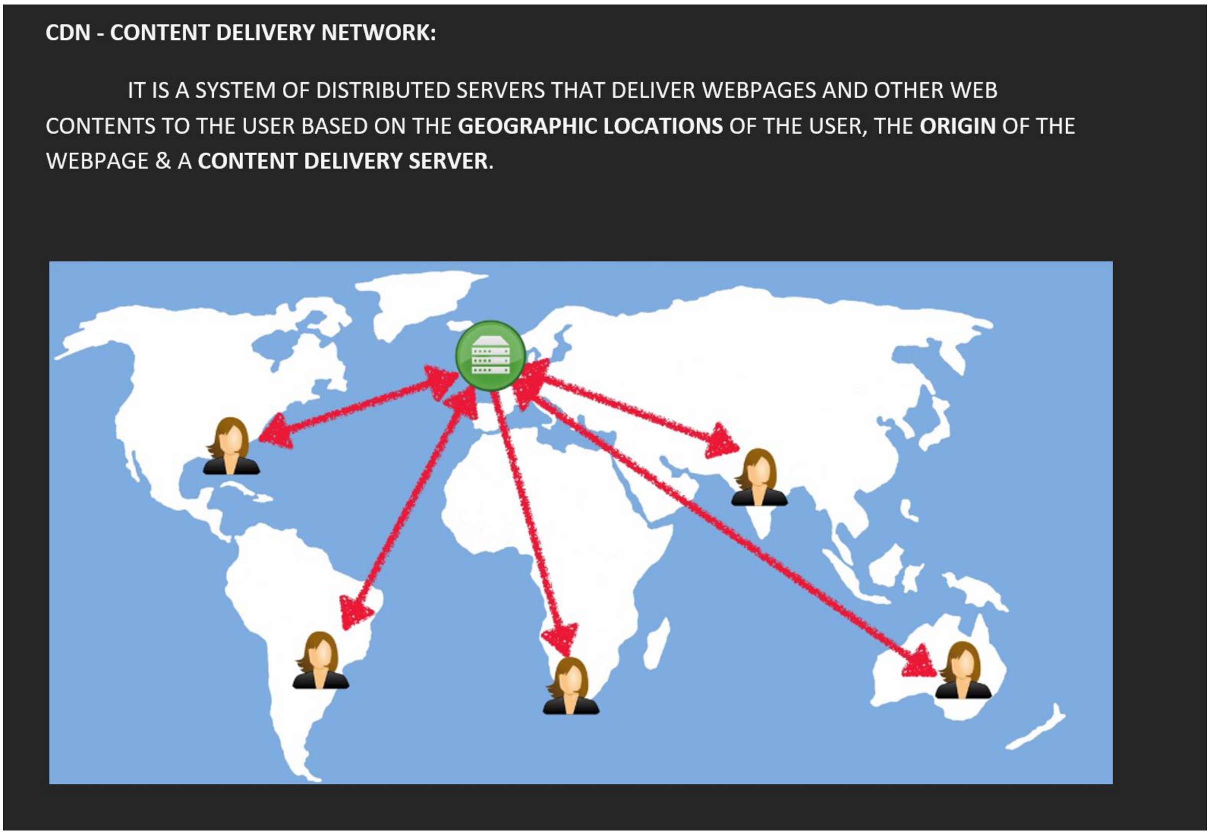
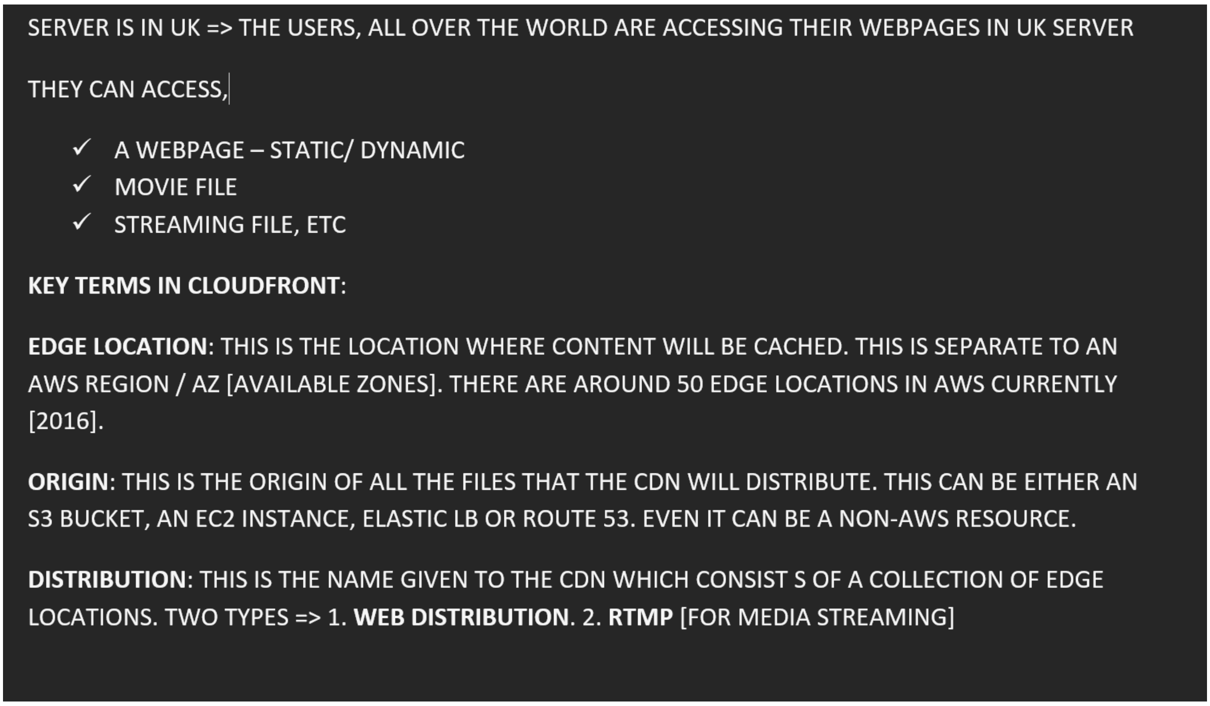
CLOUD FRONT AND CLOUD FORMATION

CLOUD FRONT network and content delivery



CDN - CONTENT DELIVERY NETWORK:

IT IS A SYSTEM OF DISTRIBUTED SERVERS THAT DELIVER WEBPAGES AND OTHER WEB CONTENTS TO THE USER BASED ON THE **GEOGRAPHIC LOCATIONS** OF THE USER, THE **ORIGIN** OF THE WEBPAGE & A **CONTENT DELIVERY SERVER**.



SERVER IS IN UK => THE USERS, ALL OVER THE WORLD ARE ACCESSING THEIR WEBPAGES IN UK SERVER

THEY CAN ACCESS,

- ✓ A WEBPAGE – STATIC/ DYNAMIC
- ✓ MOVIE FILE
- ✓ STREAMING FILE, ETC

KEY TERMS IN CLOUDFRONT:

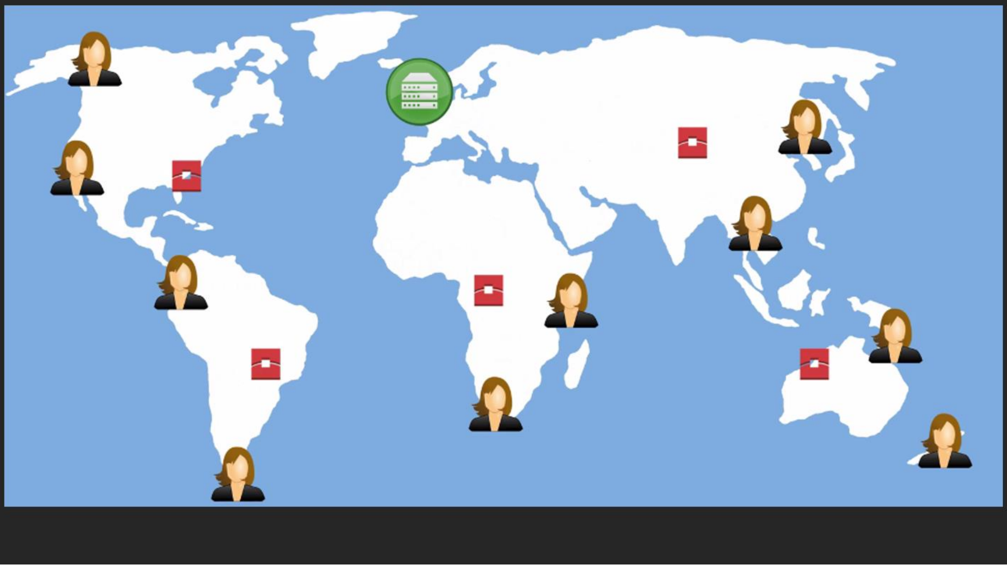
EDGE LOCATION: THIS IS THE LOCATION WHERE CONTENT WILL BE CACHED. THIS IS SEPARATE TO AN AWS REGION / AZ [AVAILABLE ZONES]. THERE ARE AROUND 50 EDGE LOCATIONS IN AWS CURRENTLY [2016].

ORIGIN: THIS IS THE ORIGIN OF ALL THE FILES THAT THE CDN WILL DISTRIBUTE. THIS CAN BE EITHER AN S3 BUCKET, AN EC2 INSTANCE, ELASTIC LB OR ROUTE 53. EVEN IT CAN BE A NON-AWS RESOURCE.

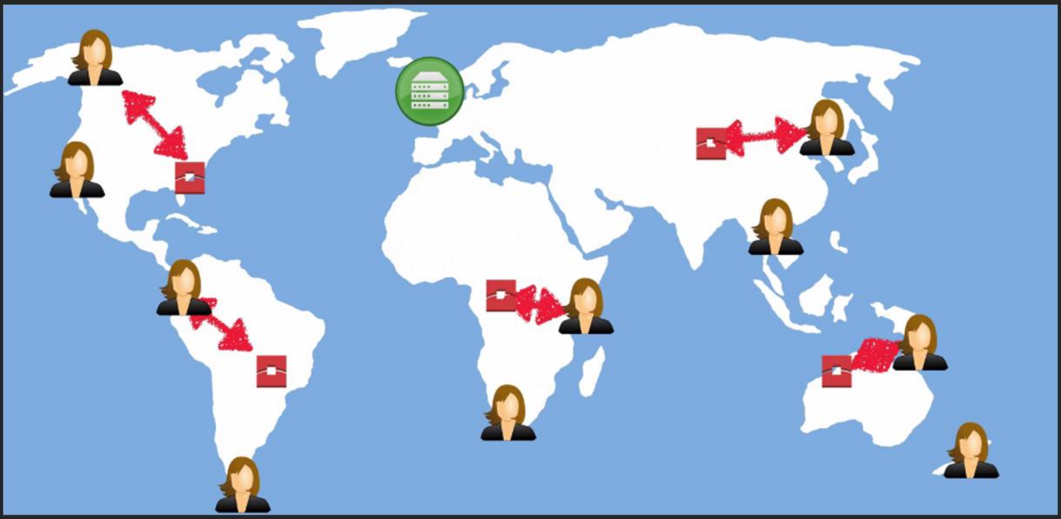
DISTRIBUTION: THIS IS THE NAME GIVEN TO THE CDN WHICH CONSIST S OF A COLLECTION OF EDGE LOCATIONS. TWO TYPES => 1. **WEB DISTRIBUTION**. 2. **RTMP** [FOR MEDIA STREAMING]

MULTIPLE USERS IN MULTIPLE PART OF THE WORLD:

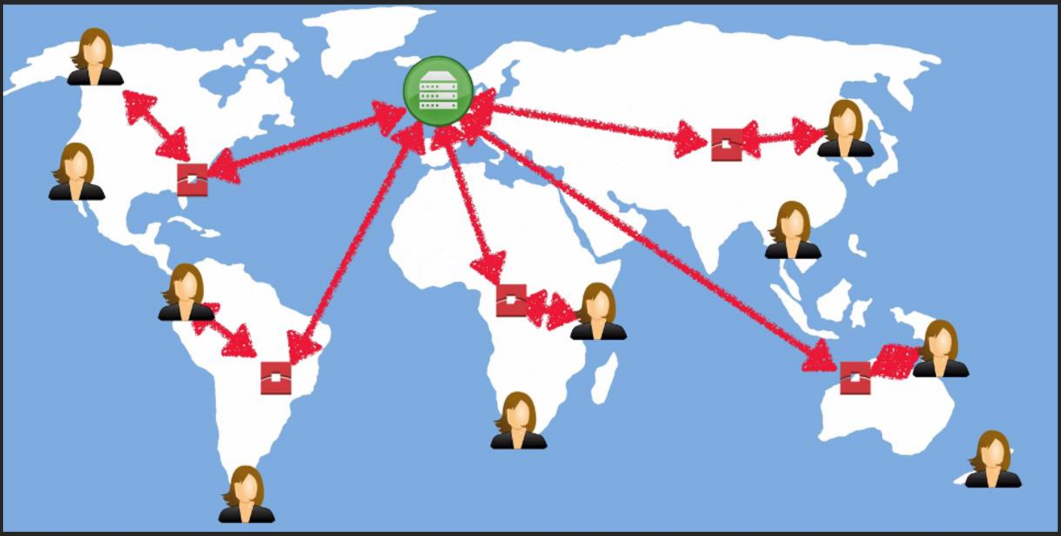
EDGE LOCATIONS SPREADS ALL ACROSS THE WORLD:



WHEN THE FIRST USER ACCESS TO THE CONTENT & THAT GOES TO THE E.L:



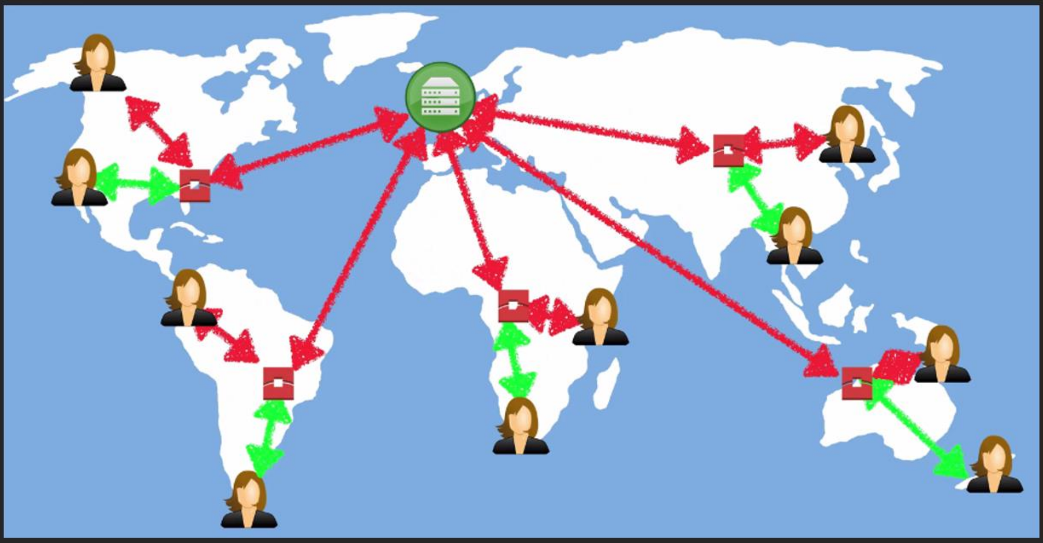
IF IT NOT CACHED IN THE EDGE LOC => THEN AS PER DISTRIBUTION, IT ROUTES TO THE CDN SERVER:



THUS THE FIRST USER ACCESSES THE CONTENT WITH NO SPEACILITY, RATHER THAN A NORMALE CASE.

