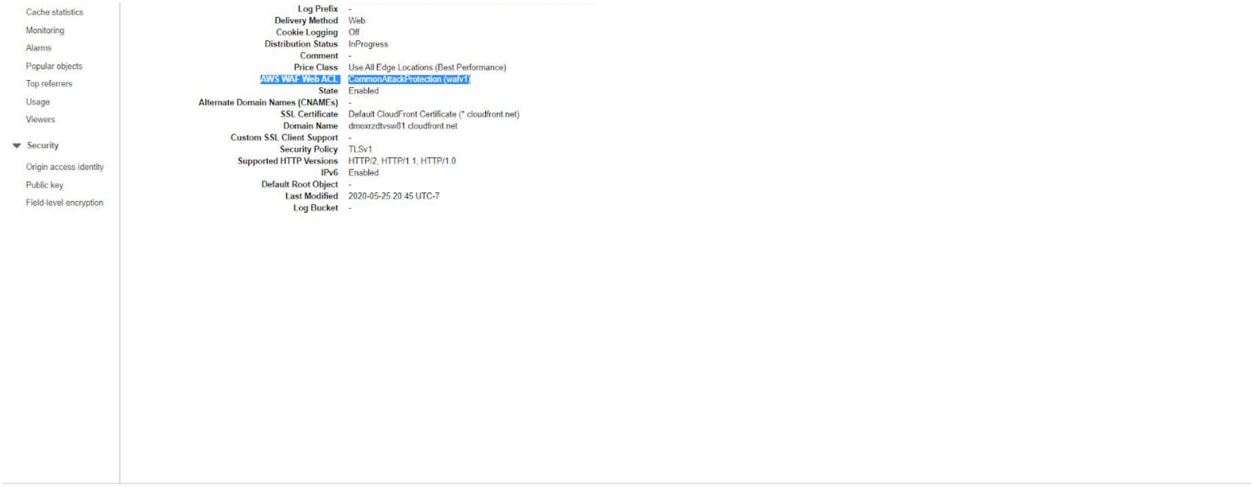
Module 8 Lab 2: Preconfigured Rules w/ Lambda

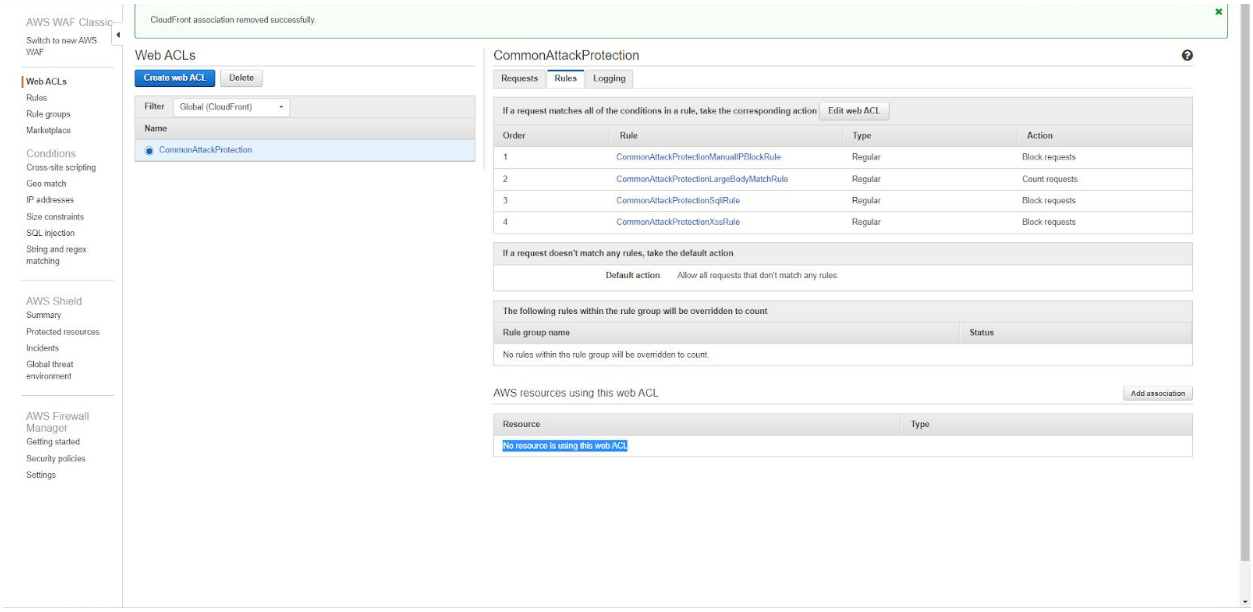
CloudFront - General tab



Log Prefix	-
Delivery Method	Web
Cookie Logging	Off
Distribution Status	InProgress
Comment	-
Price Class	Use All Edge Locations (Best Performance)
AWS WAF Web ACL	CommonAttackProtection (wafv1)
State	Enabled
Alternate Domain Names (CNAMEs)	-
SSL Certificate	Default CloudFront Certificate (*.cloudfront.net)
Domain Name	dmoxrzdtvsw81.cloudfront.net
Custom SSL Client Support	-
Security Policy	TLSv1
Supported HTTP Versions	HTTP/2, HTTP/1.1, HTTP/1.0
IPv6	Enabled
Default Root Object	-
Last Modified	2020-05-25 20:45 UTC-7
Log Bucket	-

In the previous lab, the CloudFront Distribution was provisioned with CommonAttackProtection WAF. For this lab, that will be replaced with preconfigured rules and lambda called “aws waf security automations”.

AWS WAF - Web ACL



CloudFront association removed successfully.

Web ACLs

Filter: Global (CloudFront)

Name
● CommonAttackProtection

CommonAttackProtection

If a request matches all of the conditions in a rule, take the corresponding action

Order	Rule	Type	Action
1	CommonAttackProtectionManualIPBlockRule	Regular	Block requests
2	CommonAttackProtectionLargeBodyMatchRule	Regular	Count requests
3	CommonAttackProtectionSqliRule	Regular	Block requests
4	CommonAttackProtectionXssRule	Regular	Block requests

If a request doesn't match any rules, take the default action

Default action: Allow all requests that don't match any rules

The following rules within the rule group will be overridden to count

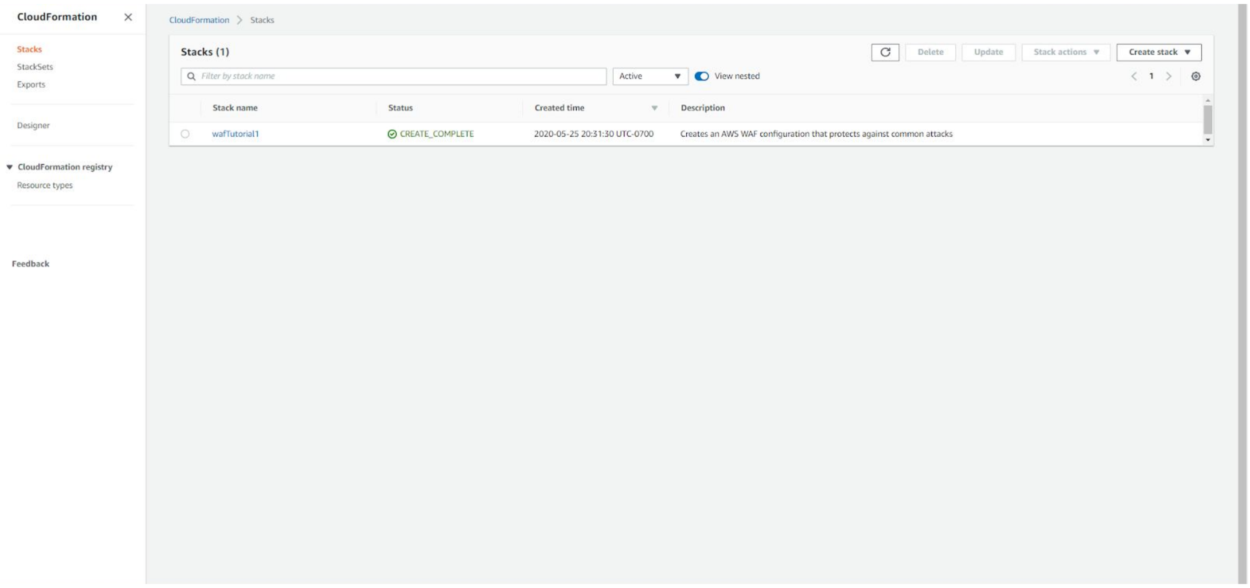
Rule group name	Status
No rules within the rule group will be overridden to count.	

AWS resources using this web ACL

Resource	Type
No resource is using this web ACL	

Note there are no resources using this unwanted web ACL.

