**Lesson 7 Demo 8**

**AWS Config S3 bucket encryption compliance**

**Objectives:** To config an S3 bucket encryption compliance in AWS

**Tools required:** AWS workspace

**Prerequisites:** AWS account

**Steps to be followed:**

1. Setting up the AWS Config
2. Creating rules in AWS Config Console

**Step** **1:** **Setting up the AWS Config**

1. Users need to sign in to the **AWS Management Console** and open the AWS Config console at **https://console.aws.amazon.com/config/** as shown in the image.

Graphical user interface, application

Description automatically generated

1. The **AWS Config console** page appears as follows if this is the first time opening  AWS Config in a new region.

Graphical user interface, website

Description automatically generated

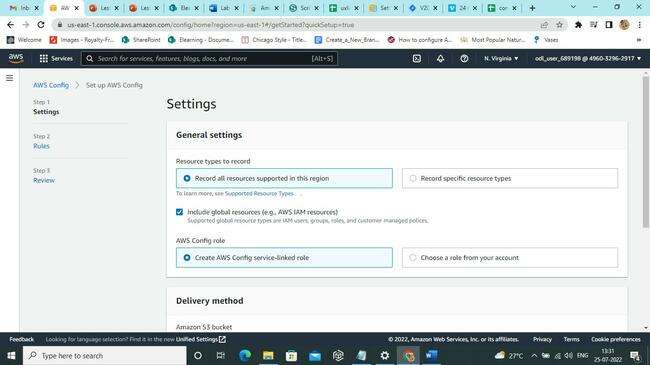
1. To launch AWS Config based on AWS best practices, select **1-click setup**. To complete the subsequent steps on their own, users may alternatively select **Get started**.

Graphical user interface, website

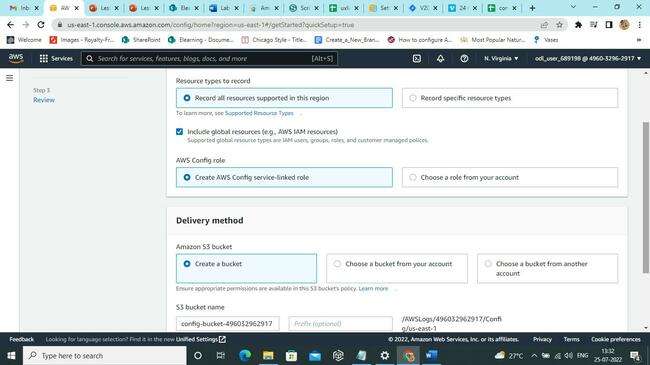
Description automatically generated

1. Enter each resource type users want AWS Config to record under Resource types to record on the Settings page. These resource kinds include customized, third-party, and AWS resources.

1.4.1 Select **Record all resources supported in this region** , **Include global resources(e.g, AWS IAM resources)** and **Create AWS Config service-linked role**.



1. Enter the account ID to select a role from the account or an existing **AWS Config service-linked role** for AWS Config. AWS Config predefines service-linked roles that contain all the permissions needed for a service to call other AWS services.



1. Select the **Amazon S3 bucket** where AWS Config transmits configuration history and configuration snapshot files under the **Delivery method**:

