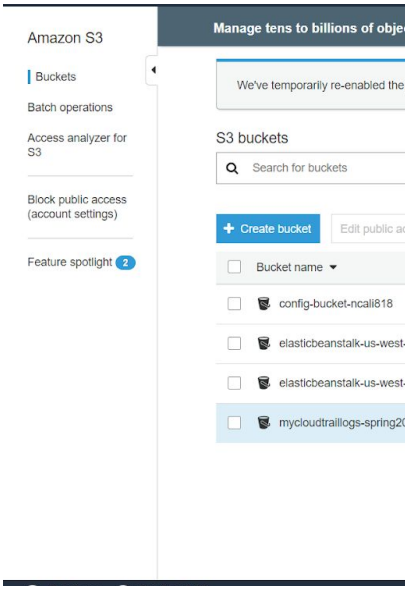
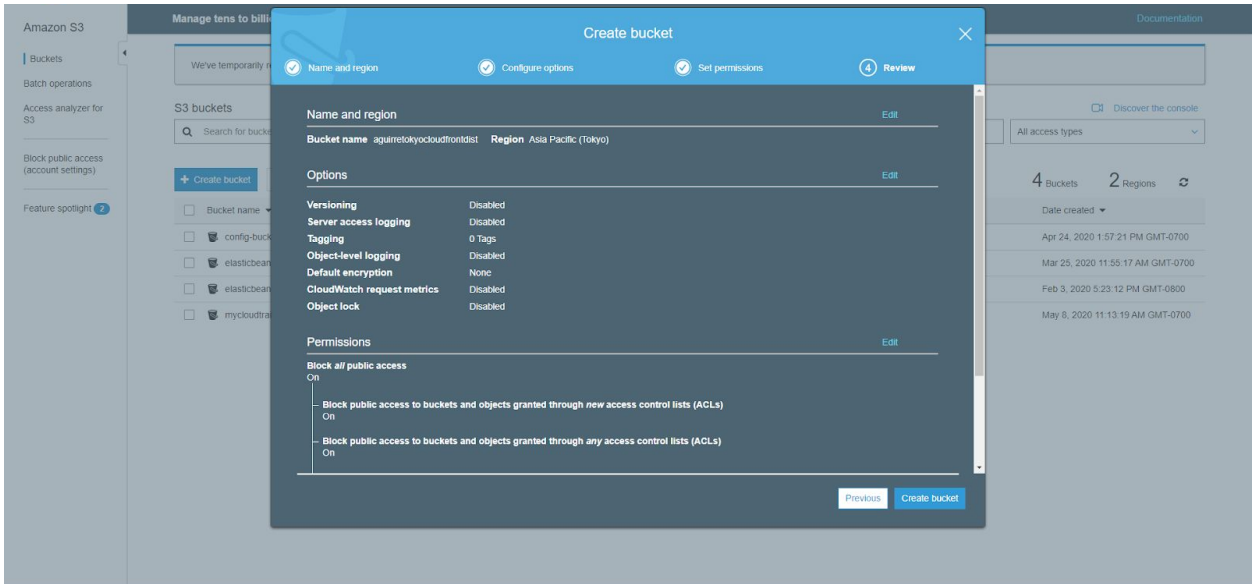
Module 8 Lab 1: WAF Tutorial

Amazon S3 - S3 buckets



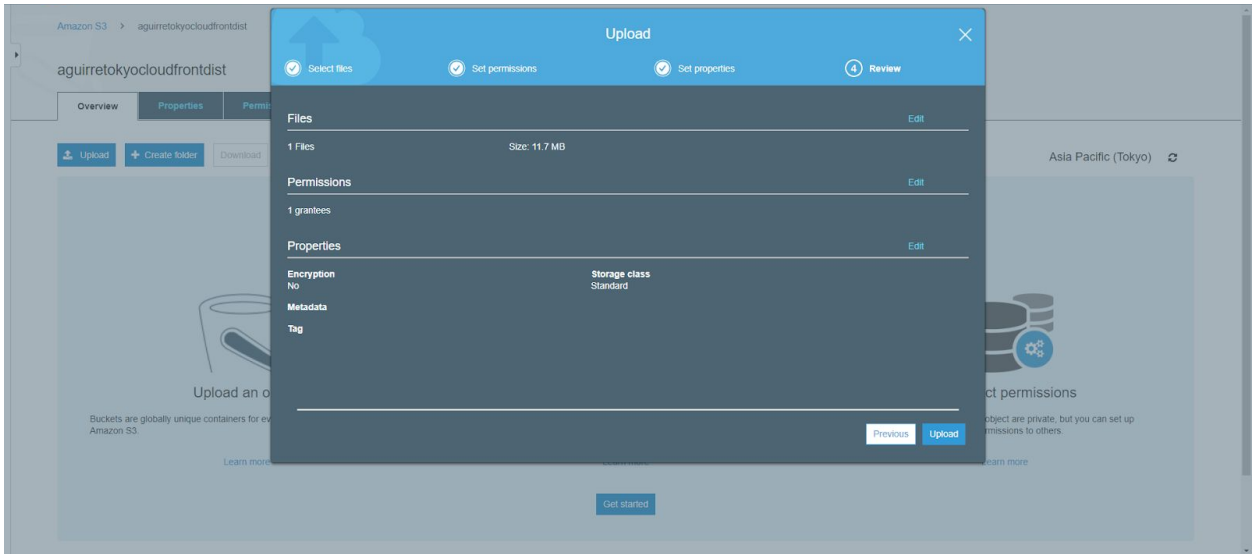
Starting with a S3 bucket, use a large file to help realize benefits of the CloudFront service.

Amazon S3 - Create bucket Review



Note that all settings were left default. Choose a distant Region in locality.

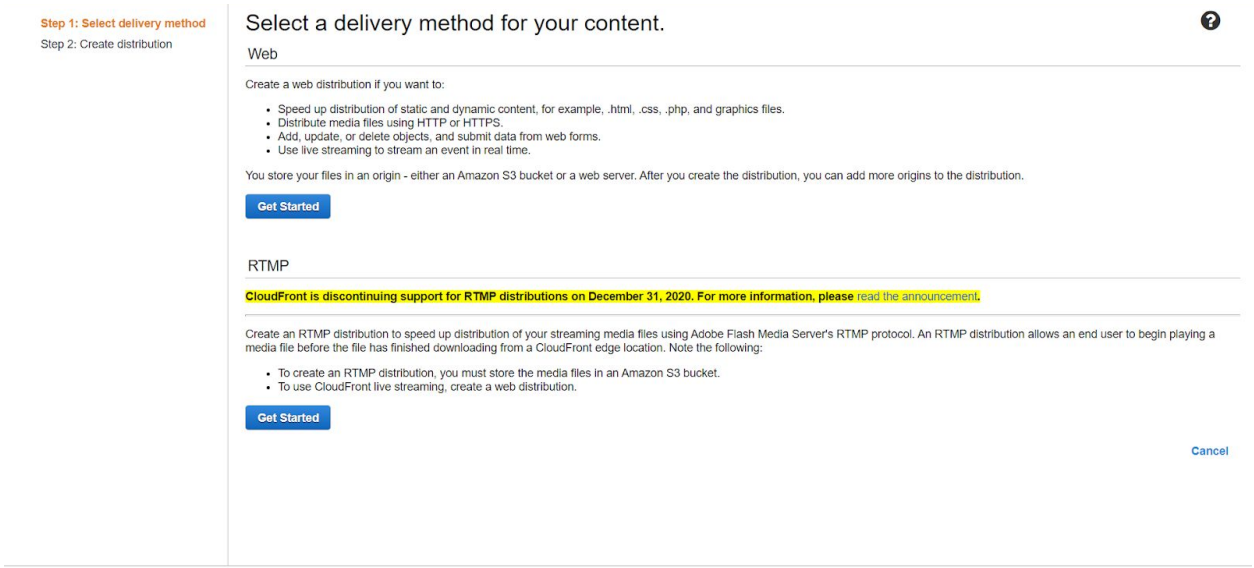
S3 - Upload



No permissions are changed when uploading to the S3 bucket. This is because CloudFront will do those changes for us. Note the 11.7MB size

