N. Virginia odf\_user\_1058469 @ 5549-3633-222

Step 2  
Rules

Step 3  
**Review**

**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

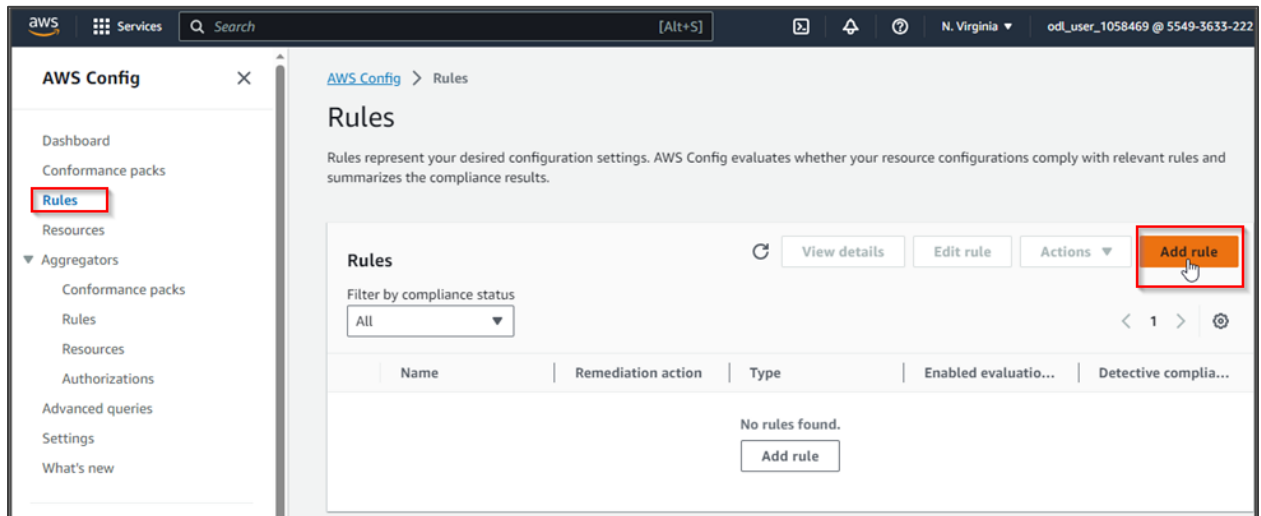
► AWS Config rules (0)

Cancel Previous **Confirm**

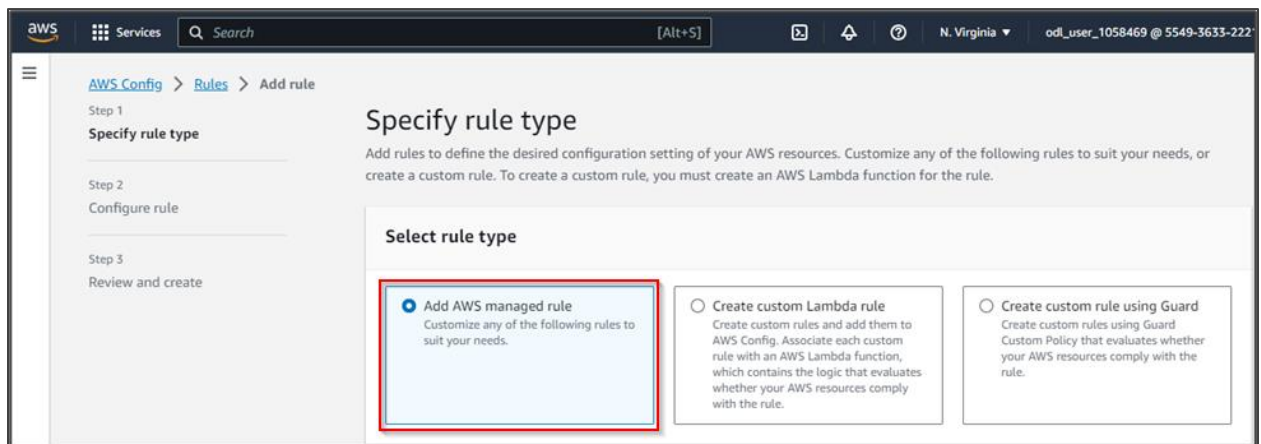
The set up for AWS Config is completed.

