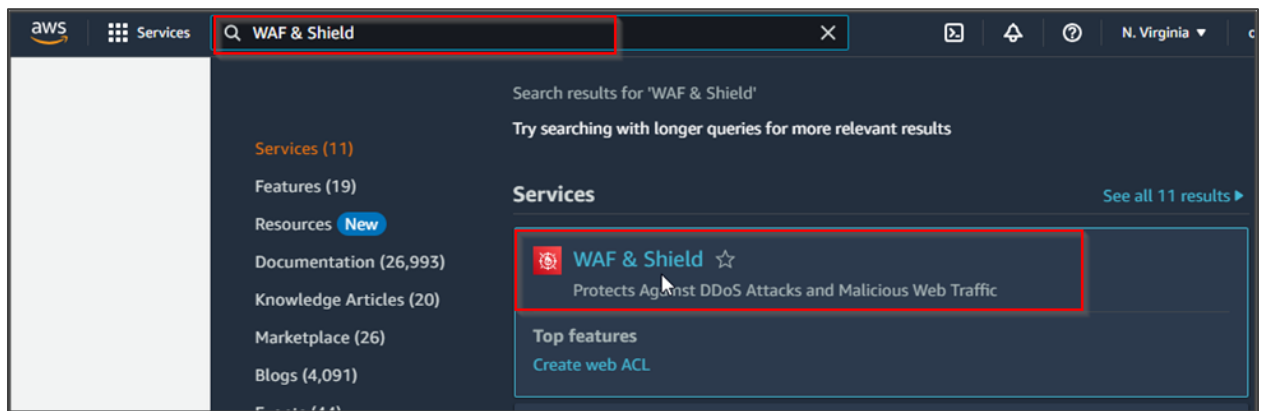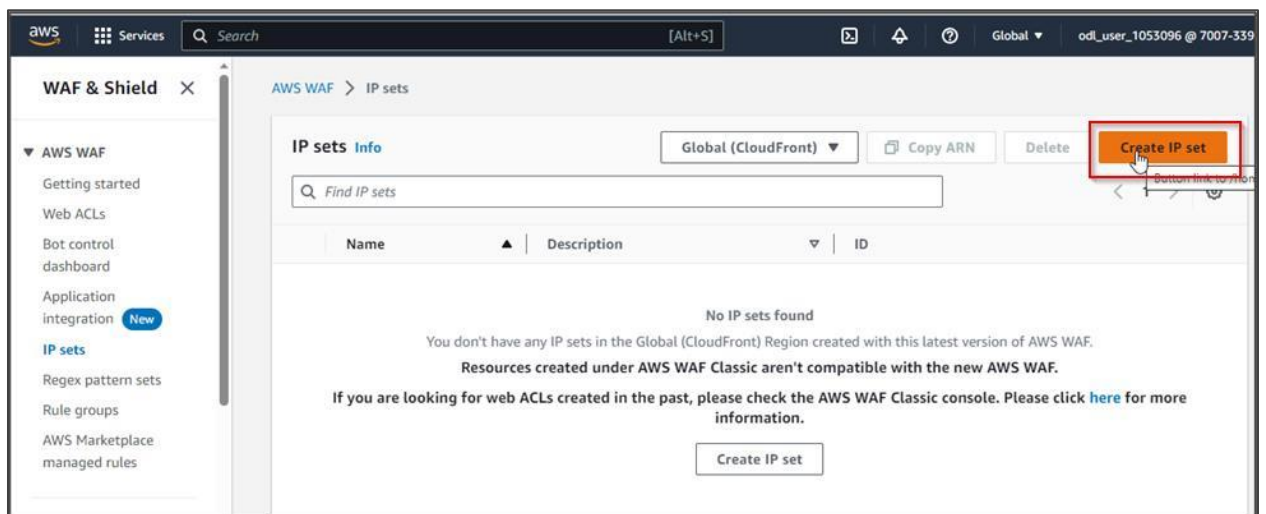.

AWS WAF

Step 1: Create an IP set

1.1 Navigate to the AWS Management Console, search for and select **WAF & Shield**

.

