

S3 + CloudFront

S3	1
CloudFront	3
CloudFront Origins & Behaviors	8

S3

- To keep the static content for the front-end team, Let's create a bucket. Go to S3
- Enter the details as shown below.
 - Note: Bucket names are globally unique. So use **[your name]-netflux**.

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type [Info](#)

☒ **General purpose**

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory - New**

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

vins-netflux

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#) [🔗](#)

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

- This bucket is for **static files**! It should NOT contain any sensitive information.
- We can go with all the default settings. Click on “Create Bucket”.

General purpose buckets

Directory buckets

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

Find buckets by name

	Name	AWS Region
	vins-netflux	US East (N. Virginia) us-east-1

- Create a dummy **index.html** and upload.

```
<html>
  <body>
    <h1>Hello World</h1>
  </body>
</html>
```

Files and folders

Configuration

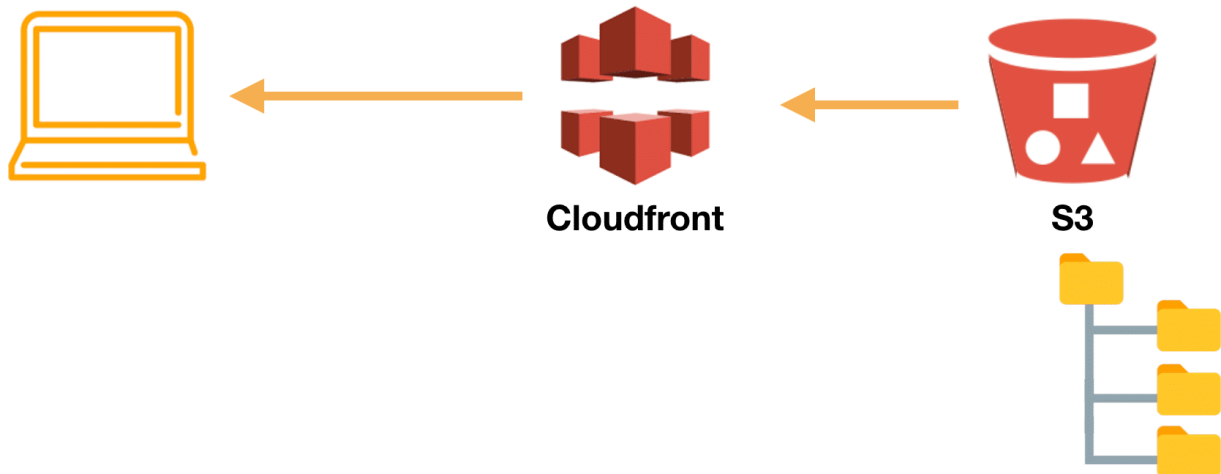
Files and folders (1 Total, 66.0 B)

Find by name

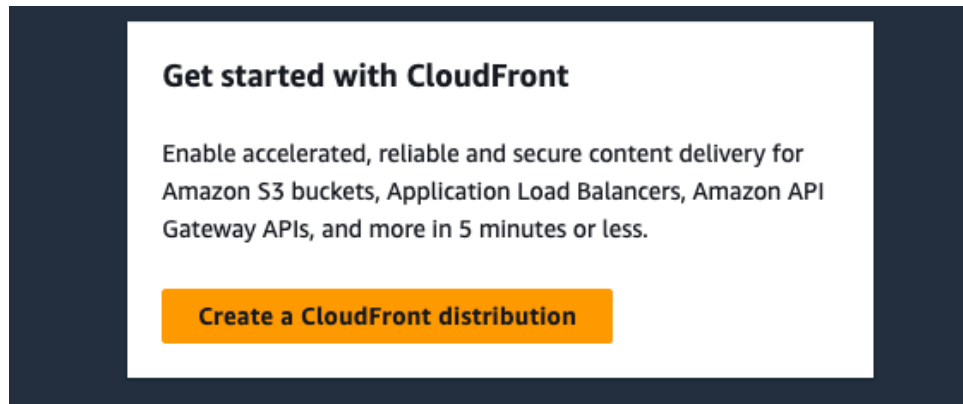
Name	Folder	Type	Size	Status	Error
index.html	-	text/html	66.0 B	✓ Succeeded	-

CloudFront

- Let's go to the cloud front.



