## ****Step-by-Step WAF Deployment with Cloud-Front (Without ALB)****

### 🔧 ****Step 1: Prepare a Test Web Server (if not already)****

**If already running**, skip this.

Else:

Launch an EC2 instance (Amazon Linux or Ubuntu)

Install a simple web server:

sudo yum update -y

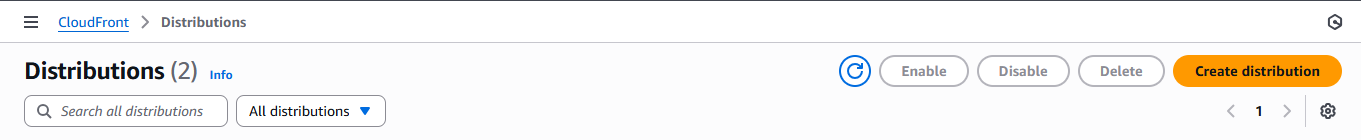
sudo yum install -y httpd

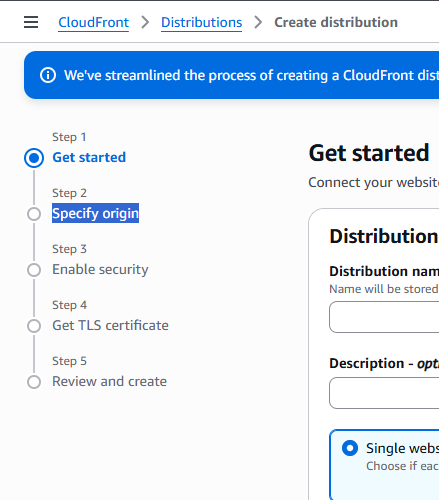
sudo systemctl start httpd

sudo systemctl enable httpd   
echo "WAF Test Page" | sudo tee /var/www/html/index.html

### 🌍 ****Step 2: Create CloudFront Distribution (acts as WAF proxy)****

CloudFront is required since **you can't associate AWS WAF directly with an EC2 instance**. Here's how to use it as a WAF proxy:

Go to **CloudFront → Create Distribution**

Name: TestWAFCDN  
  
Origin domain: **Your EC2 public DNS**  -> Click NEXT  
  
IN NEXT STEP  
  


Select Below as per your Requirement

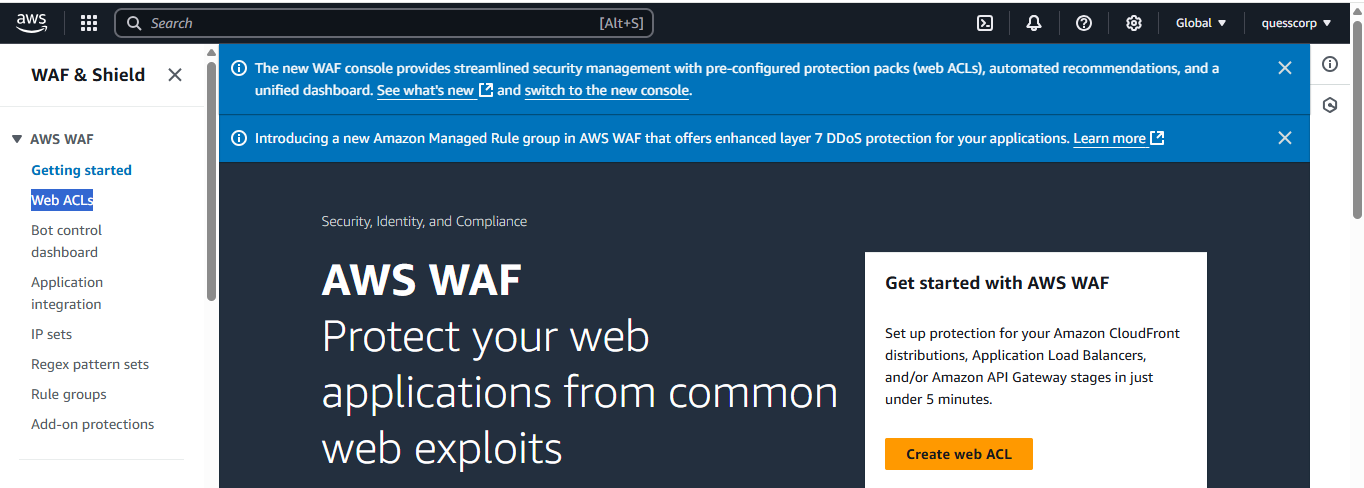
Protocol: HTTP only or HTTPS if you have certs