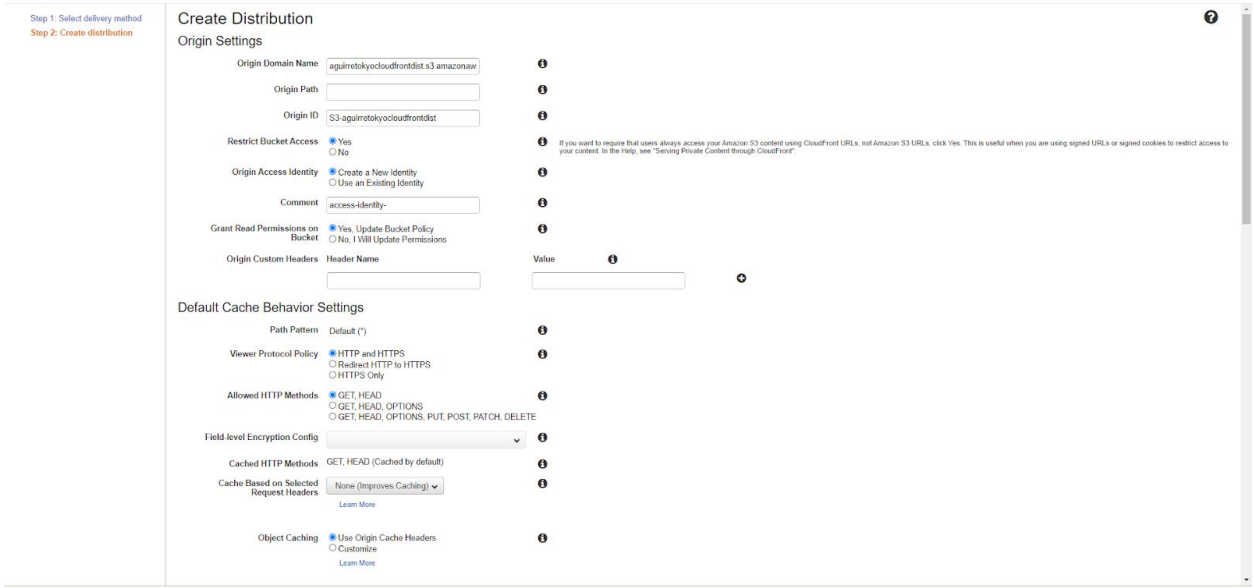
Amazon S3 - S3 bucket image

The image is stored in Tokyo. Before Cloudfront optimization the webpage load took about 14 seconds with a file size of 11.7 MB



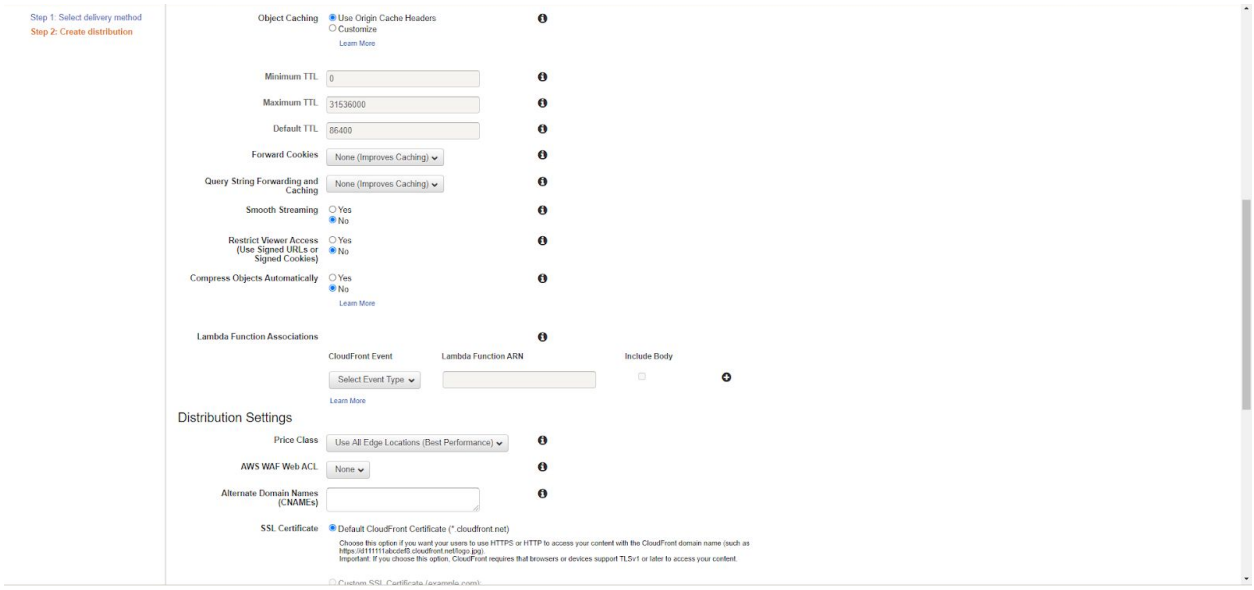
For this lab, the Web option was selected. Note the discontinuation support date for Adobe Flash Media Server's RTMP protocol is the end of 2020.

CloudFront - Create Distribution



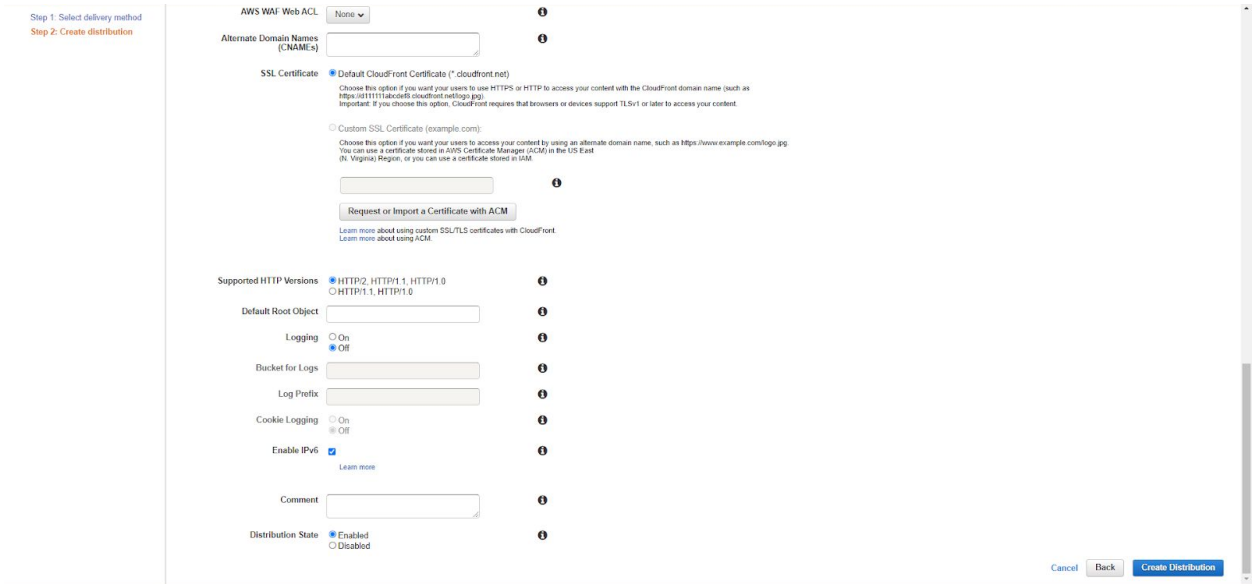
Creating a CloudFront distribution offers many options. Note Restrict Bucket Access and Grant Read Permissions on Bucket are set to yes. The previous public setting should be overridden.