CloudFormation - Stacks

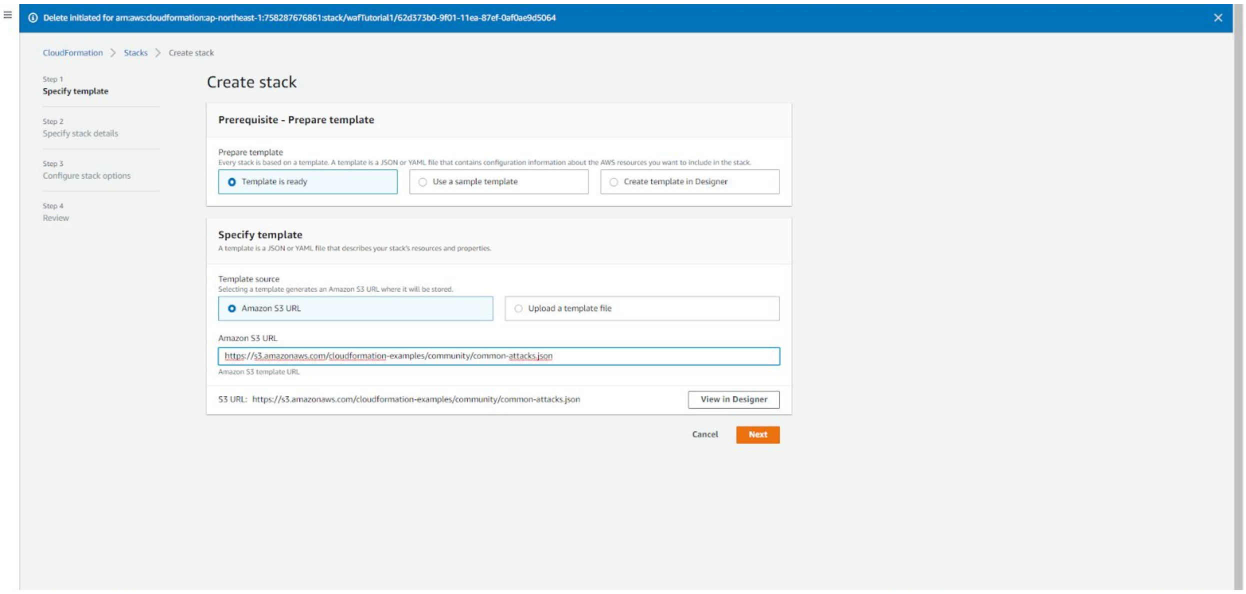


Stacks (1)

Stack name	Status	Created time	Description
wafTutorial1	CREATE_COMPLETE	2020-05-25 20:31:30 UTC-0700	Creates an AWS WAF configuration that protects against common attacks

In CloudFormation, the common attacks WAF stack can now be deleted.

CloudFormation - Create Stack



Delete initiated for arn:aws:cloudformation:ap-northeast-1:758287676861:stack/wafTutorial1/62d373b0-9f01-11ea-87ef-0af0ae9d5064

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

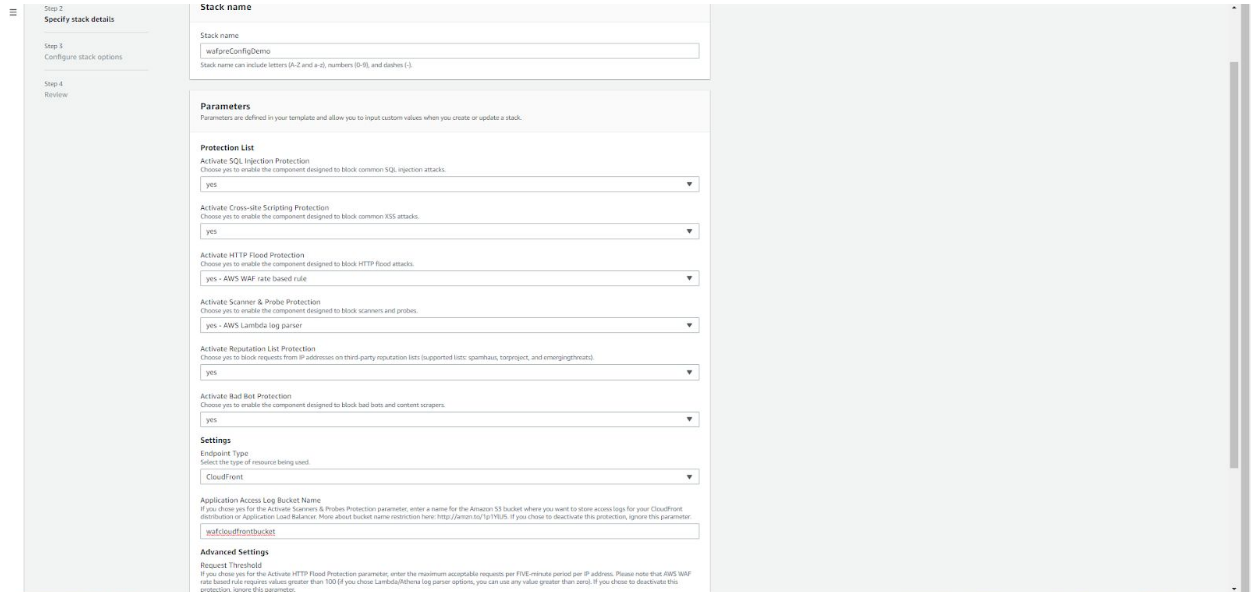
● Amazon S3 URL ○ Upload a template file

Amazon S3 URL
https://s3.amazonaws.com/cloudformation-examples/community/common-attacks.json
Amazon S3 template URL

S3 URL: https://s3.amazonaws.com/cloudformation-examples/community/common-attacks.json

The previous WAF S3 template file location is present, replaced with the new S3 URL.

CloudFormation - Create Stack



Stack name

Stack name

wafpreConfigDemo

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Protection List

Activate SQL Injection Protection
Choose yes to enable the component designed to block common SQL injection attacks.
yes ▼

Activate Cross-site Scripting Protection
Choose yes to enable the component designed to block common XSS attacks.
yes ▼

Activate HTTP Flood Protection
Choose yes to enable the component designed to block HTTP flood attacks.
yes - AWS WAF rate based rule ▼

Activate Scanner & Probe Protection
Choose yes to enable the component designed to block scanners and probes.
yes - AWS Lambda log parser ▼

Activate Reputation List Protection
Choose yes to block requests from IP addresses on third-party reputation lists (supported lists: spamhaus, torproject, and emergingthreats).
yes ▼

Activate Bad Bot Protection
Choose yes to enable the component designed to block bad bots and content scrapers.
yes ▼

Settings

Endpoint Type
Select the type of resource being used.
CloudFront ▼

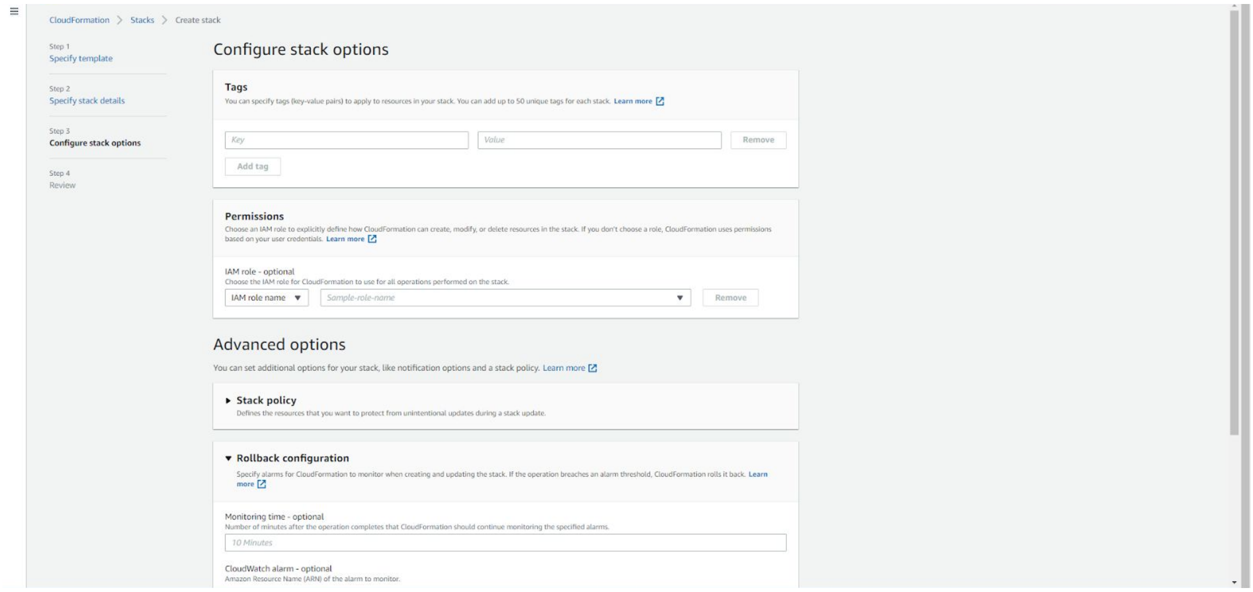
Application Access Log Bucket Name
If you chose yes for the Activate Scanners & Probes Protection parameter, enter a name for the Amazon S3 bucket where you want to store access logs for your CloudFront distribution or Application Load Balancer. More about bucket name restriction here: http://amzn.to/1p1YlU5. If you chose to deactivate this protection, ignore this parameter.
wafcloudfrontbucket

Advanced Settings

Request Threshold
If you chose yes for the Activate HTTP Flood Protection parameter, enter the maximum acceptable requests per FIVE-minute period per IP address. Please note that AWS WAF rate based rule requires values greater than 100 (if you chose Lambda/Athena log parser options, you can use any value greater than zero). If you chose to deactivate this protection, ignore this parameter.

Note the questions about what to protect. Enter a log bucket name.

CloudFormation - Create Stack



Configure stack options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. Learn more

Permissions

Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more

IAM role - optional
Choose the IAM role for CloudFormation to use for all operations performed on the stack.
IAM role name ▼ Sample-role-name ▼ Remove

Advanced options

You can set additional options for your stack, like notification options and a stack policy. Learn more

▸ **Stack policy**
Defines the resources that you want to protect from unintentional updates during a stack update.