1.2 In the WAF & Shield dashboard, select **IP sets** from the left pane

1.3 Click on **Create IP set**

.

1.4 Provide a name to the IP set, choose the **Region** as **Global (CloudFront),** select the IP version as **IPv4**, add the IP address as **8.8.8.8/32**, and then click on **Create IP set**
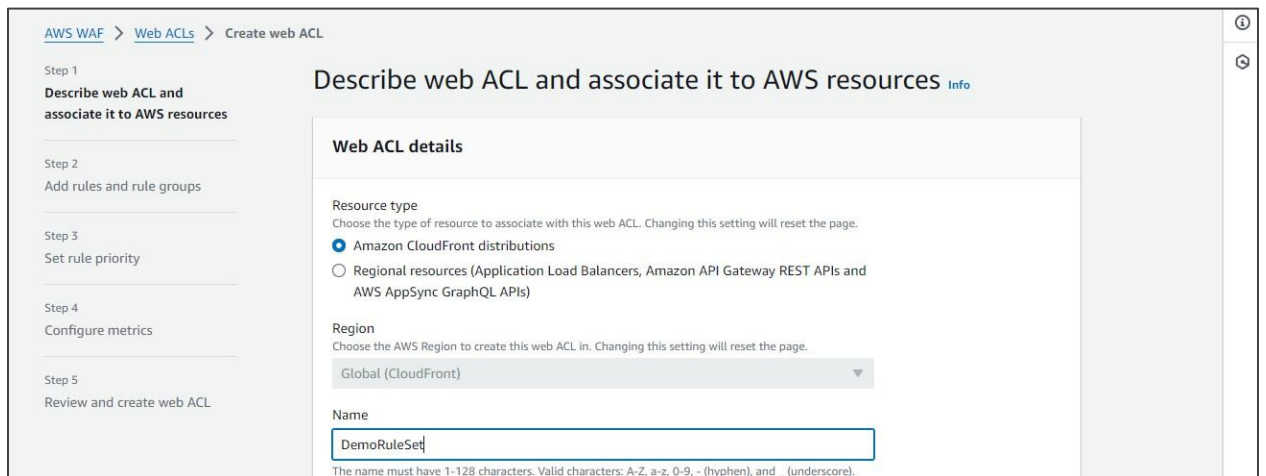

The IP set has been created successfully.

.

Step 2: Create Web ACL

2.1 Navigate to the WAF & Shield dashboard, select **Web ACLs** from the left pane, and then click on **Create web ACL**
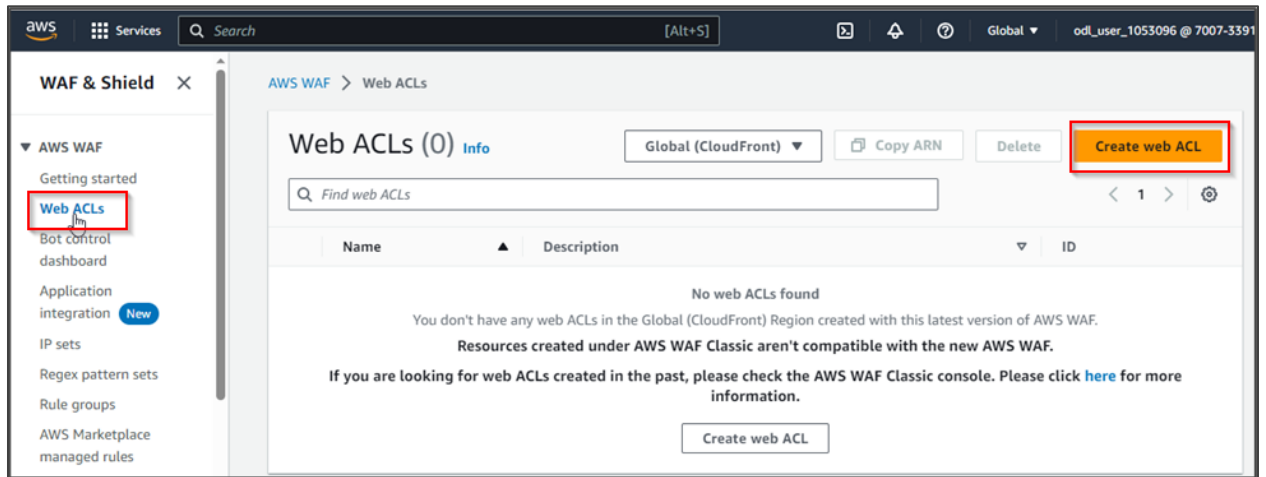
2.2 Choose the **Resource type** as **Amazon CloudFront distributions**, provide a name, scroll down and click on **Next**

.