- Create a Distribution



- Select the origin as S3

Origin

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

Amazon S3

vins-netflux.s3.amazonaws.com

- We might NOT want to provide public access to the bucket directly. Instead , we can use the “Origin Access Control (OAC)”, we will allow CloudFront to access the content and serve the static files.

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.

- This requires OAC policy creation.

Origin access control

Select an existing origin access control (recommended) or create a new control.

Select an origin access control ▼

Create new OAC

✖ This field cannot be empty

- Click on “Create new OAC”. Ensure that “**Signing behavior**” is selected as shown below.

Create new OAC

Name

The name must be unique. Valid characters: letters, numbers and most special characters. Use up to 64 characters.

vins-netflux.s3.us-east-1.amazonaws.com

Description - optional

The description can have up to 256 characters.

Enter description

Signing behavior

☐ Do not sign requests
 ☒ Sign requests (recommended)

☐ Do not override authorization header
Do not sign if incoming request has authorization header.

Origin type

S3

The origin type must be the same type as origin domain.

Cancel

Create

- Click on “Create”. You might see something as shown below. It is ok.

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

Origin access control

Select an existing origin access control (recommended) or create a new control.

vins-netflux.s3.us-east-1.amazonaws.com ▼

Create new OAC



You must update the S3 bucket policy

CloudFront will provide you with the policy statement after creating the distribution.

- WAF - This is optional.

Web Application Firewall (WAF) [Info](#)

☐ Enable security protections

Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

☒ Do not enable security protections

Select this option if your application does not need security protections from AWS WAF.

- Settings

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

- Default “root” object will be “index.html”

Default root object - *optional*

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

index.html

- Click on “Create distribution”
- Once created, CloudFront will provide a “Policy”. This policy has to be attached to the S3 bucket.



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

Origin access control

Select an existing origin access control (recommended) or create a new control.

vins-netflux.s3.us-east-1.amazonaws.com ▼

Create new OAC

 You must allow access to CloudFront using this policy statement. Learn more about [giving CloudFront permission to access the S3 bucket](#) .

 Copy policy

 [Go to S3 bucket permissions](#) 

- Copy the policy and go to S3 - bucket permissions

[Amazon S3](#) > [Buckets](#) > vins-netflux

vins-netflux Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

- We can add this policy & Save


Edit bucket policy [Info](#)

Bucket policy

[Policy examples](#)

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.

Bucket ARN

 `arn:aws:s3:::vins-netflux`

Policy

```
1 {
2   "Version": "2008-10-17",
3   "Id": "PolicyForCloudFrontPrivateContent",
4   "Statement": [
5     {
6       "Sid": "AllowCloudFrontServicePrincipal",
7       "Effect": "Allow",
8       "Principal": {
9         "Service": "cloudfront.amazonaws.com"
10      },
11      "Action": "s3:GetObject",
12      "Resource": "arn:aws:s3:::vins-netflux/*",
13      "Condition": {
14        "StringEquals": {
15          "AWS:SourceArn": "arn:aws:cloudfront::941077029185:distribution/*"
16        }
17      }
18    }
19  ]
20 }
```