## Step 2: Create rules in AWS Config

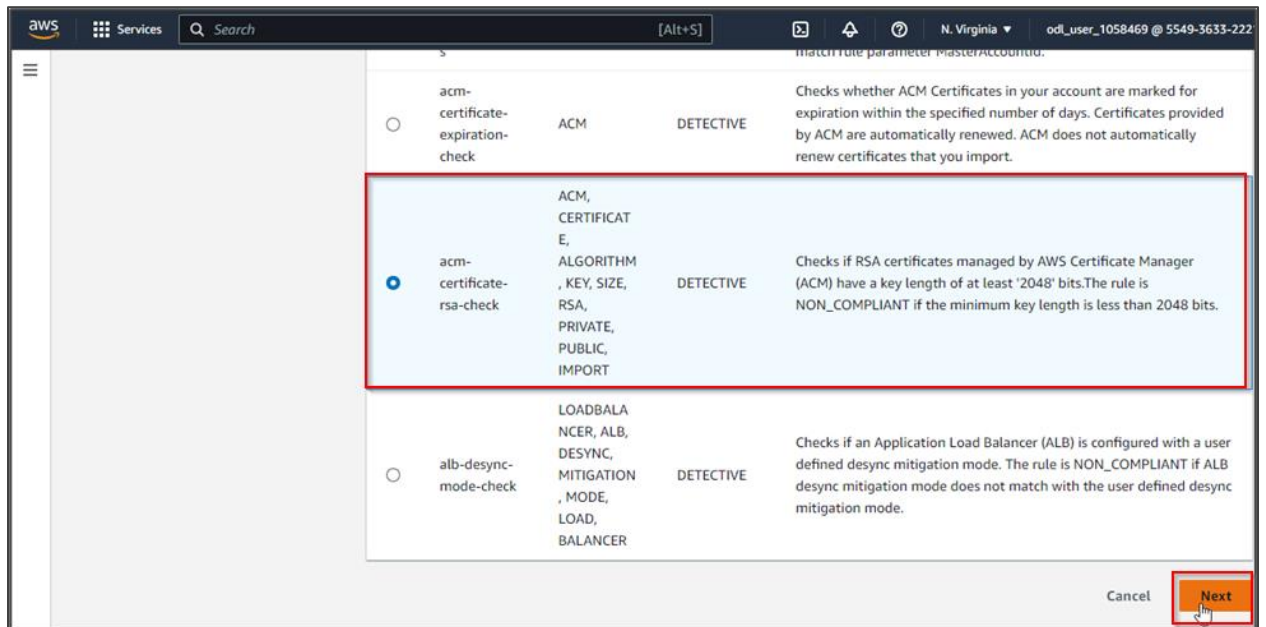
2.1 In the AWS Config dashboard, select **Rules** and then click **Add rule**



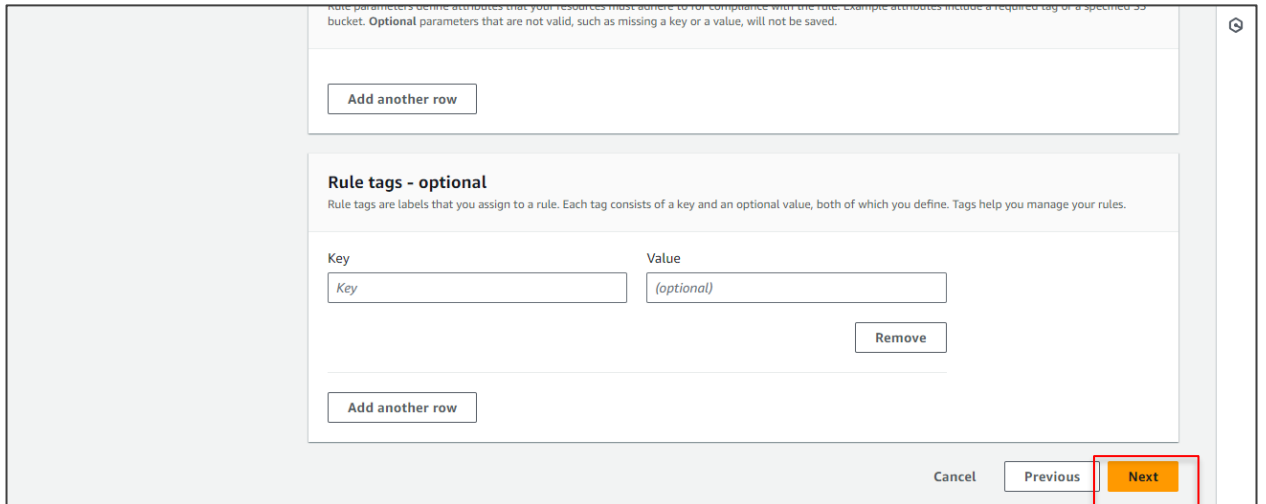
2.2 In the **Specify rule type** page, select **Add AWS managed rule** under the **Select rule type** section

