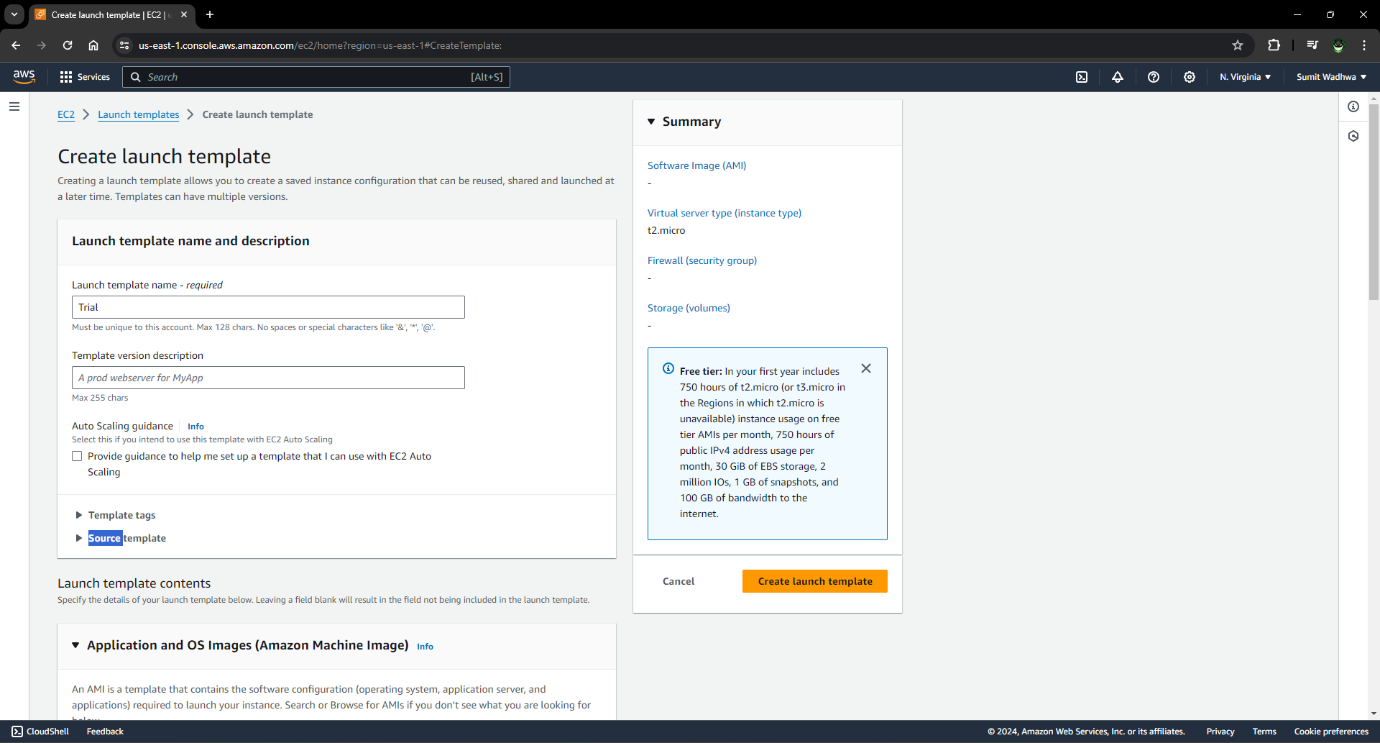
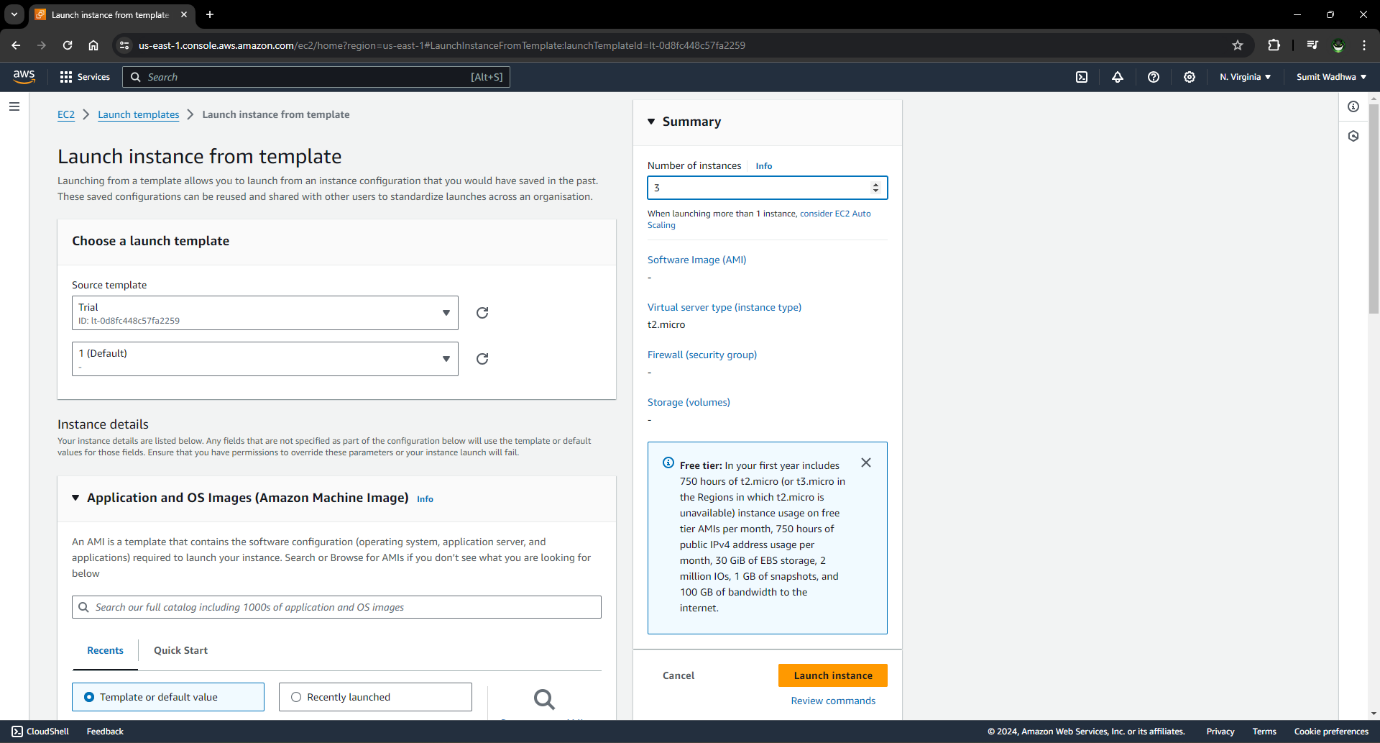


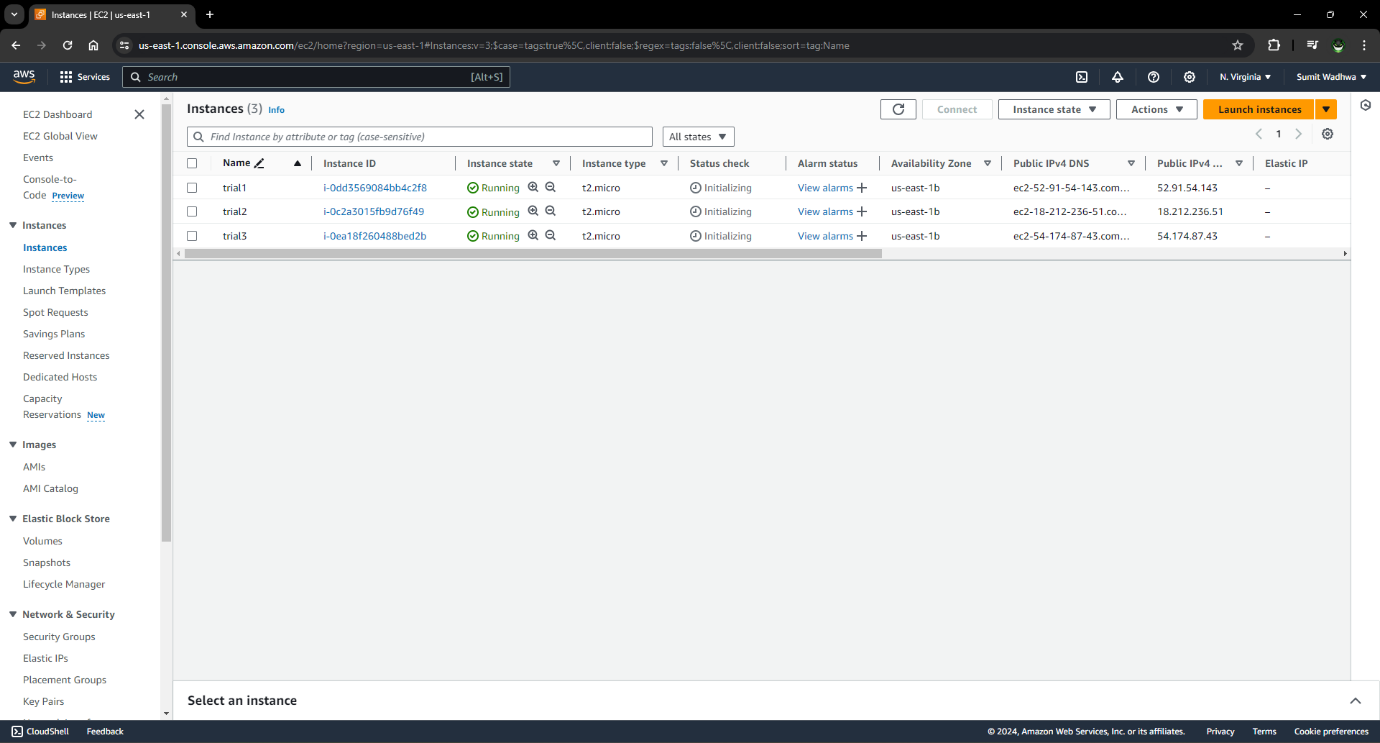
**Implementing AWS Web Application Firewall (WAF)**

