

S3 + CloudFront

S3	1
CloudFront	2
CDN Distribution Settings	5
CDN Distribution Origins - S3	6
CDN Distribution Origins - ALB	10
CDN Distribution Origins - Behavior	12

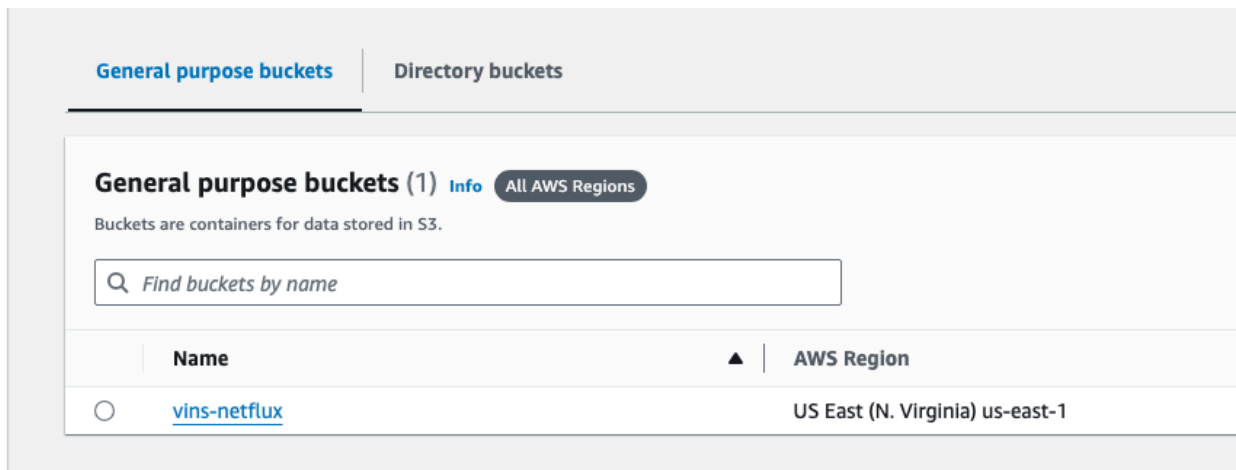
S3

- To serve the static content, 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** or any name you prefer.

The screenshot shows the 'Create bucket' page in the AWS Management Console. At the top, it says 'Create bucket' with an 'Info' link. Below that, a note states 'Buckets are containers for data stored in S3.' The main section is titled 'General configuration'. Under 'AWS Region', 'US East (N. Virginia) us-east-1' is selected. For 'Bucket type', 'General purpose' is selected with a radio button, and 'Directory - New' is unselected. The 'General purpose' option is described as recommended for most use cases and access patterns, allowing a mix of storage classes. The 'Directory - New' option is described as recommended for low-latency use cases, using only the S3 Express One Zone storage class. Below this, the 'Bucket name' field contains 'vins-netflux'. A note below the field states that the bucket name must be unique within the global namespace and follow the naming rules, with a link to 'See rules for bucket naming'. There is a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button. At the bottom, the format 's3://bucket/prefix' is shown.

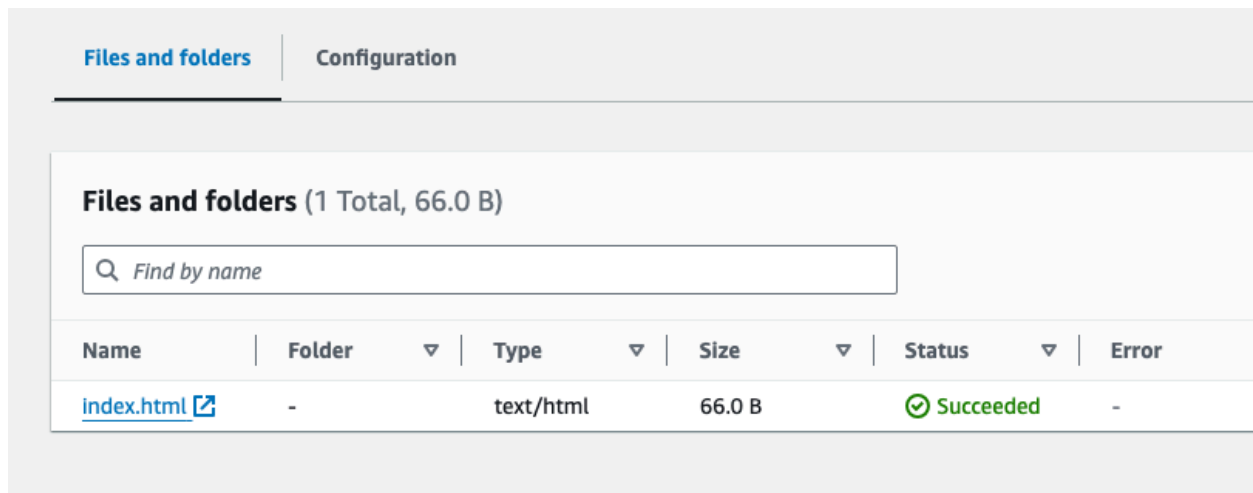
- This bucket is for **static files**! It should NOT contain any sensitive information.