Edit statement

Select

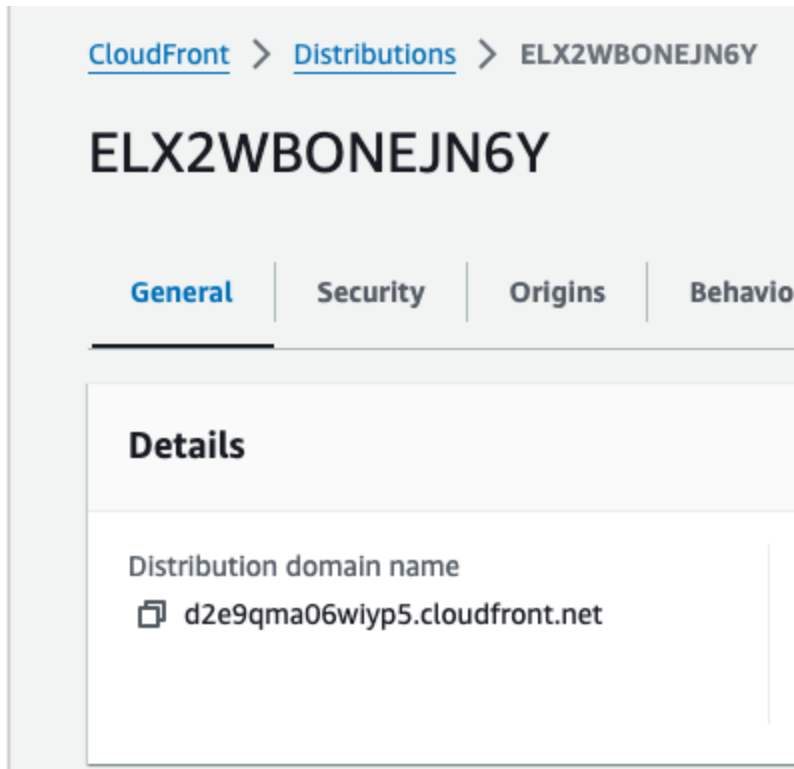
Select an existing statement or add a new one.

+ Add new statement

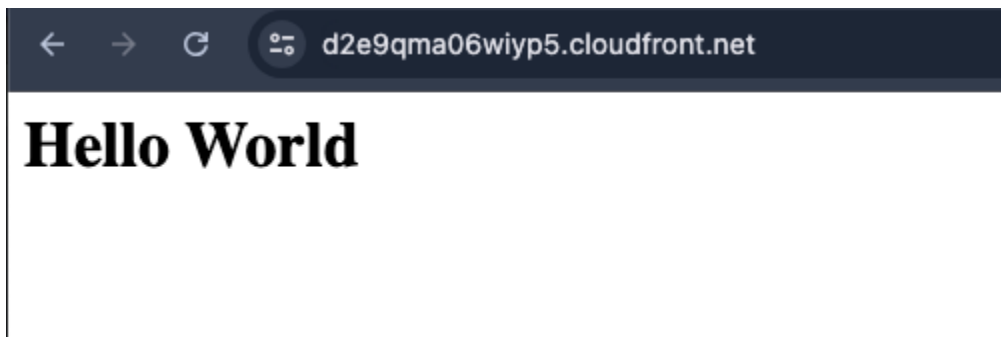
- CloudFront is integrated with S3 bucket.
- Go to CloudFront again. If it is “Deploying”, wait!

Distributions (1) Info							
<div><div></div><div><div>Enable</div><div>Disable</div><div>Delete</div><div>Create distribution</div></div></div>							
<div><div><input type="text" value="Search all distributions"/></div><div><div>< 1 ></div><div></div></div></div>							
ID	Descrip...	Type	Domai...	Alterna...	Origins	Status	Last m...
ELX2WBONEJN6Y	-	Production	d2e9qma...	-	vins-netflux.s3.i	 Enabled	 Deploying...

- Once it is deployed, (It will show the last modified date, instead of “Deploying”), click on the Distribution. Get the domain name.