Step 1: Create a launch template in EC2



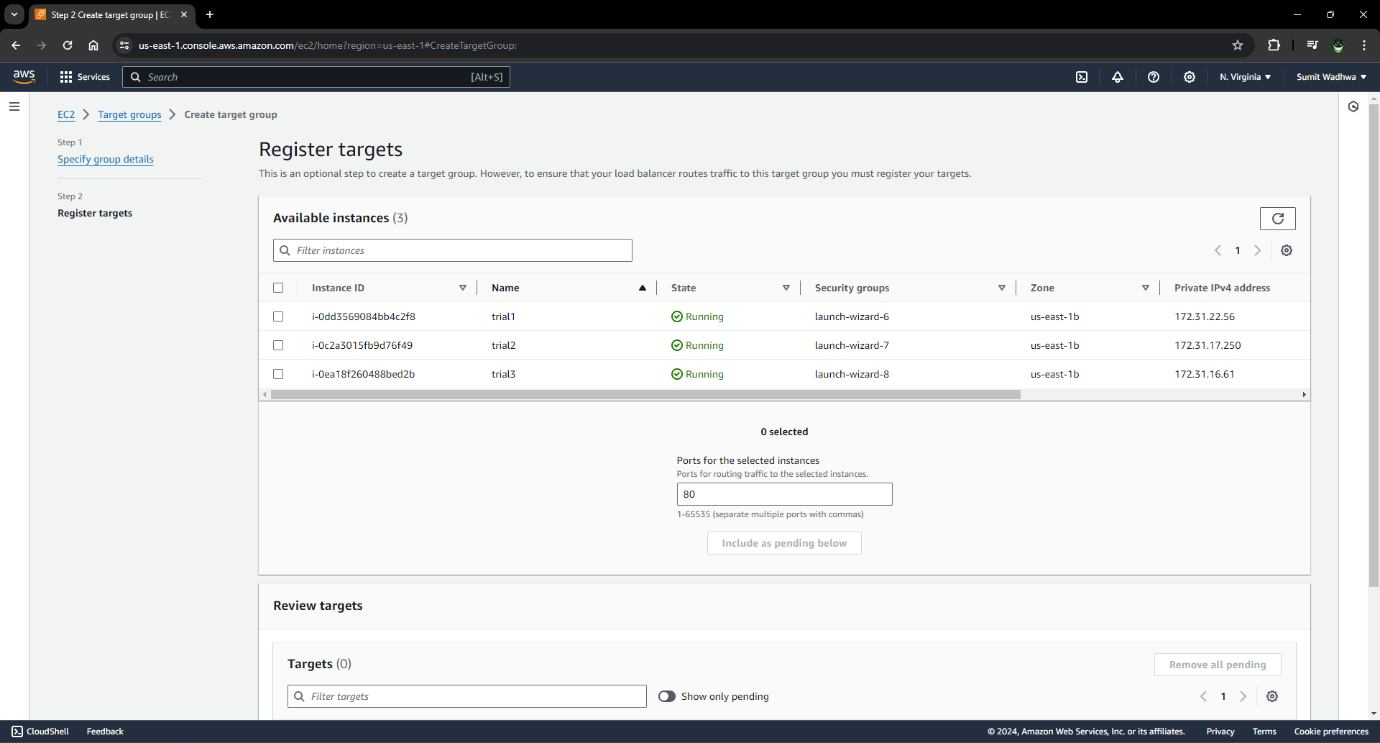
Step 2: Launch EC2 instance from launch template