- We can go with all the default settings. Click on “Create Bucket”.



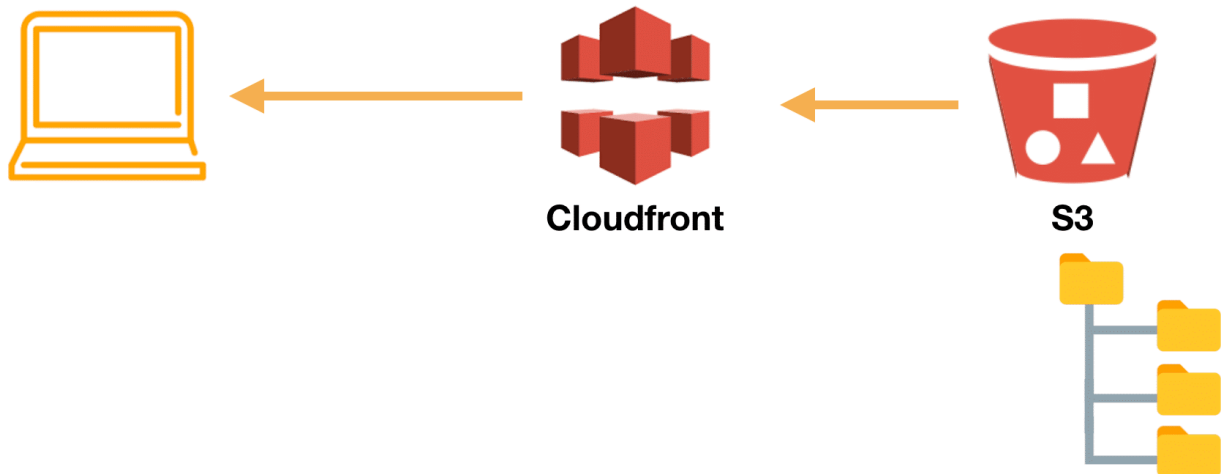
- Create a dummy **index.html** and upload.

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

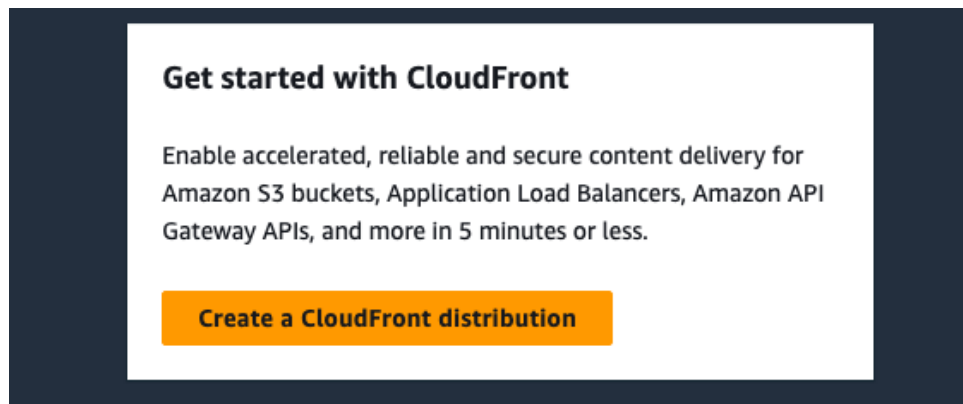


CloudFront

- Let's go to the cloud front.



- Create a Distribution



Get started

Connect your websites, apps, files, video streams, and other content to CloudFront. We optimize the performance, reliability, and security for you

Distribution options [Info](#)

Distribution name

Name will be stored as a tag on the resource. You can add a name, or more tags, later.

Description - *optional*

Distribution type



Single website or app

Choose if each website or application will have a unique configuration.



Multi-tenant architecture - New

Choose when you have multiple domains that need to share configurations. This is a common architecture for SaaS providers.

- Select the origin as S3

Origin type

Your origin is where your content (such as a website or app) lives. CloudFront works with AWS-based origins and origins hosted on other cloud providers.



Amazon S3

Deliver static assets like files and images, statically generated websites or single page applications (SPA).



Elastic Load Balancer

Deliver applications hosted behind ELB such as dynamic websites, web services, and APIs.