A screenshot of a computer

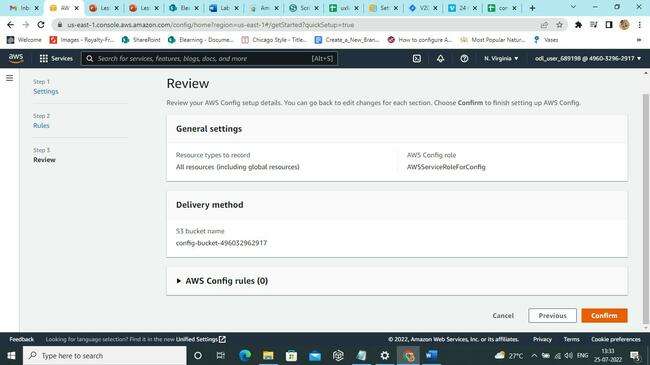
Description automatically generated

1. Select **Next** if users are installing **AWS Config** in a region that supports rules.

A screenshot of a computer

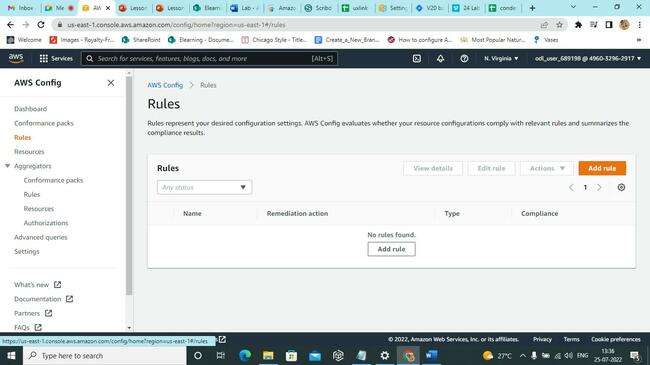
Description automatically generated

1. Next, select **Confirm.**

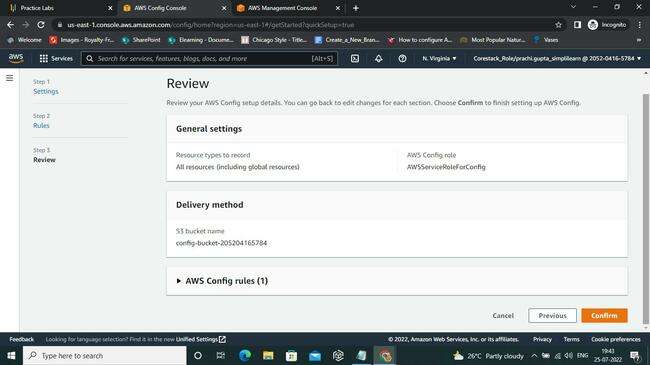


**Step 2: Creating rules in AWS Config Console**

1. On the **Rules page**, select the rules as required. After the account is set up, users may modify these rules and add other restrictions:

****

1. On the **Review** screen, verify the setup information and click **Confirm**.

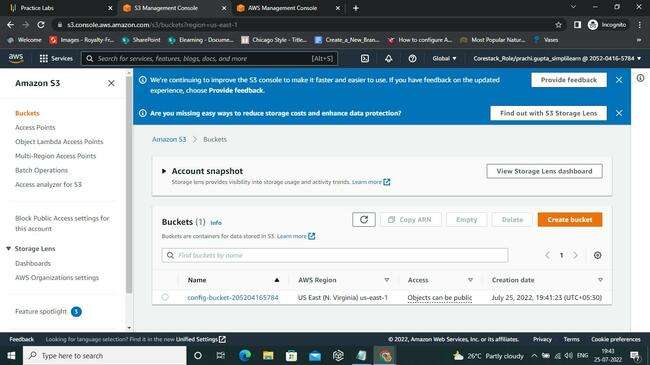


1. The rules are shown on the **Rules** page along with a table of their current compliance levels. As long as **AWS Config** is assessing the resources against the rule, the outcome for each rule is evaluated.

Graphical user interface, text

Description automatically generated

1. Open **Amazon S3 console.**



1. On clicking the **Properties** we see the following.

A screenshot of a computer

Description automatically generated

1. In **Edit default Encryption** change the **Server-side encryption** to **Enable** and click on **Save changes**.

A screenshot of a computer

Description automatically generated

1. Once the changes are saved, we find this message appears above the screen.

Graphical user interface, text, website

Description automatically generated

1. On moving again to the AWS Config dashboard, we check the existing rules and their properties.

A screenshot of a computer

Description automatically generated

1. We can either create a new rule or edit the properties. Here we will show a new rule creation allowing the **s3 encryption enabling feature**.

A screenshot of a computer

Description automatically generated

2.10 Now we can select **s3-bucket-server-side-encryption-enabled** from **AWS Managed Rules.** Once the rule is selected, click on **Next.**

A screenshot of a computer

Description automatically generated

2.11 On **Review and create**,click **Confirm**.

A screenshot of a computer

Description automatically generated

2.12 Select **s3-bucket-logging-enabled** from the Rule name drop-down menu on the Rules page, and then click Add Rule to include it in the rule list. (If the rule is already in place, pick it from the list of rules and then click Edit.)

Graphical user interface, application

Description automatically generated

2.13 To automatically repair non-compliant resources, choose Yes in the Auto remediation section.

Graphical user interface, text, application, email

Description automatically generated

2.14 Enter the settings for the necessary parameters in the **Parameters** section, such as **AutomationAssumeRole**, the Grantee information needed to carry out the remediation action, and the Target bucket needed to store logs.

Graphical user interface, table

Description automatically generated

2.15 Select **Save**. Resources that don't comply with the "**s3-bucket-logging-enabled**" AWS Config rule can now be automatically fixed. In the **Action** status column, it confirms that the corrective action was carried out.

Graphical user interface

Description automatically generated

2.16 To configure S3 Bucket Server Side Encryption Enabled Auto Remediation. The "**s3-bucket-server-side-encryption-enabled**" AWS Config rule verifies that either S3 default encryption is enabled or that put-object requests without server-side encryption are expressly forbidden by the S3 bucket policy in S3 bucket.

Graphical user interface, text

Description automatically generated

2.17 Select Edit on the Rules page

2.18 Select AWS-EnableS3BucketEncryption from the Remedial action list in the area labeled "Choose a remediation action."

2.19 (The AWS SSM Automation document AWS-EnableS3BucketEncryption provides server-side encryption on an S3 bucket using SSM Automation.)

2.20 To automatically repair non-compliant resources, choose **Yes** in the Auto remediation section.

Graphical user interface, text, application, email

Description automatically generated

2.21 Enter the settings for AutomationAssumeRole and the SSE algorithm needed to carry out the corrective action in the Parameters section.

Graphical user interface, text, application

Description automatically generated

2.22 Select **Save.** Resources that don't comply with the "**s3-bucket-server-side-encryption-enabled**" AWS Config rule can now be automatically fixed. In the Action status column, it confirms that the corrective action was carried out.

Graphical user interface

Description automatically generated

2.23 AWS Config rules "s3-bucket-public-read-prohibited" and "s3-bucket-public-write-prohibited" can be used to restrict public read and write access to an AWS S3 bucket.

Graphical user interface, text, application, email

Description automatically generated