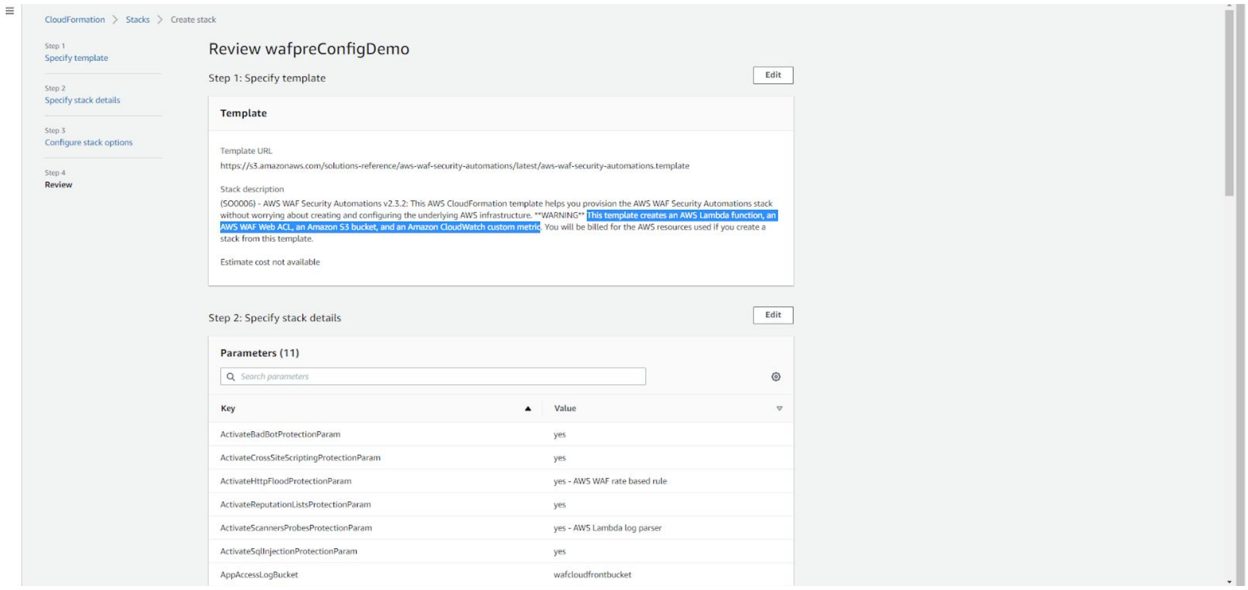
▾ **Rollback configuration**
Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back. Learn more

Monitoring time - optional
Number of minutes after the operation completes that CloudFormation should continue monitoring the specified alarms.
10 Minutes

CloudWatch alarm - optional
Amazon Resource Name (ARN) of the alarm to monitor.

Roles are made automatically. All other settings left a default.

CloudFormation - Create Stack



CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Review wafpreConfigDemo

Step 1: Specify template

Template

Template URL
https://s3.amazonaws.com/solutions-reference/aws-waf-security-automations/latest/aws-waf-security-automations.template

Stack description
(SO0006) - AWS WAF Security Automations v2.3.2: This AWS CloudFormation template helps you provision the AWS WAF Security Automations stack without worrying about creating and configuring the underlying AWS infrastructure. **WARNING** This template creates an AWS Lambda function, an AWS WAF Web ACL, an Amazon S3 bucket, and an Amazon CloudWatch custom metric. You will be billed for the AWS resources used if you create a stack from this template.

Estimate cost not available

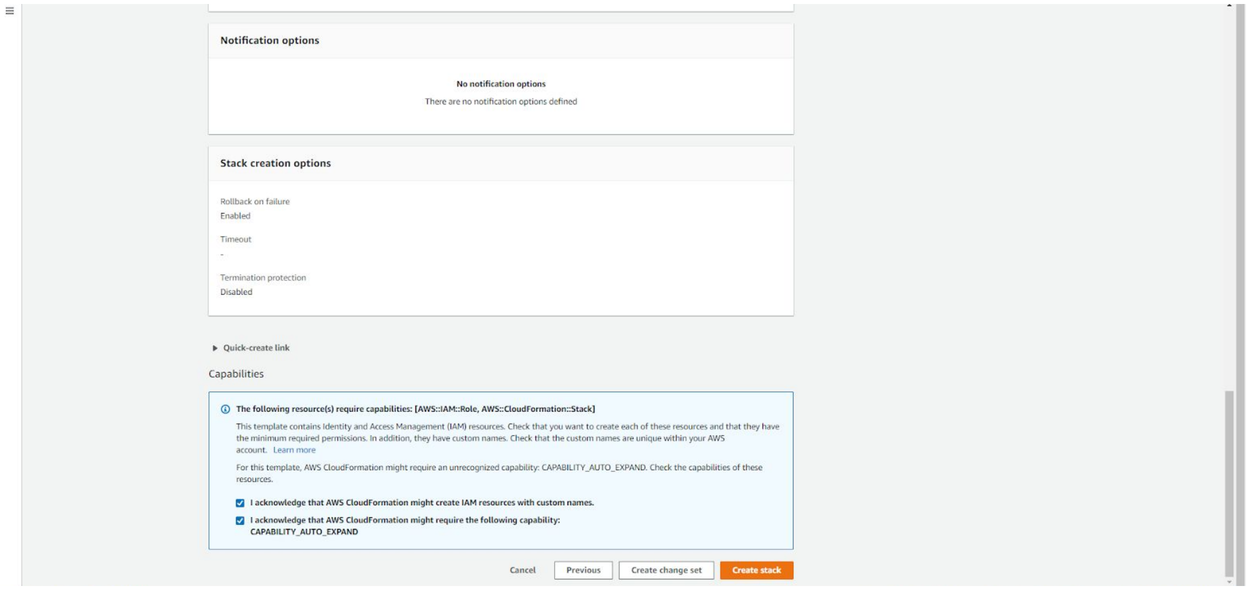
Step 2: Specify stack details

Parameters (11)

Key	Value
ActivateBadBotProtectionParam	yes
ActivateCrossSiteScriptingProtectionParam	yes
ActivateHttpFloodProtectionParam	yes - AWS WAF rate based rule
ActivateReputationListsProtectionParam	yes
ActivateScannersProbesProtectionParam	yes - AWS Lambda log parser
ActivateSqlInjectionProtectionParam	yes
AppAccessLogBucket	wafcloudfrontbucket

Note the Stack description explains what exactly will be created.

CloudFormation - Create Stack



Notification options

No notification options
There are no notification options defined

Stack creation options

Rollback on failure
Enabled

Timeout
-

Termination protection
Disabled

▸ Quick-create link

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role, AWS::CloudFormation::Stack]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more

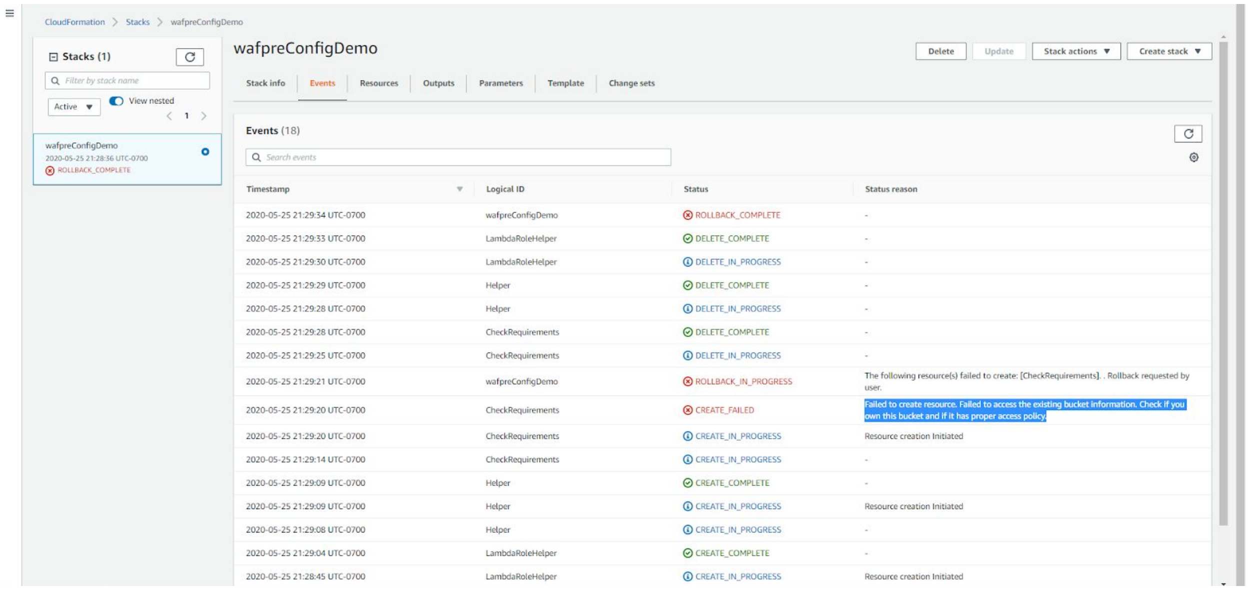
For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the capabilities of these resources.

☑ **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**

☑ **I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND**

Other capabilities will be created with this CloudFormation template in order for the stack to work.

