Solution Overview

This solution is deployed on AWS using 100% serverless services, automated with Terraform and GitHub Actions.

The following AWS Services are utilized in order to enable this solution:

- S3
- CloudFront
- ACM
- WAFv2
- Route53
- SNS
- CloudWatch
- IAM

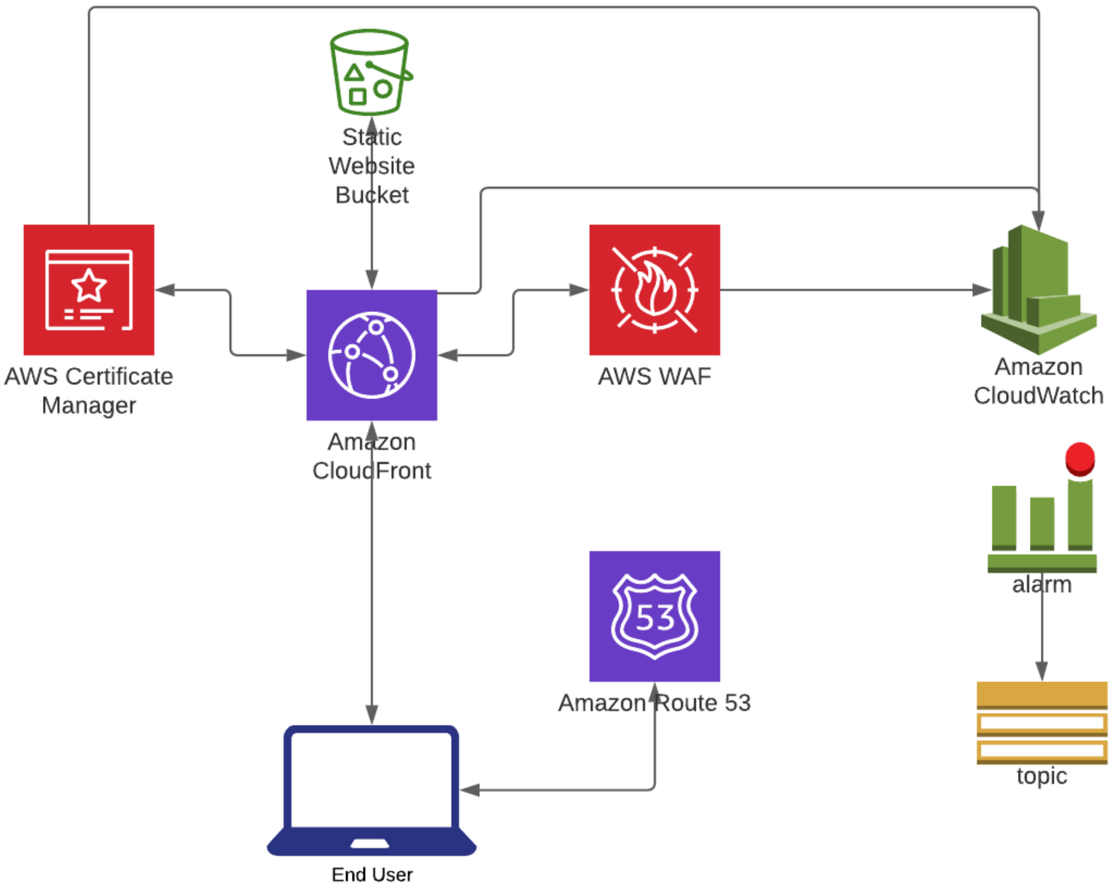
The static HTML content is stored in an S3 bucket configured for static website hosting, which is configured to only allow GET access from the OAI of the CloudFront Distribution.

A CloudFront distribution is configured in order to deliver the website globally with low latency. CloudFront is configured with a CNAME and an ACM Certificate in order to securely receive traffic using TLS to a custom domain name. CloudFront is also configured with an AWS WAFv2, to filter out malicious requests and attacks.

Route53 is utilized in order to automatically approve the ACM Certificate, and create the A record for the configured CNAME on the CloudFront distribution.

Monitoring and alerting are setup using CloudWatch/SNS, in order to maintain observability and for human intervention/investigation in the case of an error in the deployed solution.

Solution Diagram:



Automation:

The entire solution is configured in a Terraform module, so no manual AWS console actions are required in order to deploy the solution. This solution **does** assume that the AWS account is already setup along with the Terraform remote state bucket, as well as a R53 hosted zone is already configured and available.