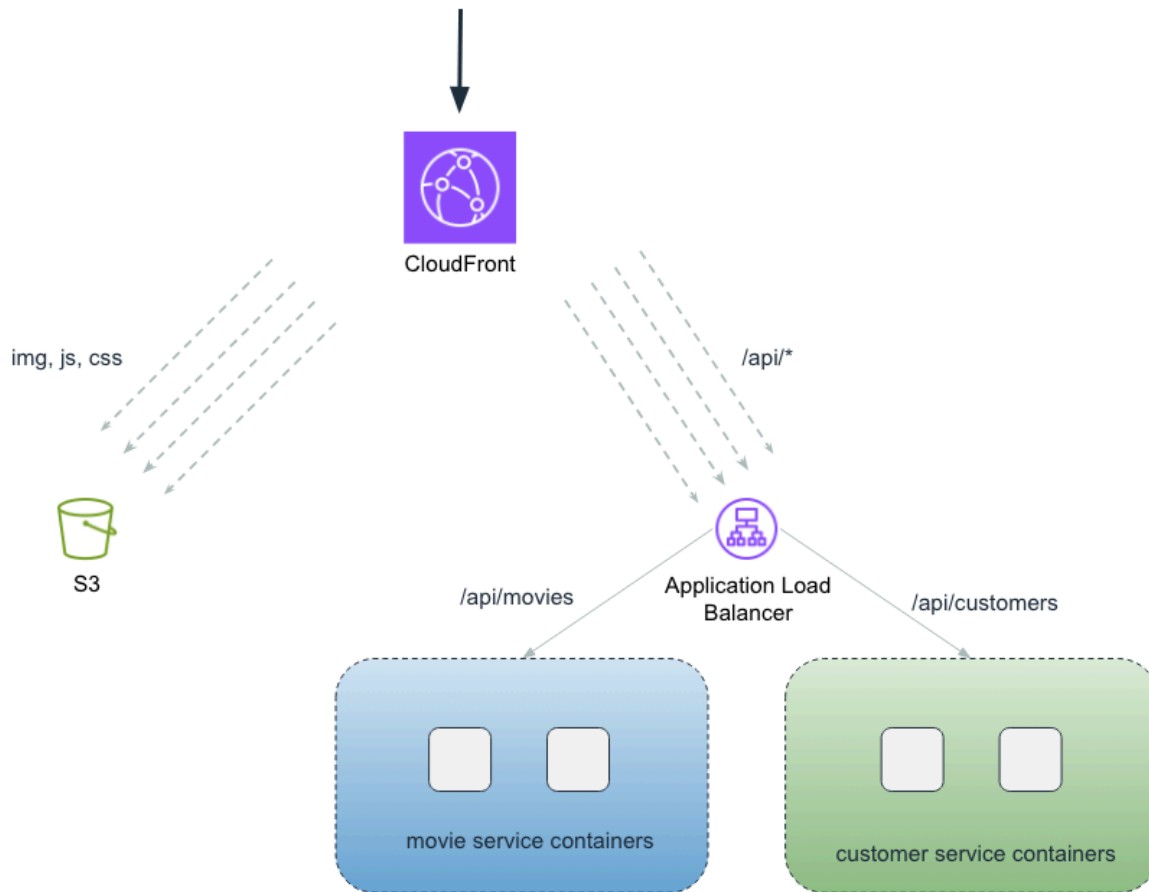


- We should be able to see our home page



CloudFront Origins & Behaviors

- S3 will be the origin for static files.
- ALB should be the origin for any API requests.



- Create another Origin for ALB.

Create origin

Settings

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

Amazon S3

vins-netflux.s3.amazonaws.com

Elastic Load Balancer

netflux-alb

- Origin Protocol should be “HTTP”
- Add the Origin.

General
Security
Origins
Behaviors
Error pages

Origins

Filter origins by property or value

	Origin name ▼	Origin domain ▼	Origin path
<input type="radio"/>	vins-netflux.s3.us-e...	vins-netflux.s3.us-e...	
<input type="radio"/>	netflux-alb-89738...	netflux-alb-89738...	

- Create new “Behavior”. Any “/api/*” will be routed to ALB.

Settings

Path pattern
Info

/api/*

Origin and origin groups

netflux-alb-685682469.us-east-1.elb.amazonaws.com

- Viewer protocol policy should be “HTTPS”
- Select the option based on the requirements.

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

|

- Create the behavior.
- We should be able to see the behaviors as shown below.

ELX2WBONEJN6Y

General | Security | Origins | **Behaviors** | Error pages | Invalidations | Tags

Behaviors Save

Filter behaviors by property or value

	Preced...	Path pattern	Origin or origin group	Viewer protocol policy
<input type="radio"/>	0	/api/*	netflux-alb-685682469.us-east-1.elb.amazon...	HTTP and HTTPS
<input type="radio"/>	1	Default (*)	vins-netflux.s3.us-east-1.amazonaws.com	HTTP and HTTPS

- We can test our configuration.
 - It shows that the request was routed to ALB. We provide the default ALB response.