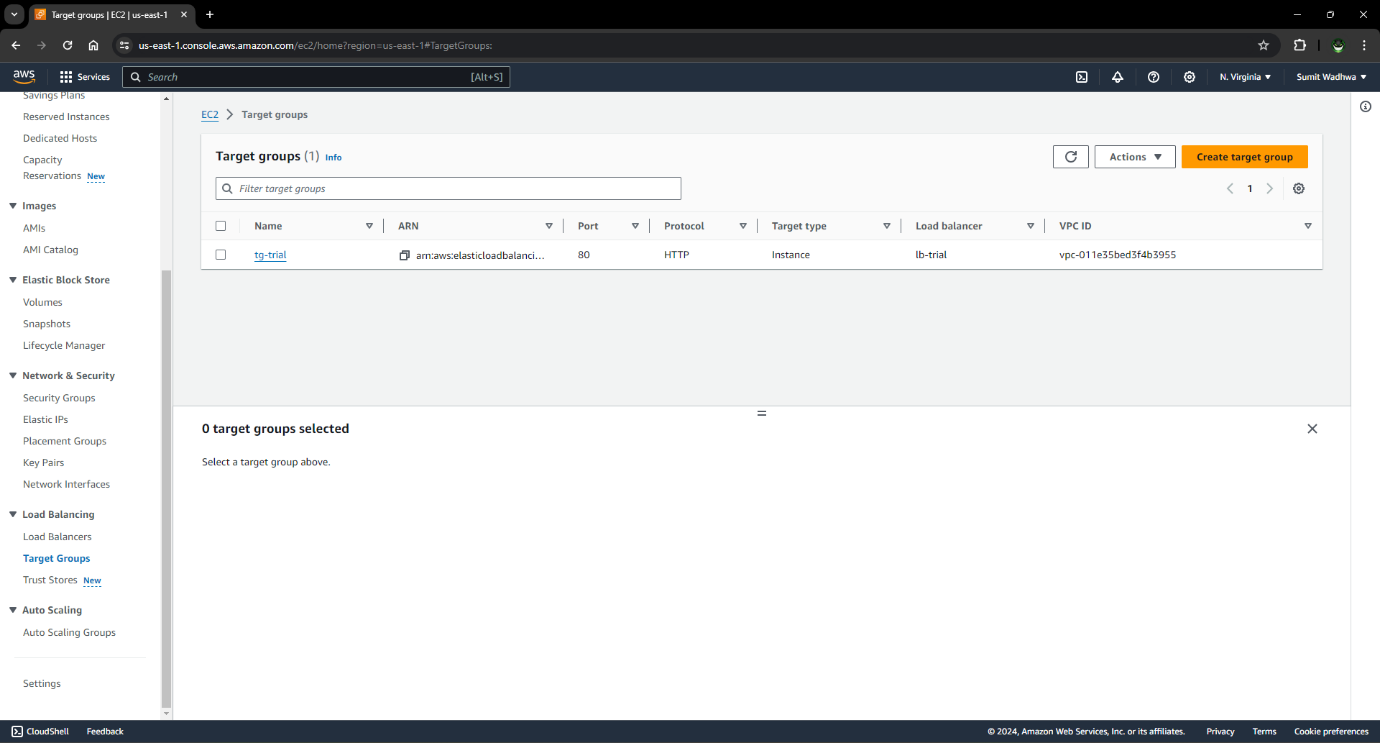


Step 3: Create a target group

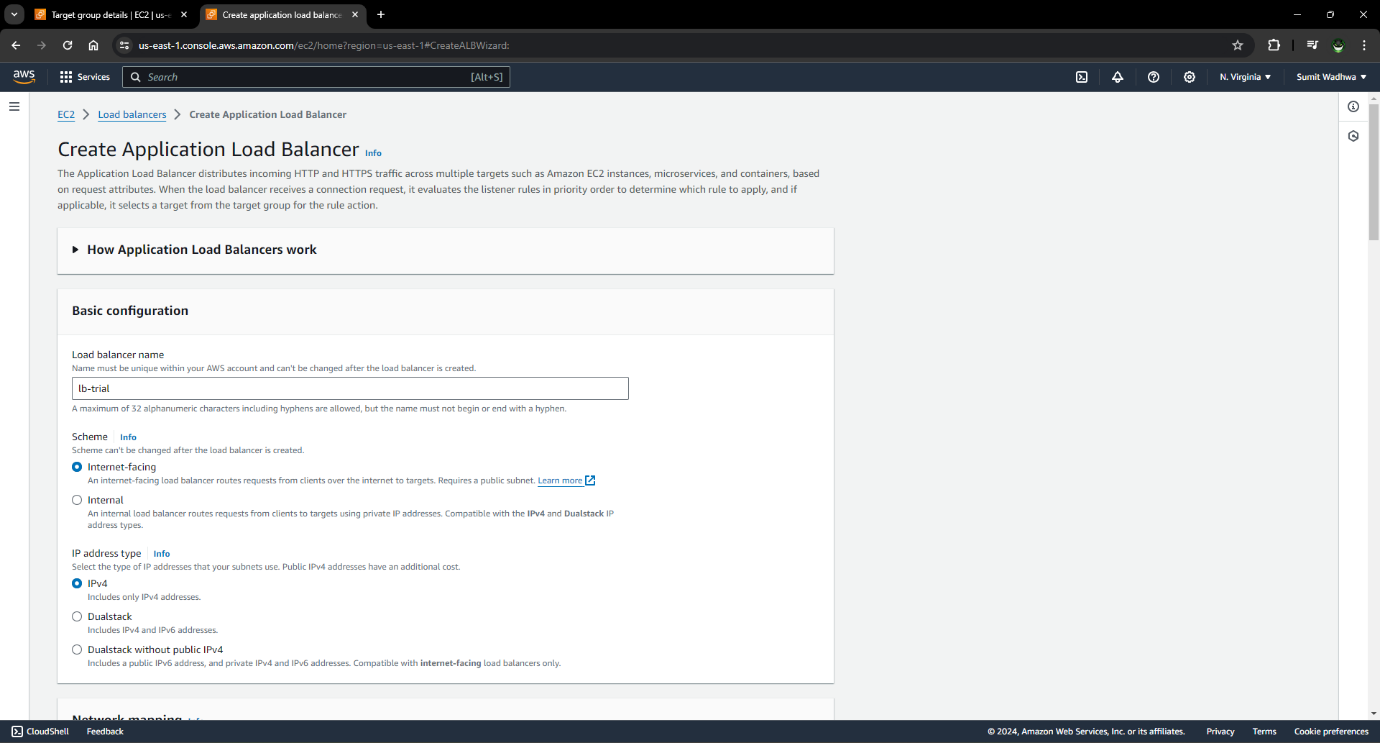
* Enter target group details



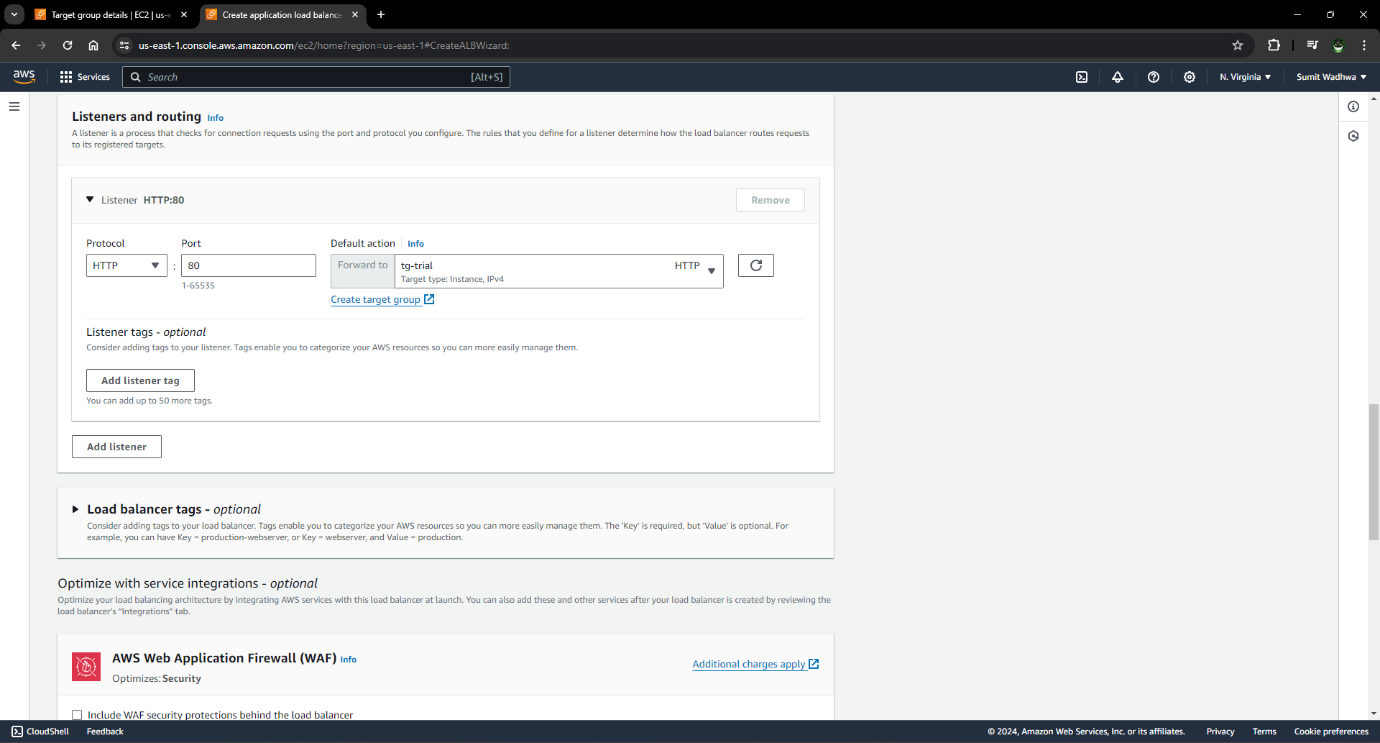
Step 4: Target group is created



Step 5: Create an Application Load Balancer