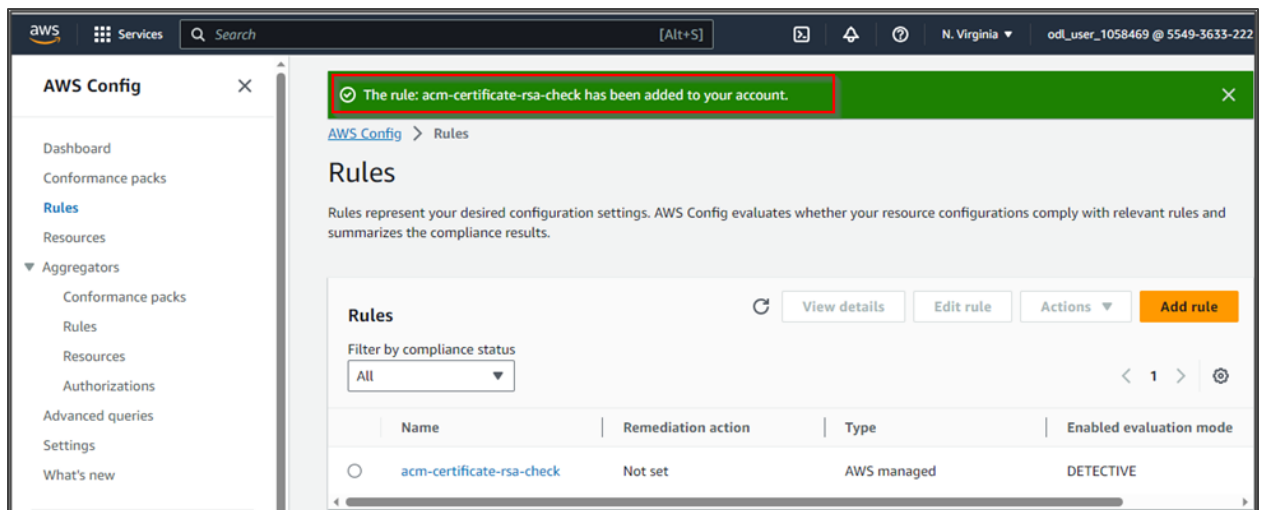


## 2.3 Select the rule as shown below and click **Next**



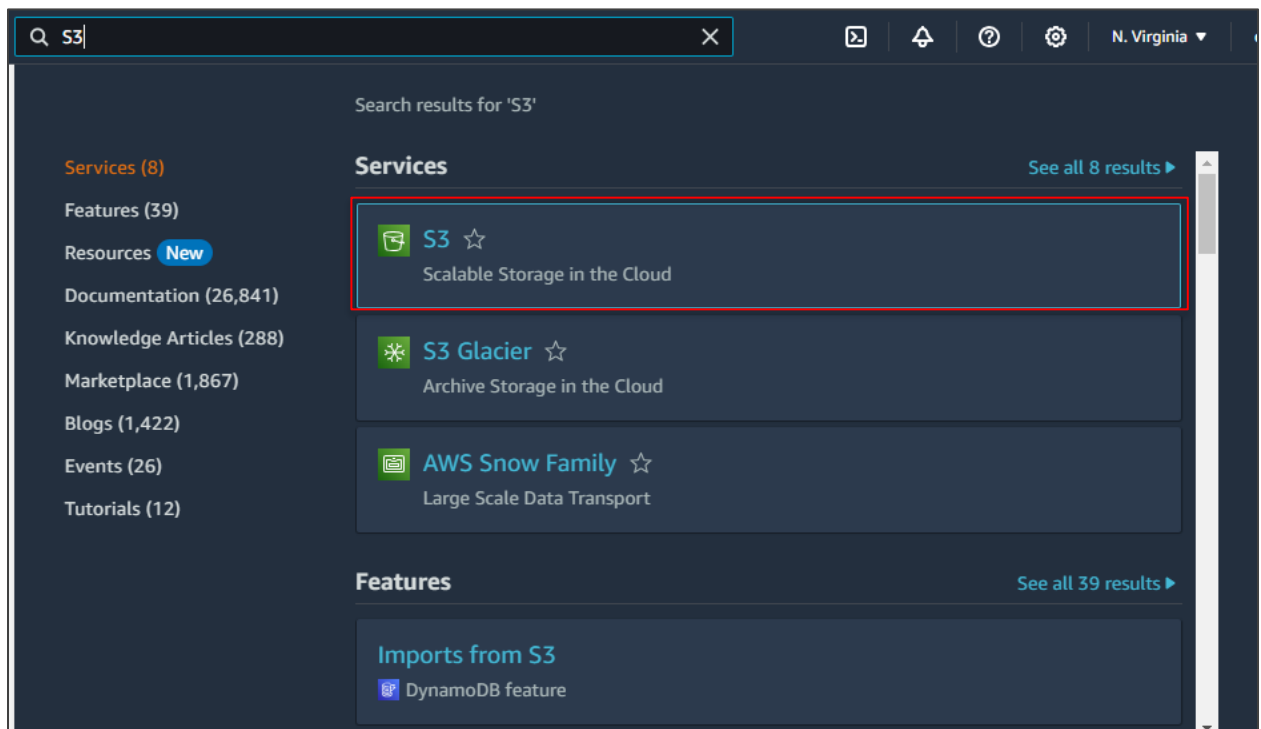
