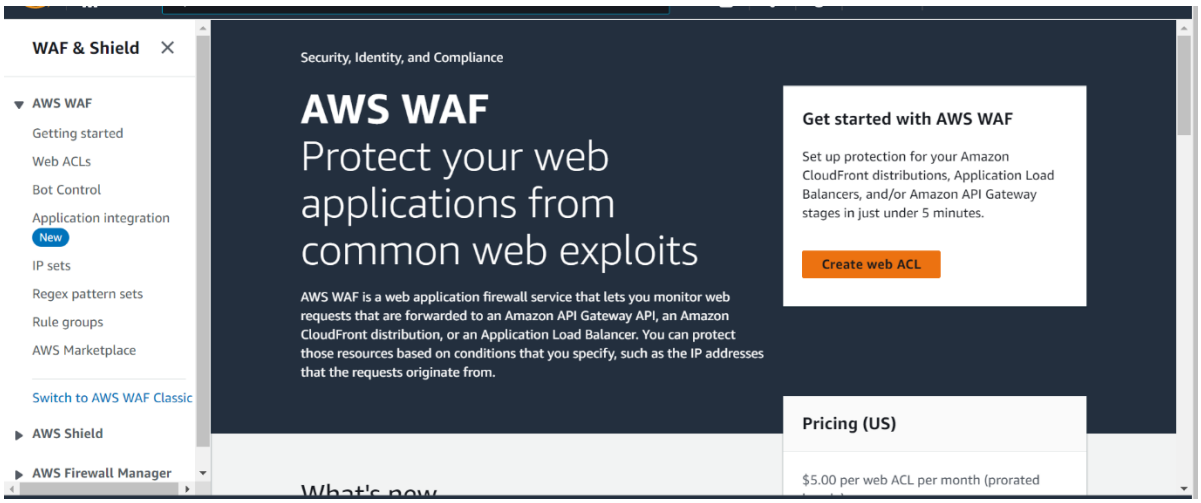
NIDHI SHARMA (BATCH-7)