CloudFront - Create Distribution



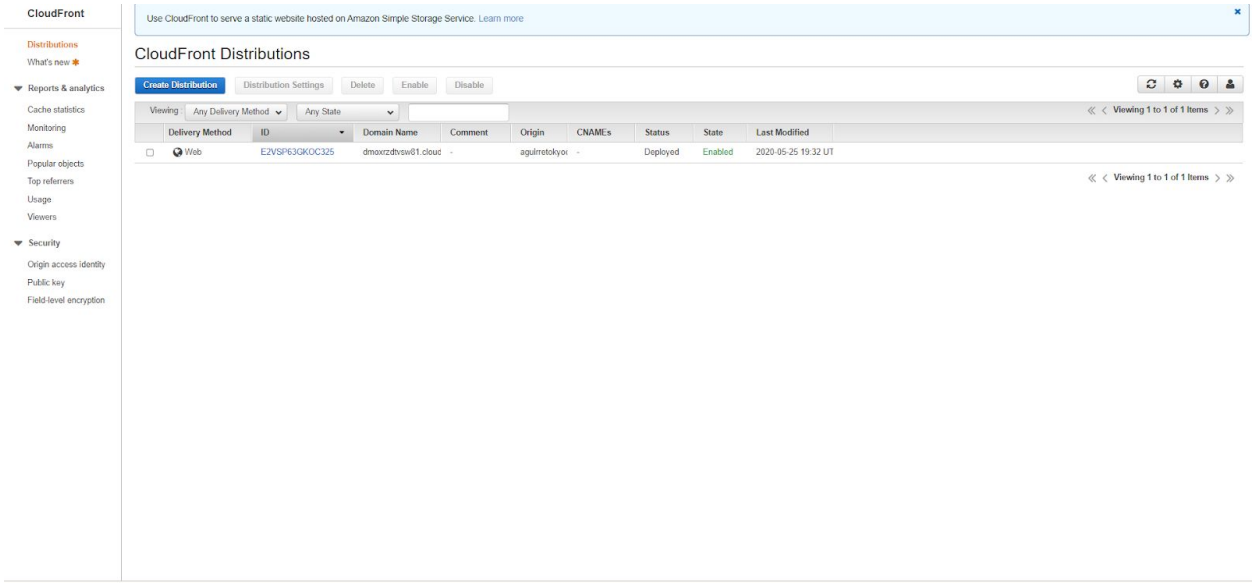
Note that the Price Class is set to Best Performance.

CloudFront - Create Distribution

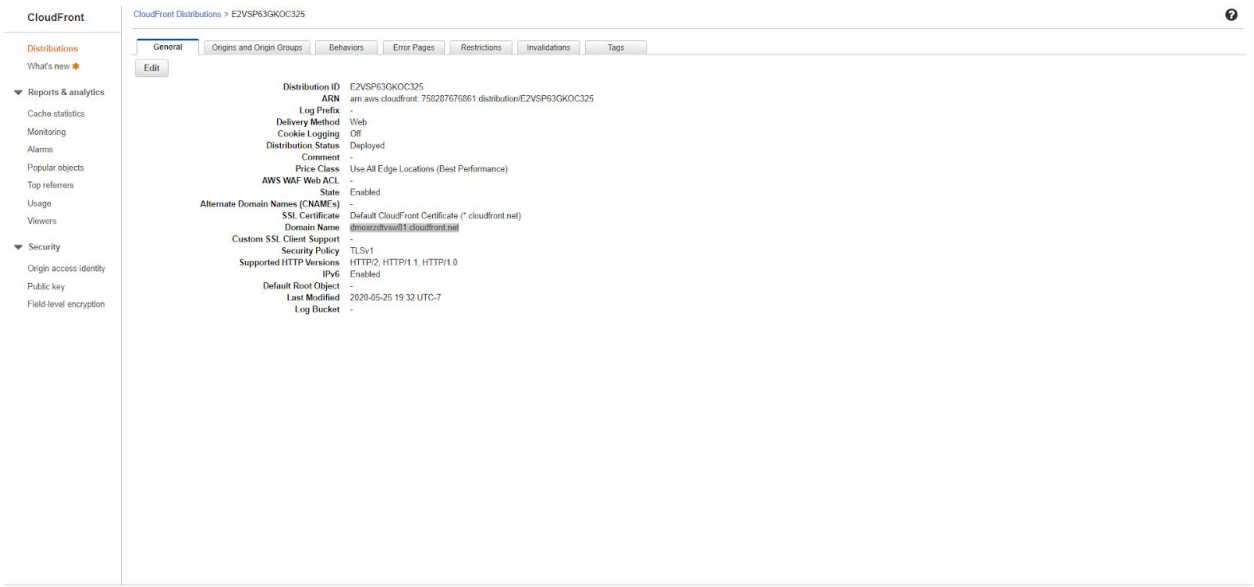


Note that AWS WAF Web ACL will be updated later in this lab. All other options left at default.

CloudFront - Distributions

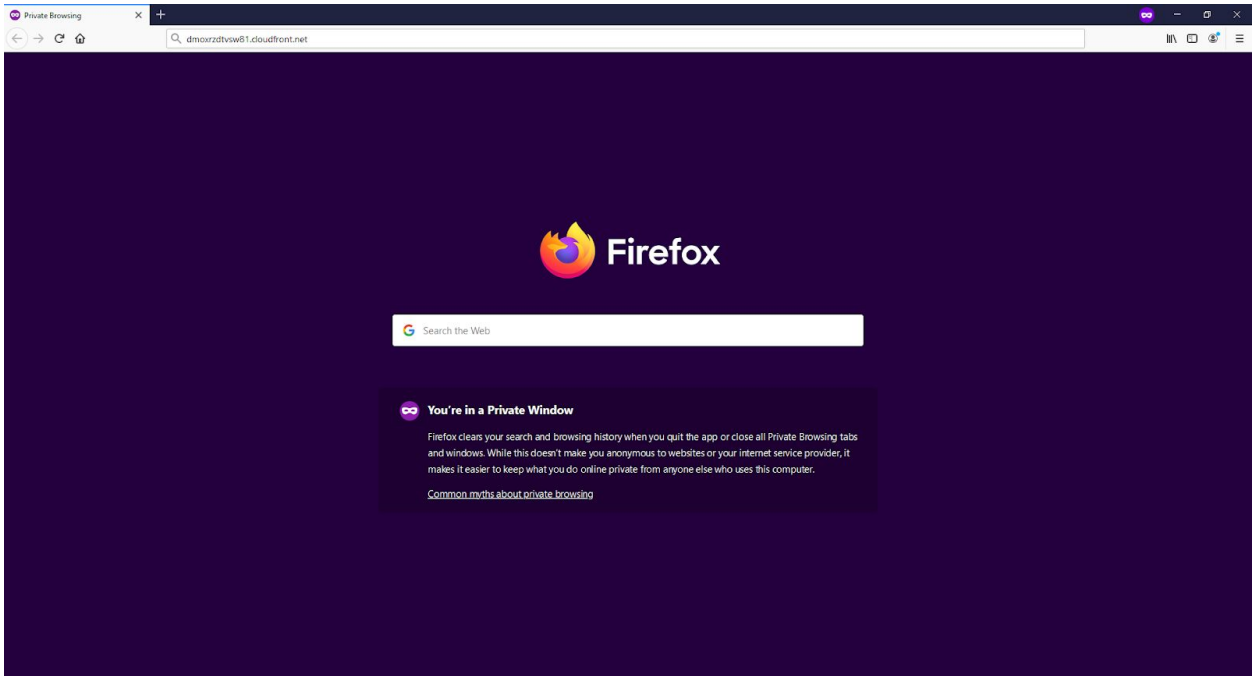


The complete CloudFront setup process took about 8 minutes.