2.3 In the **Add rules and rule groups** page, click on **Add rules** and select **Add managed rule groups**

.

2.4 Select the options in **AWS managed rule groups** as shown:

.

2.5 In the **Core rule set** option, click on **Edit**, and then select **Override to Count** from the drop-down menu in the **Override all rule actions** option

2.6 Click on **Save rule**

.

2.7 Scroll down and click on **Next**

2.8 In the **Set rule priority** page, click on **Next**

.

2.9 In the **Configure metrics** page, choose **Enable sampled requests** in the **Request sampling options**, and then click on **Next**

2.10 Review the settings, scroll down and click on **Create web ACL**
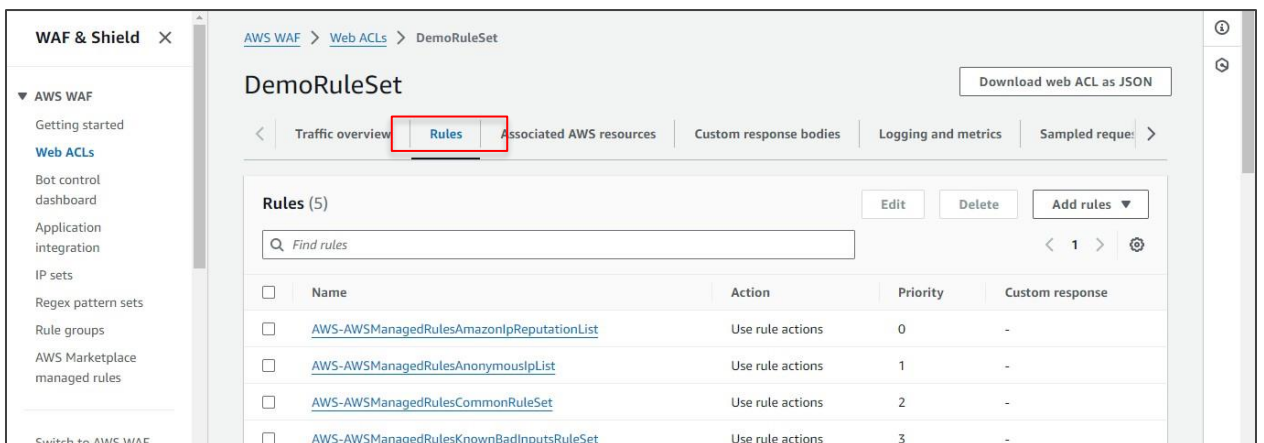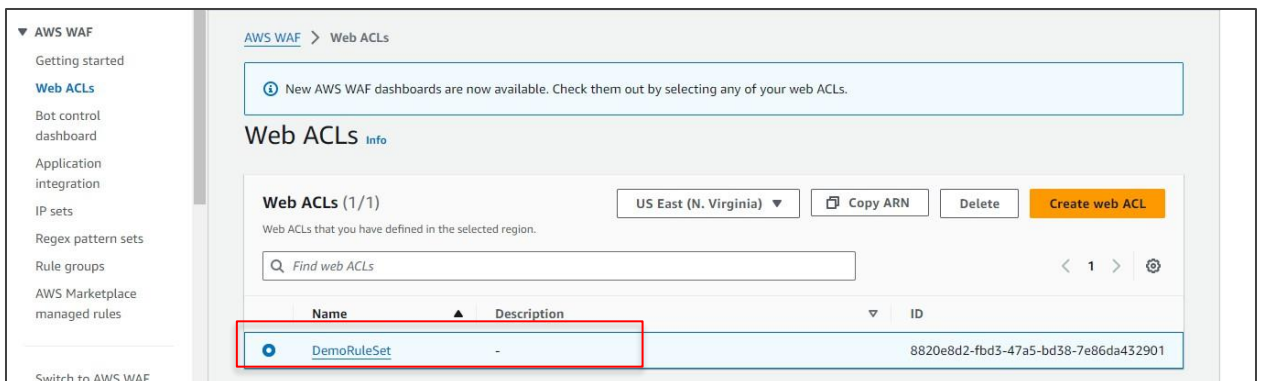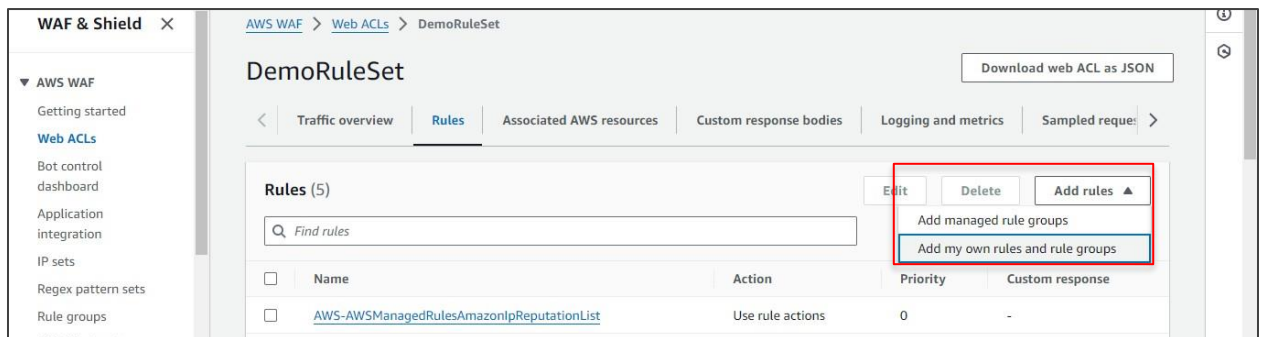
.