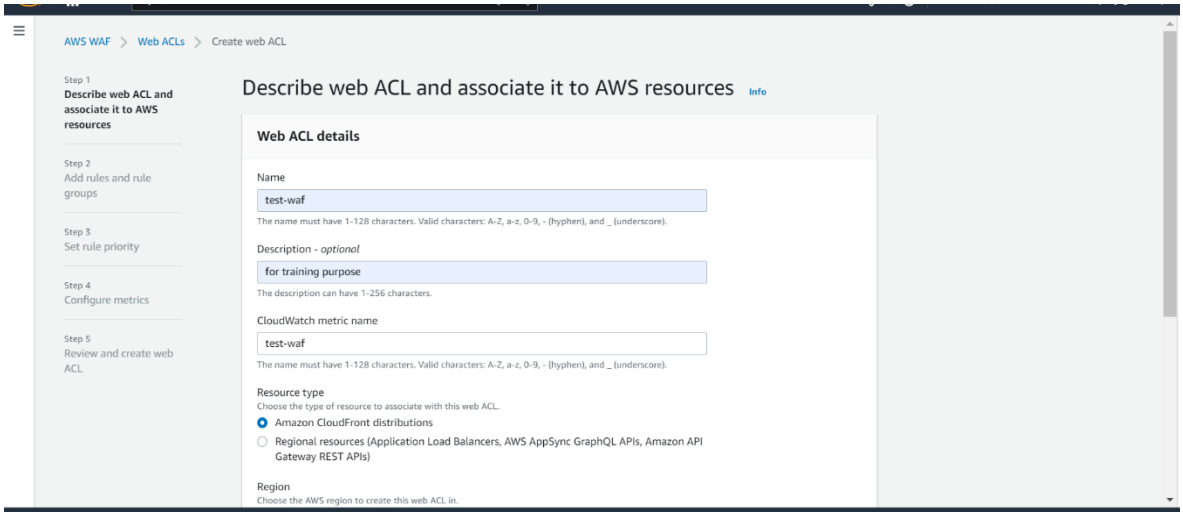
AWS APPLICATION WAF

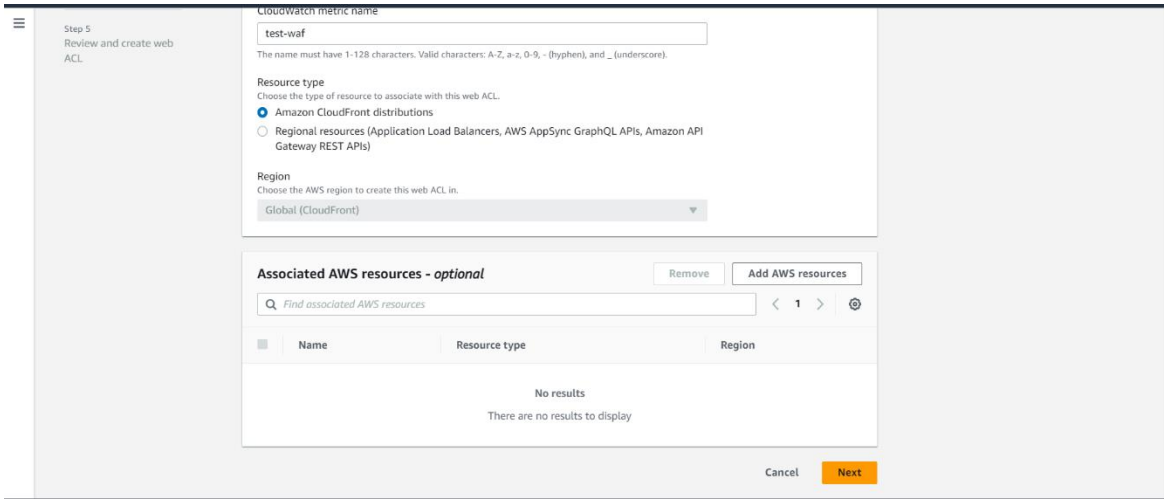
- **WAF AWS** monitors all the web incoming and outgoing requests that are forwarded to API Gateway, Amazon CloudFront, and Application Load Balancer. We will see how to get started with WAF and create web ACL in some steps.

- ✓ **Create web ACL:** First, sign-up for an AWS account, then go to AWS Console and search for Web Application Firewall. You will land on the WAF home page, and choose to **Create Web ACL**.