CloudFormation - Stacks



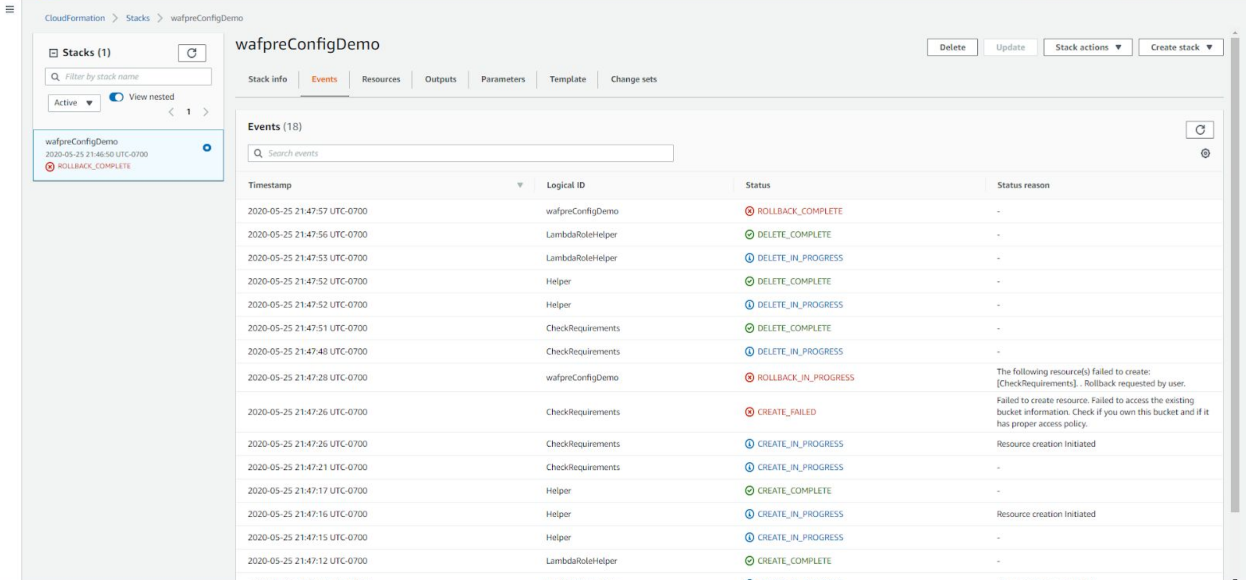
wafpreConfigDemo
2020-05-25 21:28:36 UTC-0700
ROLLBACK_COMPLETE

Events (18)

Timestamp	Logical ID	Status	Status reason
2020-05-25 21:29:34 UTC-0700	wafpreConfigDemo	ROLLBACK_COMPLETE	-
2020-05-25 21:29:33 UTC-0700	LambdaRoleHelper	DELETE_COMPLETE	-
2020-05-25 21:29:30 UTC-0700	LambdaRoleHelper	DELETE_IN_PROGRESS	-
2020-05-25 21:29:29 UTC-0700	Helper	DELETE_COMPLETE	-
2020-05-25 21:29:28 UTC-0700	Helper	DELETE_IN_PROGRESS	-
2020-05-25 21:29:28 UTC-0700	CheckRequirements	DELETE_COMPLETE	-
2020-05-25 21:29:25 UTC-0700	CheckRequirements	DELETE_IN_PROGRESS	-
2020-05-25 21:29:21 UTC-0700	wafpreConfigDemo	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [CheckRequirements]. . Rollback requested by user.
2020-05-25 21:29:20 UTC-0700	CheckRequirements	CREATE_FAILED	Failed to create resource. Failed to access the existing bucket information. Check if you own this bucket and if it has proper access policy.
2020-05-25 21:29:20 UTC-0700	CheckRequirements	CREATE_IN_PROGRESS	Resource creation Initiated
2020-05-25 21:29:14 UTC-0700	CheckRequirements	CREATE_IN_PROGRESS	-
2020-05-25 21:29:09 UTC-0700	Helper	CREATE_COMPLETE	-
2020-05-25 21:29:09 UTC-0700	Helper	CREATE_IN_PROGRESS	Resource creation Initiated
2020-05-25 21:29:08 UTC-0700	Helper	CREATE_IN_PROGRESS	-
2020-05-25 21:29:04 UTC-0700	LambdaRoleHelper	CREATE_COMPLETE	-
2020-05-25 21:28:45 UTC-0700	LambdaRoleHelper	CREATE_IN_PROGRESS	Resource creation Initiated

The stack creation failed. The S3 bucket may have an existing permission from the previous CloudFormation stack. The location is Tokyo. A new S3 bucket and Cloudfront may be required.

CloudFormation - Stacks



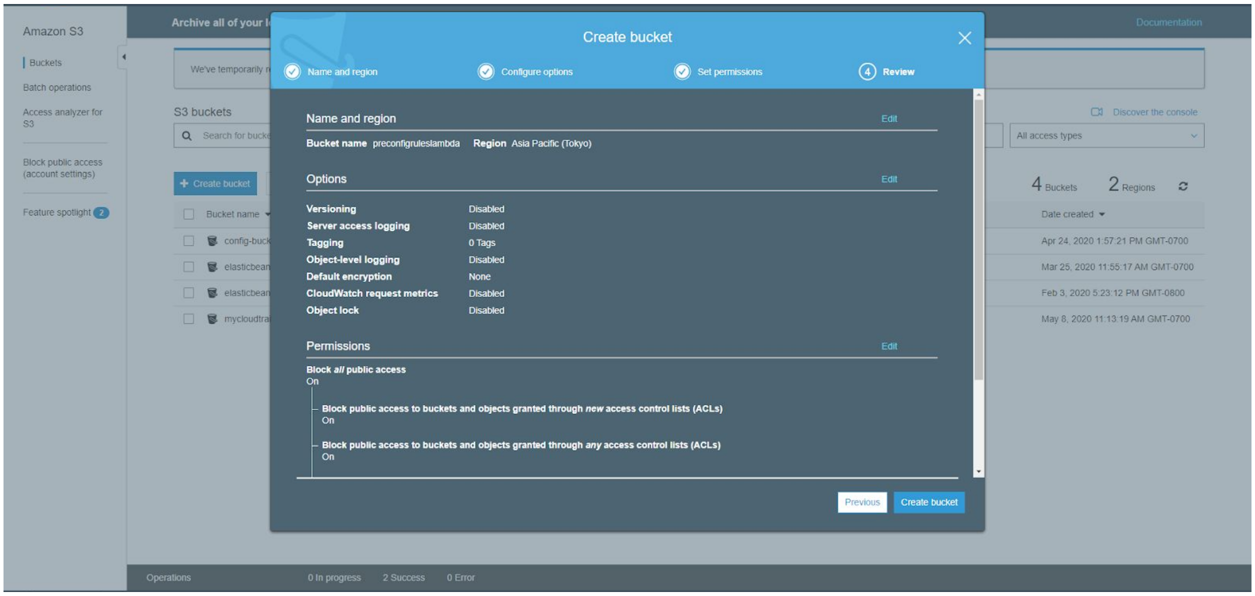
wafpreConfigDemo
2020-05-25 21:46:50 UTC-0700
ROLLBACK_COMPLETE

Events (18)

Timestamp	Logical ID	Status	Status reason
2020-05-25 21:47:57 UTC-0700	wafpreConfigDemo	ROLLBACK_COMPLETE	-
2020-05-25 21:47:56 UTC-0700	LambdaRoleHelper	DELETE_COMPLETE	-
2020-05-25 21:47:53 UTC-0700	LambdaRoleHelper	DELETE_IN_PROGRESS	-
2020-05-25 21:47:52 UTC-0700	Helper	DELETE_COMPLETE	-
2020-05-25 21:47:52 UTC-0700	Helper	DELETE_IN_PROGRESS	-
2020-05-25 21:47:51 UTC-0700	CheckRequirements	DELETE_COMPLETE	-
2020-05-25 21:47:48 UTC-0700	CheckRequirements	DELETE_IN_PROGRESS	-
2020-05-25 21:47:28 UTC-0700	wafpreConfigDemo	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [CheckRequirements]. . Rollback requested by user.
2020-05-25 21:47:26 UTC-0700	CheckRequirements	CREATE_FAILED	Failed to create resource. Failed to access the existing bucket information. Check if you own this bucket and if it has proper access policy.
2020-05-25 21:47:26 UTC-0700	CheckRequirements	CREATE_IN_PROGRESS	Resource creation Initiated
2020-05-25 21:47:21 UTC-0700	CheckRequirements	CREATE_IN_PROGRESS	-
2020-05-25 21:47:17 UTC-0700	Helper	CREATE_COMPLETE	-
2020-05-25 21:47:16 UTC-0700	Helper	CREATE_IN_PROGRESS	Resource creation Initiated
2020-05-25 21:47:15 UTC-0700	Helper	CREATE_IN_PROGRESS	-
2020-05-25 21:47:12 UTC-0700	LambdaRoleHelper	CREATE_COMPLETE	-

The same error occurred. A new S3 bucket and CloudFront will be created.

Amazon S3 - Create bucket



Create bucket

Name and region · Configure options · Set permissions · 4 Review

Name and region

Bucket name preconfigruleslambda **Region** Asia Pacific (Tokyo)

Options

Versioning	Disabled
Server access logging	Disabled
Tagging	0 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled
Object lock	Disabled

Permissions

Block *all* public access
On

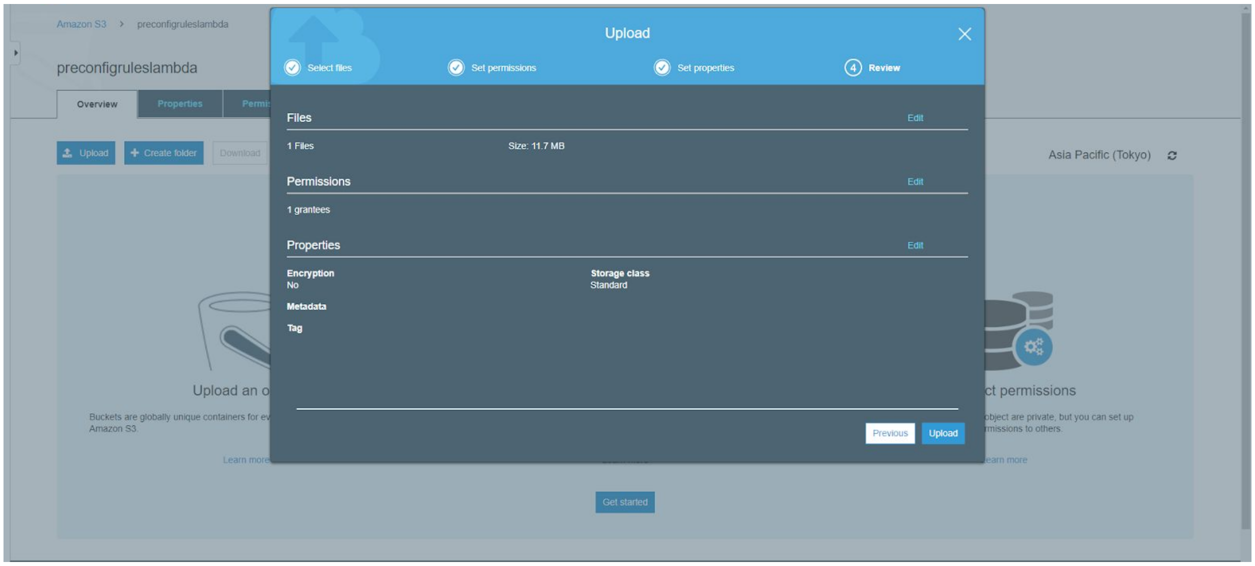
Block public access to buckets and objects granted through *new* access control lists (ACLs)
On

Block public access to buckets and objects granted through *any* access control lists (ACLs)
On

Previous | Create bucket

A new S3 bucket was created in the Tokyo region.