## 2.4 Scroll down and click on **Next**

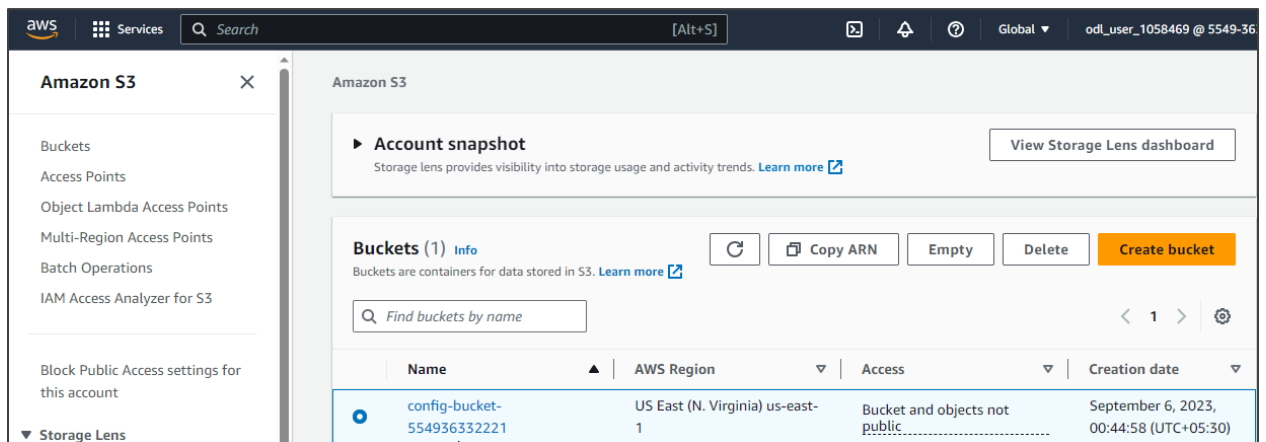




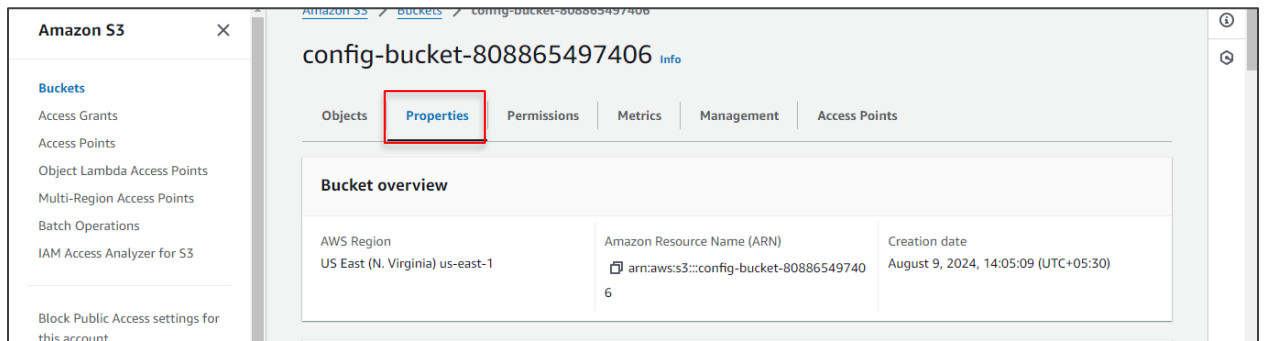
The rule is created successfully.