The Web ACL has been successfully created.

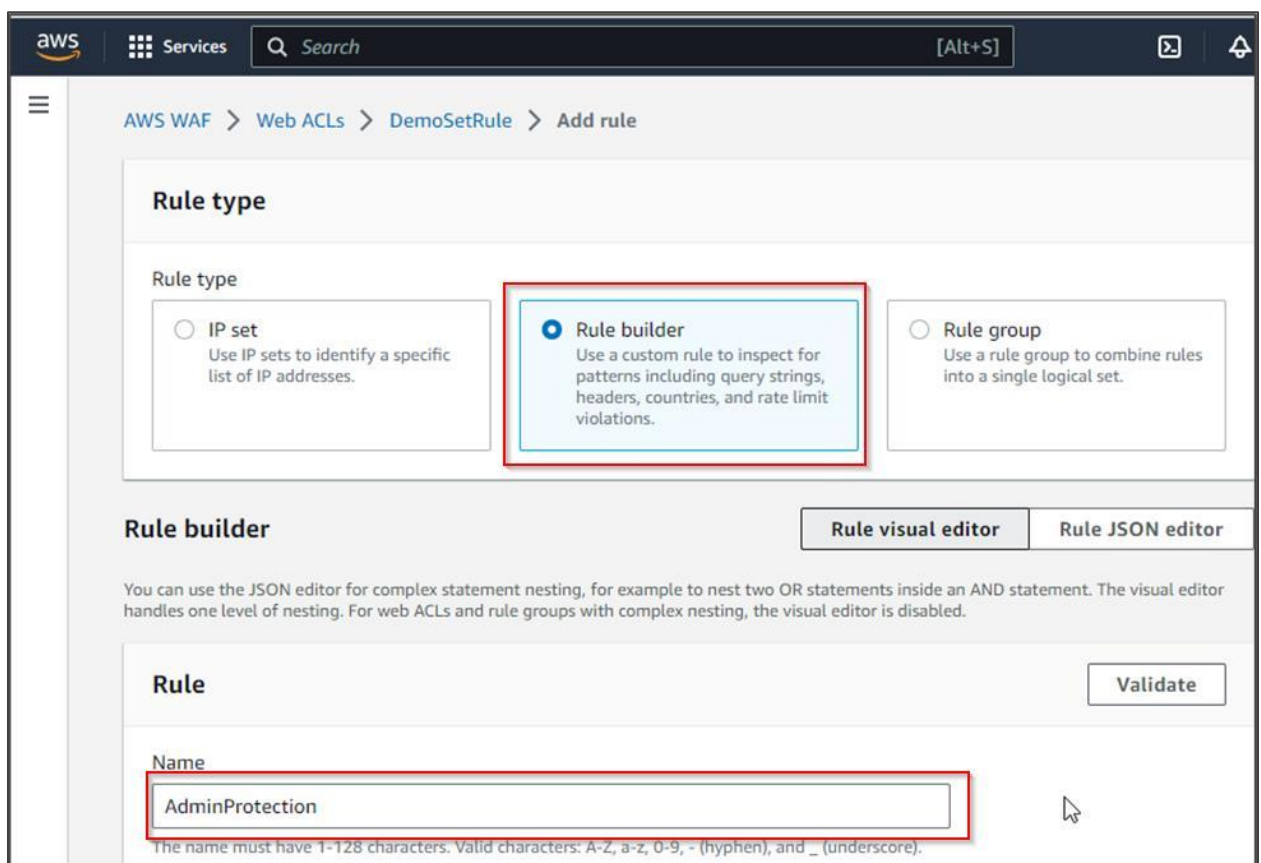## Step 3: Create a custom rule in Web ACL