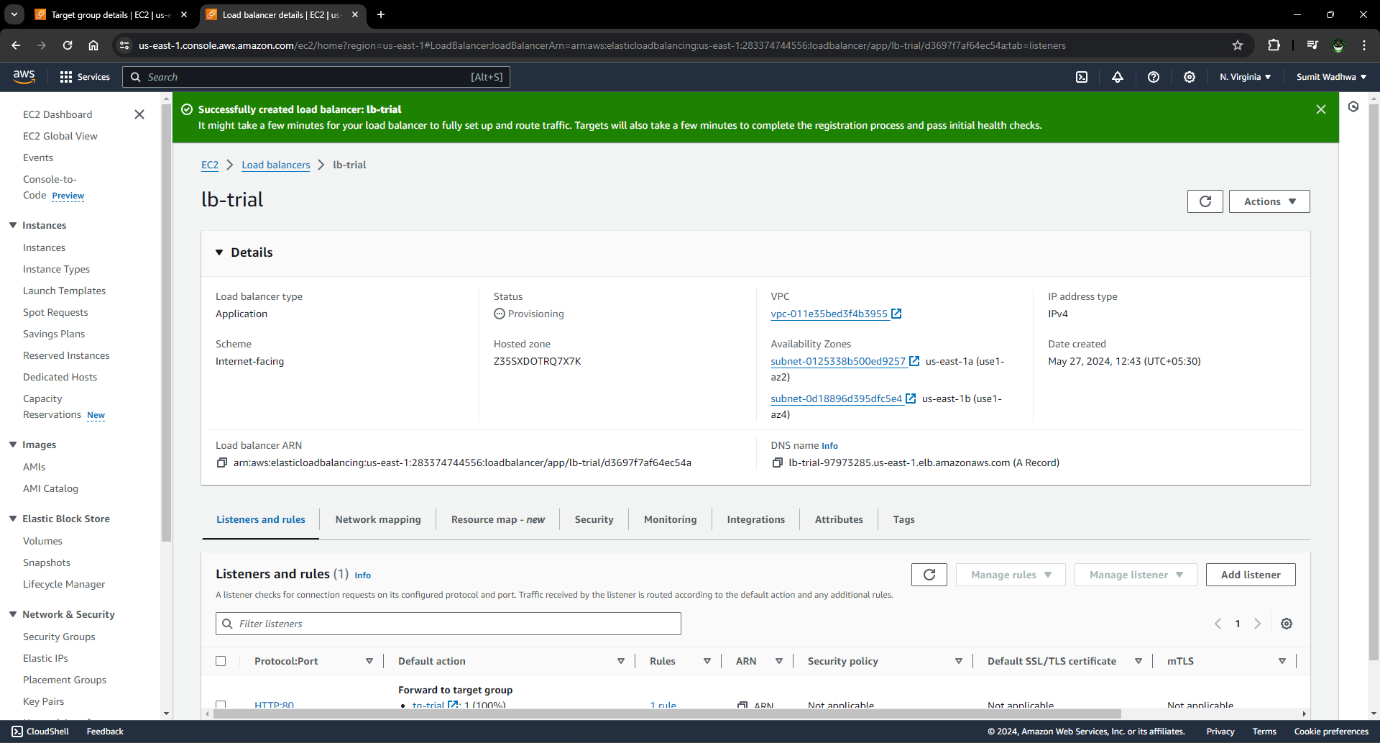


Step 6: Associate Application Load balance with target group

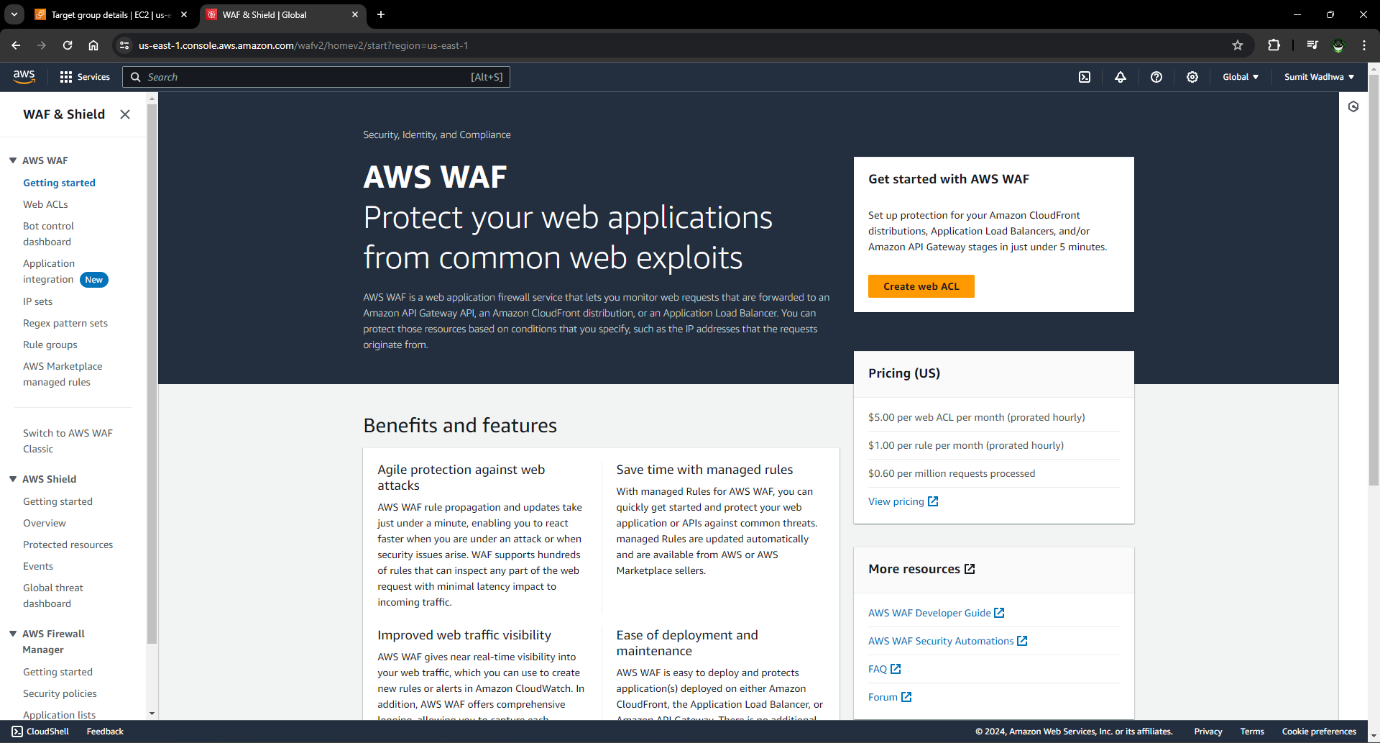


Step 7: Application load balancer is created

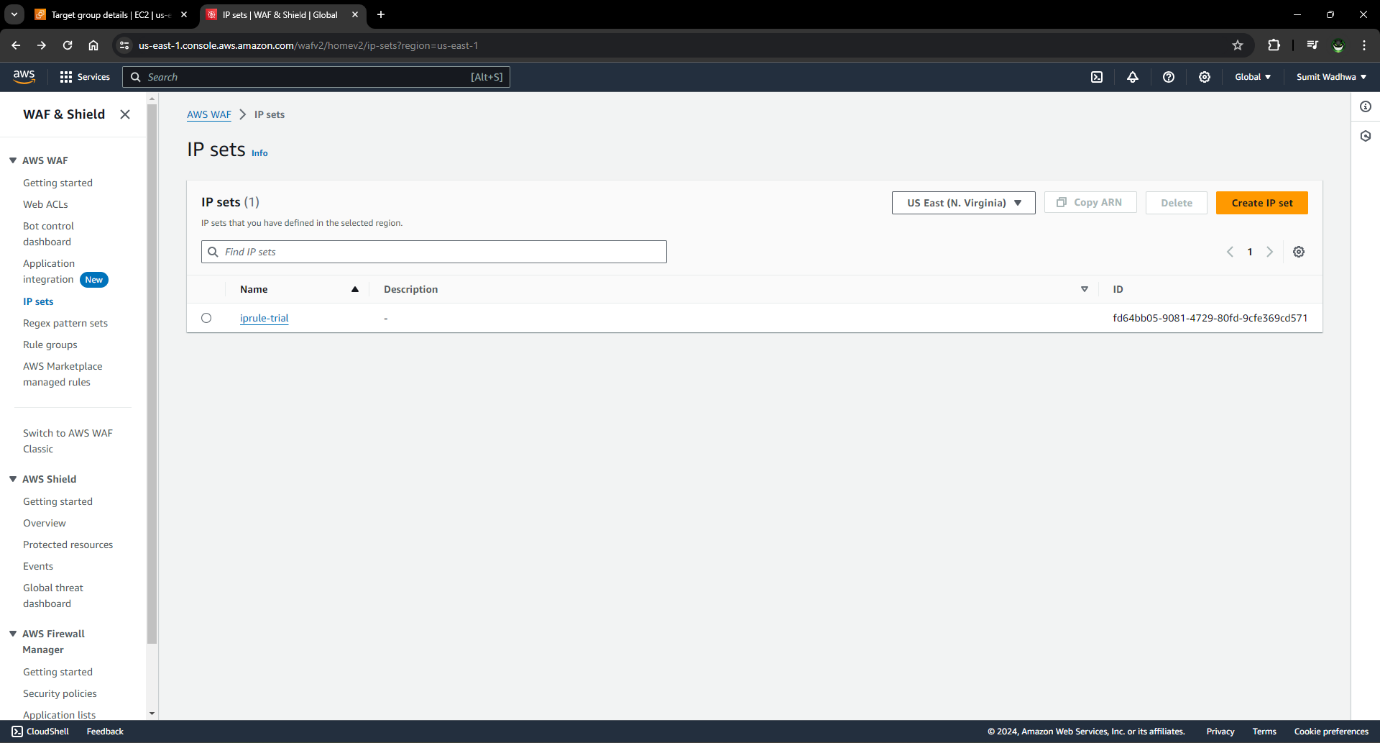
* Check it details