- 2.5 Navigate to the **S3** service, open the **Buckets** dashboard, and select the **config** bucket that is created automatically after the AWS Config setup

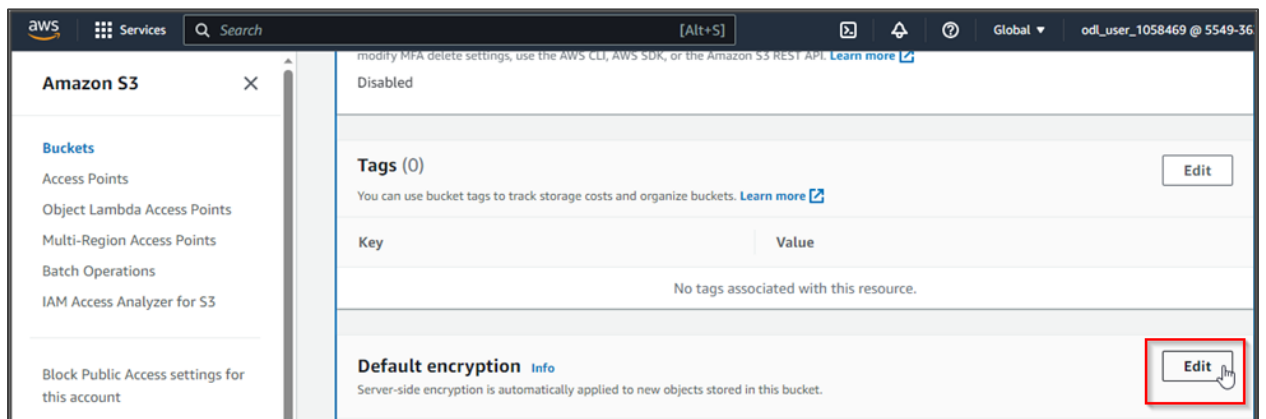




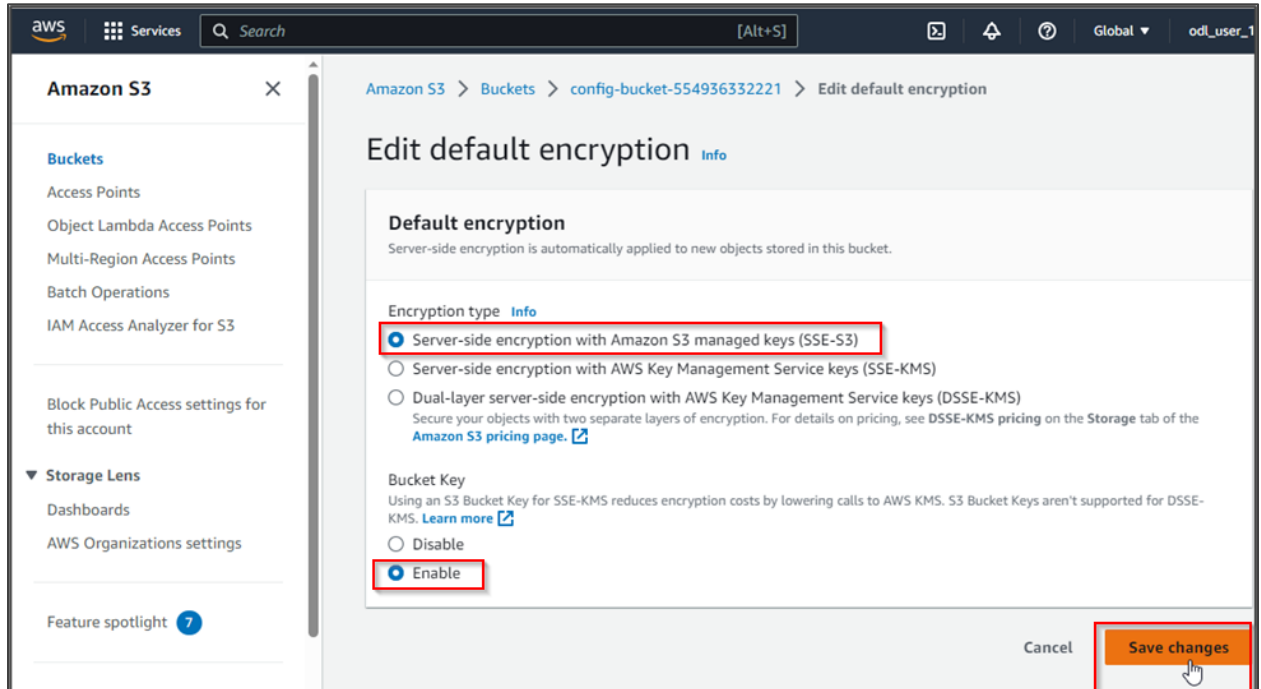