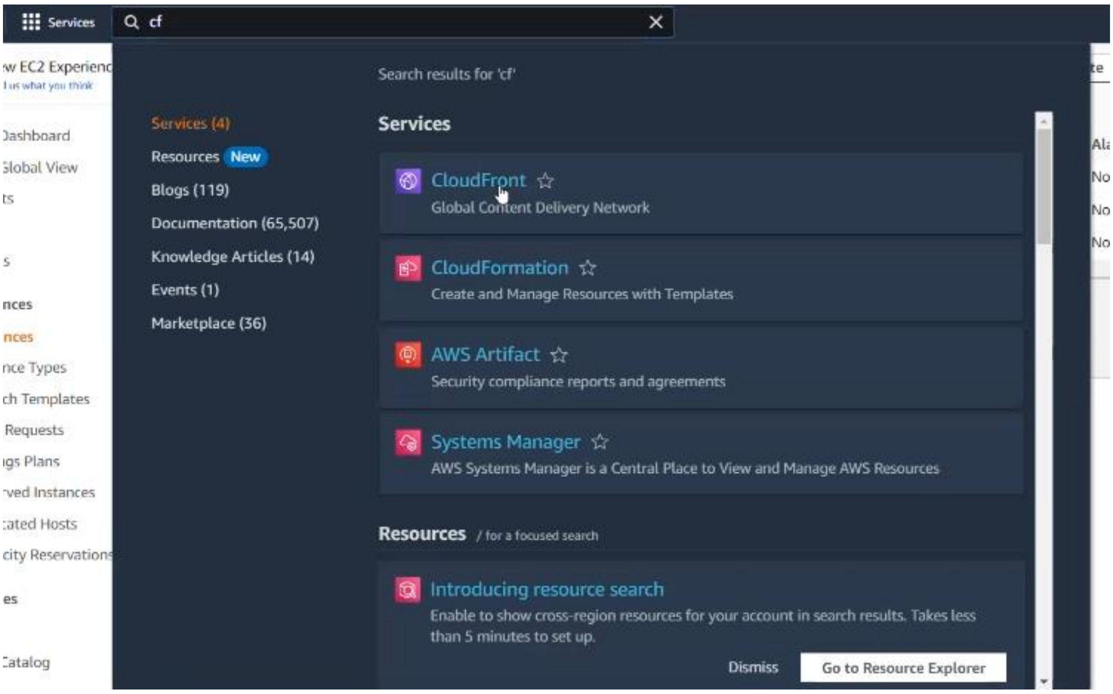
USER TO E.L => E.L TO ORIGIN [S3] => ORIGIN TO E.L => CACHES THE CONENT => SERVES THE USER.

BUT WHEN THEN SECOND USER ACCESSES THE SAME DATA, IT RETRIVES FROM THE CACHED:



IMPORTANT THINGS ABOUT CDN:

1. EDGE LOCATIONS ARE NOT JUST READ ONLY, YOU **CAN WRITE** NEW FILES TOO TO THE E.L.
2. OBJECTS ARE CACHED FOR THE LIFE OF THE TTL [**TIME TO LIVE**]
3. YOU **CAN CLEAR THE CACHED OBJECTS** FROM THE EDEGE LOCATION, BUT IT WILL BE CHARGED.



Search results for 'cf'

Services

CloudFront ☆
Global Content Delivery Network

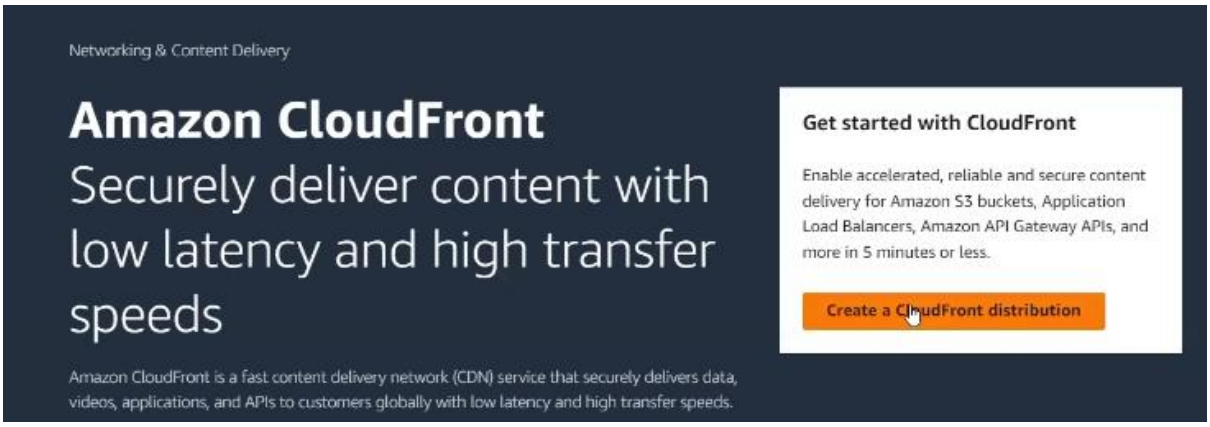
CloudFormation ☆
Create and Manage Resources with Templates

AWS Artifact ☆
Security compliance reports and agreements

Systems Manager ☆
AWS Systems Manager is a Central Place to View and Manage AWS Resources

Resources / for a focused search

Introducing resource search
Enable to show cross-region resources for your account in search results. Takes less than 5 minutes to set up.



Networking & Content Delivery

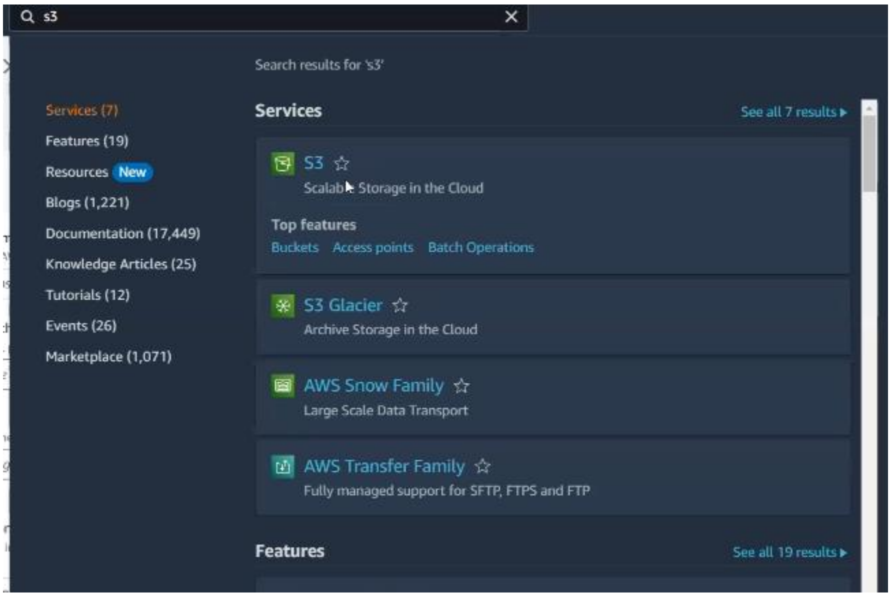
Amazon CloudFront
Securely deliver content with low latency and high transfer speeds

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

Get started with CloudFront

Enable accelerated, reliable and secure content delivery for Amazon S3 buckets, Application Load Balancers, Amazon API Gateway APIs, and more in 5 minutes or less.

WE ARE GOING TO USE S3



Search results for 's3'

Services

S3 ☆
Scalable Storage in the Cloud

Top features
Buckets Access points Batch Operations

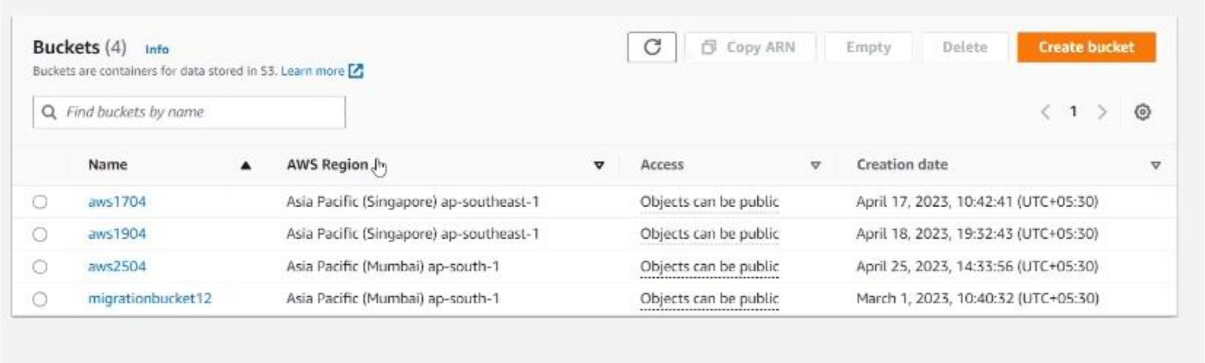
S3 Glacier ☆
Archive Storage in the Cloud

AWS Snow Family ☆
Large Scale Data Transport

AWS Transfer Family ☆
Fully managed support for SFTP, FTPS and FTP

Features

(*) create a bucket

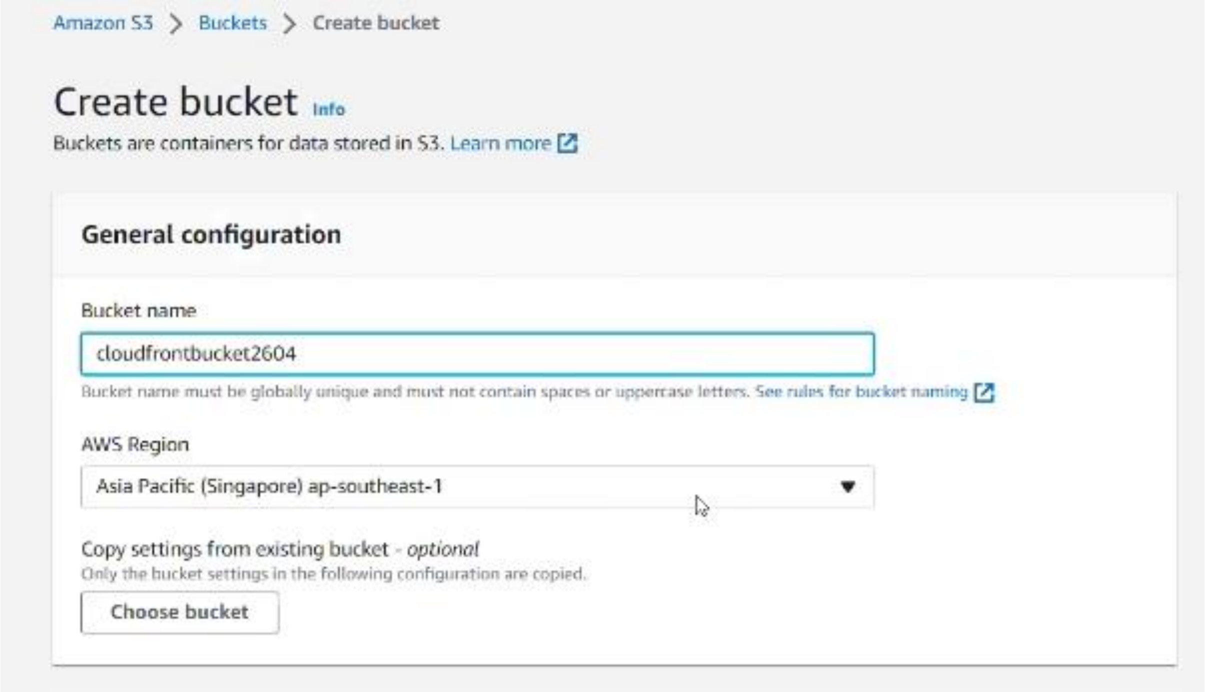


Buckets (4)

Buckets are containers for data stored in S3. Learn more

Find buckets by name

	Name	AWS Region	Access	Creation date
○	aws1704	Asia Pacific (Singapore) ap-southeast-1	Objects can be public	April 17, 2023, 10:42:41 (UTC+05:30)
○	aws1904	Asia Pacific (Singapore) ap-southeast-1	Objects can be public	April 18, 2023, 19:32:43 (UTC+05:30)
○	aws2504	Asia Pacific (Mumbai) ap-south-1	Objects can be public	April 25, 2023, 14:33:56 (UTC+05:30)
○	migrationbucket12	Asia Pacific (Mumbai) ap-south-1	Objects can be public	March 1, 2023, 10:40:32 (UTC+05:30)



Create bucket

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name: cloudfrontbucket2604

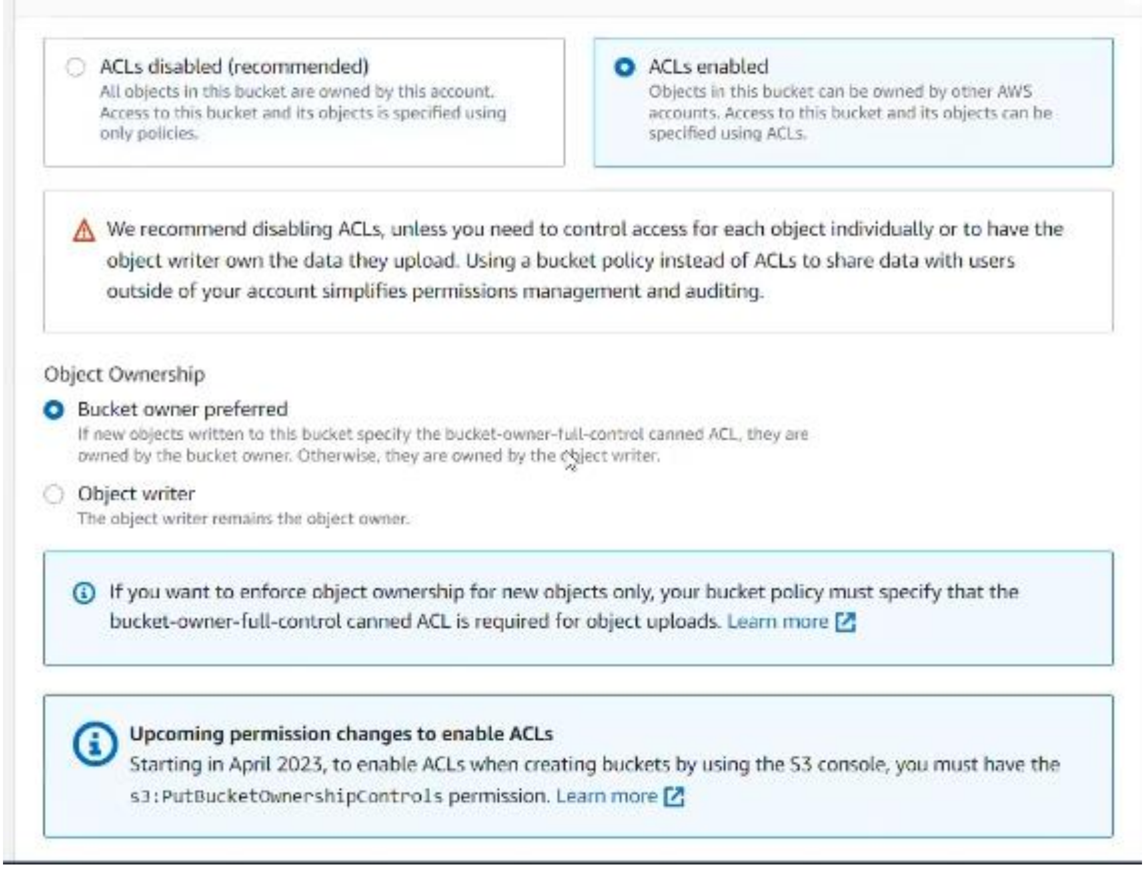
Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region: Asia Pacific (Singapore) ap-southeast-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

(*) ACLS ENABLED



○ ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

● ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

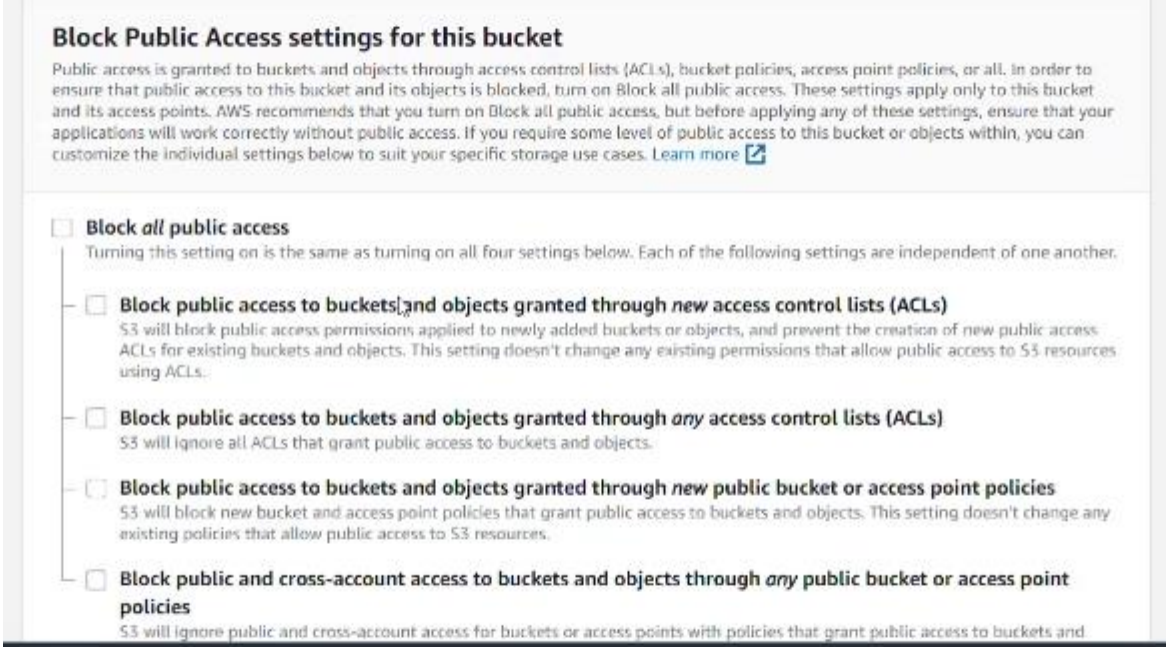
● Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