Amazon S3 - Upload



Upload

Select files · Set permissions · Set properties · 4 Review

Files

1 Files Size: 11.7 MB

Permissions

1 grantees

Properties

Encryption
No

Storage class
Standard

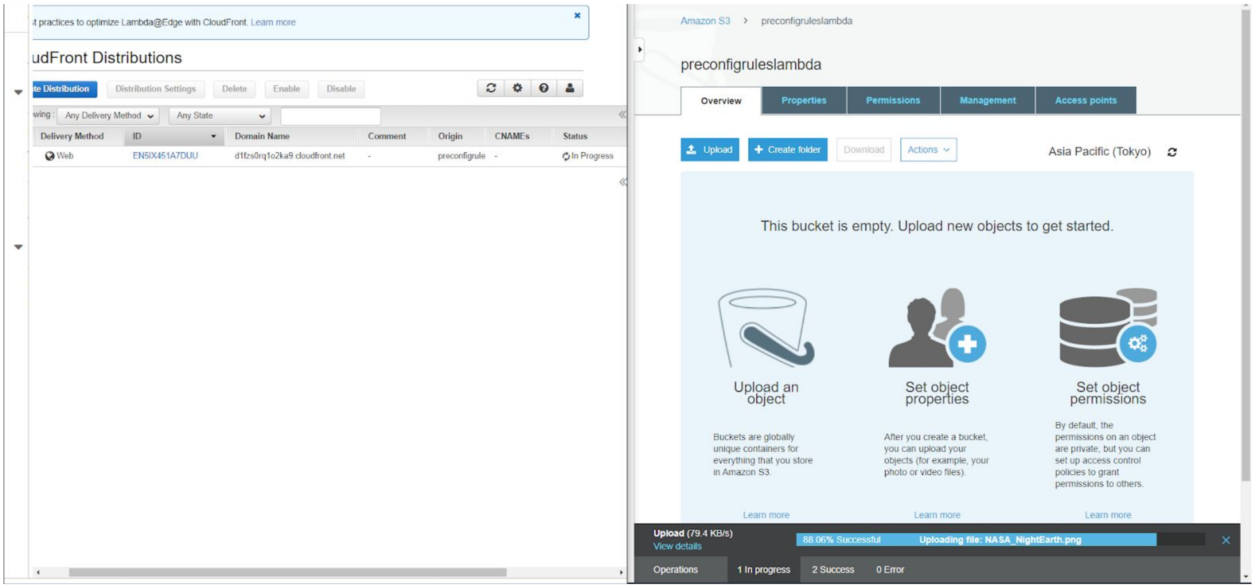
Metadata

Tag

Previous | Upload

All settings were left at default.

CloudFront/S3 Upload



:t practices to optimize Lambda@Edge with CloudFront. Learn more

udFront Distributions

wing : Any Delivery Method | Any State

Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status
Web	EN5IX451A7DUU	d1fzs0rq1o2ka9.cloudfront.net	-	preconfigrule	-	In Progress

Amazon S3 > preconfigruleslambda

preconfigruleslambda

Asia Pacific (Tokyo)

This bucket is empty. Upload new objects to get started.

Upload an object

Buckets are globally unique containers for everything that you store in Amazon S3.

Learn more

Set object properties

After you create a bucket, you can upload your objects (for example, your photo or video files).

Learn more

Set object permissions

By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.

Learn more

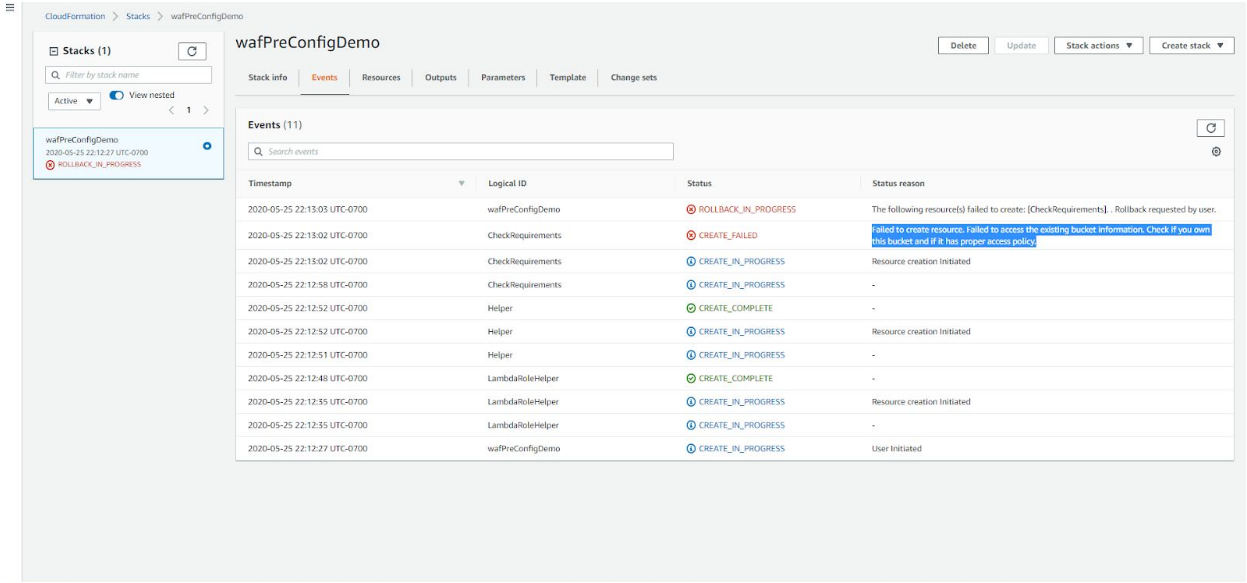
Upload (79.4 KB/s)
View details

88.06% Successful Uploading file: NASA_NightEarth.png

Operations | 1 In progress | 2 Success | 0 Error

Note that the CloudFront distribution and a file upload occurred simultaneously.

CloudFormation - Stacks



CloudFormation > Stacks > wafPreConfigDemo

Stacks (1)

Filter by stack name

Active | View nested

wafPreConfigDemo
2020-05-25 22:12:27 UTC-0700
ROLLBACK_IN_PROGRESS

wafPreConfigDemo

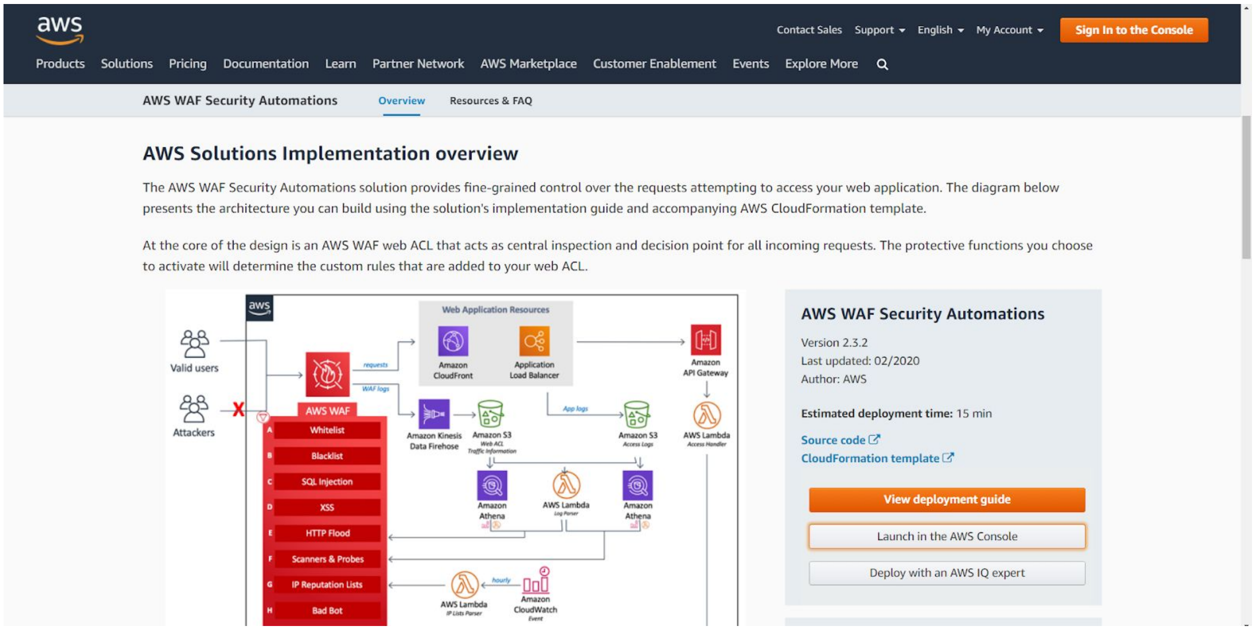
Events (11)