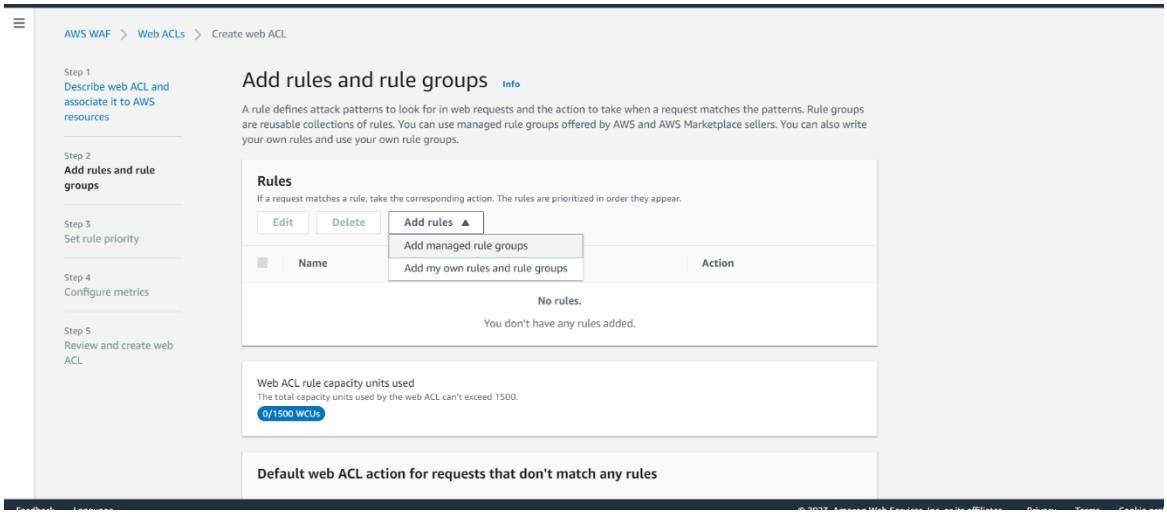


- ✓ **Give a Name:** Type the name you want to use to identify this web ACL. After that, enter Description if you want (optional) and then hit **Next.**

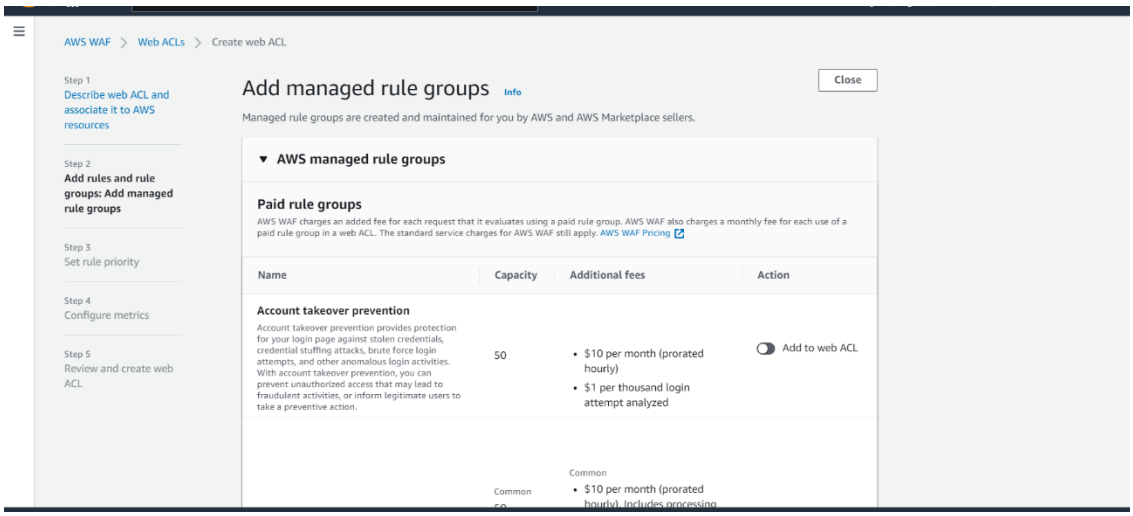




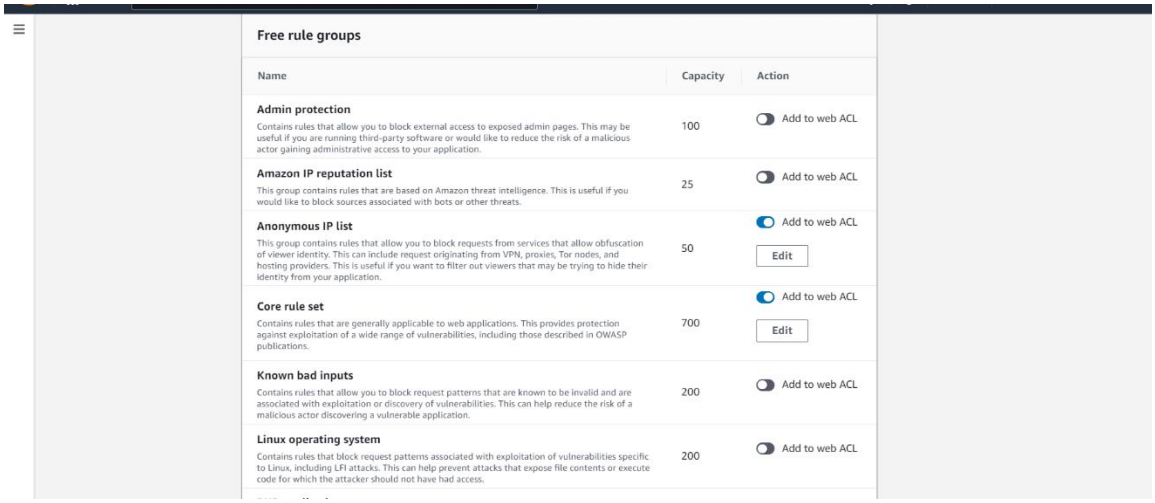
- ✓ **Add an AWS Managed Rules rule group:** In the next step, you need to add rules and rule groups. Click on **Add managed rule groups.** You will land on a new page to manage the ruling group.