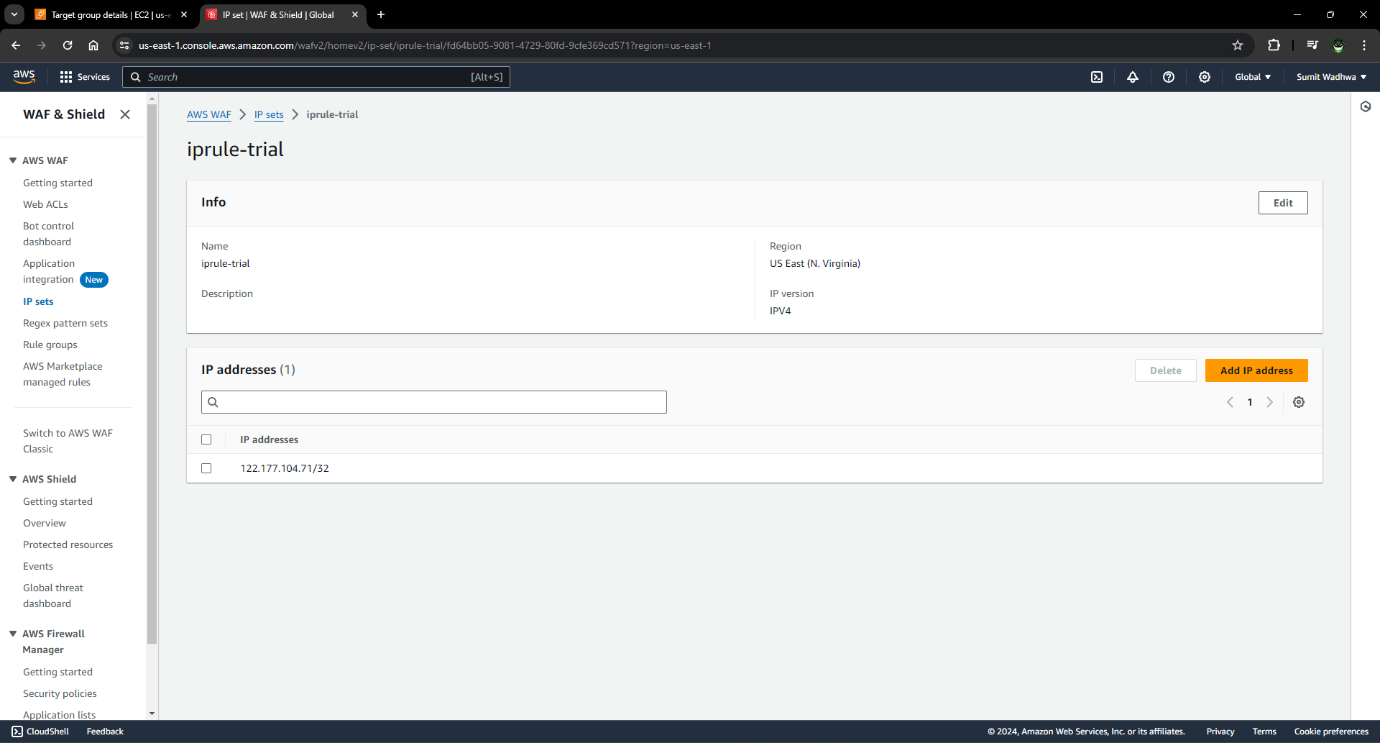
Step 8: Go to the search bar and open WAF & Shield



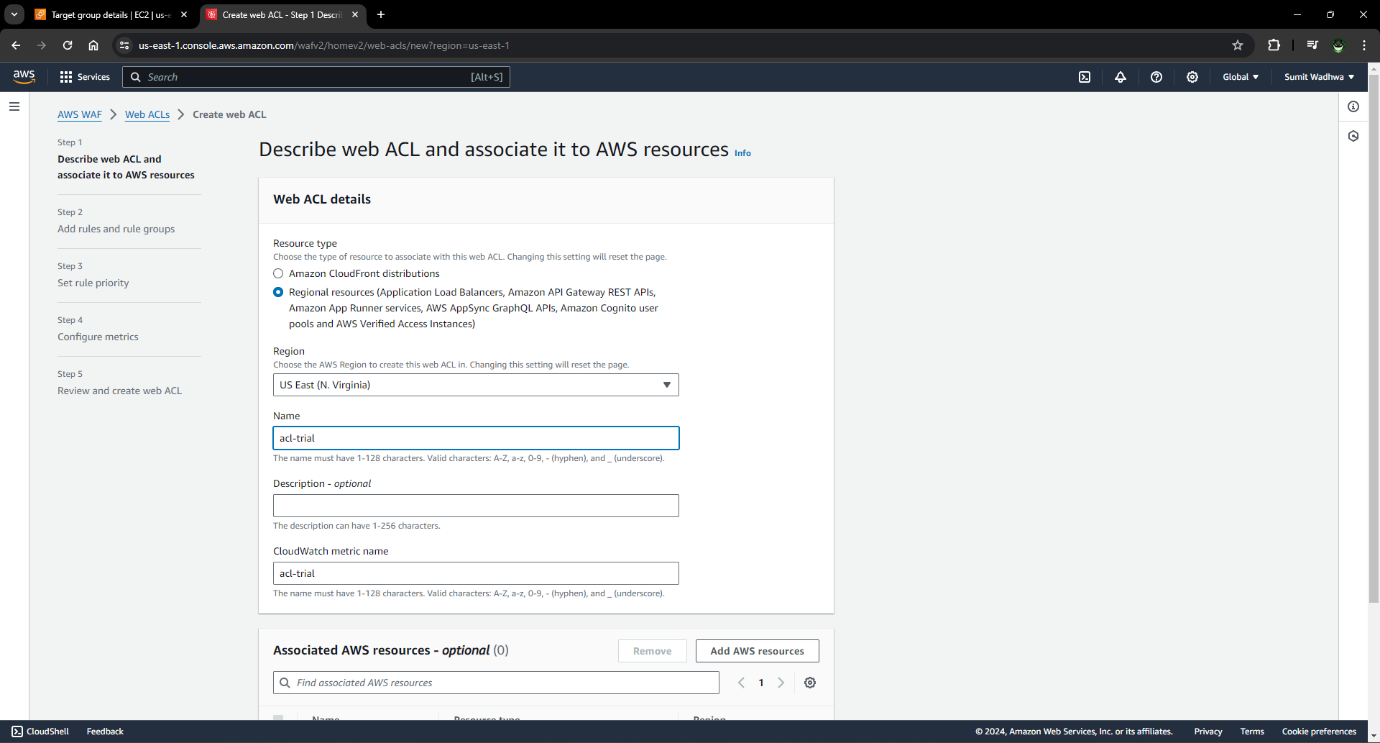
Step 9: Create IP sets



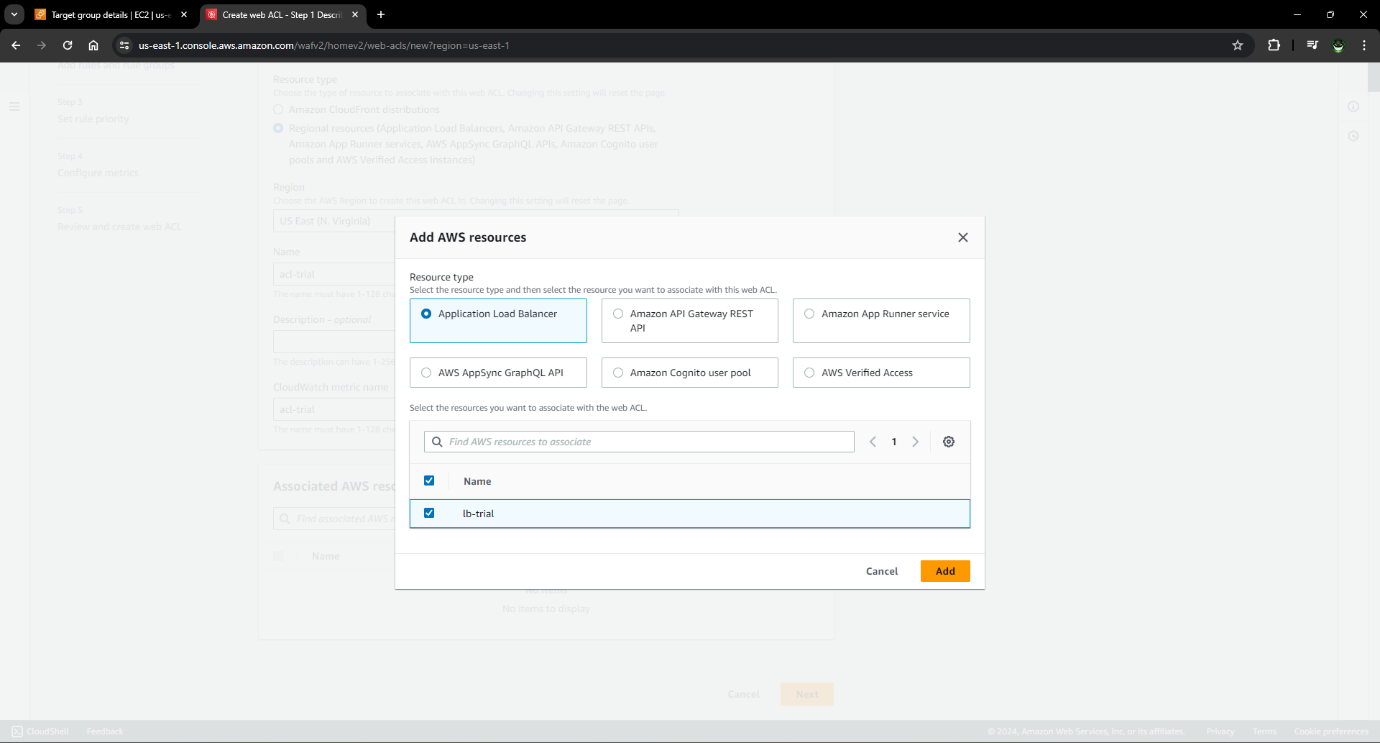
Step 9: Check IP set details and make sure your IP address is added



