How to integrate your application with AWS Config for security using AWS CLI

Step 1: Install AWS CLI

First, ensure you have AWS CLI installed on your machine. If you haven't you can install it by following the instruction on the AWS CLI documentation page.

Step 2: Configure AWS CLI

Next, configure your WS CLI with your credentials. You can do this by running the following command and entering your access key, secret key and default region:

Aws configure

Step 3 : Create an AWS Config Recorder

To start recording configuration changes, you need to create a recorder:

Aws configservice create-config-recorder –-config -recorder-name "MyConfigRecorder"

Step 4: Start the AWS Config Recorder

Aws configservice start-config-recorder –config-recorder-name “MyConfigRecorder”

Step 5: Create a Delivery Channel

AWS Config needs a delivery channel to send the configuration changes to an S3 bucket :

Aws configservice create-delivery-channel -name “MyDeliveryChannel” --s3-bucket-name “my-config-bucket”

Step 6 : Associate the Delivery Channel with the Recorder

Now, associate the delivery channel with the recorder:

Aws configservice put-config-recorder –config-recorder-name “MyConfigRecorder” –delivery-channel-configuration “MyDeliveryChannel”

Step 7: Enable AWS Config Rules

To enforce security policies, you can enable AWS Config rule:

Aws configservice put-confg-rule –-config-rule-name “MyConfigRule” –-config-rule-status “ENABLED”

Step 8: Verify Configuration
Finally verify that everything is set up correctly but checking the configuration:

Aws configservice describe-config-recorders

Aws configservice describe-delivery-channels

Aws configservice describ-config-rules