Note the domain name. The S3 bucket permissions should have been reset, thus removing the bucket from public access.

Firefox - Before CloudFront Redirect

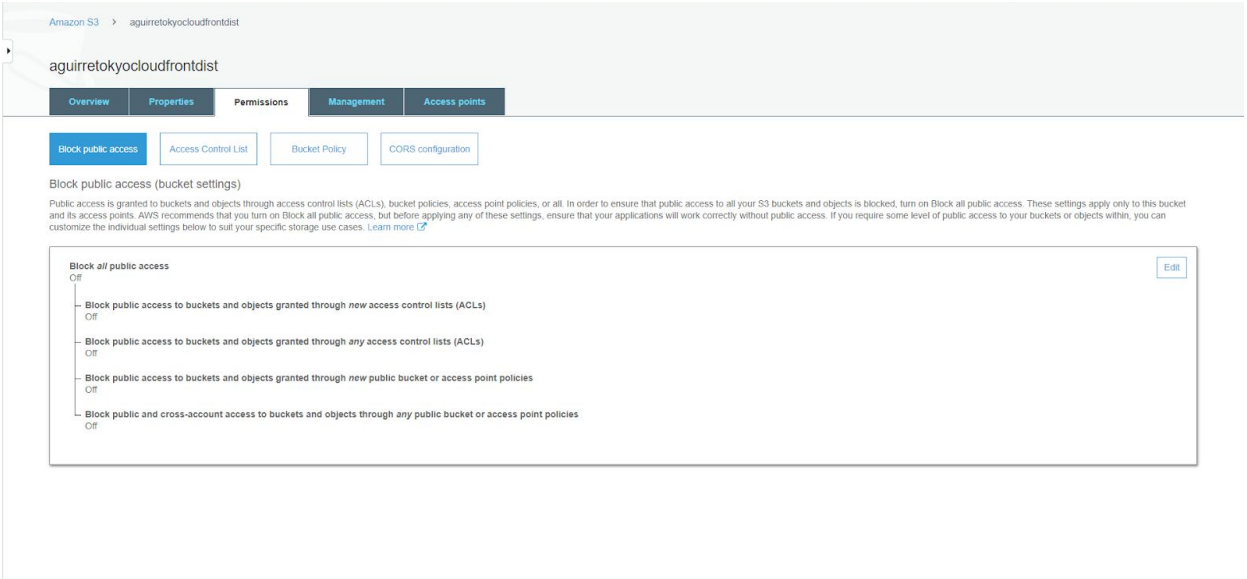


The new domain is entered.

Firefox - After Redirect

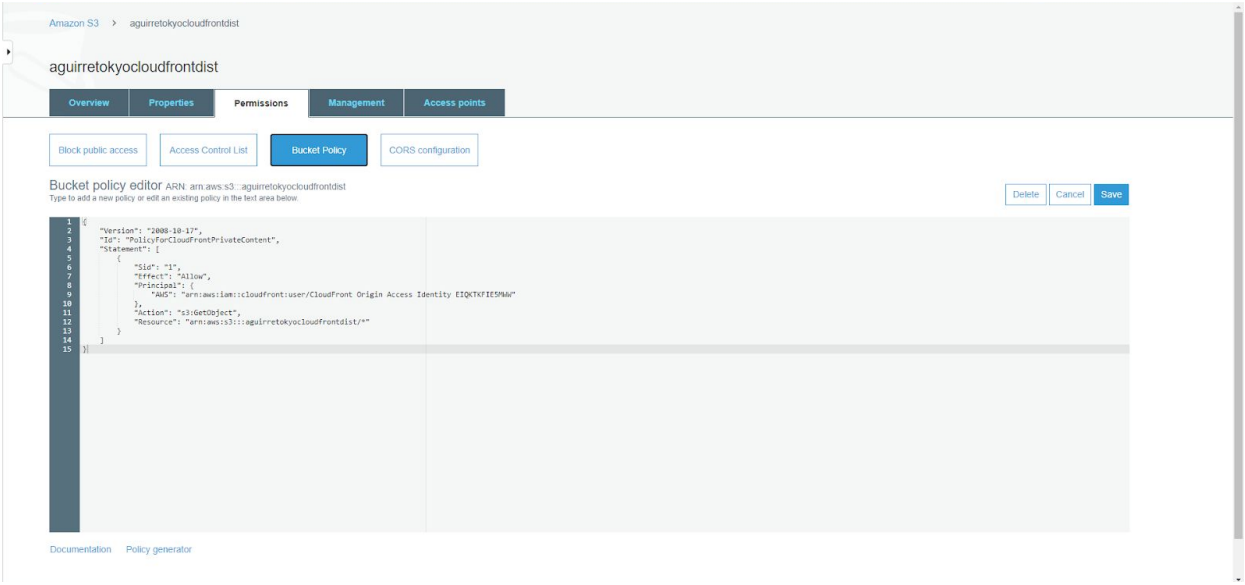
The access is blocked due to CloudFront.

Amazon S3 - Bucket Permissions



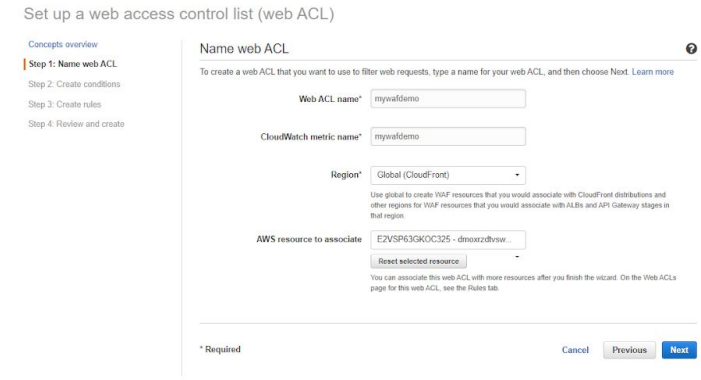
Note the bucket setting to block all public access