Search events

Timestamp	Logical ID	Status	Status reason
2020-05-25 22:13:03 UTC-0700	wafPreConfigDemo	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [CheckRequirements]. . Rollback requested by user.
2020-05-25 22:13:02 UTC-0700	CheckRequirements	CREATE_FAILED	Failed to create resource. Failed to access the existing bucket information. Check if you own this bucket and if it has proper access policy.
2020-05-25 22:13:02 UTC-0700	CheckRequirements	CREATE_IN_PROGRESS	Resource creation Initiated
2020-05-25 22:12:58 UTC-0700	CheckRequirements	CREATE_IN_PROGRESS	-
2020-05-25 22:12:52 UTC-0700	Helper	CREATE_COMPLETE	-
2020-05-25 22:12:52 UTC-0700	Helper	CREATE_IN_PROGRESS	Resource creation Initiated
2020-05-25 22:12:51 UTC-0700	Helper	CREATE_IN_PROGRESS	-
2020-05-25 22:12:48 UTC-0700	LambdaRoleHelper	CREATE_COMPLETE	-
2020-05-25 22:12:35 UTC-0700	LambdaRoleHelper	CREATE_IN_PROGRESS	Resource creation Initiated
2020-05-25 22:12:35 UTC-0700	LambdaRoleHelper	CREATE_IN_PROGRESS	-
2020-05-25 22:12:27 UTC-0700	wafPreConfigDemo	CREATE_IN_PROGRESS	User Initiated

The same error occurred again even with a new S3 bucket and CloudFront distribution.

AWS web



AWS Solutions Implementation overview

The AWS WAF Security Automations solution provides fine-grained control over the requests attempting to access your web application. The diagram below presents the architecture you can build using the solution's implementation guide and accompanying AWS CloudFormation template.

At the core of the design is an AWS WAF web ACL that acts as central inspection and decision point for all incoming requests. The protective functions you choose to activate will determine the custom rules that are added to your web ACL.

AWS WAF Security Automations

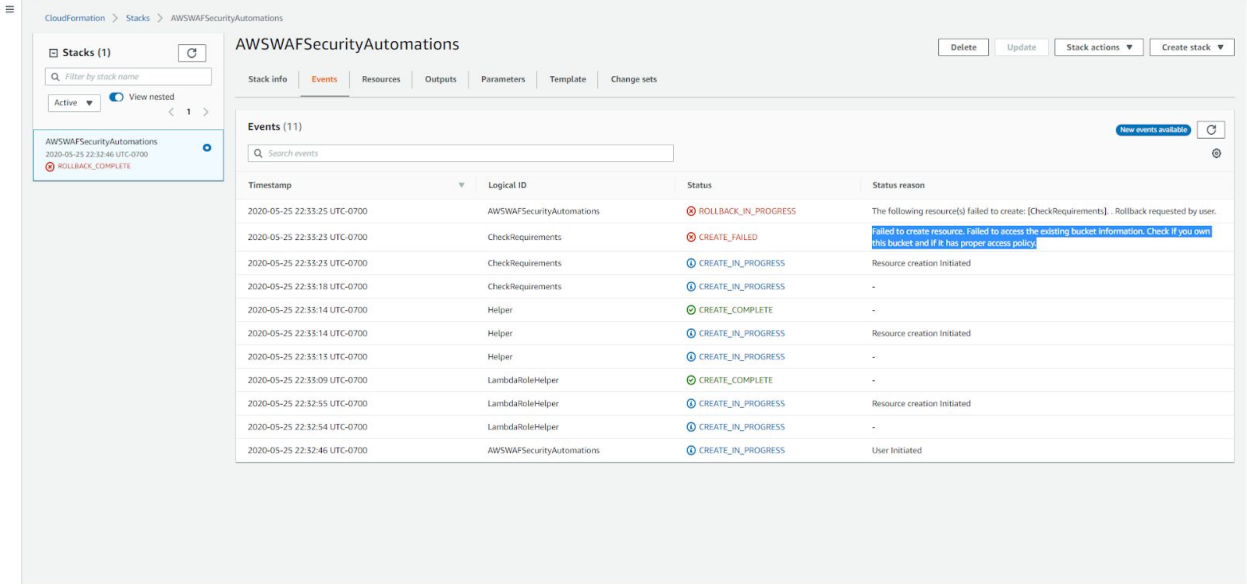
Version 2.3.2
Last updated: 02/2020
Author: AWS

Estimated deployment time: 15 min

Source code
CloudFormation template

Amazon provides a solution with a Launch in the AWS console option.

CloudFormation - Stacks



AWSWAFSecurityAutomations
2020-05-25 22:32:46 UTC-0700
ROLLBACK_COMPLETE

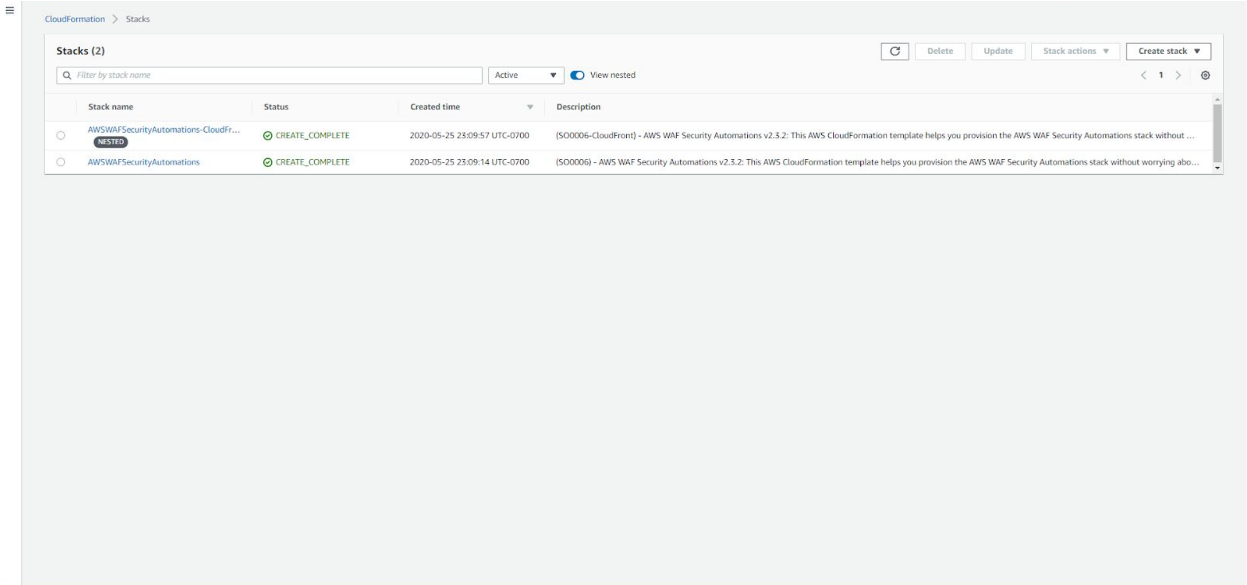
AWSWAFSecurityAutomations

Events (11)

Timestamp	Logical ID	Status	Status reason
2020-05-25 22:33:25 UTC-0700	AWSWAFSecurityAutomations	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [CheckRequirements]. . Rollback requested by user.
2020-05-25 22:33:23 UTC-0700	CheckRequirements	CREATE_FAILED	Failed to create resource. Failed to access the existing bucket information. Check if you own this bucket and if it has proper access policy.
2020-05-25 22:33:23 UTC-0700	CheckRequirements	CREATE_IN_PROGRESS	Resource creation Initiated
2020-05-25 22:33:18 UTC-0700	CheckRequirements	CREATE_IN_PROGRESS	-
2020-05-25 22:33:14 UTC-0700	Helper	CREATE_COMPLETE	-
2020-05-25 22:33:14 UTC-0700	Helper	CREATE_IN_PROGRESS	Resource creation Initiated
2020-05-25 22:33:13 UTC-0700	Helper	CREATE_IN_PROGRESS	-
2020-05-25 22:33:09 UTC-0700	LambdaRoleHelper	CREATE_COMPLETE	-
2020-05-25 22:32:55 UTC-0700	LambdaRoleHelper	CREATE_IN_PROGRESS	Resource creation Initiated
2020-05-25 22:32:54 UTC-0700	LambdaRoleHelper	CREATE_IN_PROGRESS	-
2020-05-25 22:32:46 UTC-0700	AWSWAFSecurityAutomations	CREATE_IN_PROGRESS	User Initiated

However the same issue applies.