○ Object writer
The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

ⓘ **Upcoming permission changes to enable ACLs**
Starting in April 2023, to enable ACLs when creating buckets by using the S3 console, you must have the `s3:PutBucketOwnershipControls` permission. Learn more

(*) REMOVE block all public access



Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

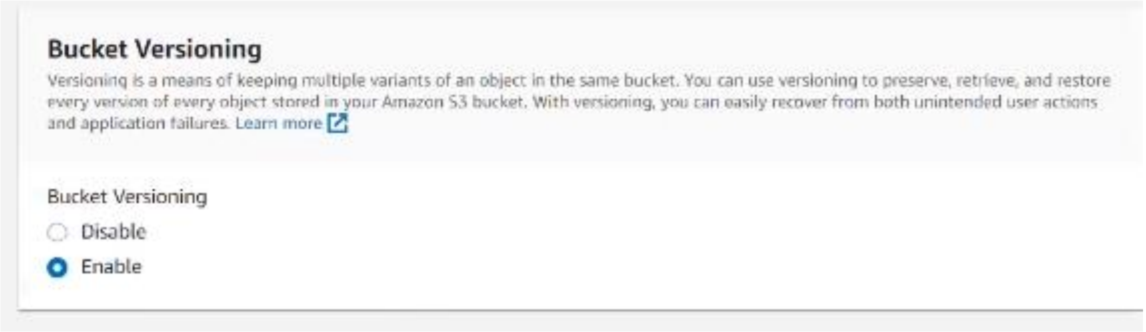
□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

□ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

□ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

□ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

□ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and



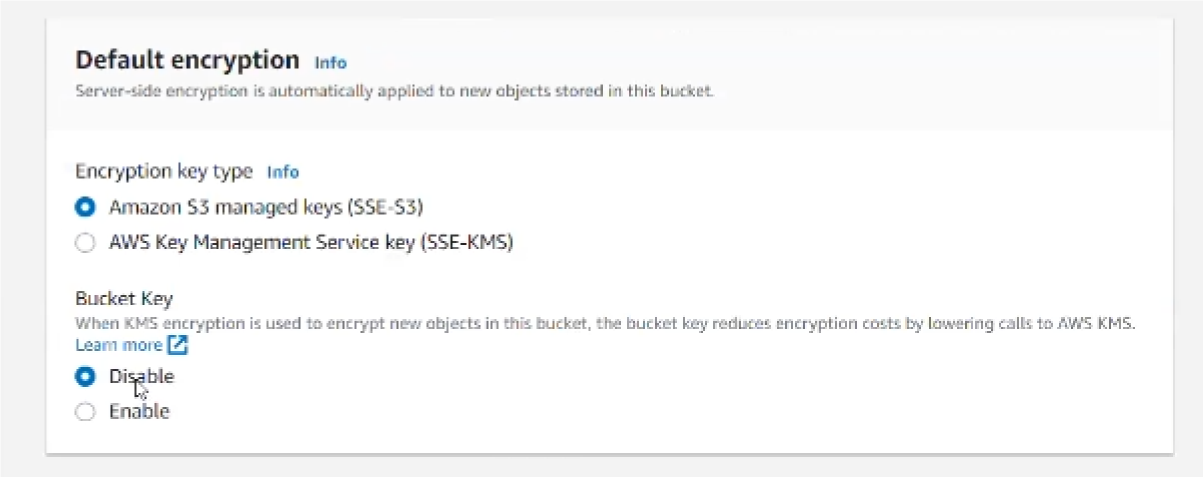
Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

○ Disable

● Enable



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type Info

● Amazon S3 managed keys (SSE-S3)

○ AWS Key Management Service key (SSE-KMS)

Bucket Key

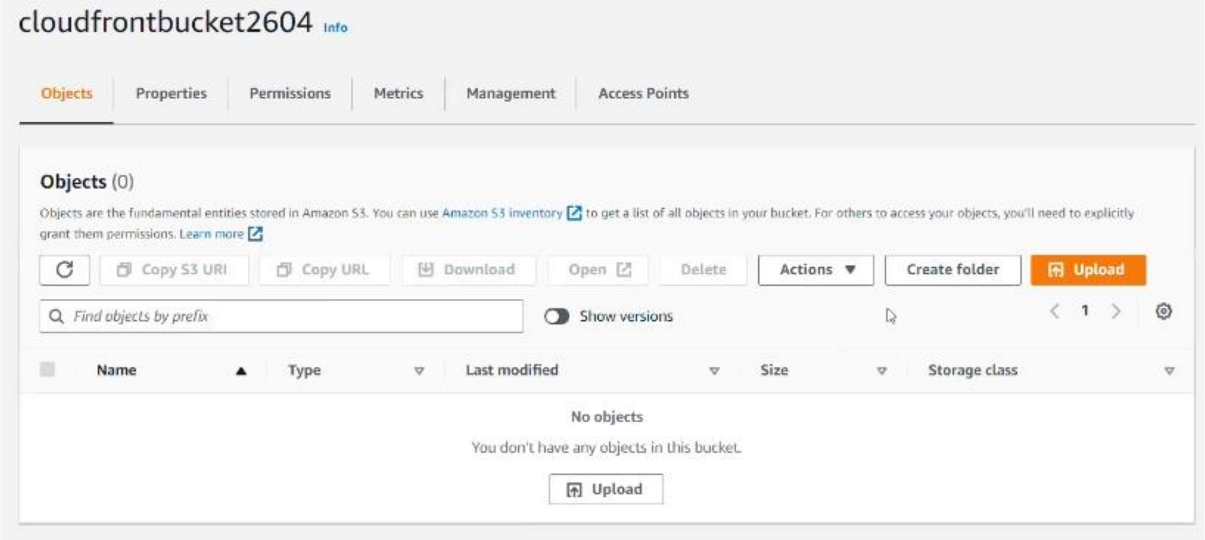
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more

● Disable

○ Enable

(*) press create bucket – bucket created

(*) upload a file in the bucket



cloudfrontbucket2604 Info

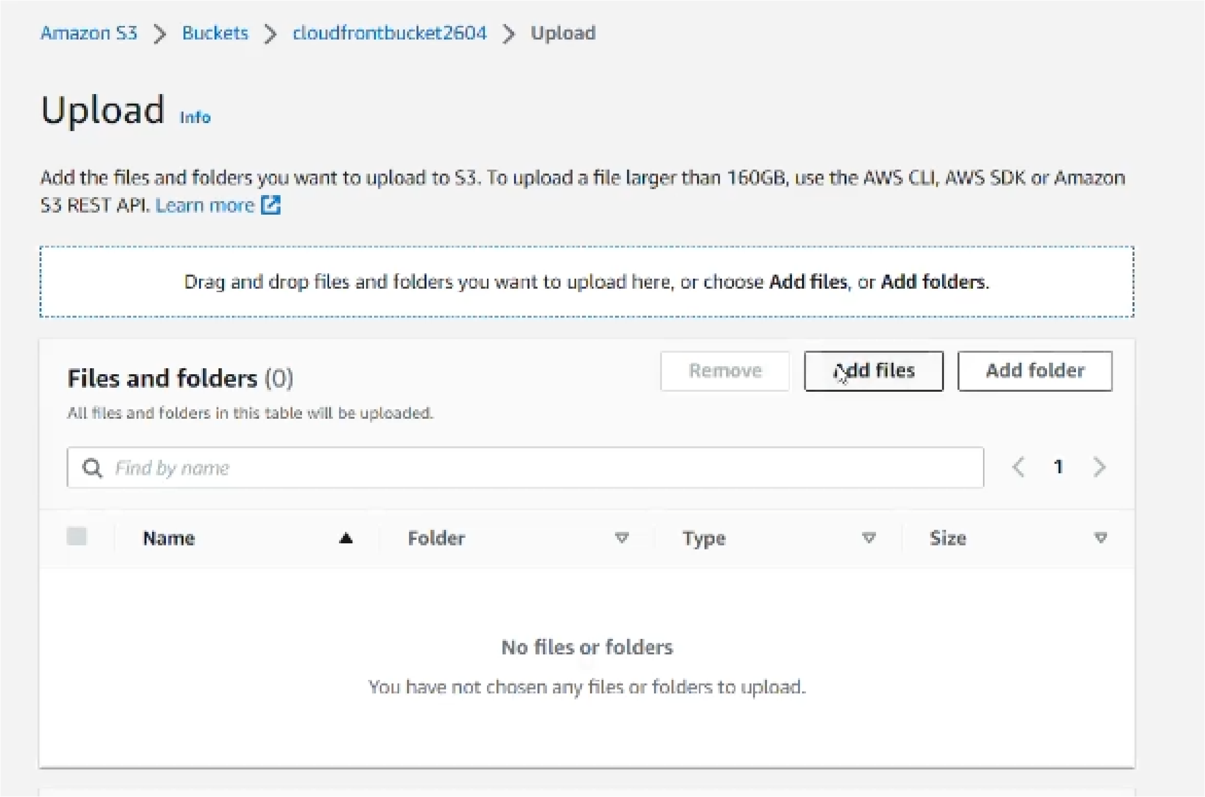
Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

	Name ▲	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.



Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (0)

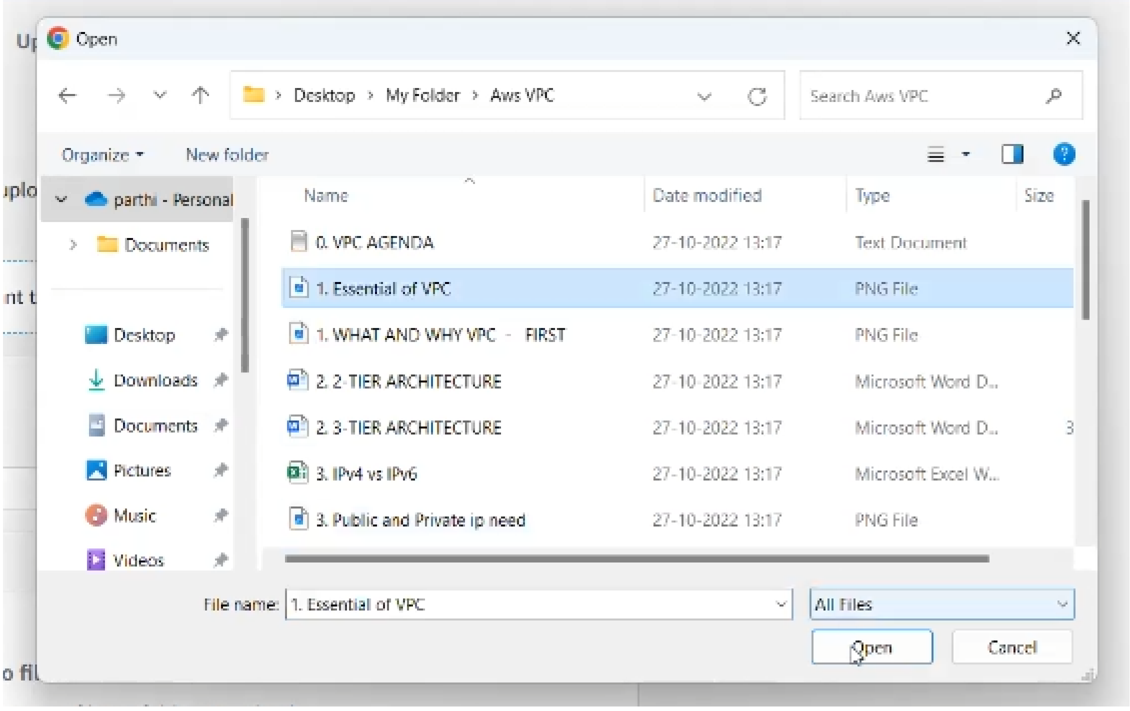
All files and folders in this table will be uploaded.

Name	Folder	Type	Size

No files or folders

You have not chosen any files or folders to upload.

(*) add files

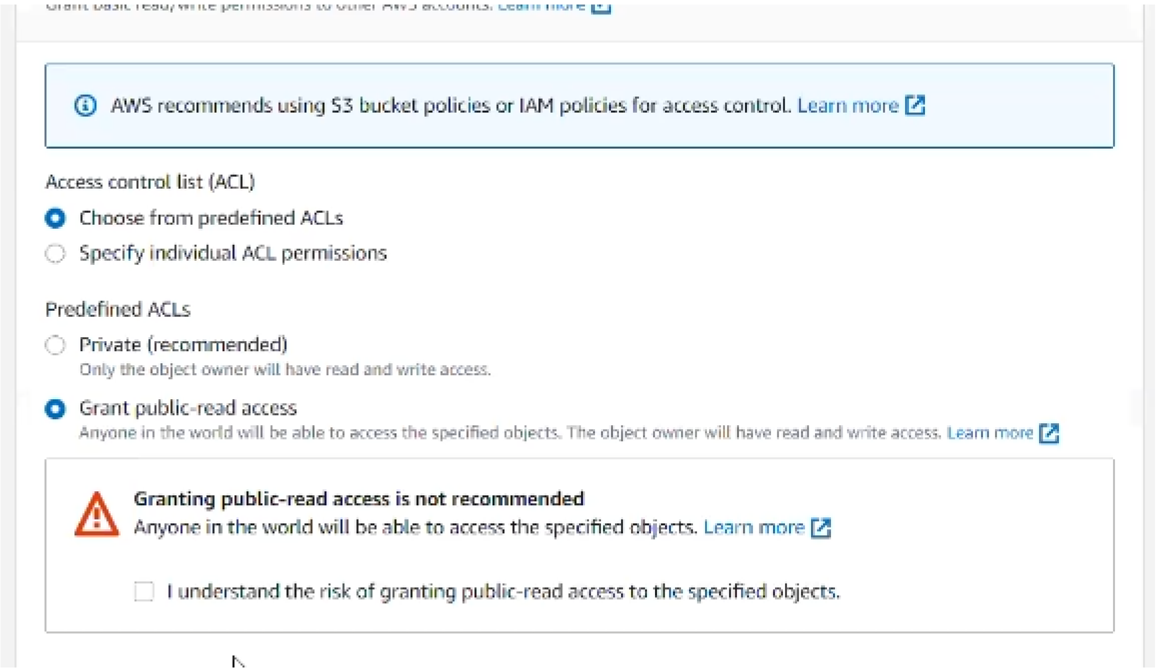


Name	Date modified	Type	Size
0. VPC AGENDA	27-10-2022 13:17	Text Document	
1. Essential of VPC	27-10-2022 13:17	PNG File	
1. WHAT AND WHY VPC - FIRST	27-10-2022 13:17	PNG File	
2. 2-TIER ARCHITECTURE	27-10-2022 13:17	Microsoft Word D...	
2. 3-TIER ARCHITECTURE	27-10-2022 13:17	Microsoft Word D...	3
3. IPv4 vs IPv6	27-10-2022 13:17	Microsoft Excel W...	
3. Public and Private ip need	27-10-2022 13:17	PNG File	

File name: 1. Essential of VPC

All Files

(*) grant permission -- upload



Grant basic read/write permissions to other AWS accounts. Learn more

ⓘ AWS recommends using S3 bucket policies or IAM policies for access control. Learn more

Access control list (ACL)

● Choose from predefined ACLs

○ Specify individual ACL permissions

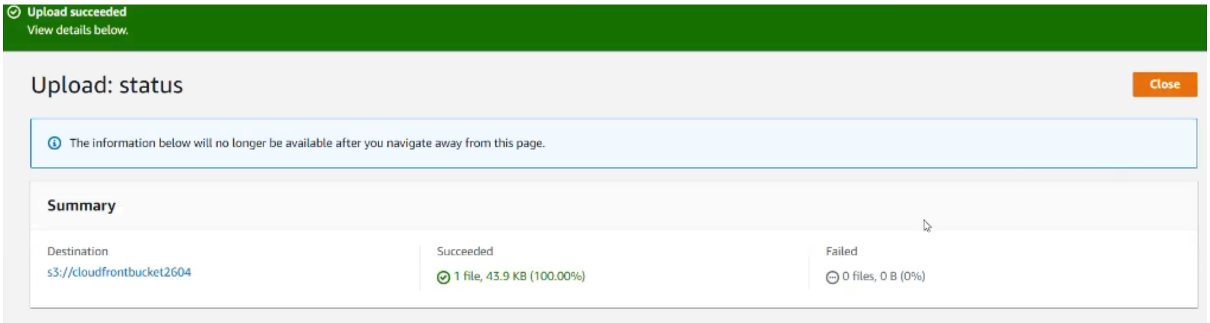
Predefined ACLs

○ Private (recommended)
Only the object owner will have read and write access.

● Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. Learn more

Granting public-read access is not recommended
Anyone in the world will be able to access the specified objects. Learn more

□ I understand the risk of granting public-read access to the specified objects.



Upload succeeded
View details below.

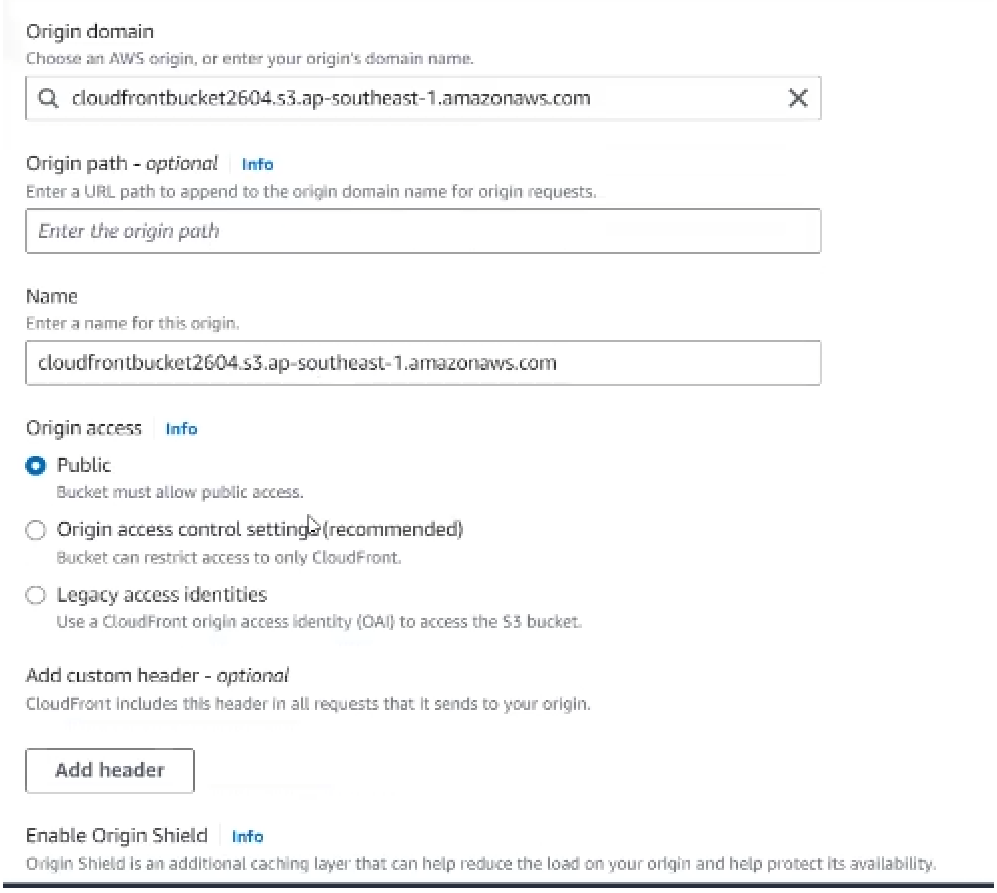
Upload: status

ⓘ The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://cloudfrontbucket2604	✓ 1 file, 43.9 KB (100.00%)	⊖ 0 files, 0 B (0%)

(*) go to CloudFront



Origin domain

Choose an AWS origin, or enter your origin's domain name.

cloudfrontbucket2604.s3.ap-southeast-1.amazonaws.com

Origin path - *optional* Info

Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

Name

Enter a name for this origin.

cloudfrontbucket2604.s3.ap-southeast-1.amazonaws.com

Origin access Info

● Public

Bucket must allow public access.

○ Origin access control settings (recommended)

Bucket can restrict access to only CloudFront.

○ Legacy access identities

Use a CloudFront origin access identity (OAI) to access the S3 bucket.

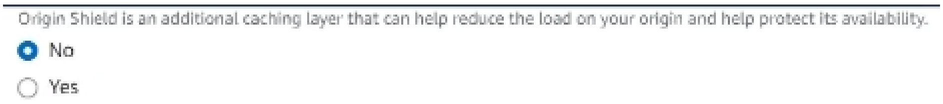
Add custom header - *optional*

CloudFront includes this header in all requests that it sends to your origin.

Add header

Enable Origin Shield Info

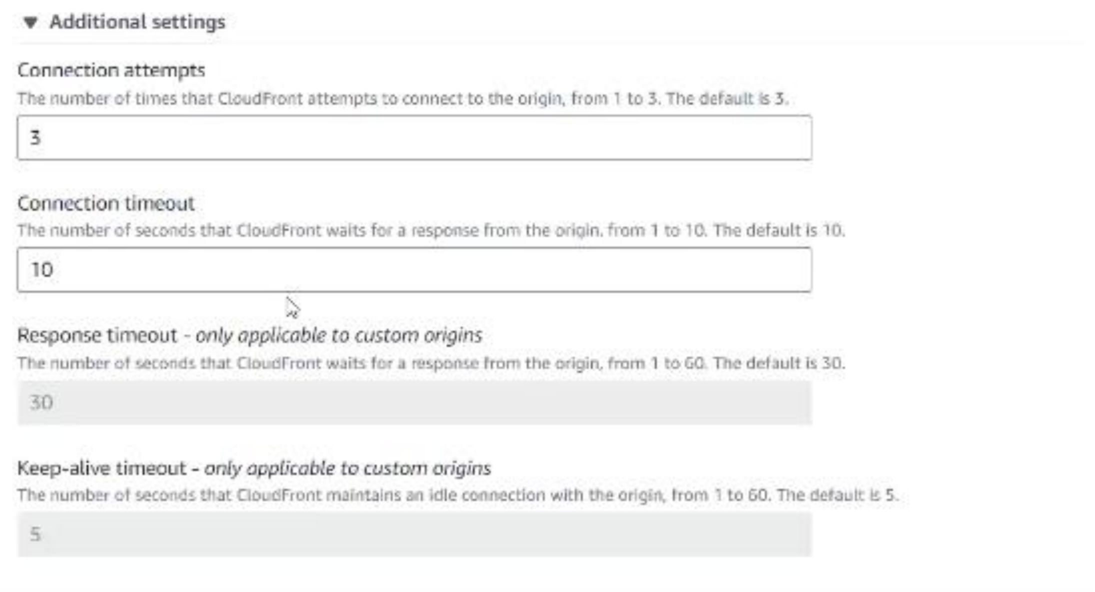
Origin Shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.



Origin Shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.

● No

○ Yes



▼ Additional settings

Connection attempts

The number of times that CloudFront attempts to connect to the origin, from 1 to 3. The default is 3.

3

Connection timeout

The number of seconds that CloudFront waits for a response from the origin, from 1 to 10. The default is 10.

10

Response timeout - *only applicable to custom origins*

The number of seconds that CloudFront waits for a response from the origin, from 1 to 60. The default is 30.

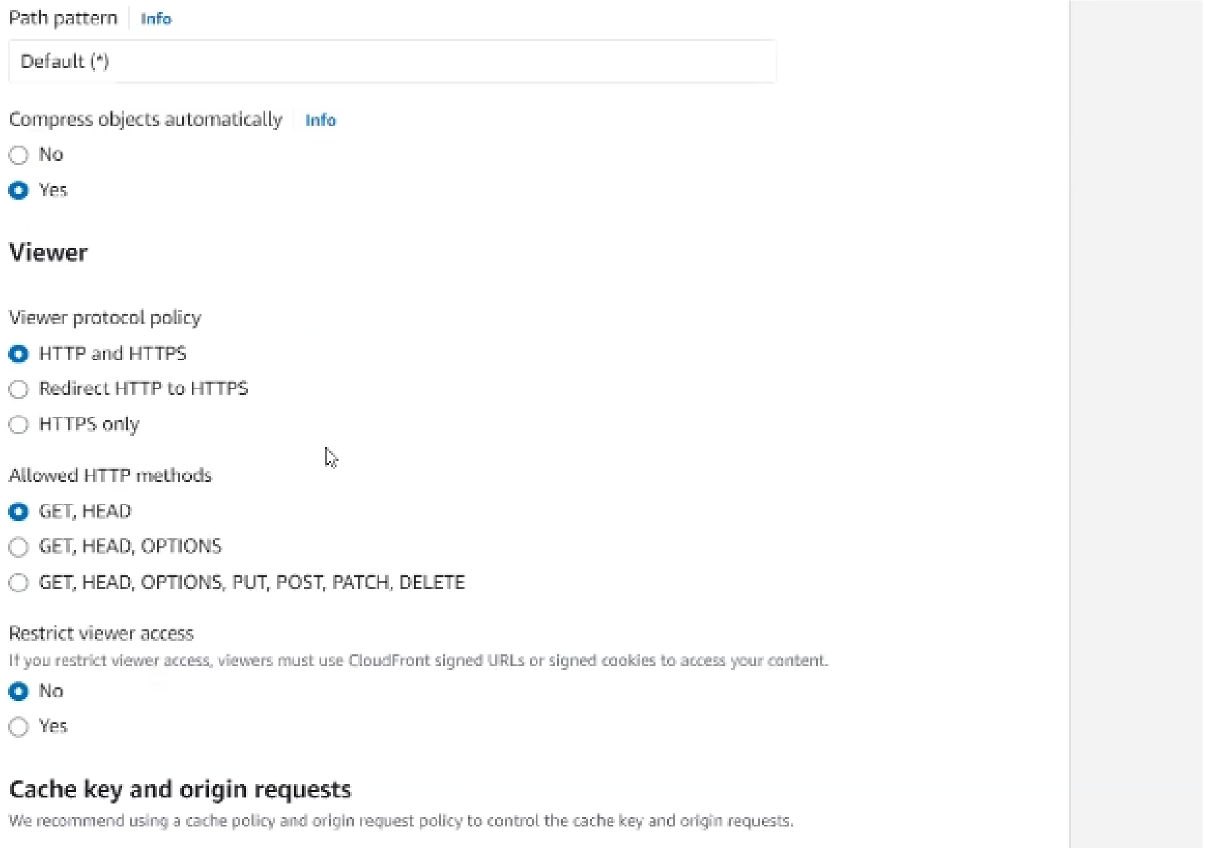
30

Keep-alive timeout - *only applicable to custom origins*

The number of seconds that CloudFront maintains an idle connection with the origin, from 1 to 60. The default is 5.

5

(*) behavior settings



Path pattern Info

Default (*)

Compress objects automatically Info

○ No

● Yes

Viewer

Viewer protocol policy

● HTTP and HTTPS

○ Redirect HTTP to HTTPS

○ HTTPS only

Allowed HTTP methods

● GET, HEAD

○ GET, HEAD, OPTIONS

○ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Restrict viewer access

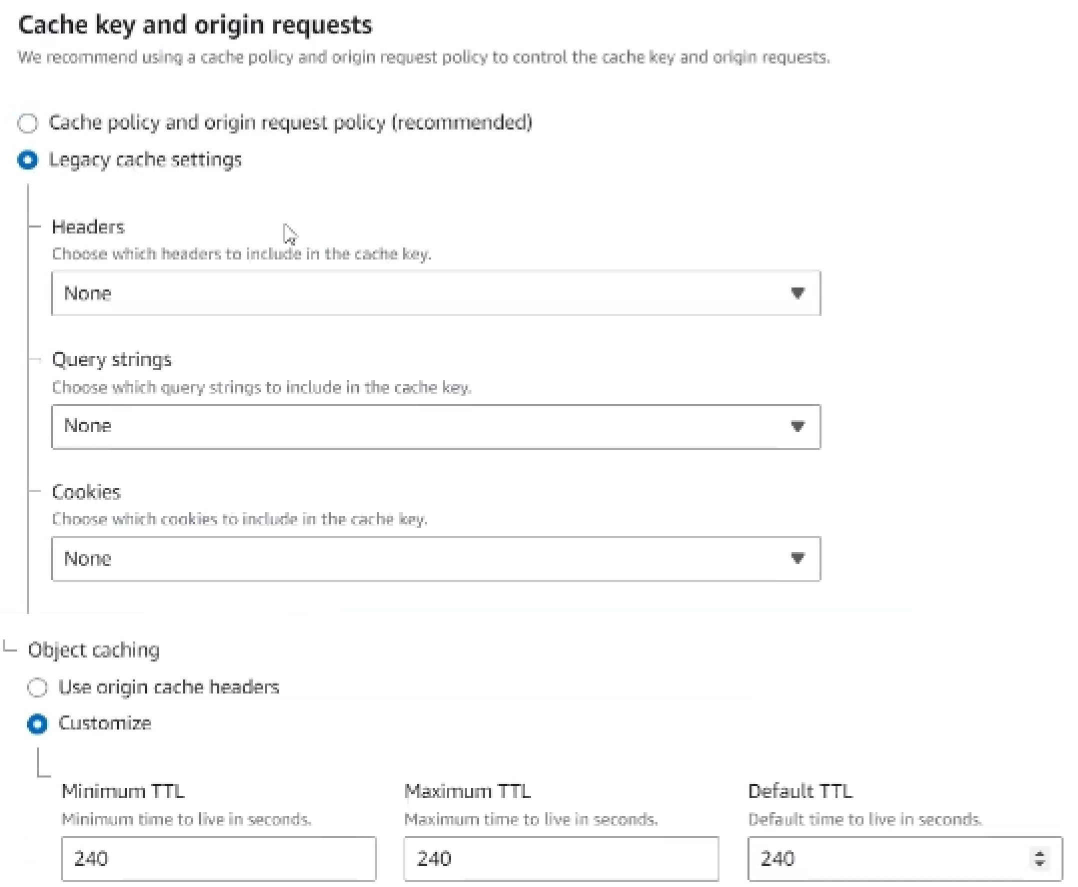
If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content.

● No

○ Yes

Cache key and origin requests

We recommend using a cache policy and origin request policy to control the cache key and origin requests.



Cache key and origin requests

We recommend using a cache policy and origin request policy to control the cache key and origin requests.

○ Cache policy and origin request policy (recommended)

● Legacy cache settings

Headers

Choose which headers to include in the cache key.

None ▼

Query strings

Choose which query strings to include in the cache key.

None ▼

Cookies

Choose which cookies to include in the cache key.

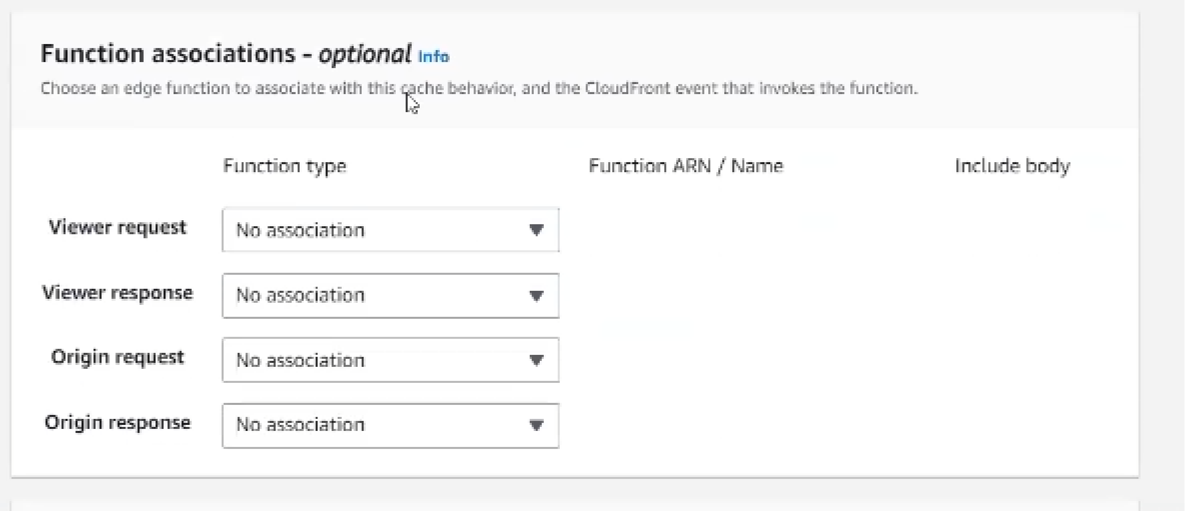
None ▼

Object caching

○ Use origin cache headers

● Customize

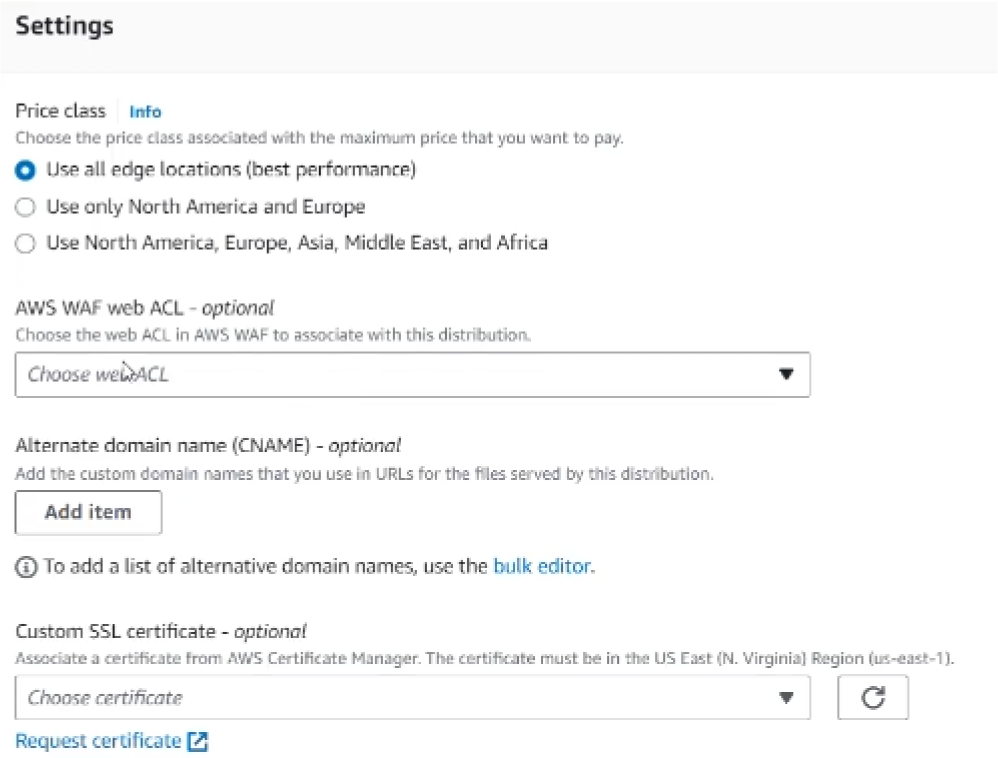
Minimum TTL Minimum time to live in seconds.	Maximum TTL Maximum time to live in seconds.	Default TTL Default time to live in seconds.
240	240	240



Function associations - *optional* Info

Choose an edge function to associate with this cache behavior, and the CloudFront event that invokes the function.