Amazon S3 - Bucket Policy



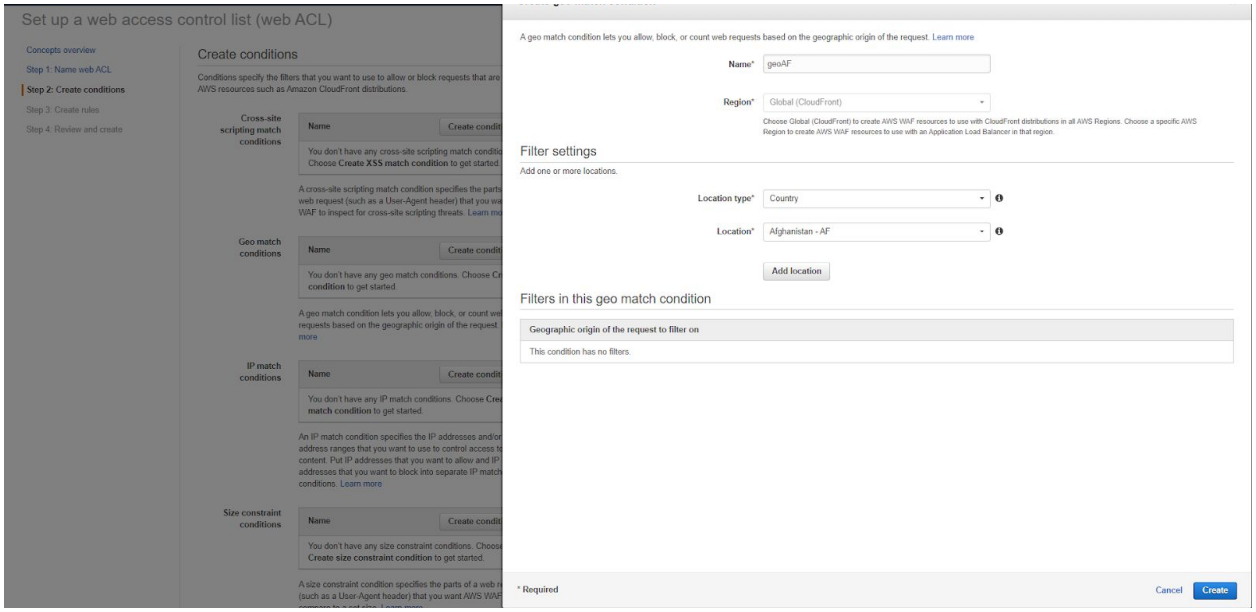
However, the Bucket policy is set to allow GetObject.

AWS WAF



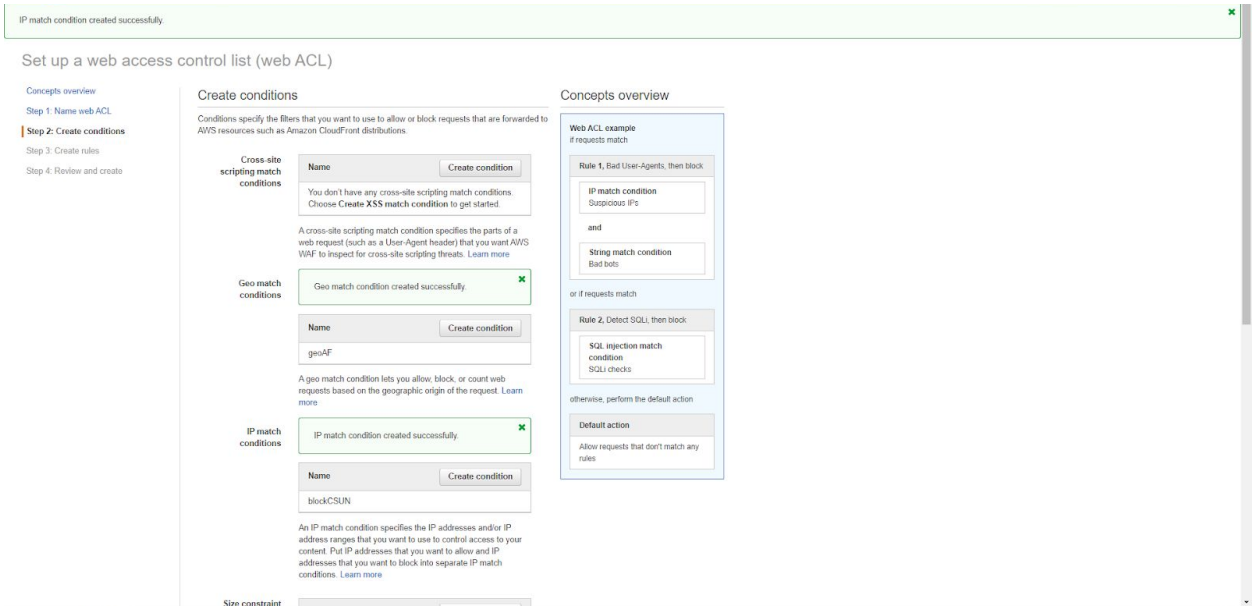
Setting up the web ACL as a WAF service.

AWS WAF - web ACL



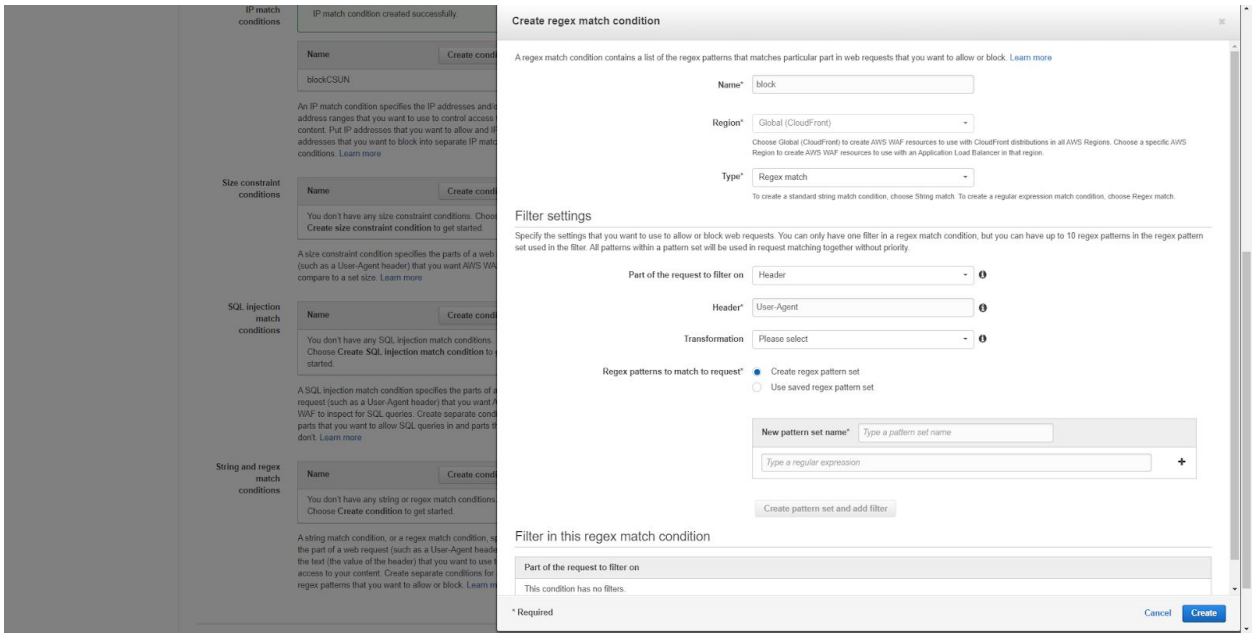
AWS WAF works via creating conditions that point to a desired outcome. In this case the Afghanistan geolocation will be blocked.