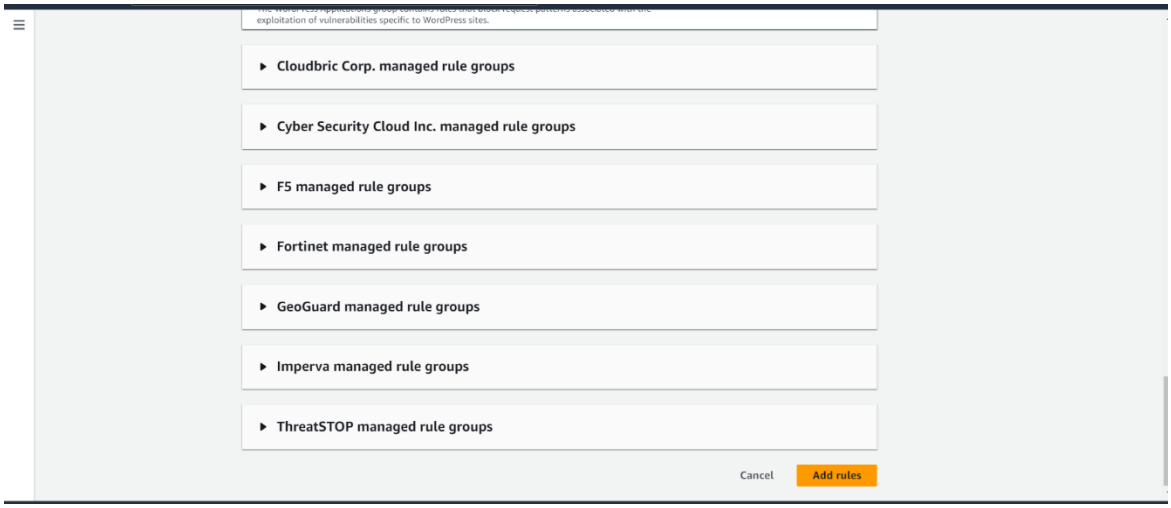
- ✓ AWS Managed Rules provides you with a collection of managed rule groups. The majority of these are free for Amazon WAF users. After adding managed rule group, choose to save the rule