	Function type	Function ARN / Name	Include body
Viewer request	No association ▼		
Viewer response	No association ▼		
Origin request	No association ▼		
Origin response	No association ▼		



Settings

Price class Info

Choose the price class associated with the maximum price that you want to pay.

● Use all edge locations (best performance)

○ Use only North America and Europe

○ Use North America, Europe, Asia, Middle East, and Africa

AWS WAF web ACL - *optional*

Choose the web ACL in AWS WAF to associate with this distribution.

Choose web ACL ▼

Alternate domain name (CNAME) - *optional*

Add the custom domain names that you use in URLs for the files served by this distribution.

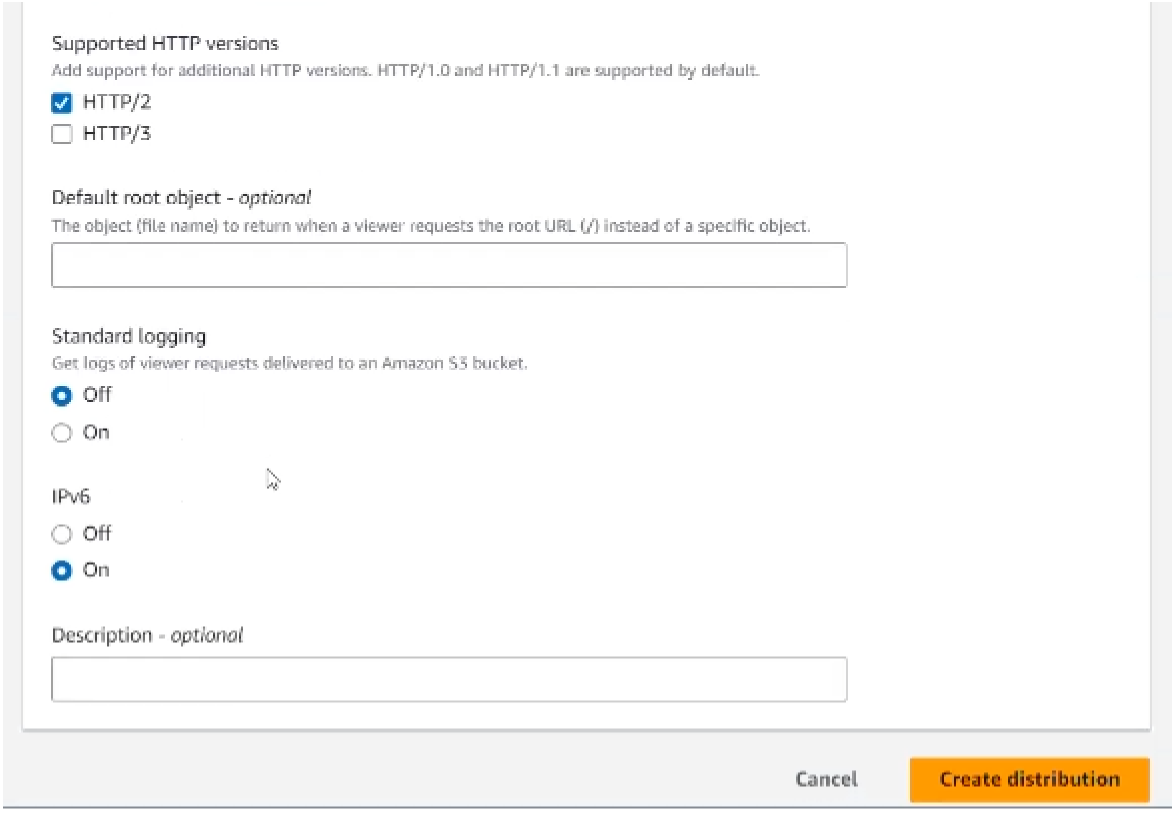
ⓘ To add a list of alternative domain names, use the bulk editor.

Custom SSL certificate - *optional*

Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region (us-east-1).

Choose certificate ▼

Request certificate



Supported HTTP versions

Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.

☑ HTTP/2

□ HTTP/3

Default root object - *optional*

The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.

Standard logging

Get logs of viewer requests delivered to an Amazon S3 bucket.

● Off

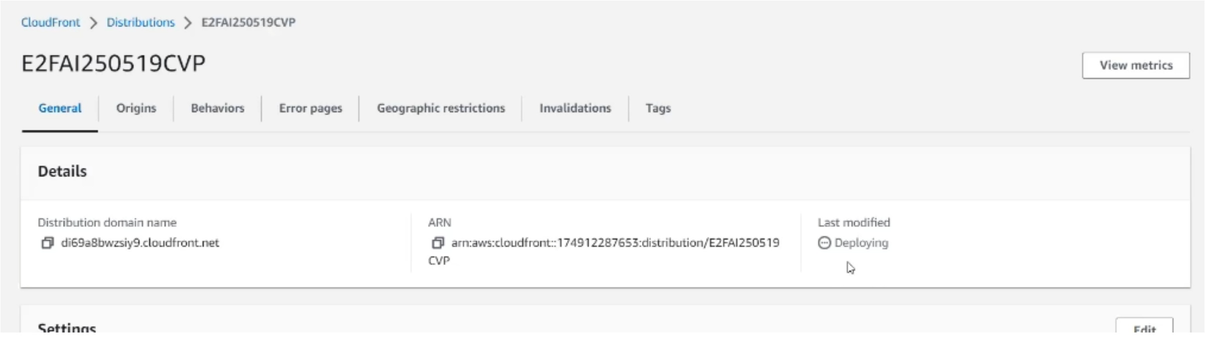
○ On

IPv6

○ Off

● On

Description - *optional*



E2FAI250519CVP

Details

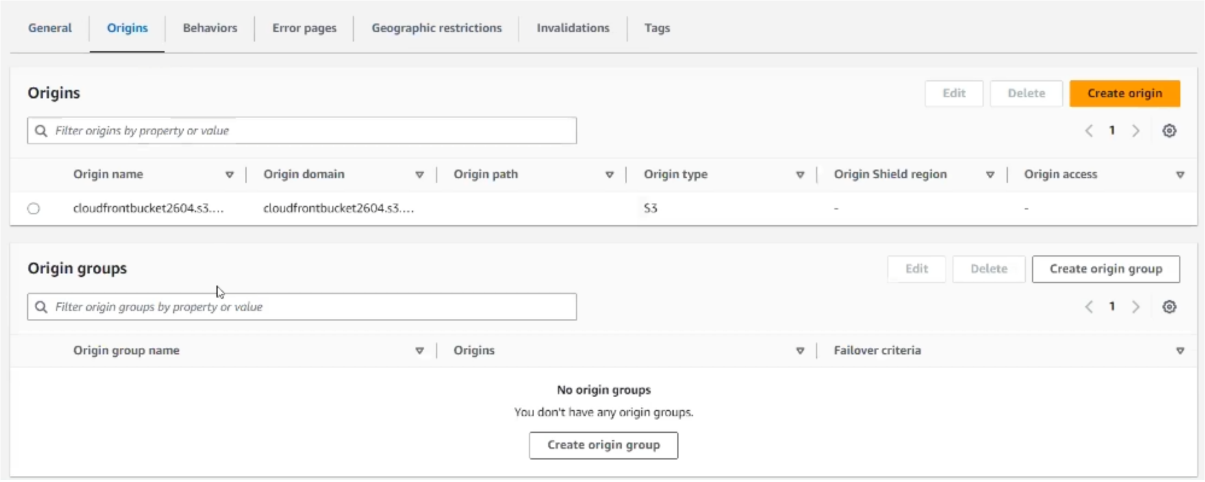
Distribution domain name: di69a8bwzsiy9.cloudfront.net

ARN: arn:aws:cloudfront::174912287653:distribution/E2FAI250519CVP

Last modified: Deploying

Settings

(*) origin groups



Origins

	Origin name	Origin domain	Origin path	Origin type	Origin Shield region	Origin access
○	cloudfrontbucket2604.s3....	cloudfrontbucket2604.s3....		S3	-	-

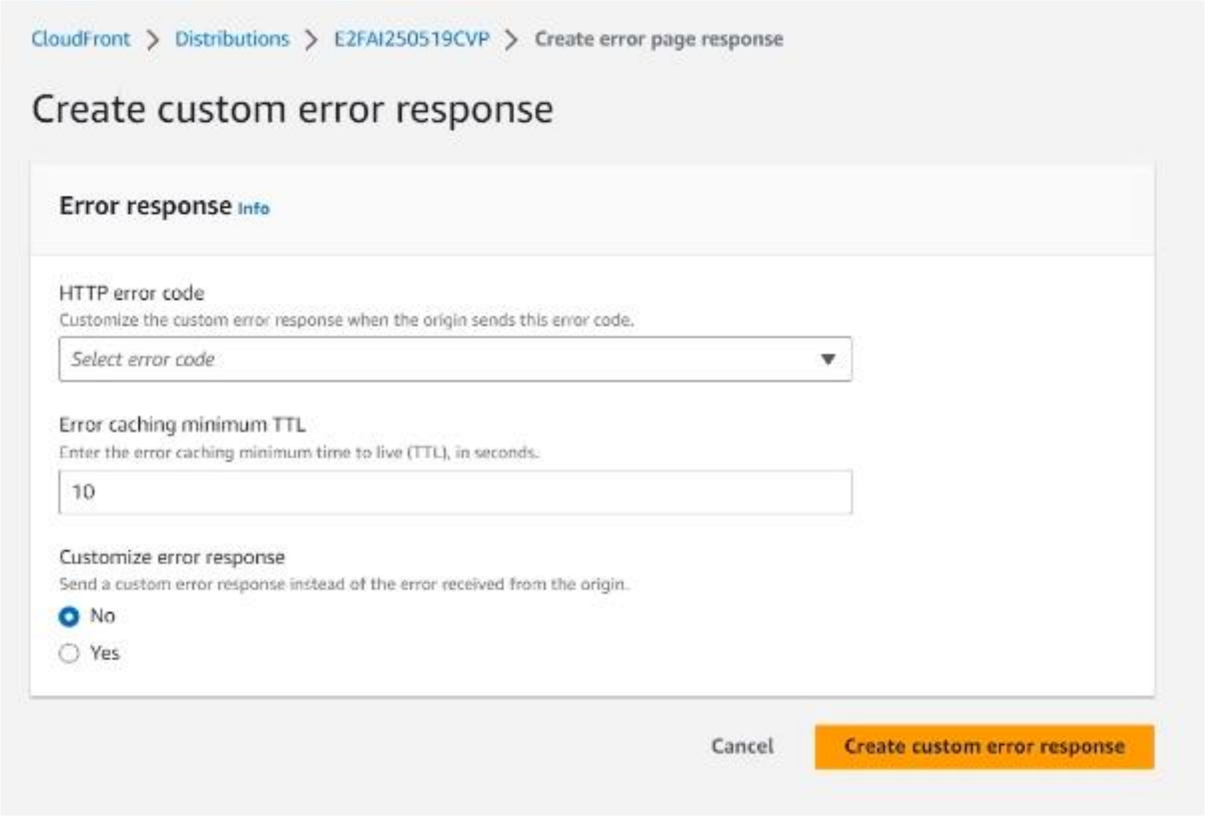
Origin groups

Origin group name	Origins	Failover criteria

No origin groups

You don't have any origin groups.

(*) error page response


CloudFront > Distributions > E2FAI250519CVP > Create error page response
Info
Cancel
Create custom error response

Create custom error response

Error response

HTTP error code

Customize the custom error response when the origin sends this error code.

Select error code ▼

Error caching minimum TTL

Enter the error caching minimum time to live (TTL), in seconds.

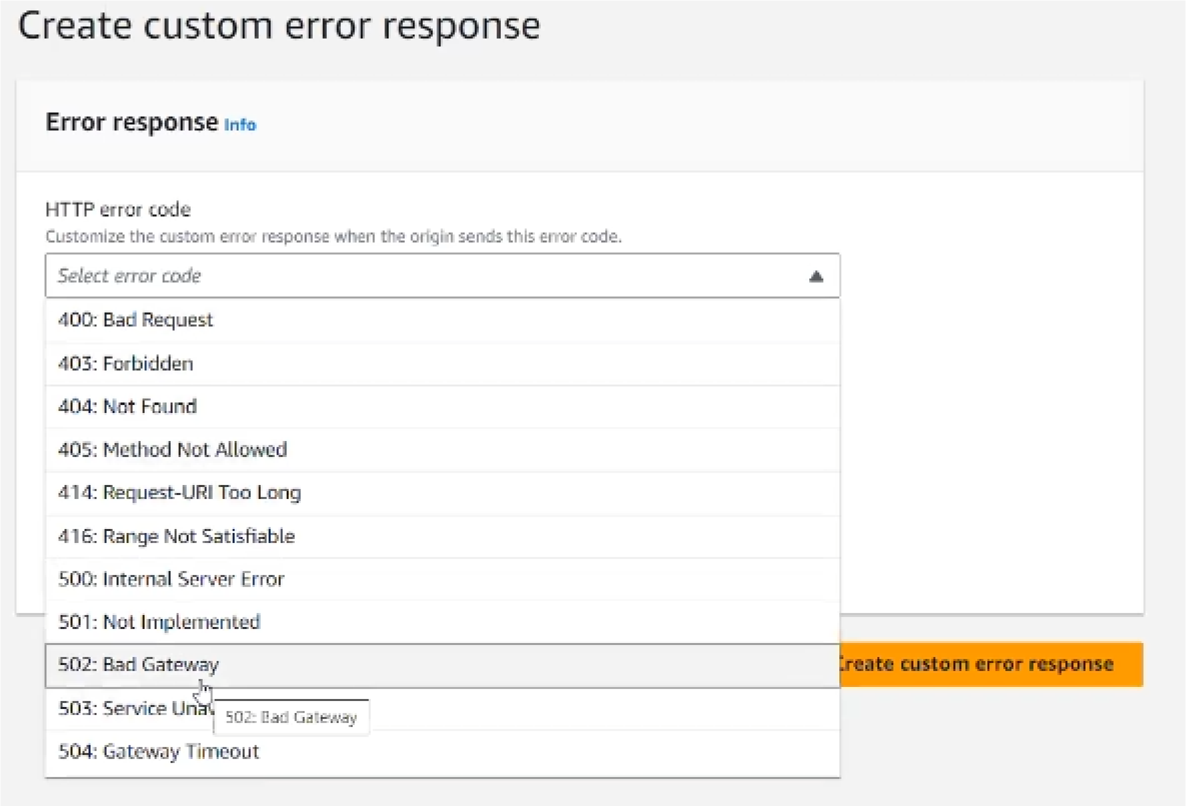
10

Customize error response

Send a custom error response instead of the error received from the origin.