AWS WAF - web ACL



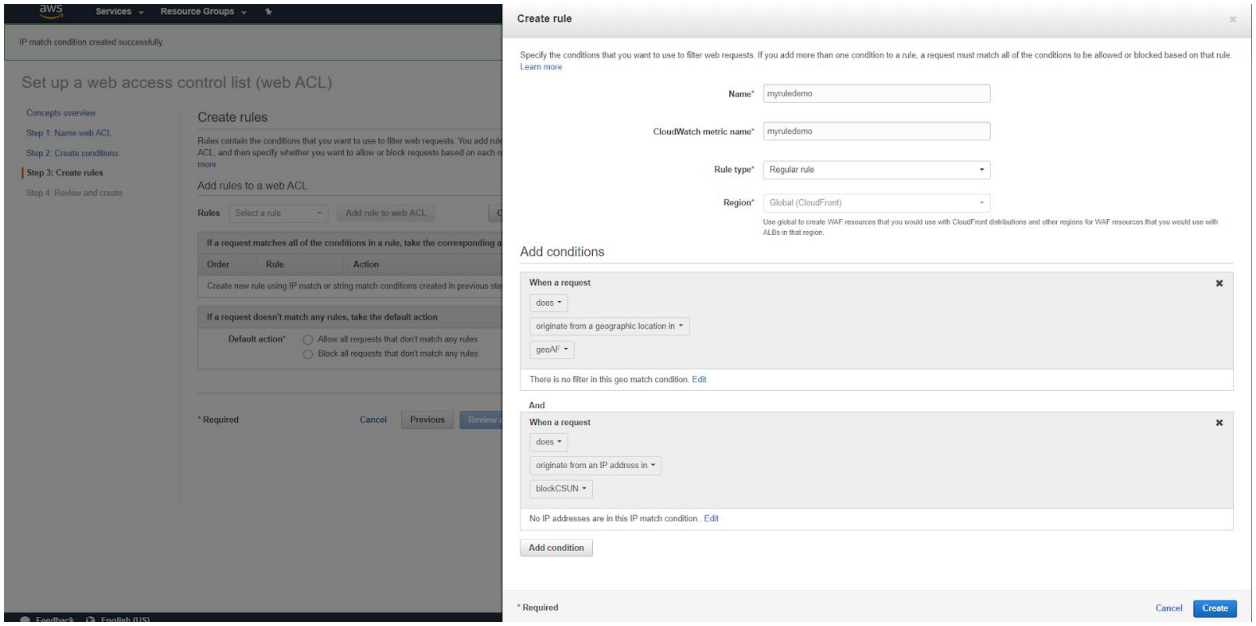
A specific IP will be blocked when a IP condition match.

AWS WAF - Create Conditions



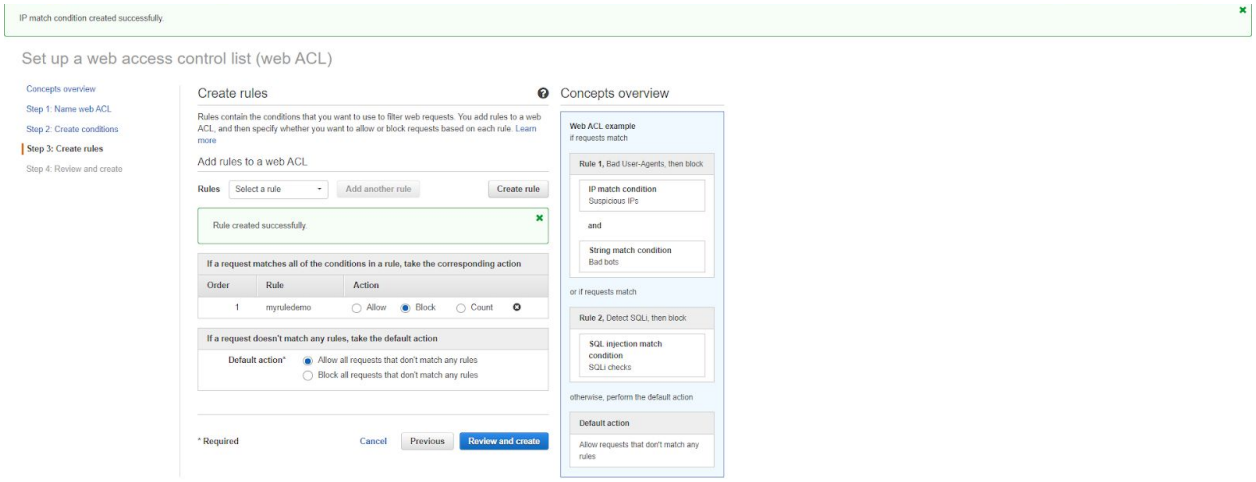
Note that regex match conditions can also be utilized.

AWS WAF - Create rules



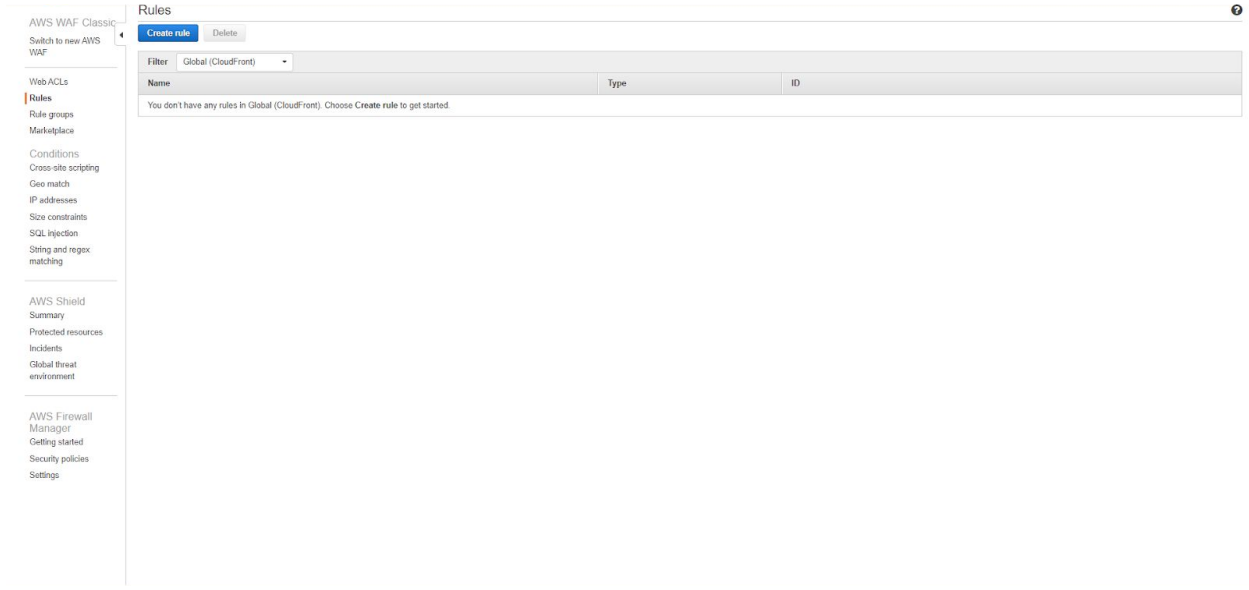
A rule must be created to give meaning to the conditions.

AWS WAF - Create Rules



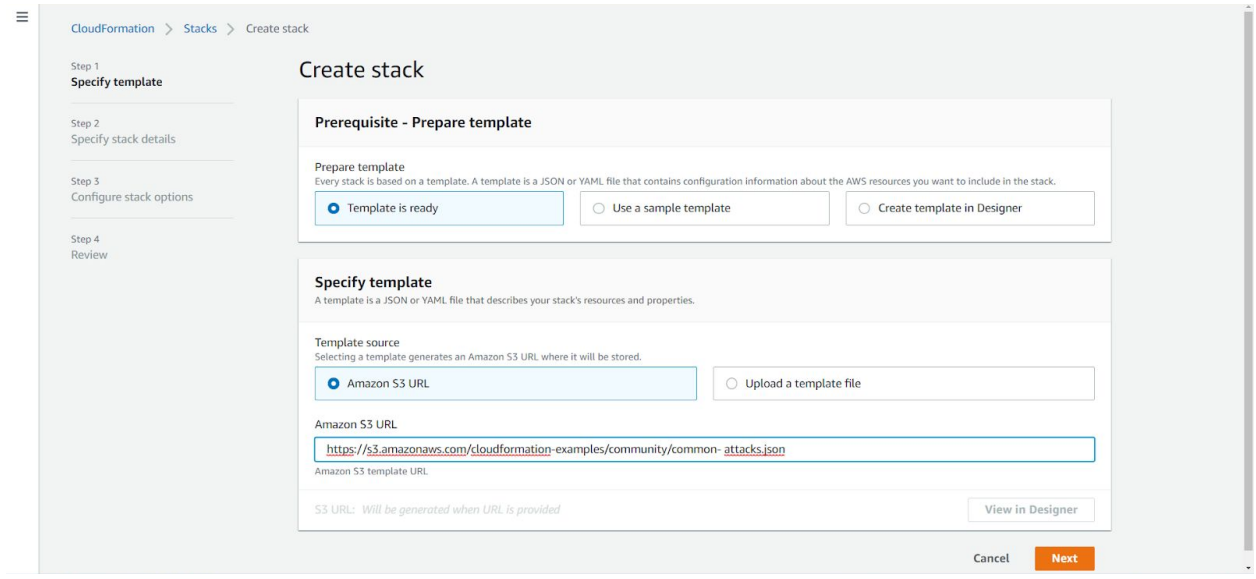
Note what actions are taken when a request matches all conditions in a rule. Conversely, note what will happen when a request does not match any rules.