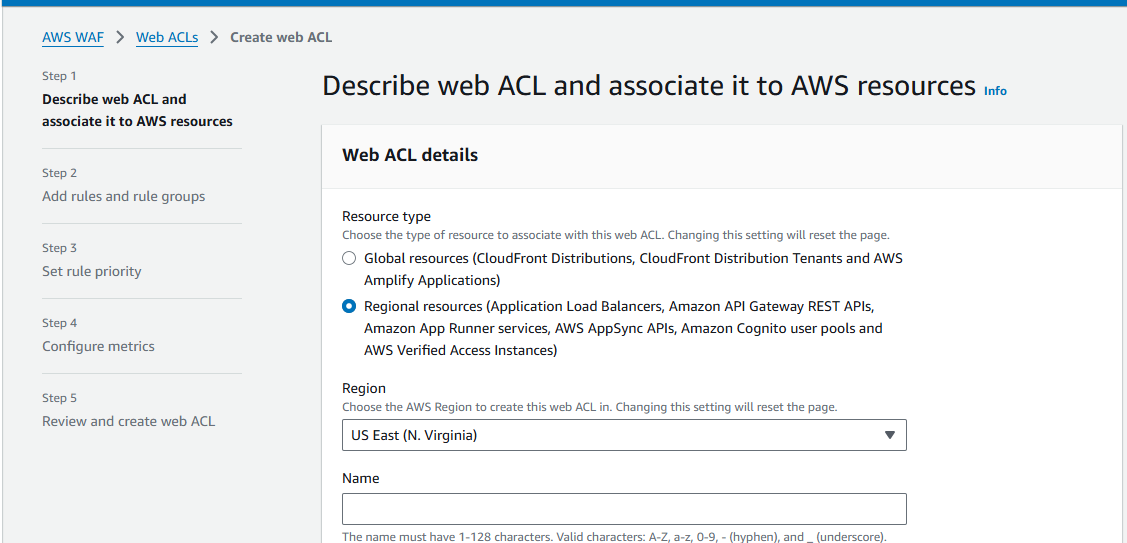
Leave defaults for now

Click **Create**

⛳ This makes all web requests go through CloudFront → then to EC2.

### 🔐 ****Step 3: Create AWS WAF Web ACL and Attach to CloudFront****

Go to **AWS WAF → Web ACLs**

Click **Create web ACL**

Name: TestWebACL

Scope: **CloudFront**

Region: Global (CloudFront only uses global WAF)

Add **AWS Managed Rule Groups**

AWSManagedRulesCommonRuleSet

AWSManagedRulesAmazonIpReputationList

(Optional) Add a rate-based rule

Default action: Allow

Click **Next** → Associate with **your CloudFront distribution**

Click **Create**

### 🌐 ****Step 4: Update DNS (Optional)****

If you have a company domain (e.g., app.company.com), point it to your **CloudFront Distribution domain name**, like:

d1234abcdef.cloudfront.net

Update your DNS A/AAAA or CNAME record to point to CloudFront.

### 🧪 ****Step 5: Testing the WAF****

Try the following:

❌ SQL Injection:

curl "https://your-cloudfront-domain.com/?id=1' OR '1'='1"

→ Should be **blocked** by managed rules

❌ Bad bot user-agent:

curl -A "BadBot" https://your-cloudfront-domain.com

❌ Country block test (if added GeoMatch rule)

✅ Normal access:

curl https://your-cloudfront-domain.com