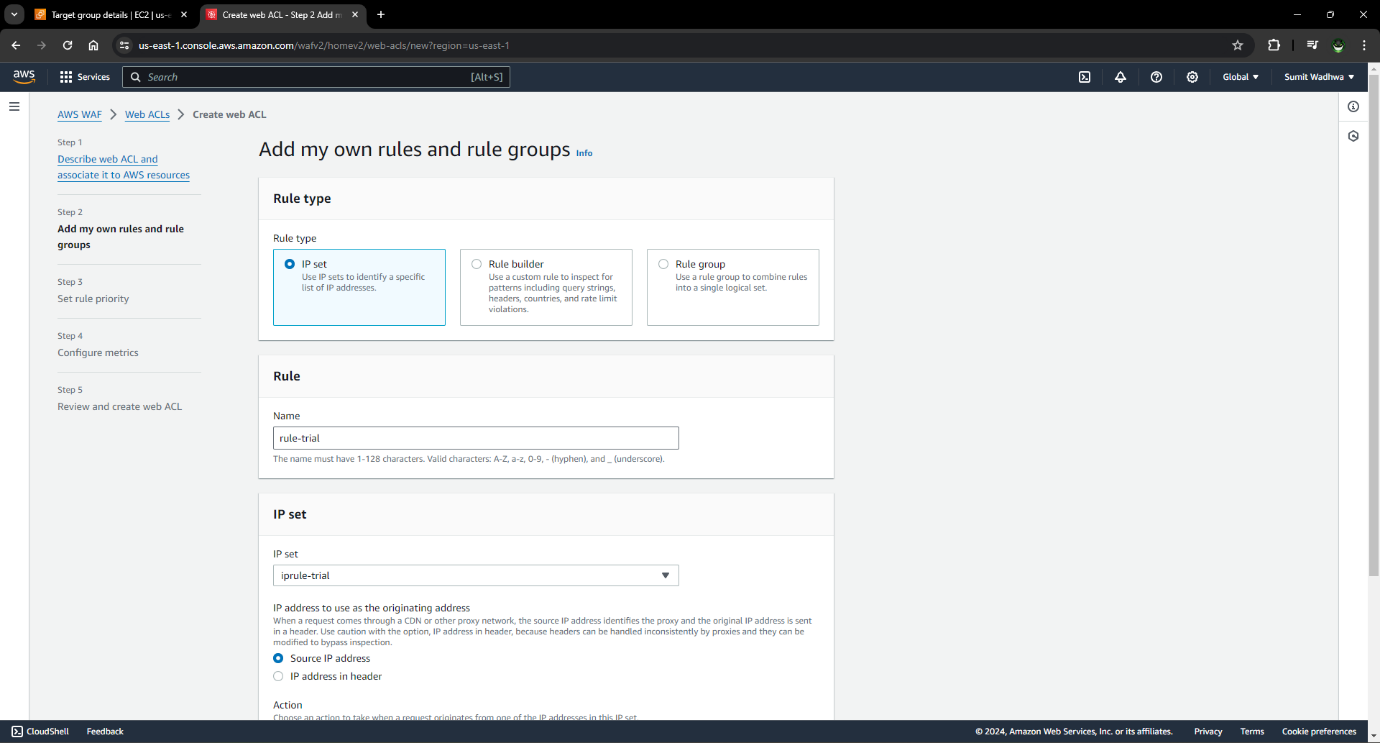
Step 10: Create Web ACL (Access Control List)