CloudFormation - Stacks

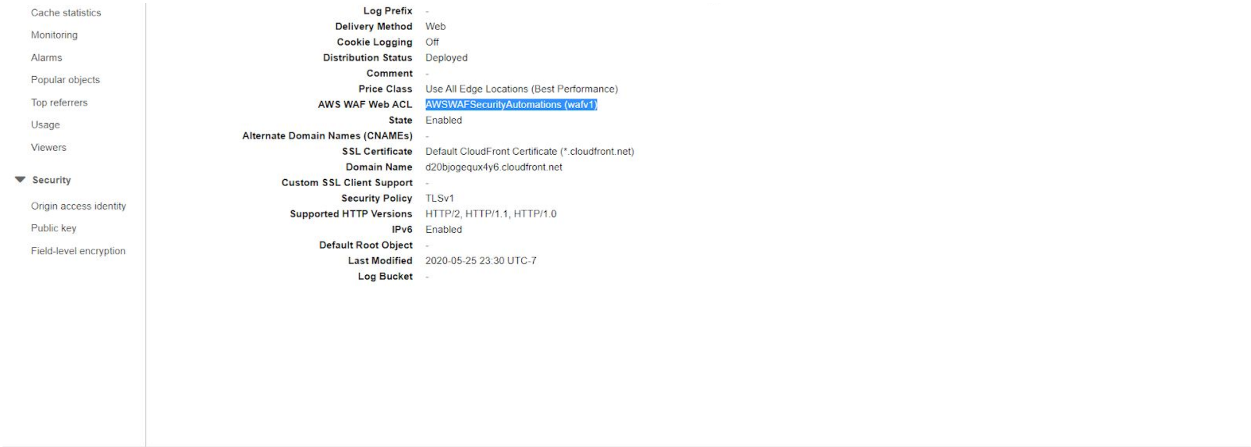


Stacks (2)

	Stack name	Status	Created time	Description
○	AWSWAFSecurityAutomations-CloudFr... NESTED	CREATE_COMPLETE	2020-05-25 23:09:57 UTC-0700	(SO0006-CloudFront) - AWS WAF Security Automations v2.3.2: This AWS CloudFormation template helps you provision the AWS WAF Security Automations stack without ...
○	AWSWAFSecurityAutomations	CREATE_COMPLETE	2020-05-25 23:09:14 UTC-0700	(SO0006) - AWS WAF Security Automations v2.3.2: This AWS CloudFormation template helps you provision the AWS WAF Security Automations stack without worrying abo...

Success! The following changes occured, N. Virginia bucket, smaller file upload, creating a new CloudFront Distribution, and using the AWS WAF Security Automations Launch in the AWS console option.

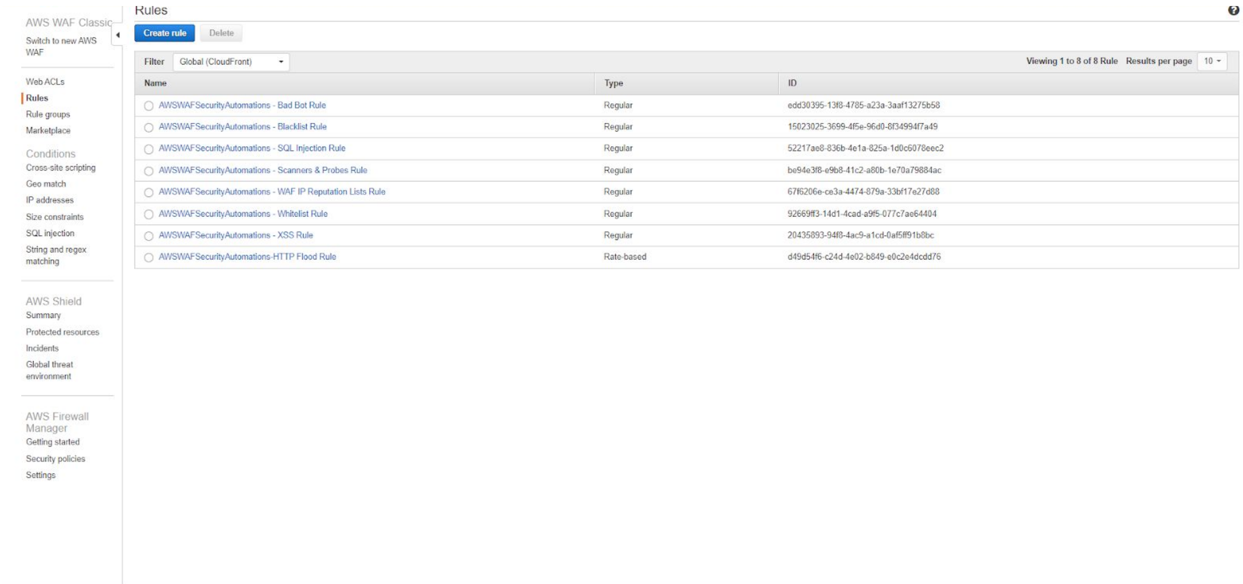
CloudFront - General tab



Log Prefix	-
Delivery Method	Web
Cookie Logging	Off
Distribution Status	Deployed
Comment	-
Price Class	Use All Edge Locations (Best Performance)
AWS WAF Web ACL	AWSWAFSecurityAutomations (wafv1)
State	Enabled
Alternate Domain Names (CNAMEs)	-
SSL Certificate	Default CloudFront Certificate (*.cloudfront.net)
Domain Name	d20bjogequx4y6.cloudfront.net
Custom SSL Client Support	-
Security Policy	TLSv1
Supported HTTP Versions	HTTP/2, HTTP/1.1, HTTP/1.0
IPv6	Enabled
Default Root Object	-
Last Modified	2020-05-25 23:30 UTC-7
Log Bucket	-

To verify the correct WAF has been set, note that AWS WAF Security Automations is defined.

AWS WAF Classic - Rules



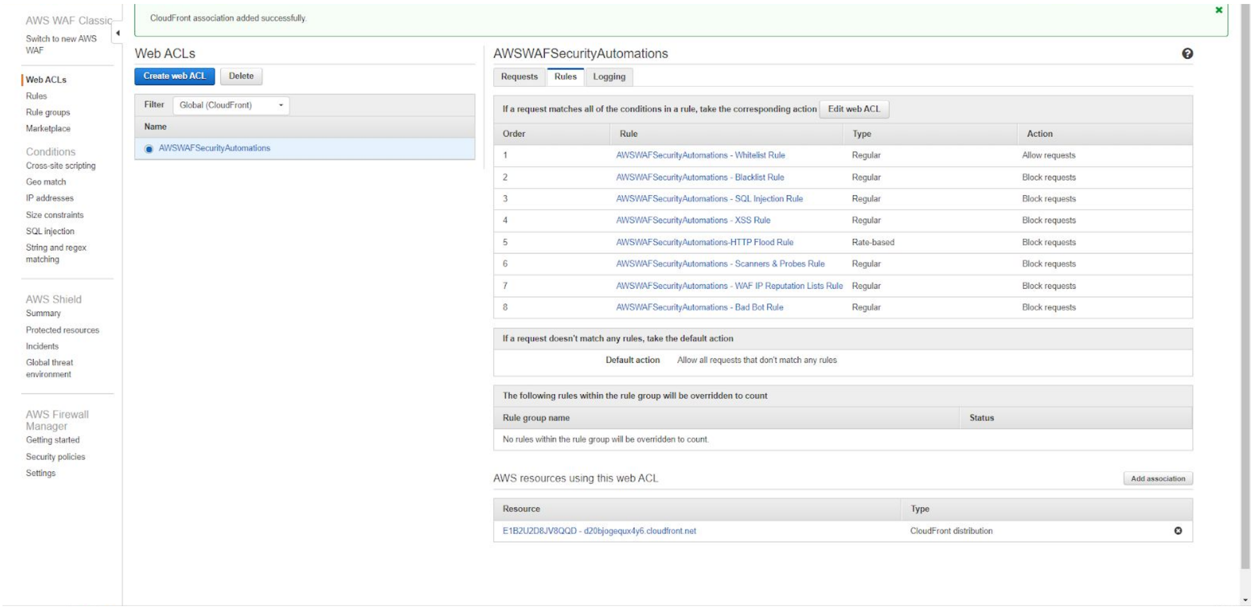
Filter: Global (CloudFront)

Viewing 1 to 8 of 8 Rule Results per page 10

Name	Type	ID
○ AWSWAFSecurityAutomations - Bad Bot Rule	Regular	edd30395-13f8-4785-a23a-3aaf13275b58
○ AWSWAFSecurityAutomations - Blacklist Rule	Regular	15023025-3699-4f5e-96d0-8f34994f7a49
○ AWSWAFSecurityAutomations - SQL Injection Rule	Regular	52217ae8-836b-4e1a-825a-1d0c6078eec2
○ AWSWAFSecurityAutomations - Scanners & Probes Rule	Regular	be94e3f8-e9b8-41c2-a80b-1e70a79884ac
○ AWSWAFSecurityAutomations - WAF IP Reputation Lists Rule	Regular	67f6206e-ce3a-4474-879a-33bf17e27d88
○ AWSWAFSecurityAutomations - Whitelist Rule	Regular	92669ff3-14d1-4cad-a9f5-077c7ae64404
○ AWSWAFSecurityAutomations - XSS Rule	Regular	20435893-94f8-4ac9-a1cd-0af5ff91b8bc
○ AWSWAFSecurityAutomations-HTTP Flood Rule	Rate-based	d49d54f6-c24d-4e02-b849-e0c2e4dcdd76

The rule sets have been created.

AWS WAF Classic - Web ACLs



CloudFront association added successfully.