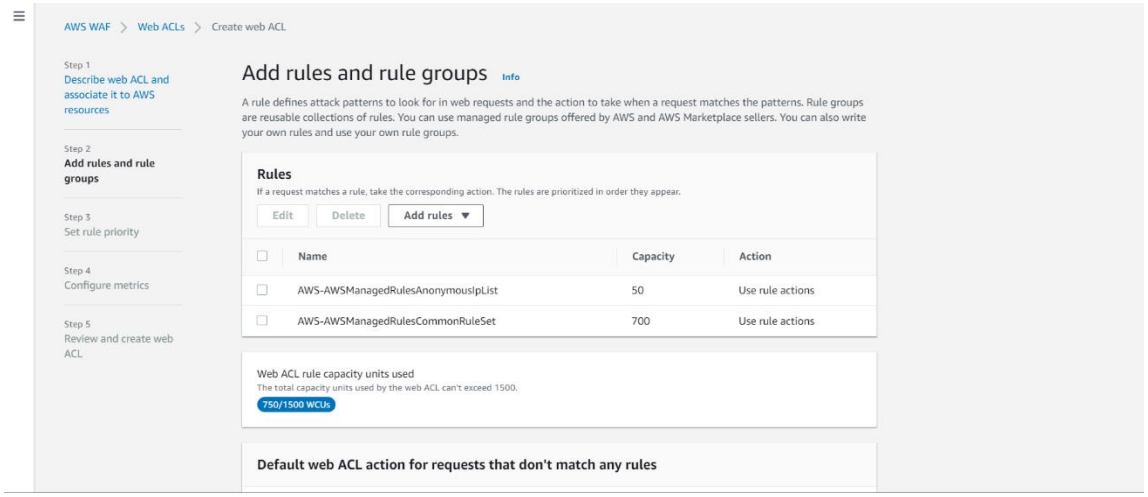


- ✓ The rules we're going to create will define the patterns we want to allow/block. We'll add 2 rules only.
  - ♦ **Regular rule:** This rule protects the application from SQL injection attacks. It will check if the URI path contains an SQL injection.
  - ♦ **Rate-based rule:** This rule blocks the requests made from the same IP address after they exceed a certain limit in a time period.