AWS WAF Classic



All rules were deleted.

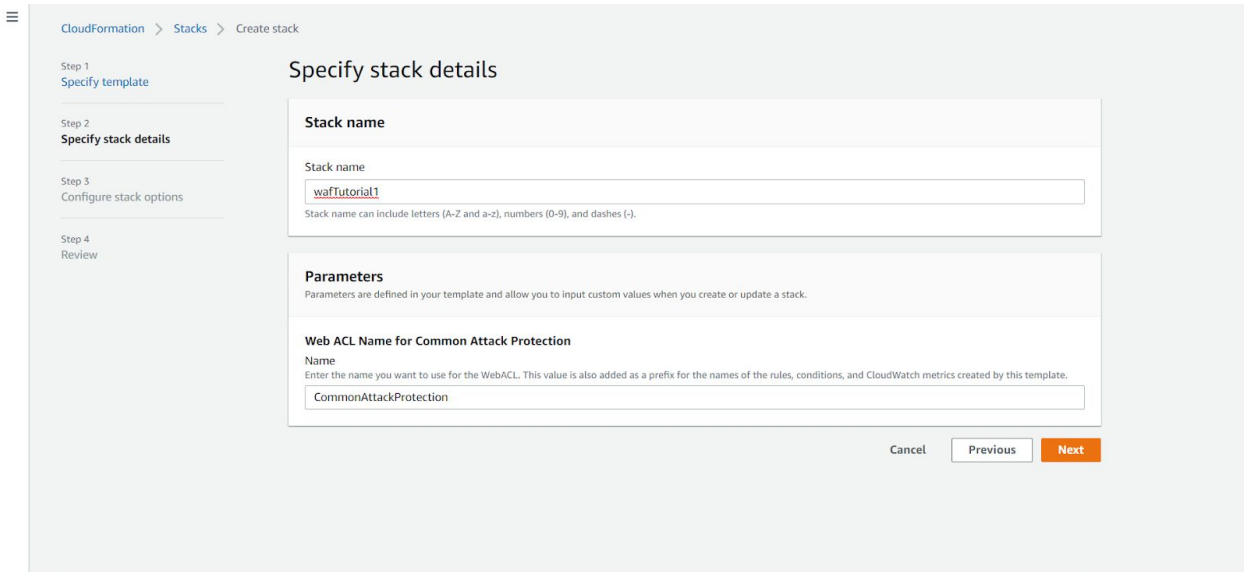
CloudFormation - Create Stack



Using CloudFormation, a tutorial template will be created that already contains the proper WAF settings.[1]

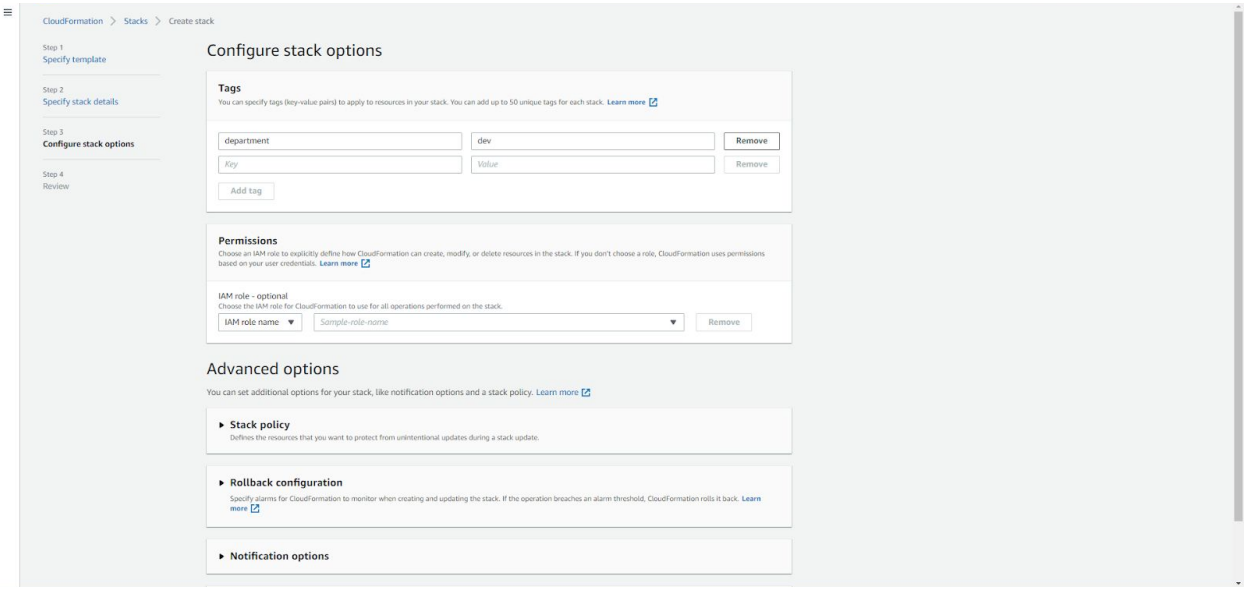
[1] https://s3.amazonaws.com/cloudformation-examples/community/common-attacks.json

CloudFormation - Create stack



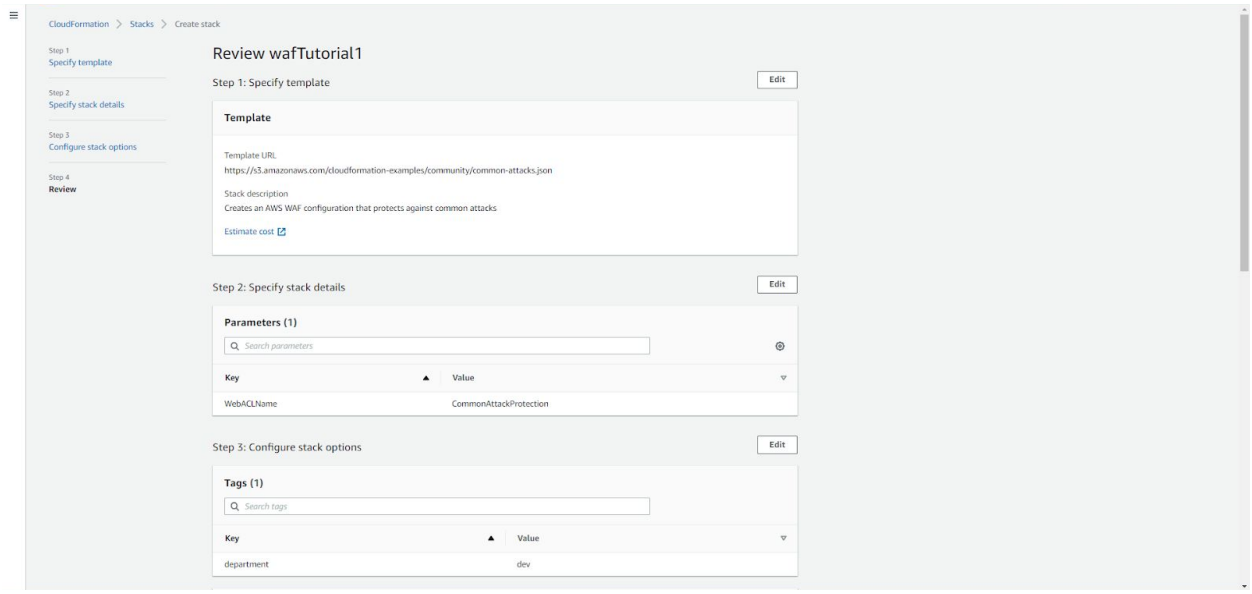
The stack is defined as wafTutorial1. All other settings left at default.