## 2.6 Click on Properties



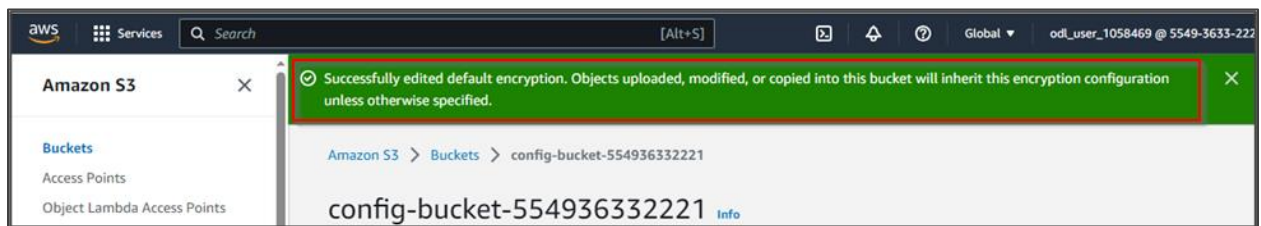
## 2.7 Scroll down and click on Edit under the Default encryption section



2.8 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**

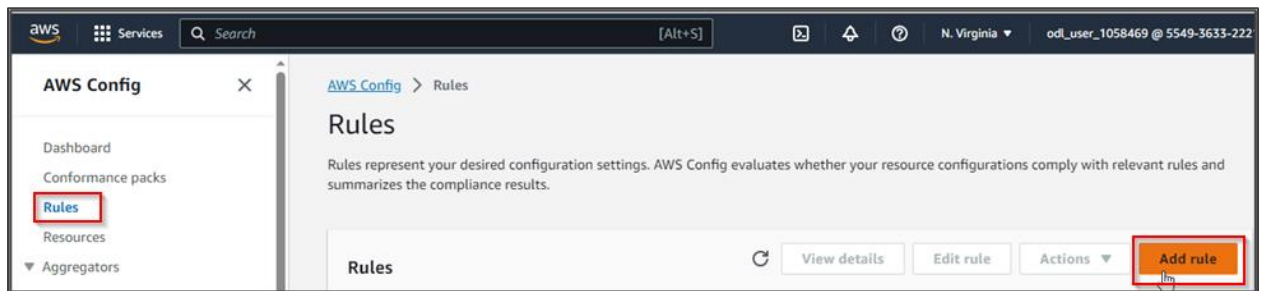


The default encryption is updated successfully.