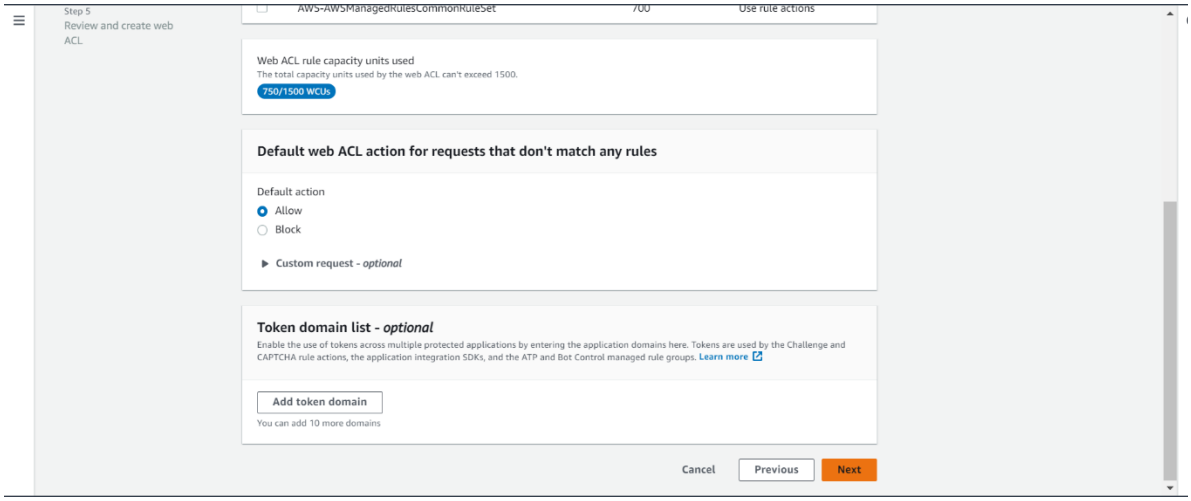


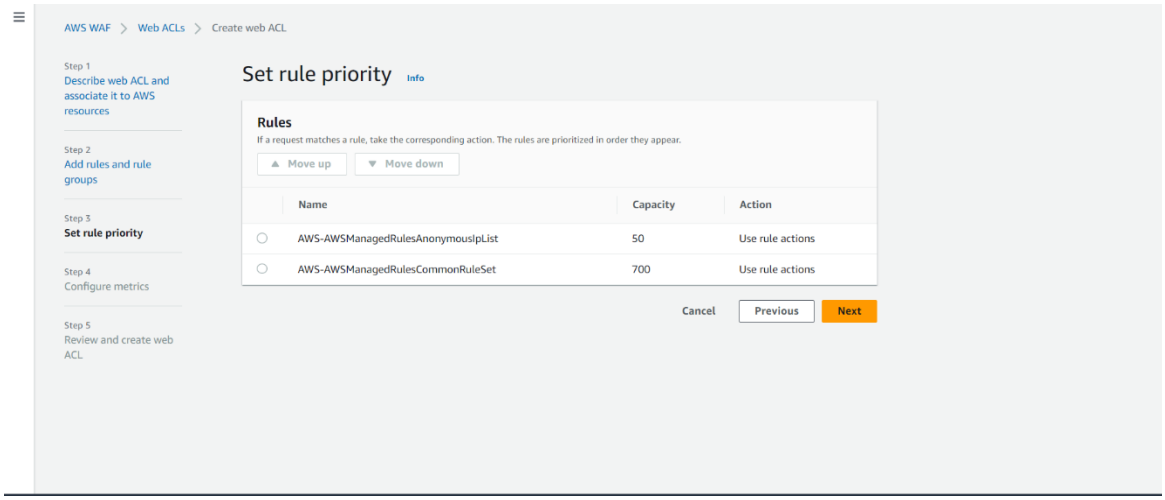
✓ Click on ADD RULES.