● No

○ Yes



Create custom error response

Error response Info

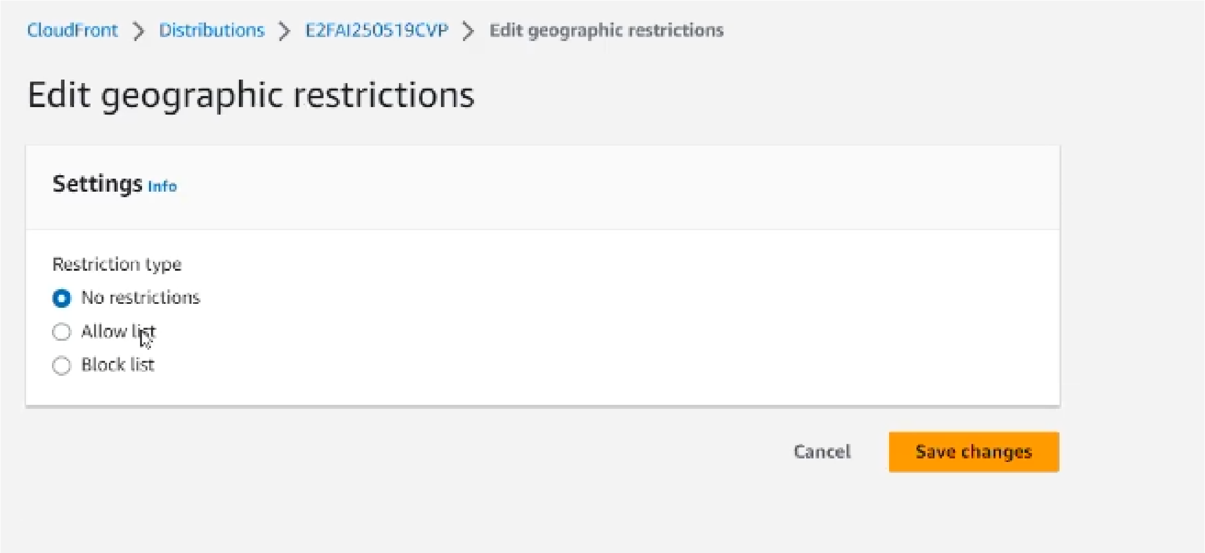
HTTP error code

Customize the custom error response when the origin sends this error code.

Select error code ▲

- 400: Bad Request
- 403: Forbidden
- 404: Not Found
- 405: Method Not Allowed
- 414: Request-URI Too Long
- 416: Range Not Satisfiable
- 500: Internal Server Error
- 501: Not Implemented
- 502: Bad Gateway
- 503: Service Una 502: Bad Gateway
- 504: Gateway Timeout

(*) geographic restrictions



CloudFront > Distributions > E2FAI250519CVP > Edit geographic restrictions

Edit geographic restrictions

Settings Info

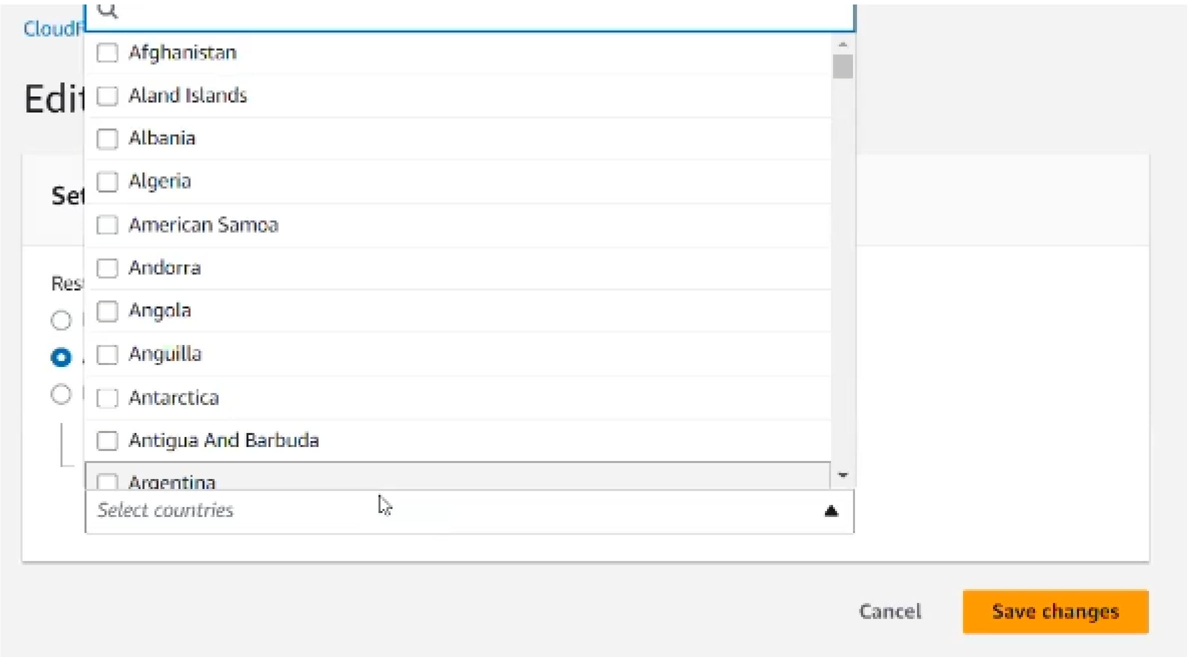
Restriction type

● No restrictions

○ Allow list

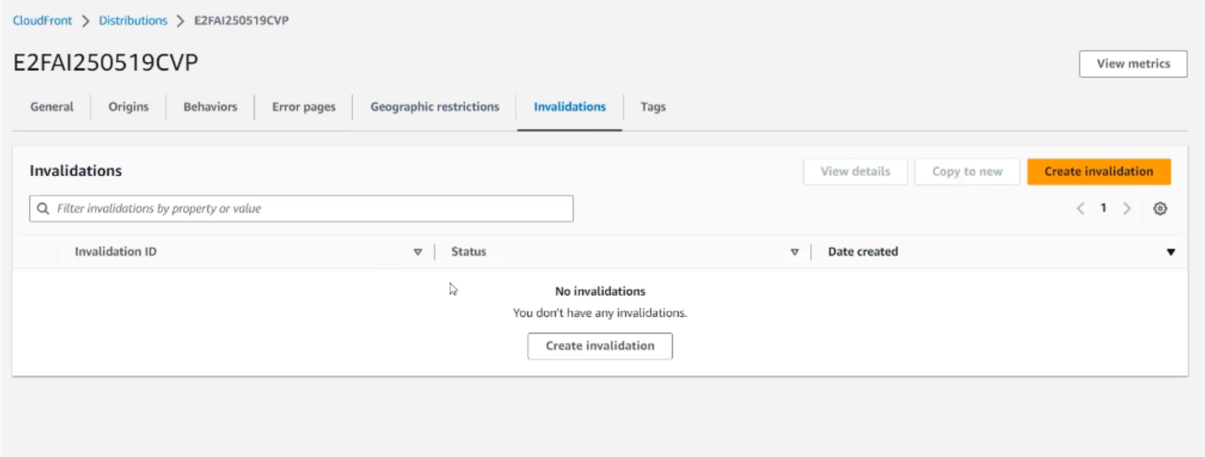
○ Block list

(*) Allow list



□ Afghanistan
□ Aland Islands
□ Albania
□ Algeria
□ American Samoa
□ Andorra
□ Angola
□ Anguilla
□ Antarctica
□ Antigua And Barbuda
□ Argentina

Select countries



E2FAI250519CVP

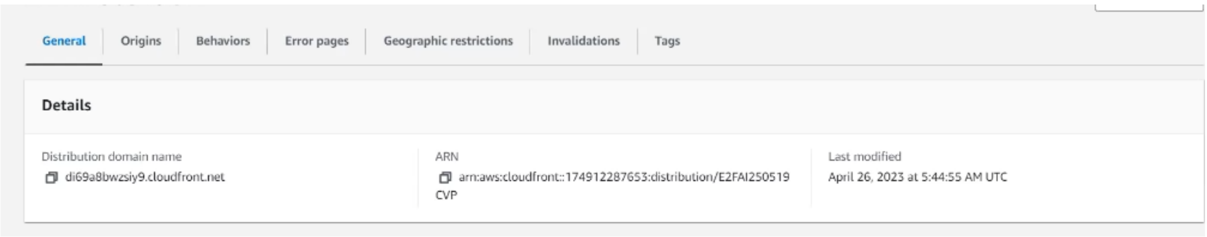
Invalidations

Invalidation ID	Status	Date created

No invalidations

You don't have any invalidations.

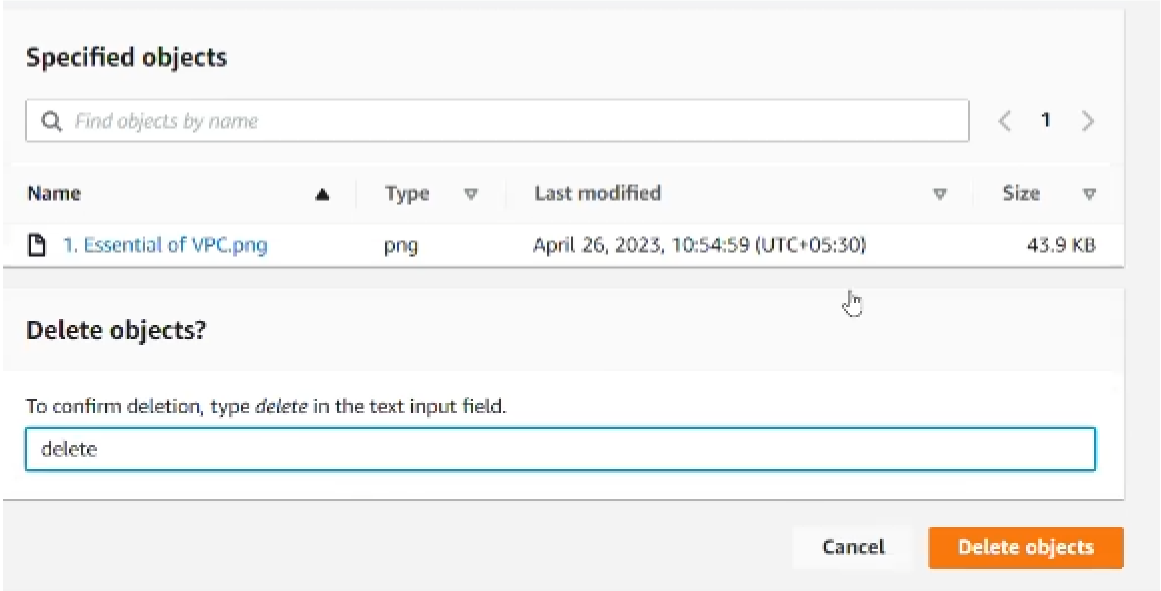
(*) domain name hit the domain name in the browser



Details

Distribution domain name	ARN	Last modified
di69a8bwzsiy9.cloudfront.net	arn:aws:cloudfront::174912287653:distribution/E2FAI250519CVP	April 26, 2023 at 5:44:55 AM UTC

(*) now delete the object in the s3 bucket



Specified objects

Find objects by name

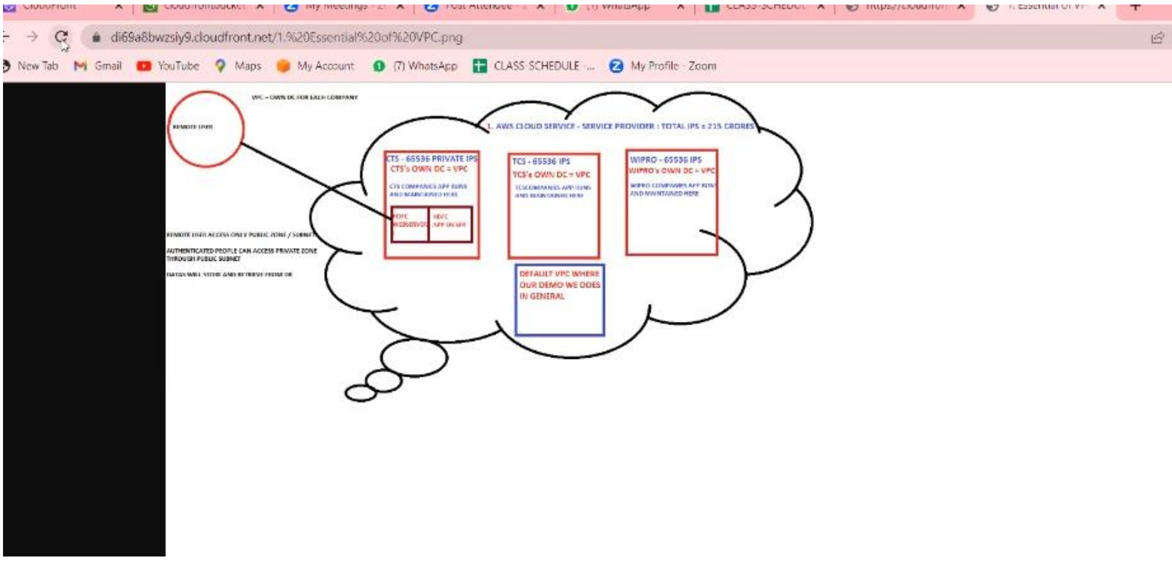
Name	Type	Last modified	Size
1. Essential of VPC.png	png	April 26, 2023, 10:54:59 (UTC+05:30)	43.9 KB

Delete objects?

To confirm deletion, type *delete* in the text input field.

delete

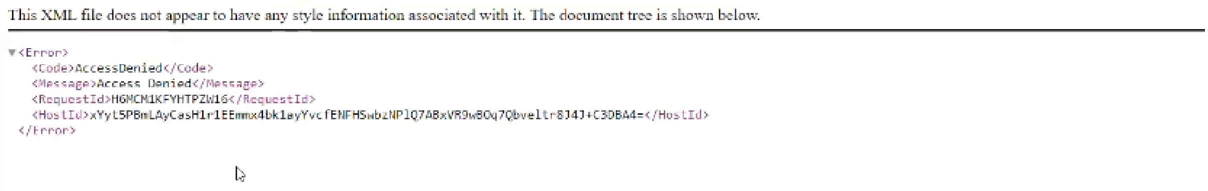
(*) in S3 it wont work but in cloud front it works because it is taken in memory after 240 seconds it wont work shows error



di69a8bwzsiy9.cloudfront.net/1.%20Essential%20of%20VPC.png

New Tab
Gmail
YouTube
Maps
My Account
(7) WhatsApp
CLASS SCHEDULE ...
My Profile · Zoom
VPC = OWN DC FOR EACH COMPANY
REMOTE USER
1. AWS CLOUD SERVICE - SERVICE PROVIDER : TOTAL IPS ≥ 215 CRORES
CTS - 65536 PRIVATE IPS
CTS's OWN DC = VPC
CTS COMPANIES APP RUNS AND MAINTAINED HERE
HDFC WEBSERVER
HDFC APP OR API
TCS - 65536 IPS
TCS's OWN DC = VPC
TCSCOMPANIES APP RUNS AND MAINTAINED HERE
WIPRO - 65536 IPS
WIPRO's OWN DC = VPC
WIPRO COMPANIES APP RUNS AND MAINTAINED HERE
DEFAULT VPC WHERE OUR DEMO WE DOES IN GENERAL
REMOTE USER ACCESS ONLY PUBLIC ZONE / SUBNET
AUTHENTICATED PEOPLE CAN ACCESS PRIVATE ZONE THROUGH PUBLIC SUBNET
DATAS WILL STORE AND RETRIVE FROM DB