CloudFormation - Create stack



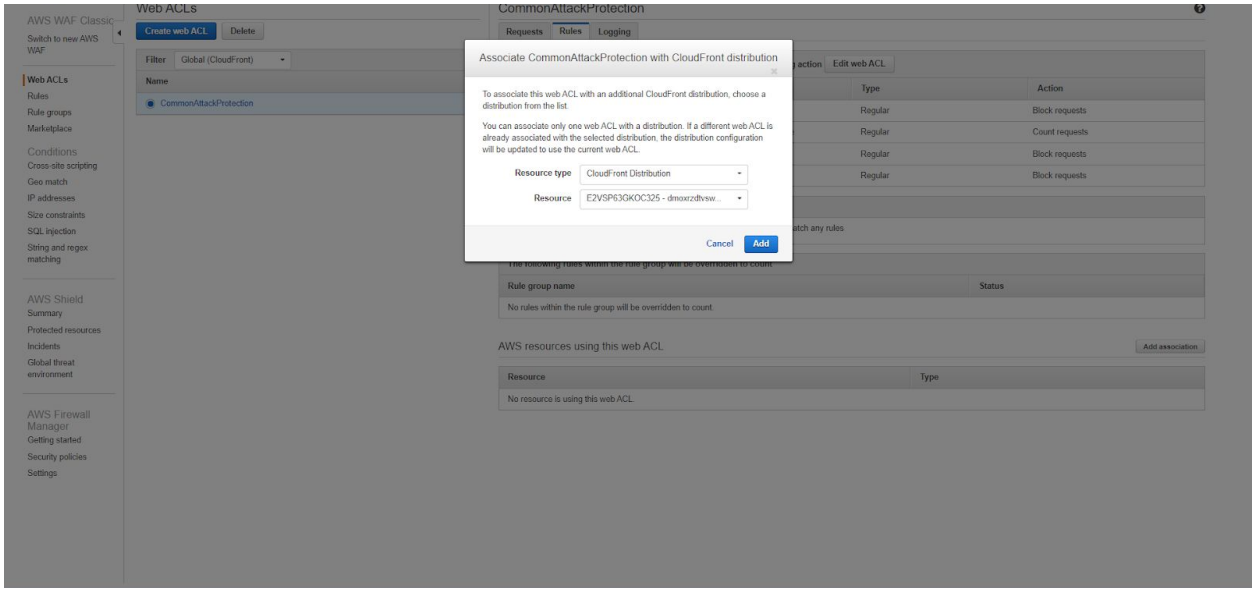
Tags established while no roles were set. CloudFormation will create one automatically.

CloudFormation - Create stack



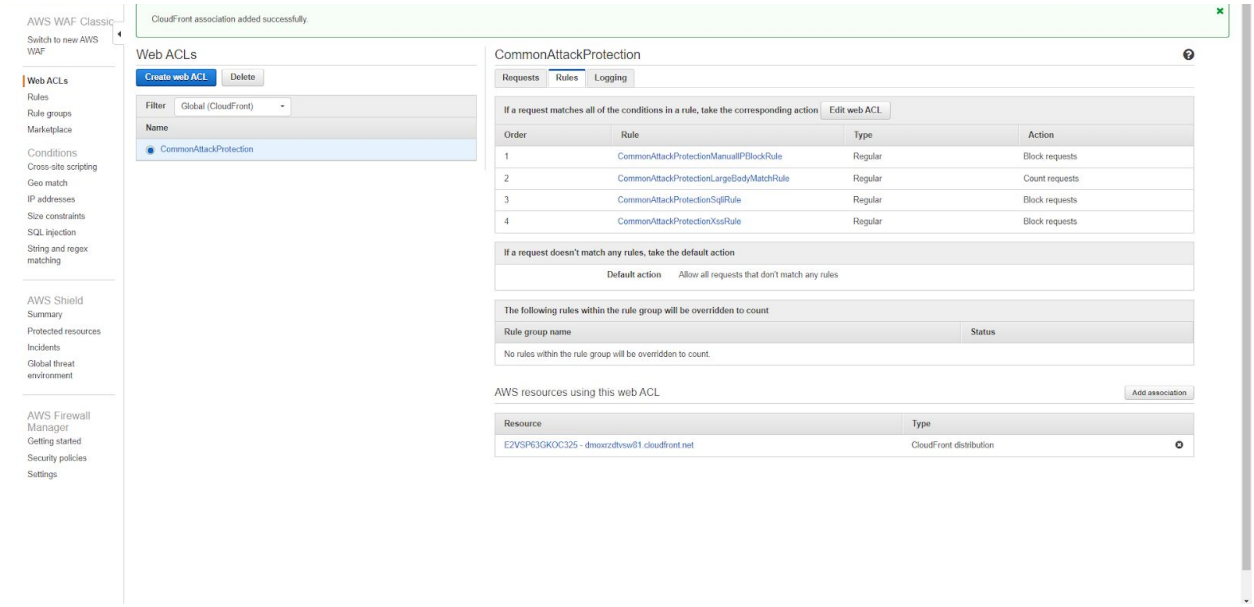
The review page for the CloudFormation stack, wafTutorial1.

AWS WAF - Web ACLs



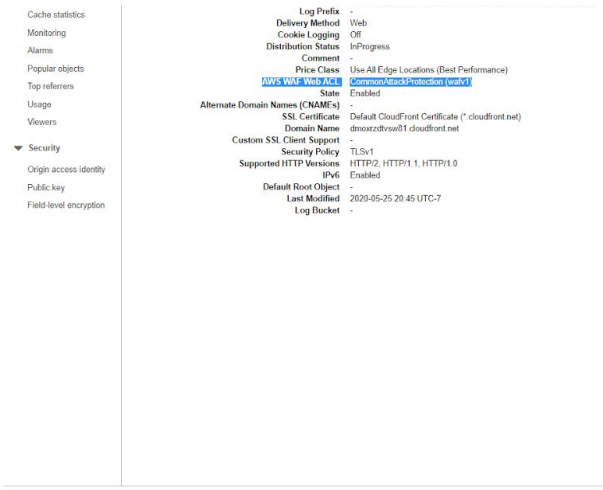
Once the CloudFormation stack is complete, to enable protections an association will be made with the CloudFront distribution.

AWS WAF - CommonAttackProtection WAF



The CloudFront resource has been provisioned with the CommonAttackProtecion WAF.

CloudFront - General tab



To verify correct AWS WAF provisioning, check the CloudFront distribution created at the beginning of the lab. This WAF can be applied to other CloudFront projects.