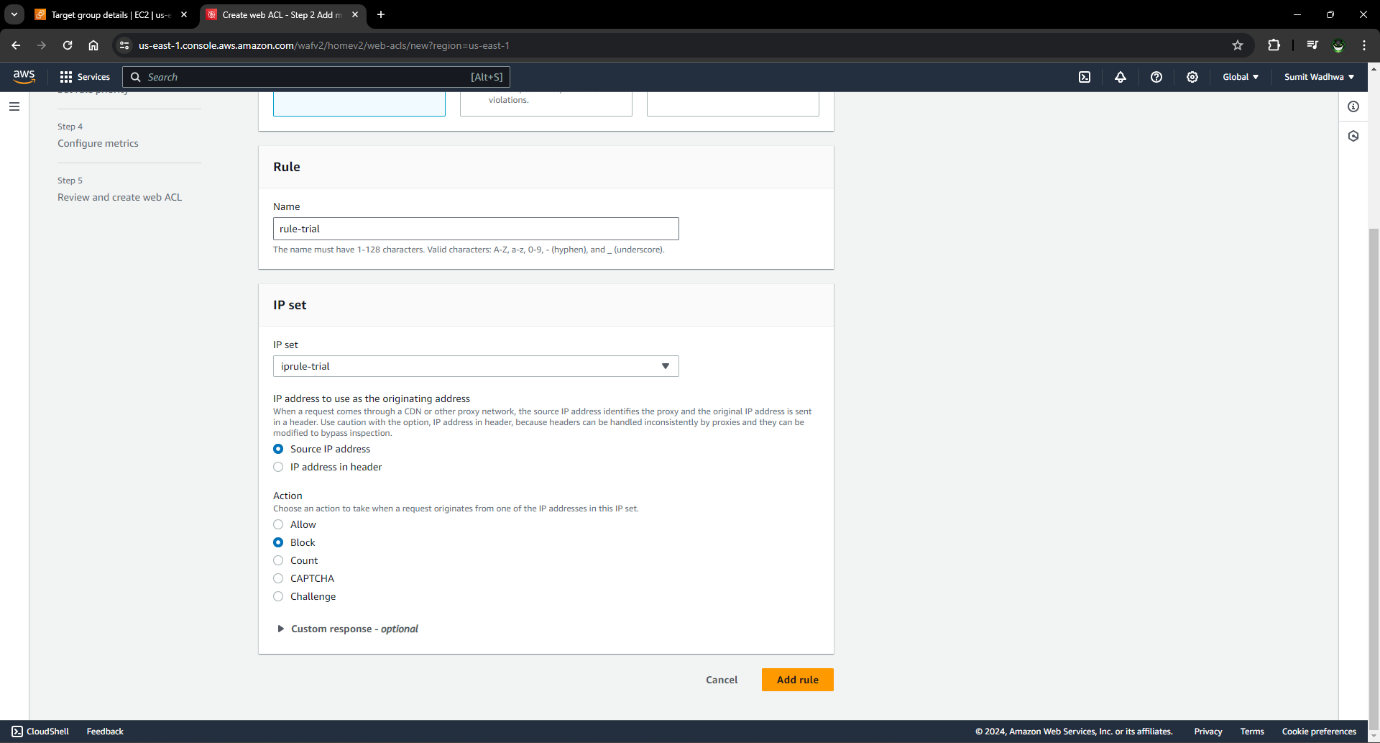


Step 11: Add AWS resources

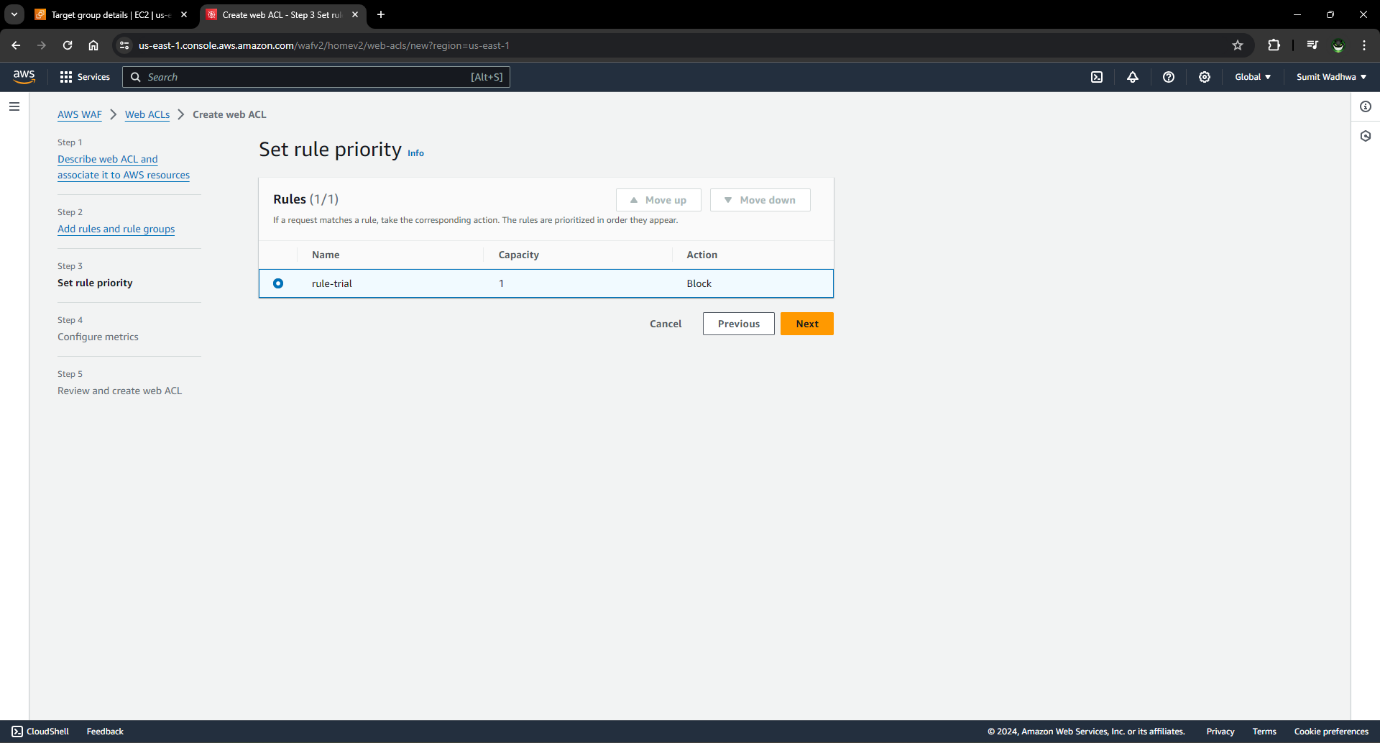


Step 12: Add rule and rule groups

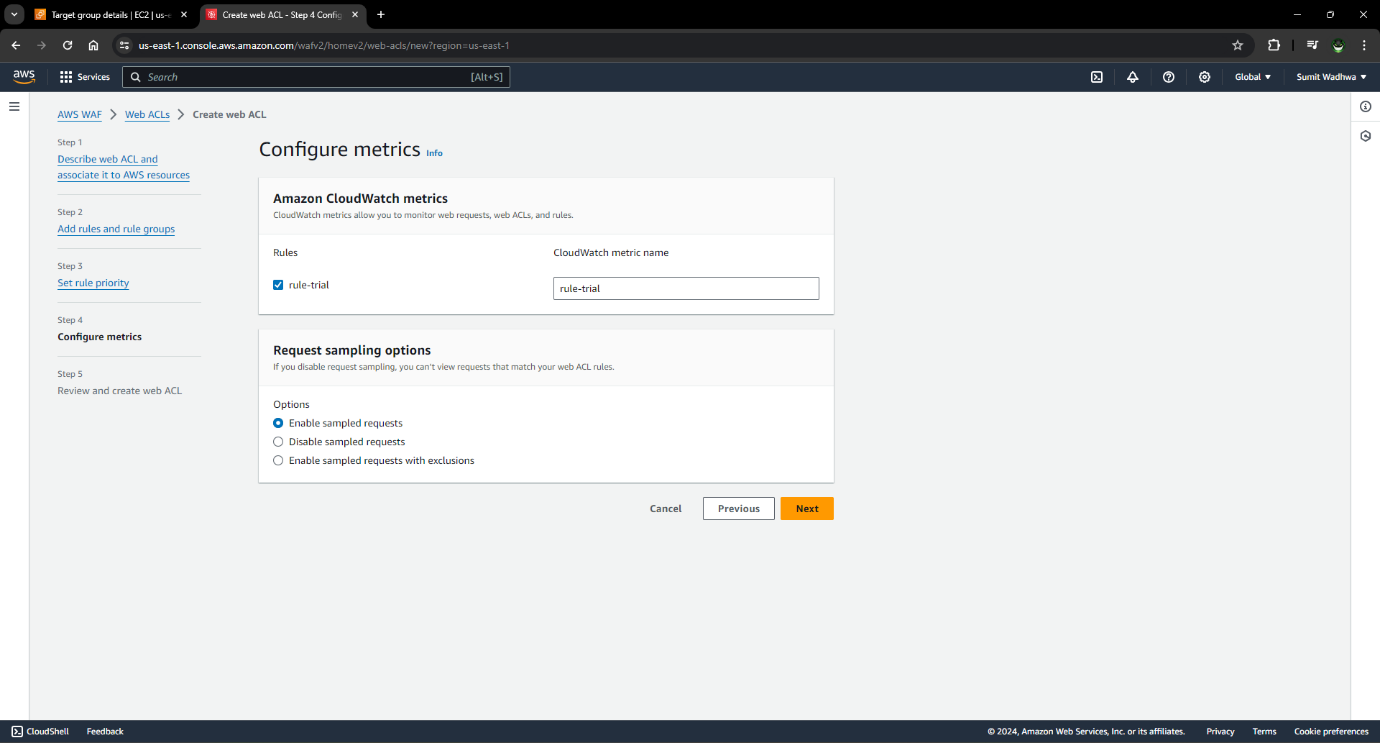




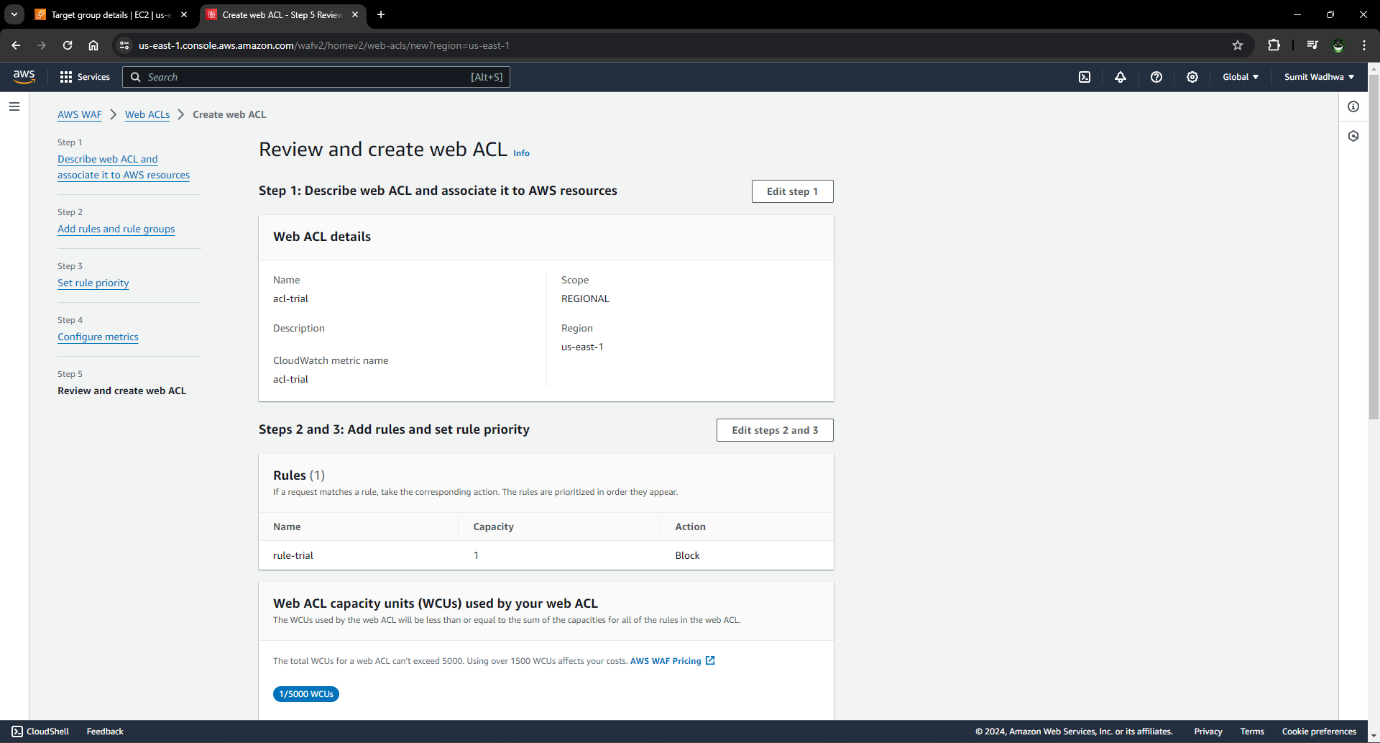
Step 13: Set rule priority



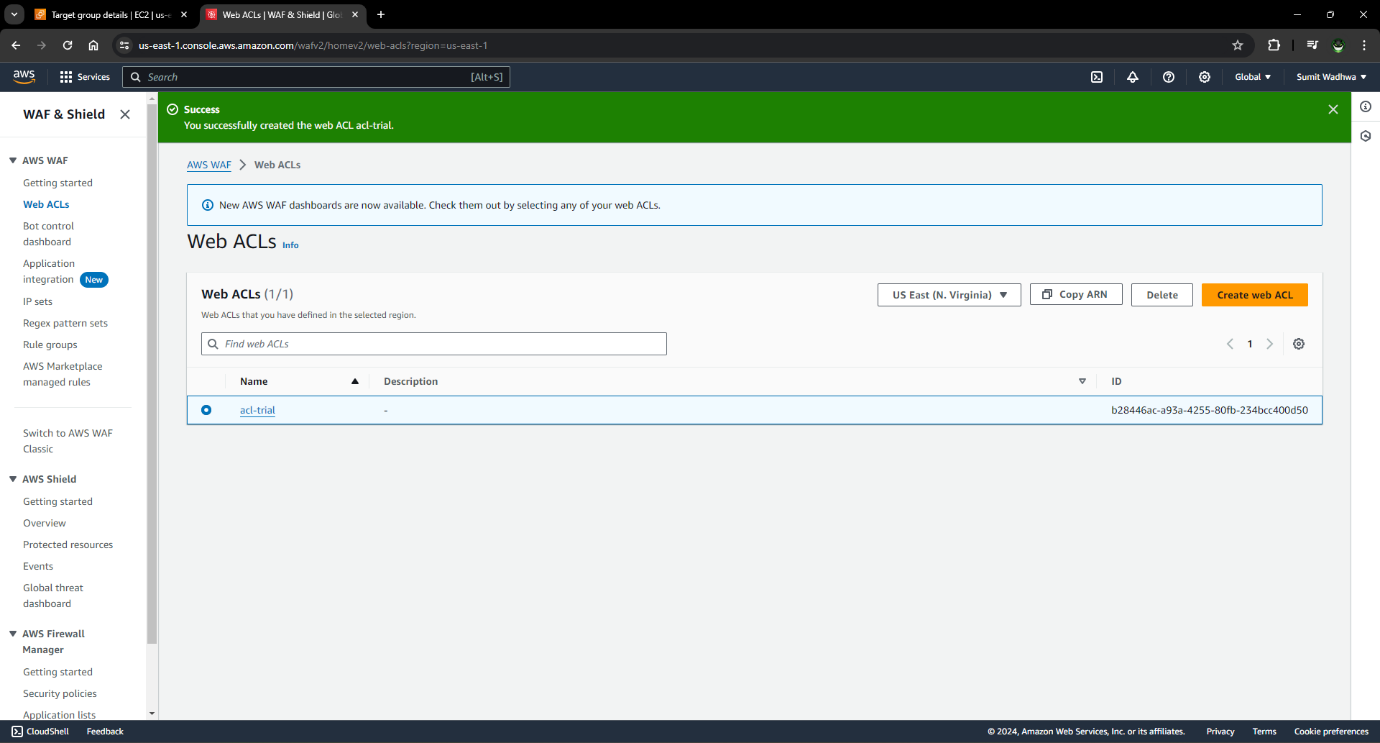
Step 14: Configure metrics



Step 15: Review and create web ACL

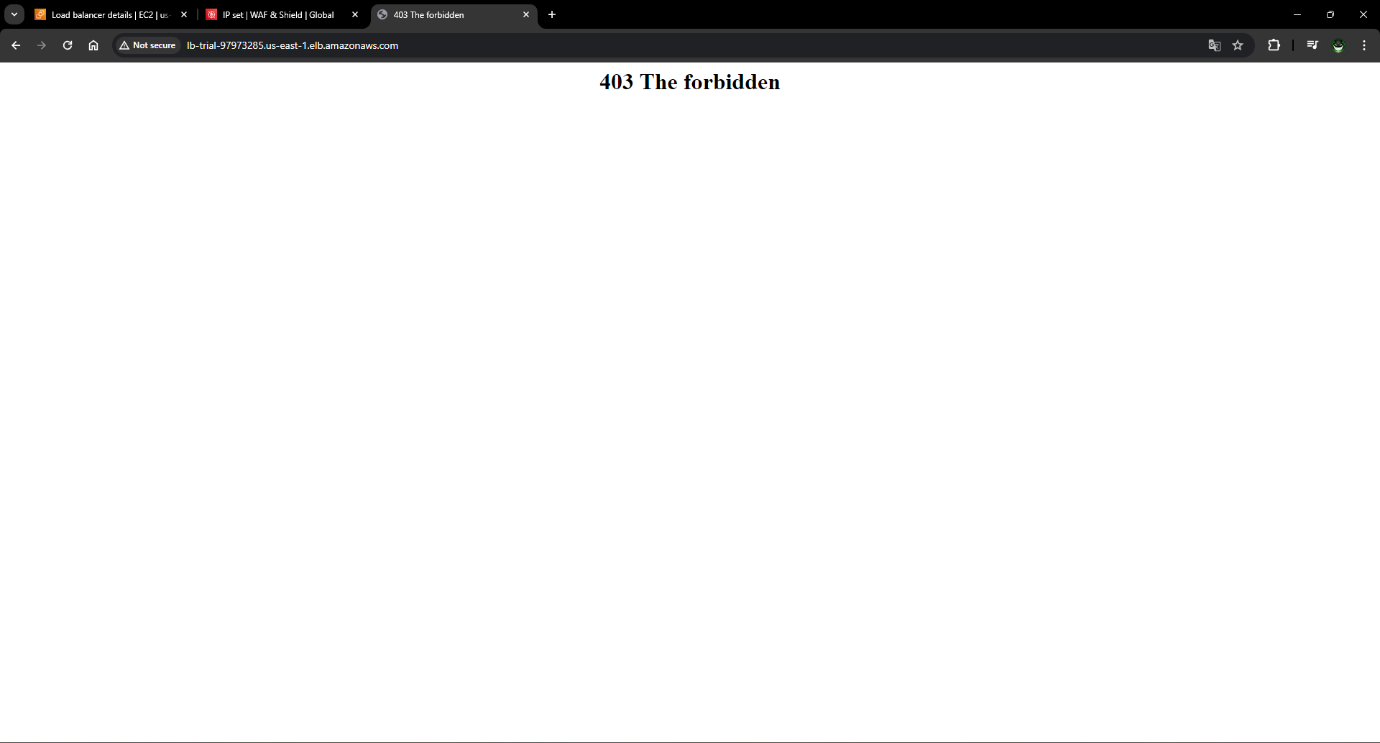


Step 16: Web ACL is created



Step 17: Check the result

* You can check the result by trying to access load balancer from IP which is define in the IP set rules group
* There is 403 forbidden message because WAF blocked that IP
* The 403 error indicates that the website owner has set up rules that are blocking your IP address



Step 18: From Web ACL traffic can be filtered and all the details can be checked like sample of bot detection, client device types, attack type, top 10 countries, blocked , allowed IPs