(*) after 240 sec error page

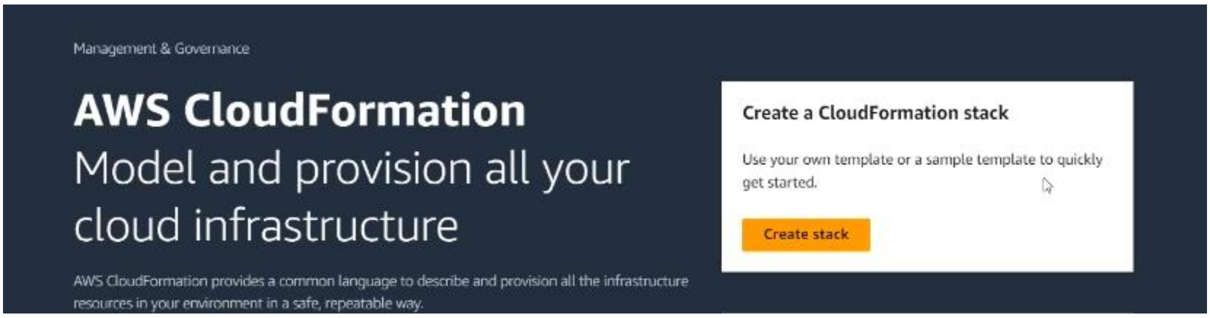


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>H6MCM1KFYHTPZW16</RequestId>
   <HostId>xYyL5PBmLAyCasH1r1EEmmx4bk1ayYvcfENFHSwbzNP1Q7ABxVR9wBOq7Qbveltr8J4J+C3DBA4=</HostId>
 </Error>
```

CLOUD FORMATION

infrastructure as a code concept



Management & Governance

AWS CloudFormation

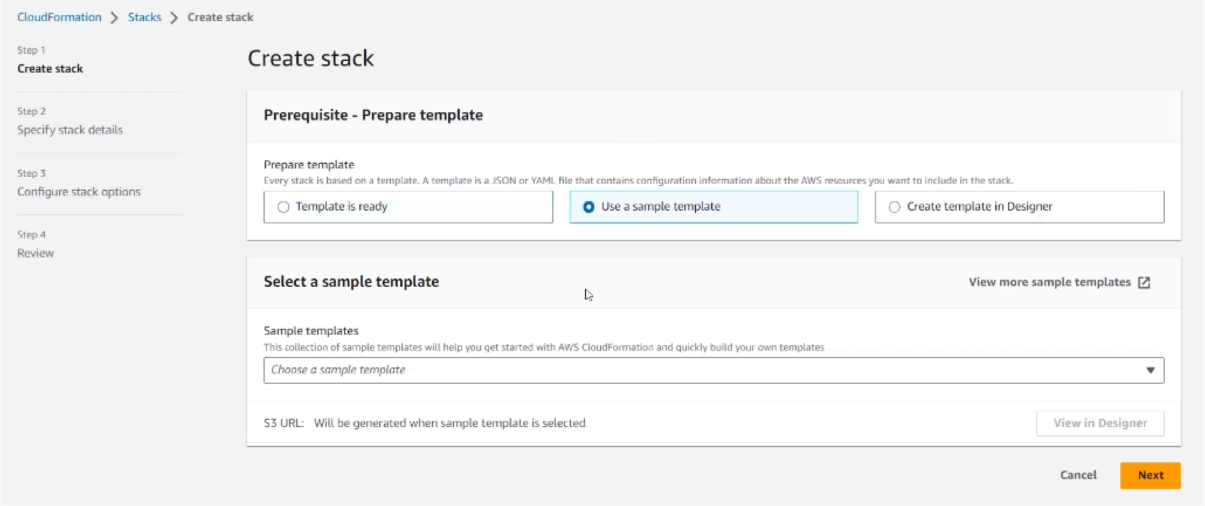
Model and provision all your cloud infrastructure

AWS CloudFormation provides a common language to describe and provision all the infrastructure resources in your environment in a safe, repeatable way.

Create a CloudFormation stack

Use your own template or a sample template to quickly get started.

(*) use a sample template



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

Select a sample template

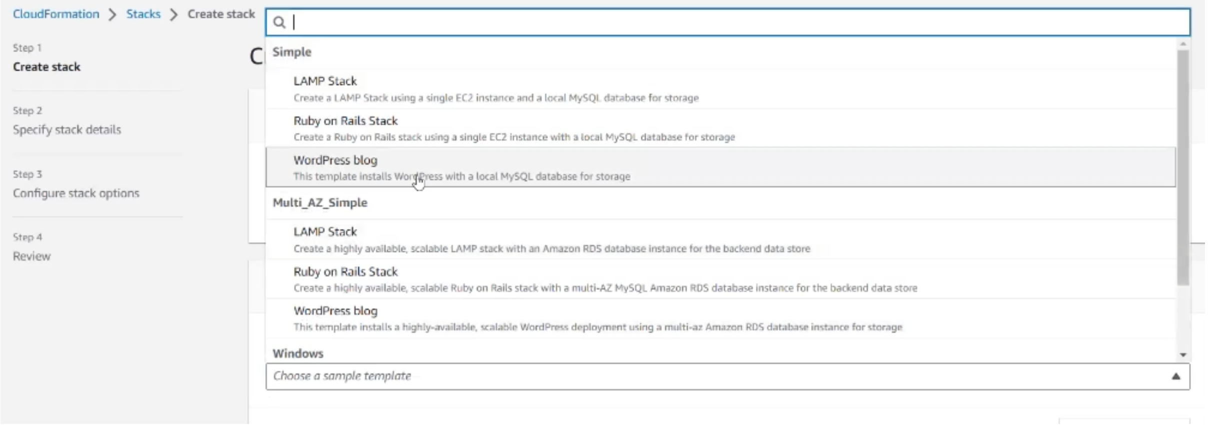
Sample templates

This collection of sample templates will help you get started with AWS CloudFormation and quickly build your own templates

Choose a sample template

S3 URL: Will be generated when sample template is selected

(*) sample templates WordPress blog



Simple

LAMP Stack
Create a LAMP Stack using a single EC2 instance and a local MySQL database for storage

Ruby on Rails Stack
Create a Ruby on Rails stack using a single EC2 instance with a local MySQL database for storage

WordPress blog
This template installs WordPress with a local MySQL database for storage

Multi_AZ_Simple

LAMP Stack
Create a highly available, scalable LAMP stack with an Amazon RDS database instance for the backend data store

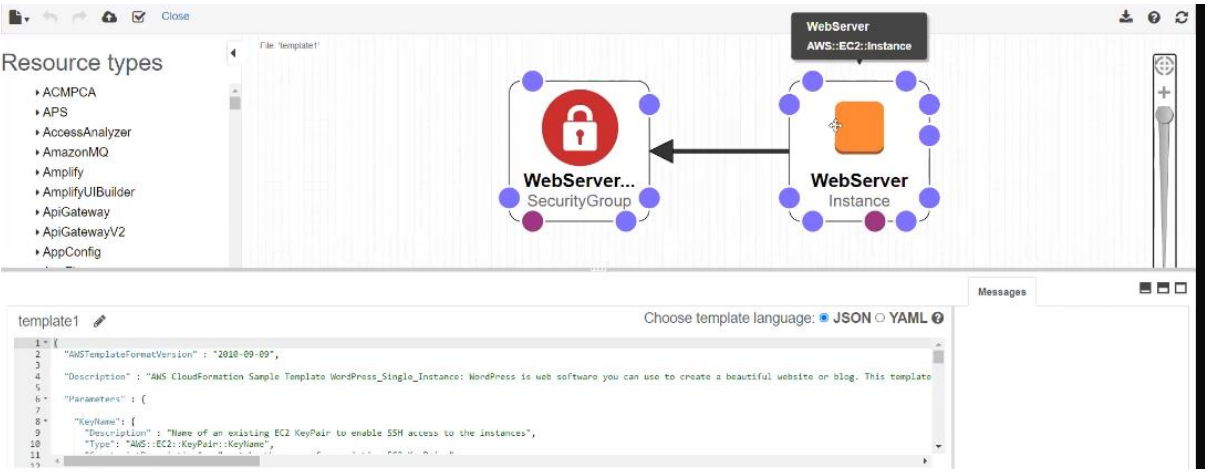
Ruby on Rails Stack
Create a highly available, scalable Ruby on Rails stack with a multi-AZ MySQL Amazon RDS database instance for the backend data store

WordPress blog
This template installs a highly-available, scalable WordPress deployment using a multi-az Amazon RDS database instance for storage

Windows

Choose a sample template

(*) view in designer



template1

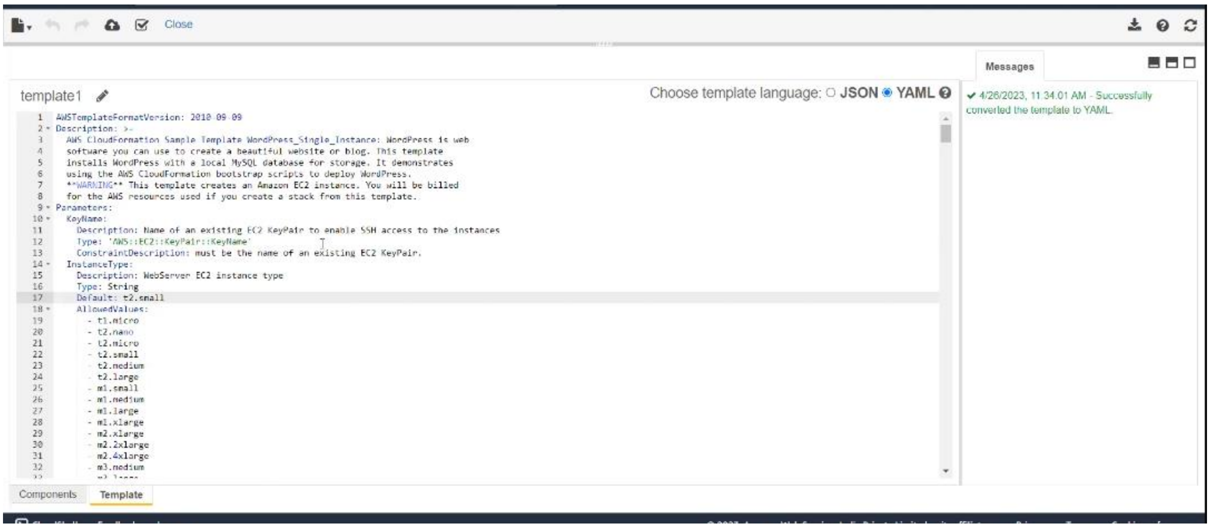
Choose template language: ● JSON ○ YAML

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",

  "Description" : "AWS CloudFormation Sample Template WordPress_Single_Instance: WordPress is web software you can use to create a beautiful website or blog. This template

  "Parameters" : {

    "KeyName": {
      "Description" : "Name of an existing EC2 KeyPair to enable SSH access to the instances",
      "Type": "AWS::EC2::KeyPair::KeyName",
```

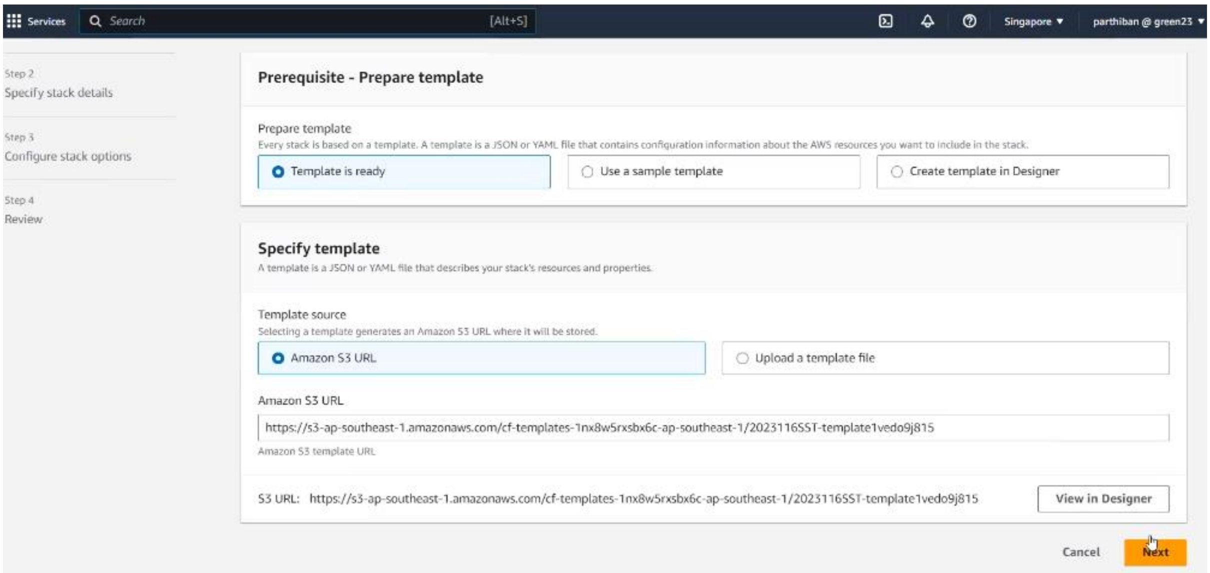


template1

Choose template language: ○ JSON ● YAML

✔ 4/26/2023, 11:34:01 AM - Successfully converted the template to YAML.

```
AWSTemplateFormatVersion: 2010-09-09
Description: >-
  AWS CloudFormation Sample Template WordPress_Single_Instance: WordPress is web
  software you can use to create a beautiful website or blog. This template
  installs WordPress with a local MySQL database for storage. It demonstrates
  using the AWS CloudFormation bootstrap scripts to deploy WordPress.
  **WARNING** This template creates an Amazon EC2 instance. You will be billed
  for the AWS resources used if you create a stack from this template.
Parameters:
  KeyName:
    Description: Name of an existing EC2 KeyPair to enable SSH access to the instances
    Type: 'AWS::EC2::KeyPair::KeyName'
    ConstraintDescription: must be the name of an existing EC2 KeyPair.
  InstanceType:
    Description: WebServer EC2 instance type
    Type: String
    Default: t2.small
    AllowedValues:
      - t1.micro
      - t2.nano
      - t2.micro
      - t2.small
      - t2.medium
      - t2.large
      - m1.small
      - m1.medium
      - m1.large
      - m1.xlarge
      - m2.xlarge
      - m2.2xlarge
      - m2.4xlarge
      - m3.medium
```



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.

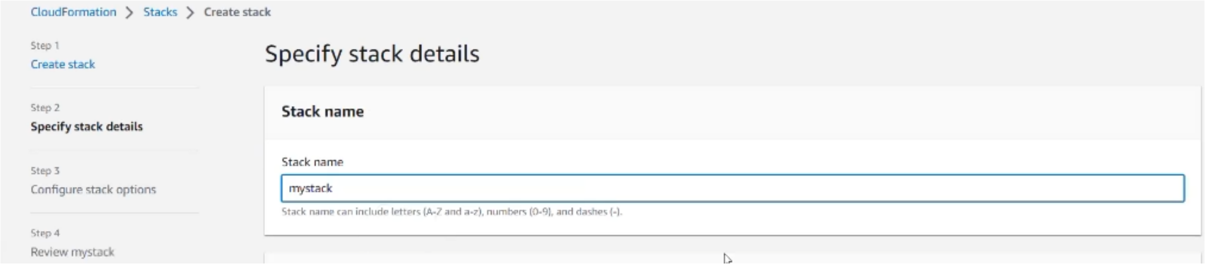
● Amazon S3 URL ○ Upload a template file

Amazon S3 URL

https://s3-ap-southeast-1.amazonaws.com/cf-templates-1nx8w5rxsbx6c-ap-southeast-1/2023116SST-template1vedo9j815

Amazon S3 template URL

S3 URL: https://s3-ap-southeast-1.amazonaws.com/cf-templates-1nx8w5rxsbx6c-ap-southeast-1/2023116SST-template1vedo9j815



CloudFormation > Stacks > Create stack

Step 1
Create stack

Step 2
Specify stack details

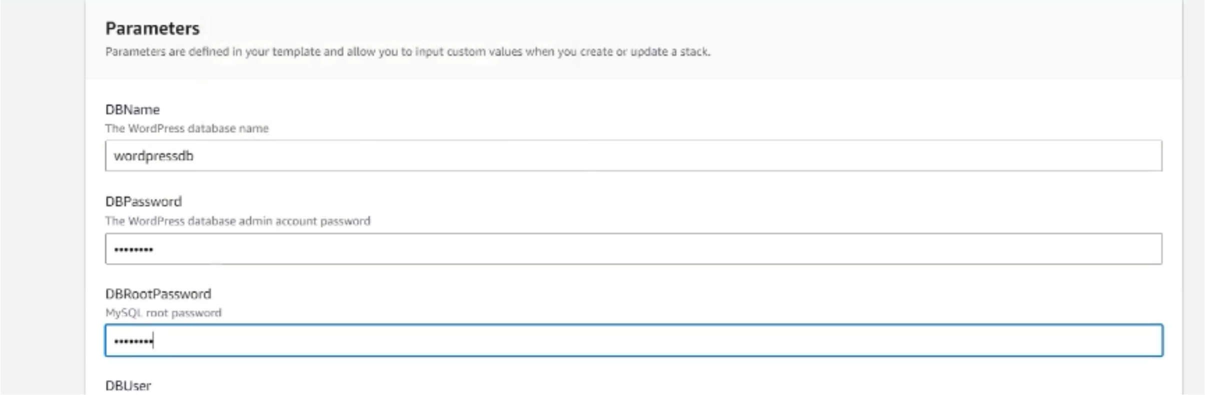
Step 3
Configure stack options

Step 4
Review mystack

Specify stack details

Stack name

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



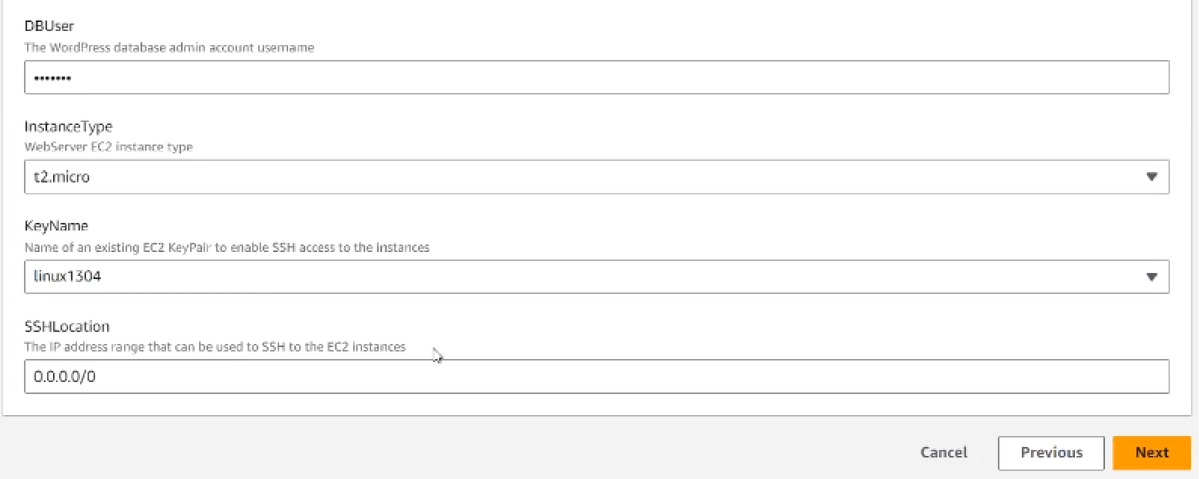
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