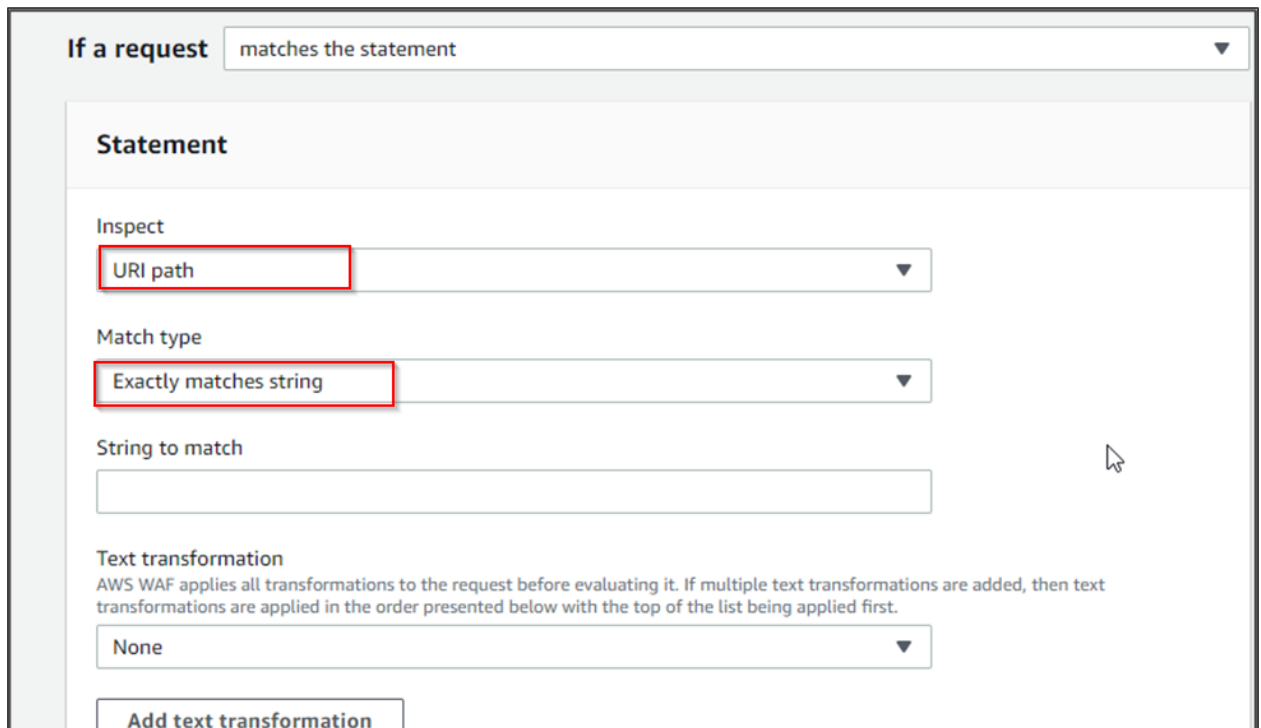1.1 Select the Web ACL that you created and then click on **Rules**