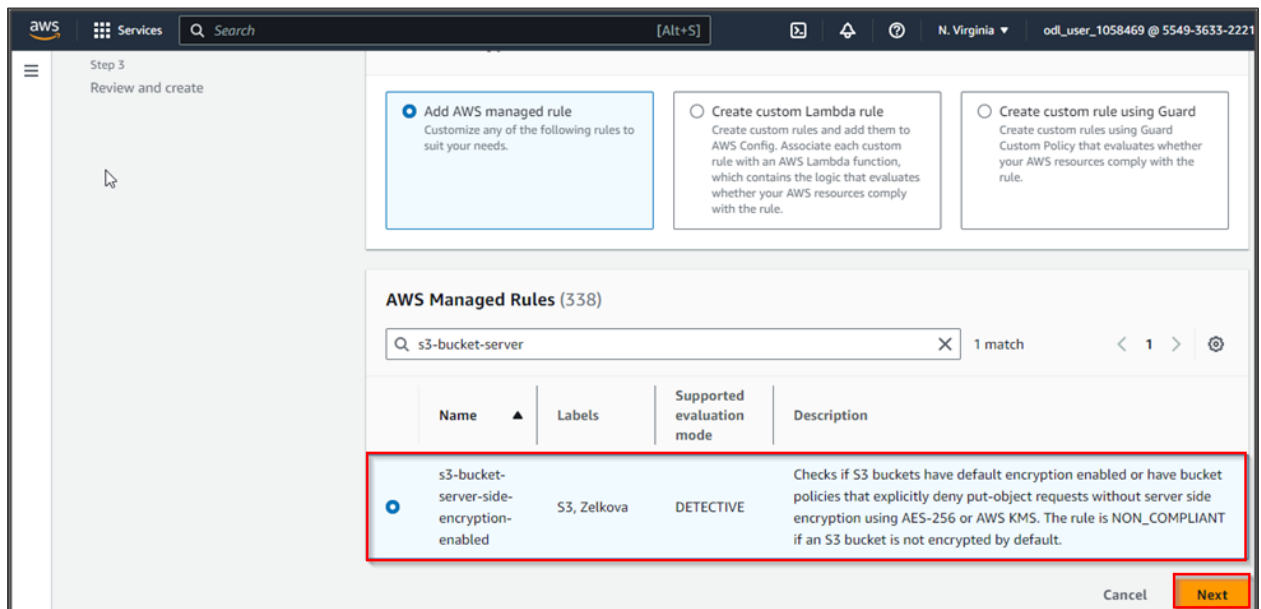




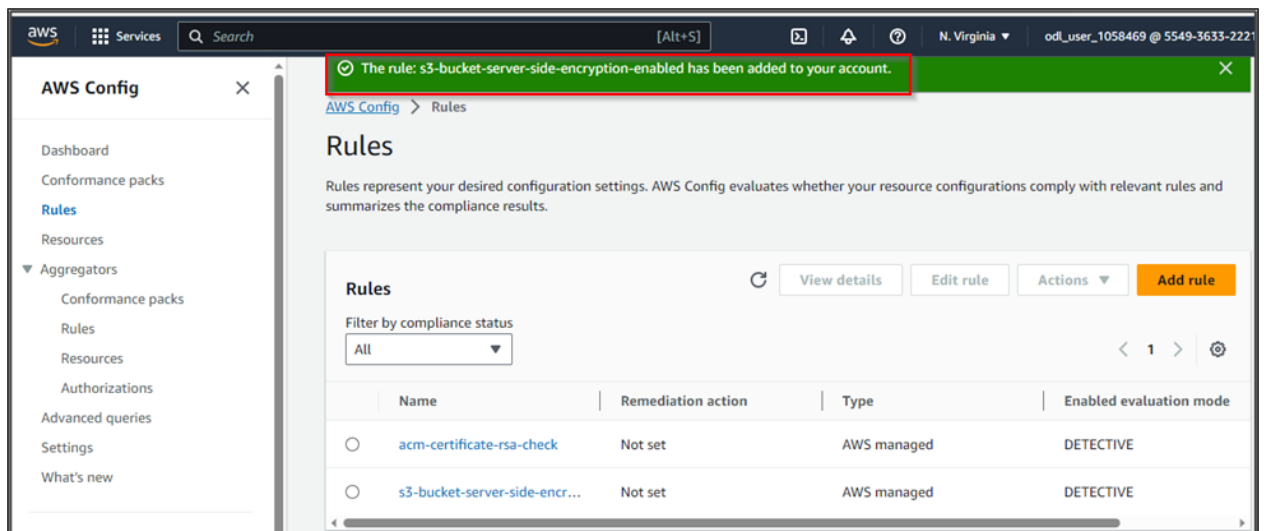
2.9 Navigate back to the **Rules** tab in the AWS Config dashboard and click **Add rule** to create another rule



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



The rule is created successfully.



By following these steps, you have successfully configured AWS Config and create rules in it to enable compliance monitoring in the AWS environment.