DBName
The WordPress database name
wordpressdb

DBPassword
The WordPress database admin account password
••••••••

DBRootPassword
MySQL root password
••••••••

DBUser

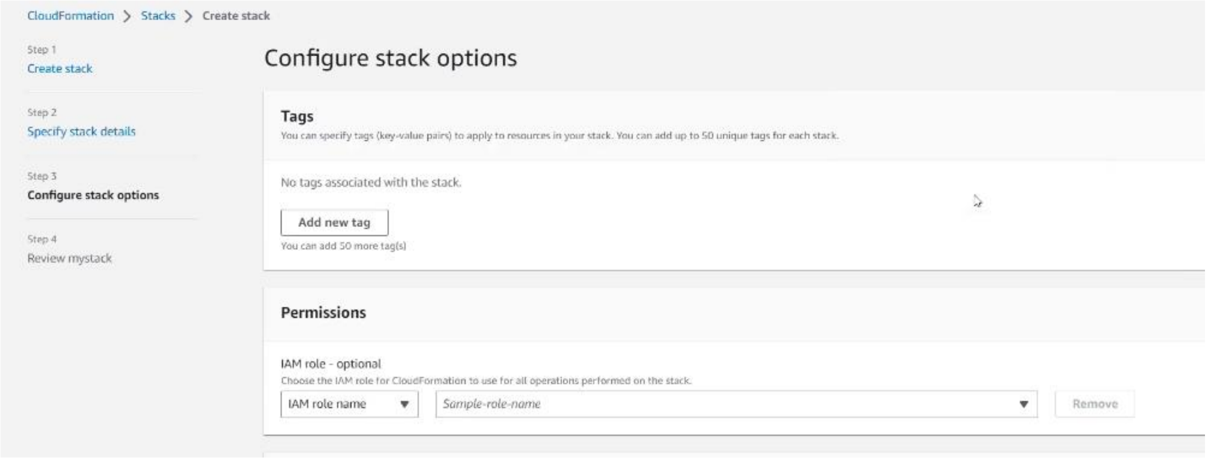


DBUser
The WordPress database admin account username
•••••••

InstanceType
WebServer EC2 instance type
t2.micro ▼

KeyName
Name of an existing EC2 KeyPair to enable SSH access to the instances
linux1304 ▼

SSHLocation
The IP address range that can be used to SSH to the EC2 instances
0.0.0.0/0



CloudFormation > Stacks > Create stack

Step 1
Create stack

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review mystack

Configure stack options

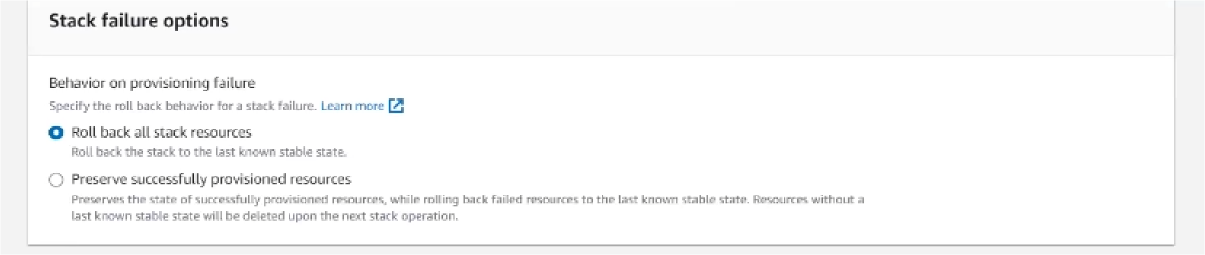
Tags
You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack.

No tags associated with the stack.

You can add 50 more tag(s)

Permissions

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



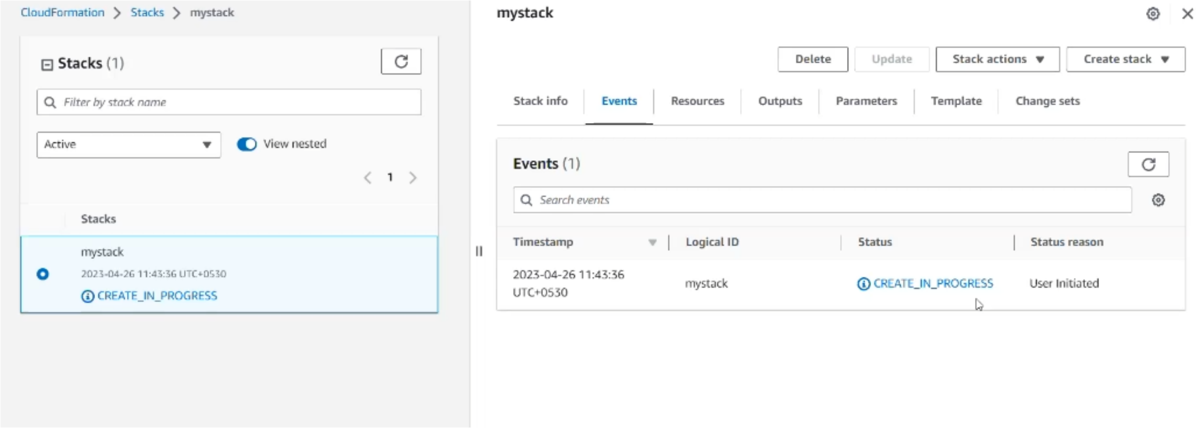
Behavior on provisioning failure

Specify the roll back behavior for a stack failure.

● Roll back all stack resources
Roll back the stack to the last known stable state.

○ Preserve successfully provisioned resources
Preserves the state of successfully provisioned resources, while rolling back failed resources to the last known stable state. Resources without a last known stable state will be deleted upon the next stack operation.

(*) review my stack – submit

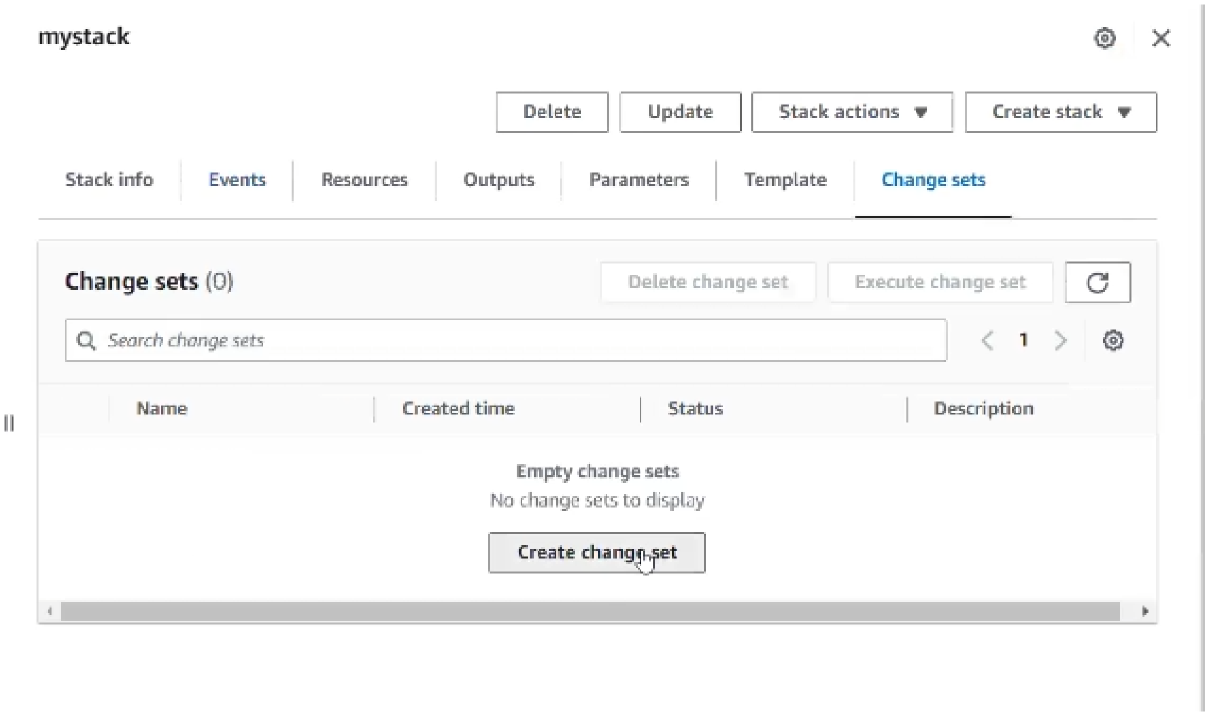


Stacks
mystack 2023-04-26 11:43:36 UTC+0530 CREATE_IN_PROGRESS

Timestamp	Logical ID	Status	Status reason
2023-04-26 11:43:36 UTC+0530	mystack	CREATE_IN_PROGRESS	User Initiated

To change t2 to t3

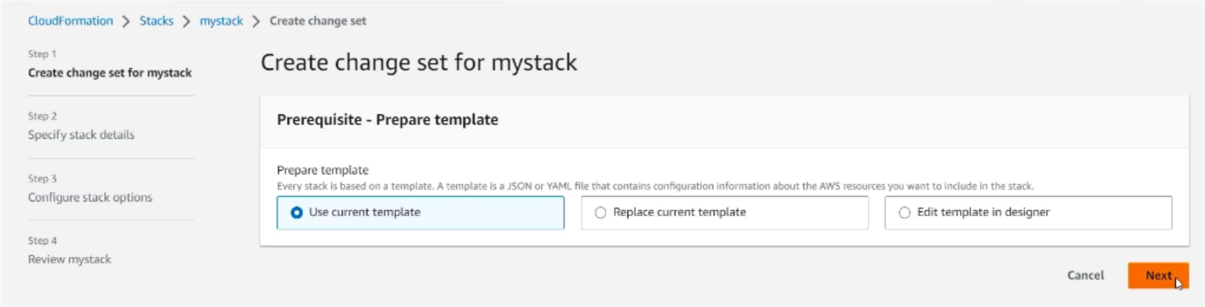
(*) go to cloud formation change sets



Name	Created time	Status	Description

Empty change sets

No change sets to display



CloudFormation > Stacks > mystack > Create change set

Step 1
Create change set for mystack

Step 2
Specify stack details

Step 3
Configure stack options

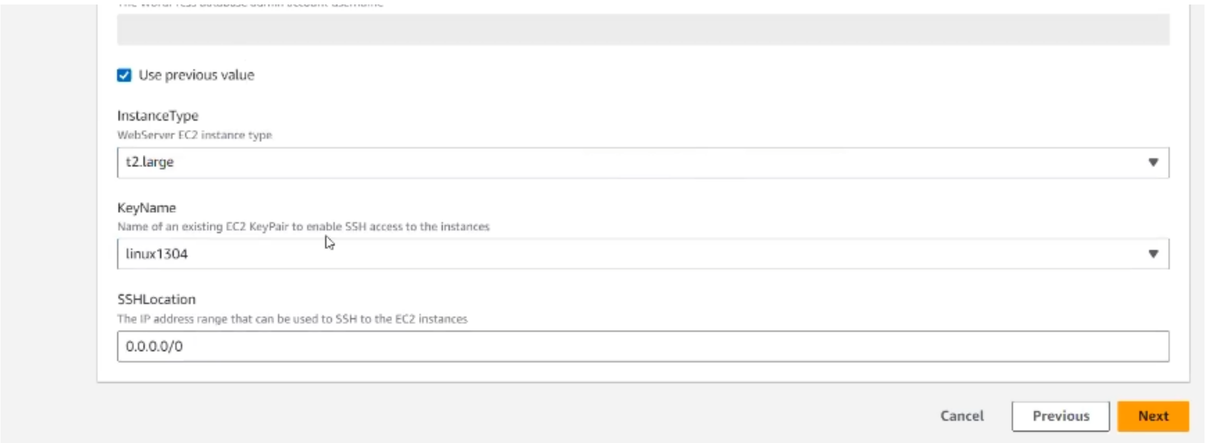
Step 4
Review mystack

Create change set for mystack

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.

● Use current template ○ Replace current template ○ Edit template in designer

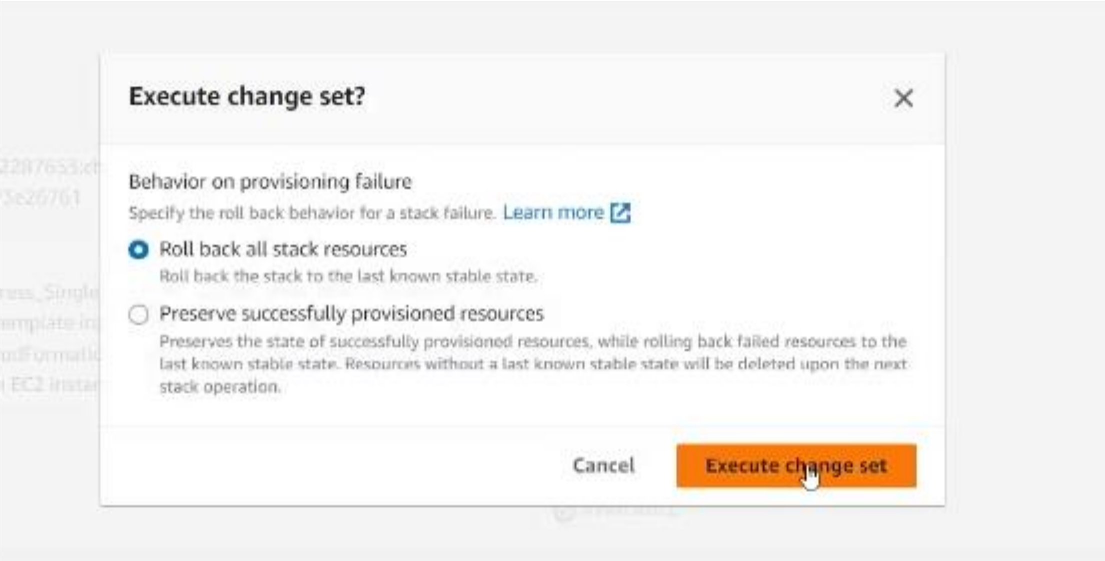


☑ Use previous value

InstanceType
WebServer EC2 instance type
t2.large

KeyName
Name of an existing EC2 KeyPair to enable SSH access to the instances
linux1304

SSHLocation
The IP address range that can be used to SSH to the EC2 instances
0.0.0.0/0

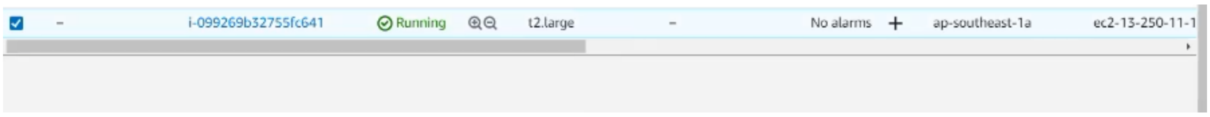


Execute change set?

Behavior on provisioning failure
Specify the roll back behavior for a stack failure. Learn more

● Roll back all stack resources
Roll back the stack to the last known stable state.

○ Preserve successfully provisioned resources
Preserves the state of successfully provisioned resources, while rolling back failed resources to the last known stable state. Resources without a last known stable state will be deleted upon the next stack operation.



☑	–	i-099269b32755fc641	✓ Running	t2.large	–	No alarms +	ap-southeast-1a	ec2-13-250-11-1