.

1.2 Click on **Add rules** and select **Add my own rule and rule groups**

1.3 Select **Rule builder** in the **Rule type** option and provide a name to the rule

.

1.4 In the **Statement** page, choose **URI path** from the drop-down in the **Inspect** option and select **Exactly matches string** from the drop-down in the **Match type** option
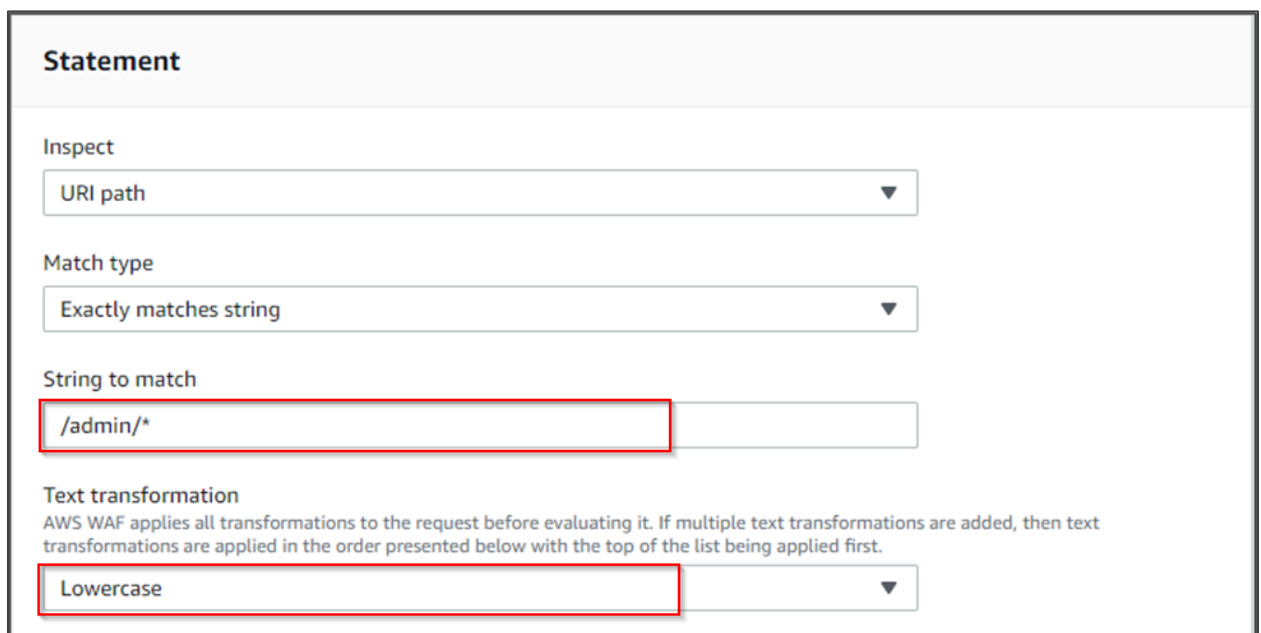
1.5 Enter **/admin/*** in the **String to match** option and choose **Lowercase** in the **Text transformation** option

.

1.6 In the **Action** option, choose **Block**, and then click on **Add rule**

.

1.7 Click on **Save**

The custom rule has been successfully added.

By following these steps, you have successfully configured AWS WAF to protect your web applications and APIs hosted on AWS environment.