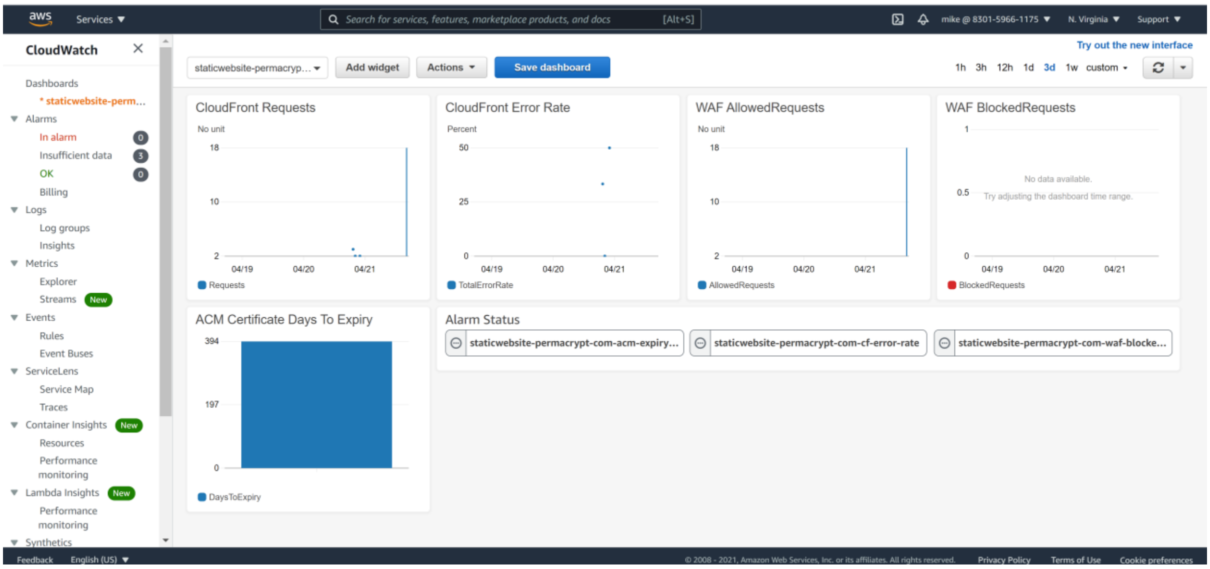
The git repo is also configured with GitHub actions for simple CI/CD, which upon a commit to the Terraform code will automatically run a Terraform plan and apply on the Terraform code.

Security:

The solution is secured using ACM which provides a TLS certificate to the CloudFront distribution to enable encrypted HTTP traffic in transit, and AWS WAFv2, which scans all HTTP requests that are made to the CloudFront distribution and runs the AWS Managed RuleSet which protects against common OWASP top 10 security vulnerabilities.

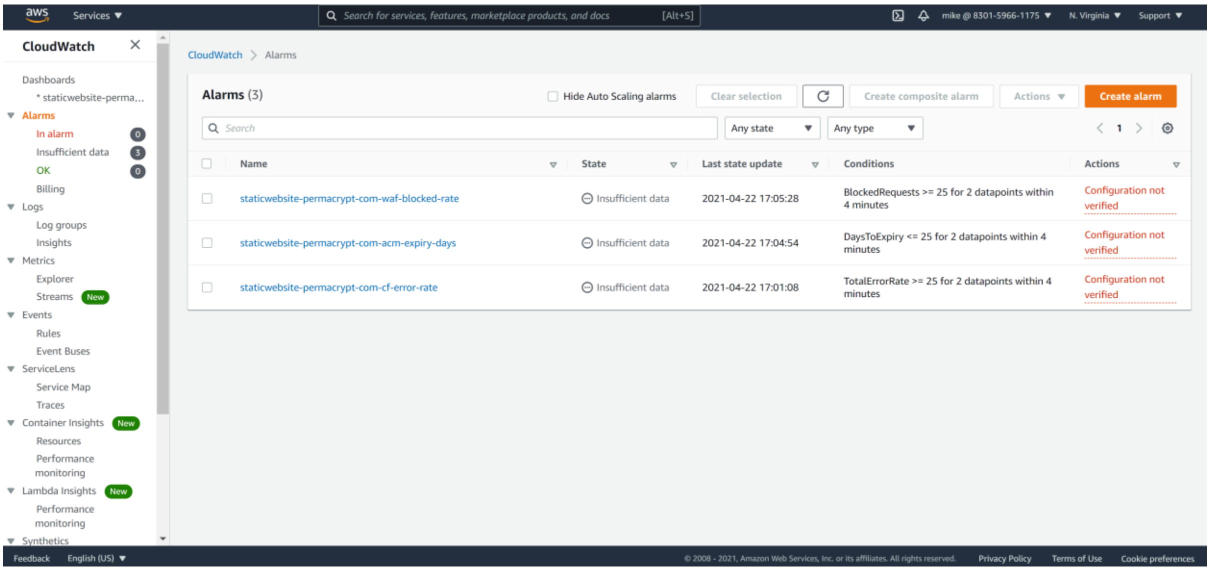
Monitoring/Alerting:

Monitoring is handled using CloudWatch. There is a dashboard that provided an overview of all of the relevant metrics and alarms in one central location:



Alerting:

Alerting is also handled using CloudWatch. CloudFront distribution error rates, WAF blocked request rates and ACM days to certificate expiry are all monitored and configured to send to an SNS topic upon entering the alarm state, the SNS topic is currently not configured to fanout anywhere but can be used to send emails or SMS messages, or can be hooked into an external platform such as PagerDuty.



Alarms (3)

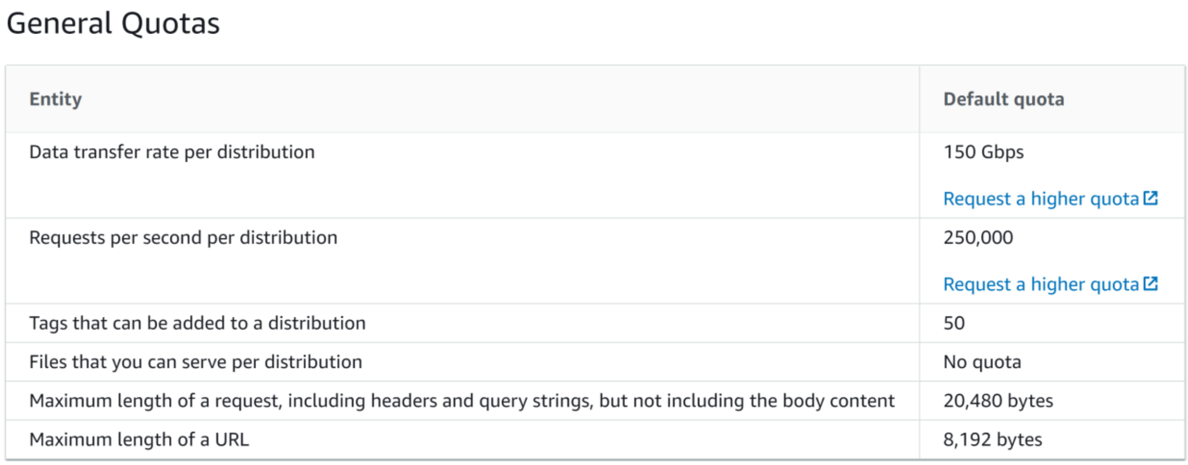
Name	State	Last state update	Conditions	Actions
staticwebsite-permacrypt-com-waf-blocked-rate	Insufficient data	2021-04-22 17:05:28	BlockedRequests >= 25 for 2 datapoints within 4 minutes	Configuration not verified
staticwebsite-permacrypt-com-acm-expiry-days	Insufficient data	2021-04-22 17:04:54	DaysToExpiry <= 25 for 2 datapoints within 4 minutes	Configuration not verified
staticwebsite-permacrypt-com-cf-error-rate	Insufficient data	2021-04-22 17:01:08	TotalErrorRate >= 25 for 2 datapoints within 4 minutes	Configuration not verified

Scaling the Solution

The solution is highly-available, multi-region and fault-tolerant out of the box. CloudFront distributes the origin content to 215+ Edge locations globally, so it is optimized for latency no matter where the end user is located. The DNS for this solution utilizes Route53 which is also a globally distributed service with high availability.

The only limitation to scaling this solution is AWS Service Limits, which out of the box are very generous for CloudFront and WAFv2, and would not pose a challenge for a significant amount of time:

CloudFront Quotas



General Quotas

Entity	Default quota
Data transfer rate per distribution	150 Gbps Request a higher quota
Requests per second per distribution	250,000 Request a higher quota
Tags that can be added to a distribution	50
Files that you can serve per distribution	No quota
Maximum length of a request, including headers and query strings, but not including the body content	20,480 bytes
Maximum length of a URL	8,192 bytes

The TTL for the CloudFront distribution is 60 minutes, so the static HTML page is only fetched from S3 once every 60 minutes which is well within S3 limits which is 5,500 GET requests per second for a specific prefix in a bucket.