Filter: Global (CloudFront)

Name
● AWSWAFSecurityAutomations

AWSWAFSecurityAutomations

If a request matches all of the conditions in a rule, take the corresponding action

Order	Rule	Type	Action
1	AWSWAFSecurityAutomations - Whitelist Rule	Regular	Allow requests
2	AWSWAFSecurityAutomations - Blacklist Rule	Regular	Block requests
3	AWSWAFSecurityAutomations - SQL Injection Rule	Regular	Block requests
4	AWSWAFSecurityAutomations - XSS Rule	Regular	Block requests
5	AWSWAFSecurityAutomations-HTTP Flood Rule	Rate-based	Block requests
6	AWSWAFSecurityAutomations - Scanners & Probes Rule	Regular	Block requests
7	AWSWAFSecurityAutomations - WAF IP Reputation Lists Rule	Regular	Block requests
8	AWSWAFSecurityAutomations - Bad Bot Rule	Regular	Block requests

If a request doesn't match any rules, take the default action

Default action: Allow all requests that don't match any rules

The following rules within the rule group will be overridden to count

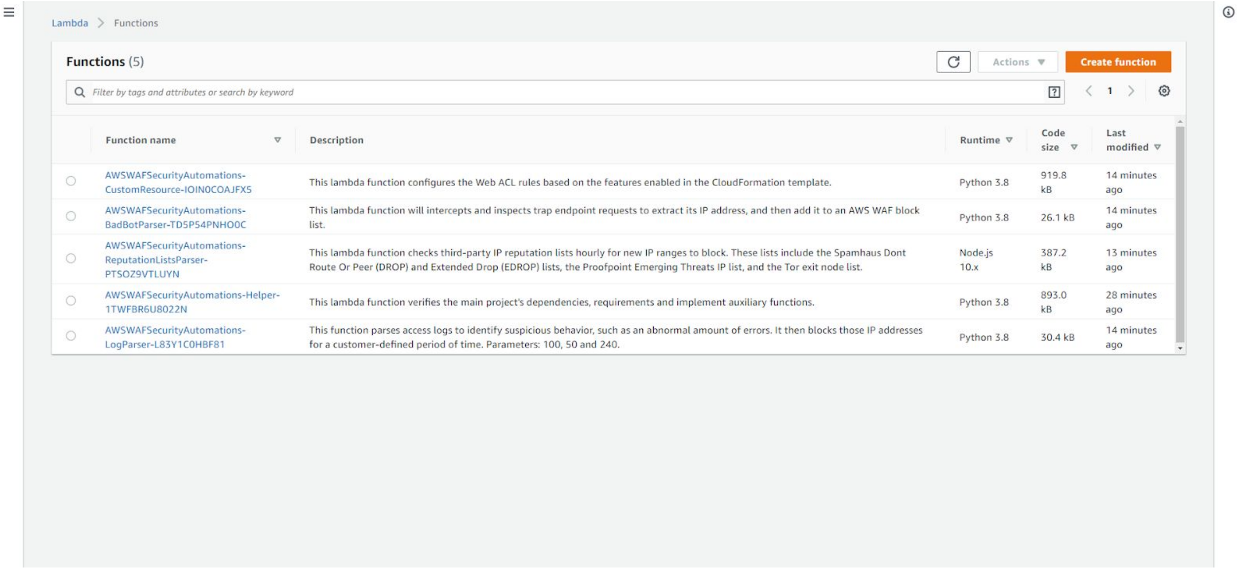
Rule group name	Status
No rules within the rule group will be overridden to count.	

AWS resources using this web ACL

Resource	Type
E1B2U2D8JV8QQD - d20bjogequx4y6.cloudfront.net	CloudFront distribution

The CloudFront resource successfully added.

Lambda - Functions



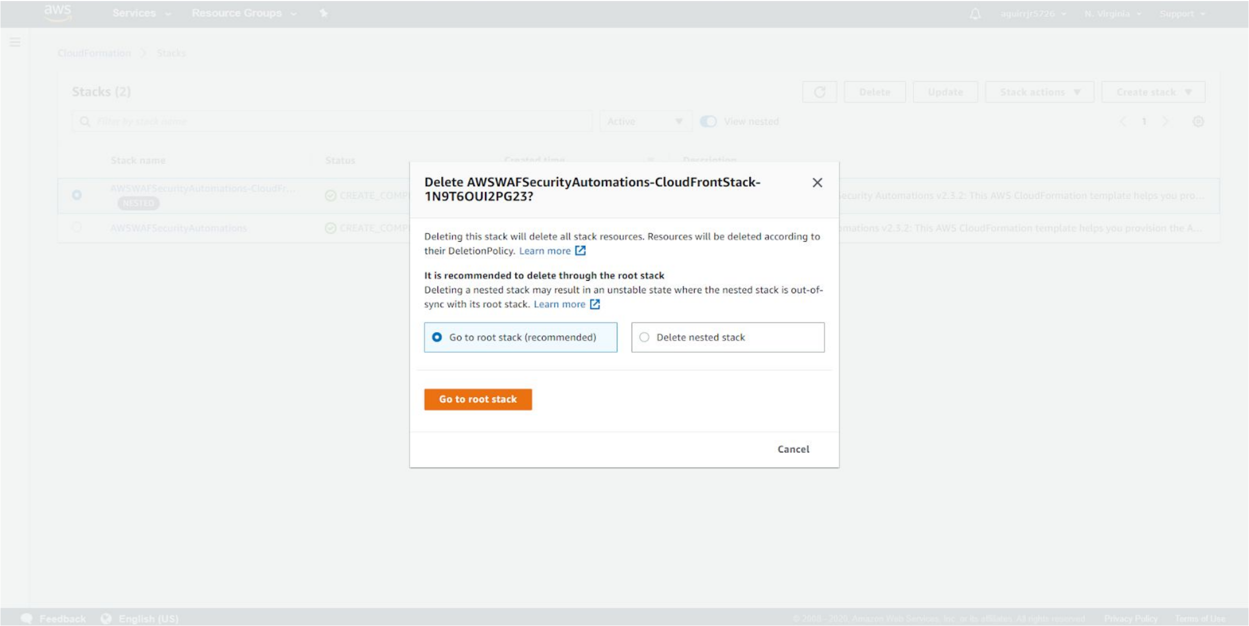
Functions (5)

Filter by tags and attributes or search by keyword

Function name	Description	Runtime	Code size	Last modified
AWSWAFSecurityAutomations-CustomResource-IOIN0COAJFX5	This lambda function configures the Web ACL rules based on the features enabled in the CloudFormation template.	Python 3.8	919.8 kB	14 minutes ago
AWSWAFSecurityAutomations-BadBotParser-TD5P54PNHO0C	This lambda function will intercepts and inspects trap endpoint requests to extract its IP address, and then add it to an AWS WAF block list.	Python 3.8	26.1 kB	14 minutes ago
AWSWAFSecurityAutomations-ReputationListsParser-PTSOZ9VTLUYN	This lambda function checks third-party IP reputation lists hourly for new IP ranges to block. These lists include the Spamhaus Dont Route Or Peer (DROP) and Extended Drop (EDROP) lists, the Proofpoint Emerging Threats IP list, and the Tor exit node list.	Node.js 10.x	387.2 kB	13 minutes ago
AWSWAFSecurityAutomations-Helper-1TWFBR6U8022N	This lambda function verifies the main project's dependencies, requirements and implement auxiliary functions.	Python 3.8	893.0 kB	28 minutes ago
AWSWAFSecurityAutomations-LogParser-L83Y1C0HBF81	This function parses access logs to identify suspicious behavior, such as an abnormal amount of errors. It then blocks those IP addresses for a customer-defined period of time. Parameters: 100, 50 and 240.	Python 3.8	30.4 kB	14 minutes ago

The lambda functions that are at the heart of the autonomous application.

Nested Stack Warning



Delete AWSWAFSecurityAutomations-CloudFrontStack-1N9T6OUI2PG23?

Deleting this stack will delete all stack resources. Resources will be deleted according to their DeletionPolicy. Learn more

It is recommended to delete through the root stack

Deleting a nested stack may result in an unstable state where the nested stack is out-of-sync with its root stack. Learn more

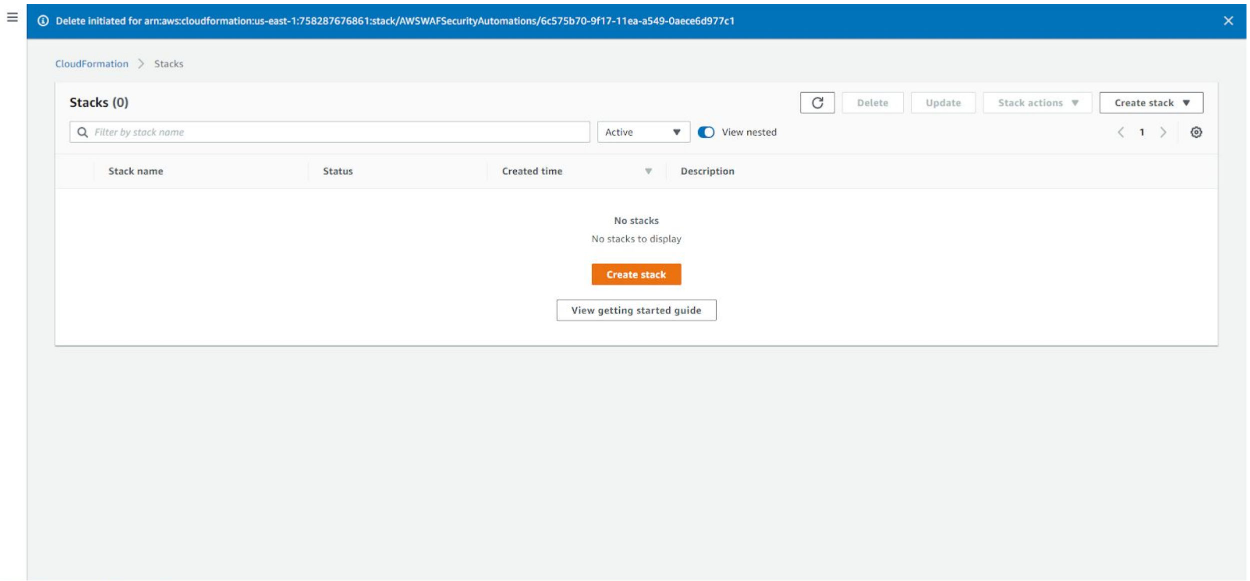
● Go to root stack (recommended)   ○ Delete nested stack

Go to root stack

Cancel

Deleting a stack containing a nested stack requires deleting the root stack first.

CloudFormation - Stacks



Delete initiated for arn:aws:cloudformation:us-east-1:758287676861:stack/AWSWAFSecurityAutomations/6c575b70-9f17-11ea-a549-0aece6d977c1

No stacks

No stacks to display

All stacks deleted.