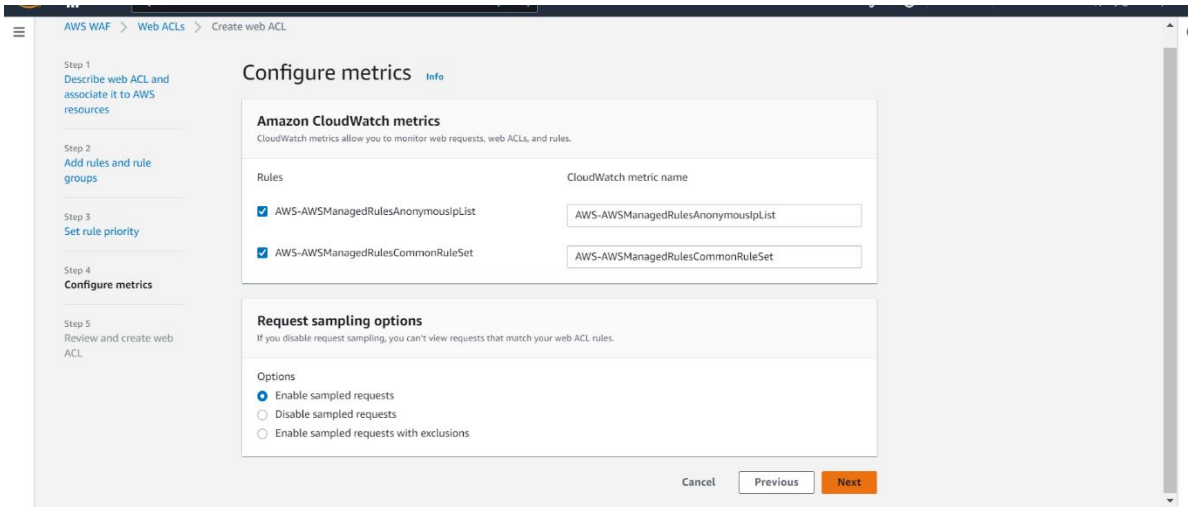


✓ After that, check the added rules and hit **Next**



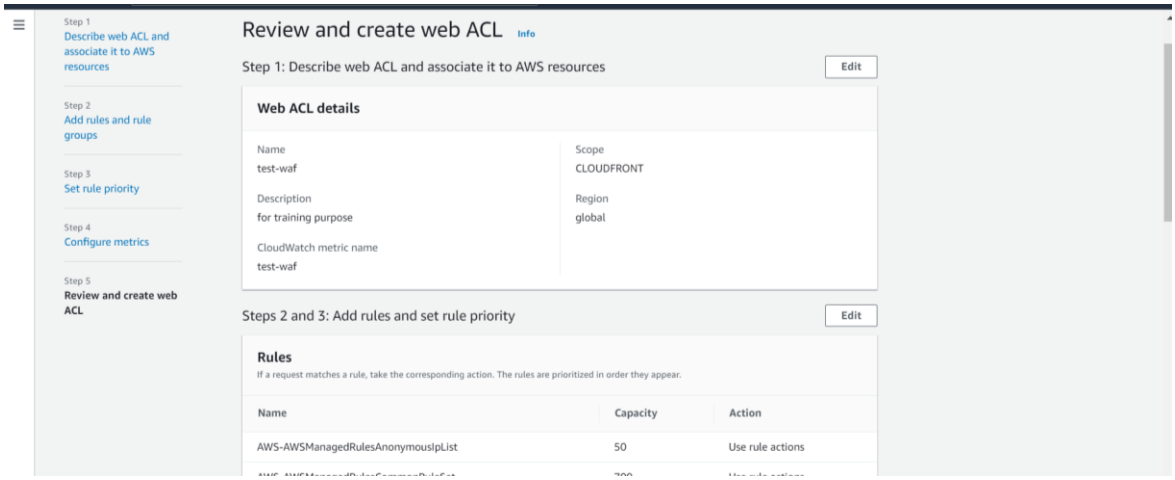


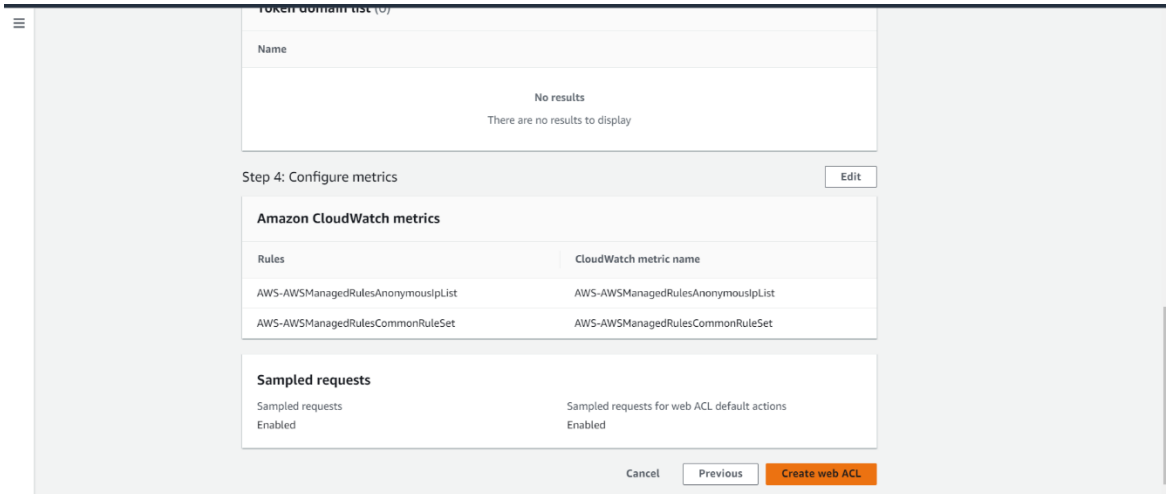
✓ Configure CloudWatch Metrics:

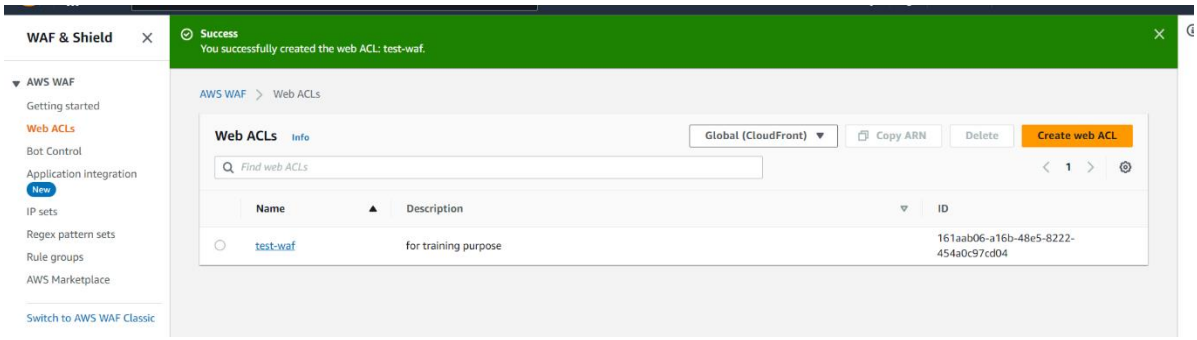


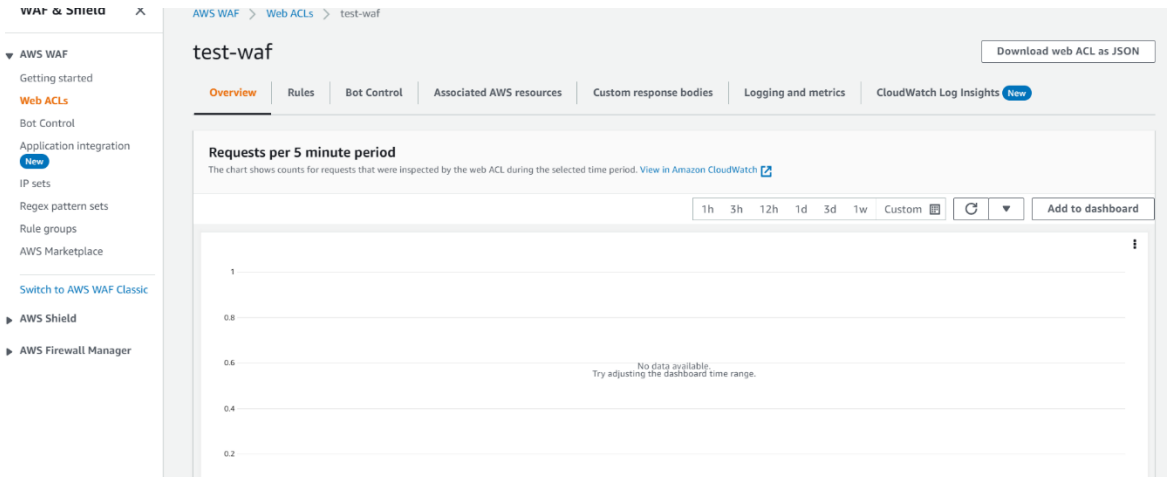
✓ **Review Web ACL Configuration:**

In the final step, check all the rules and managed groups and hit on create web ACL.

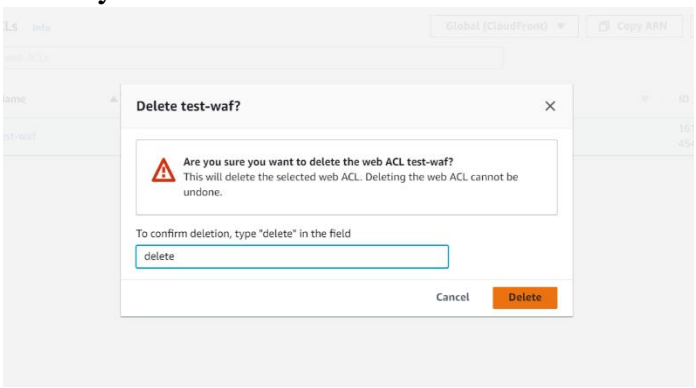








✓ **Once you done with the resources remember to delete them.**



END