API Gateway

Deliver API endpoints for REST APIs hosted on API Gateway.



Elemental MediaPackage

Deliver end-to-end live events or video on demand (VOD).



VPC origin

Deliver applications and content hosted within private VPCs, such as EC2 instances and Application Load Balancers.



Other

Refer to any AWS or non-AWS origin through its publicly resolvable URL.

Origin

S3 origin

Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

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

Origin path - optional

The directory path within your origin where your content is stored. [Learn more](#)

/path

- Lets go with default settings and click Next.

Settings

[Info](#)

CloudFront provides default origin and cache settings based on what origin you selected. [View default settings for S3](#)

Allow private S3 bucket access to CloudFront

[Info](#)

CloudFront will update your S3 bucket policy to allow CloudFront to access your S3 bucket. The policy allows CloudFront to access the bucket only when the request is on behalf of the CloudFront distribution that contains the S3 origin.

☒ Allow private S3 bucket access to CloudFront - *Recommended*

Origin settings

Origin settings control how CloudFront connects to the specified origin.



Use recommended origin settings



Customize origin settings

Cache settings

Cache settings determine when CloudFront serves cached content and when it fetches new content from the origin.



Use recommended cache settings tailored to serving S3 content



Customize cache settings

- We do NOT need additional security as part of WAF service. So select “Do not enable security protections”

- WAF will be helpful to protect the applications from SQL Injection / Cross-site scripting etc. It is a paid service. We do NOT need this for this demo.

Enable security

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.

- Create the Distribution.

CDN Distribution Settings

[CloudFront](#) > [Distributions](#) > E2SQGO9RQ97H4F

vins-netflux Standard

Details

Distribution domain name d3lvofpitbj7vv.cloudfront.net	ARN arn:aws:cloudfront::886930296652:distribution/E2SQGO9RQ97H4F	Last modified Deploying
--	--	-----------------------------------

[General](#) | [Security](#) | [Origins](#) | [Behaviors](#) | [Error pages](#) | [Invalidations](#) | [Tags](#) | [Logging](#)

Settings

Name vins-netflux	Alternate domain names - Add domain	Standard logging Off
Description -		Cookie logging Off
Price class Use all edge locations (best performance)		Default root object -
Supported HTTP versions HTTP/2, HTTP/1.1, HTTP/1.0		

- Once created, go to the “**General**” tab and Click on **Edit**
- Default root object will be **index.html**

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.

index.html

- Under Connectivity, we use all edge locations.

Connectivity

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

IPv6

- ☐ Off
- ☒ On

Anycast static IP list

Deliver traffic from a small set of IP addresses

None

There are no Anycast static IP lists available

[Create an Anycast static IP list](#) [↗](#)

- Click on Save Changes.

CDN Distribution Origins - S3

- Go to the **Origins** tab.

CloudFront > Distributions > E2SQGO9RQ97H4F

vins-netflux Standard

Details

Distribution domain name
d3ivofpitbj7vv.cloudfront.net

ARN
arn:aws:cloudfront::886930296652:distribution/E2SQGO9RQ97H4F

Last modified
Deploying

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

Settings

Name
vins-netflux

Description
-

Price class
Use all edge locations (best performance)

Supported HTTP versions
HTTP/2, HTTP/1.1, HTTP/1.0

Alternate domain names
-

[Add domain](#)

Standard logging
[Off](#)

Cookie logging
[Off](#)

Default root object
-

- Select the origin and click on **Edit**.

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

Origins (1/1) Edit Delete

Filter origins by property or value

Origin name	Origin domain	Origin path	Origin type	Origin Shield region	Origin
<input checked="" type="radio"/> vinoth-netflux.s3.us-east-1	vinoth-netflux.s3.us-...		S3	-	E1B01

- 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. CDN distribution automatically creates one for us.

Origin access control

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

oac-netflux-vins.s3.us-east-1.amazonaws.com-mhrt10xee83 ▼

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 ↗

- This policy has to be attached to the S3 bucket. Click on **“Copy policy”** & **Go to S3 bucket permissions**

☰

Amazon S3 > Buckets > netflux-vins

Amazon S3 <

General purpose buckets

Directory buckets

Table buckets

Vector buckets

Access Grants

Access Points (General Purpose Buckets, FSx file systems)

Access Points (Directory Buckets)

Object Lambda Access Points

Multi-Region Access Points

netflux-vins Info

Objects | Metadata | Properties | **Permissions** | Metrics

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM ana](#)
[View analyzer for us-east-1](#)

Block public access (bucket settings)


- Click on **Edit** Bucket Policy & replace the policy.

Edit bucket policy [Info](#)

Bucket policy

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





Bucket ARN

 arn:aws:s3:::netflux-vins

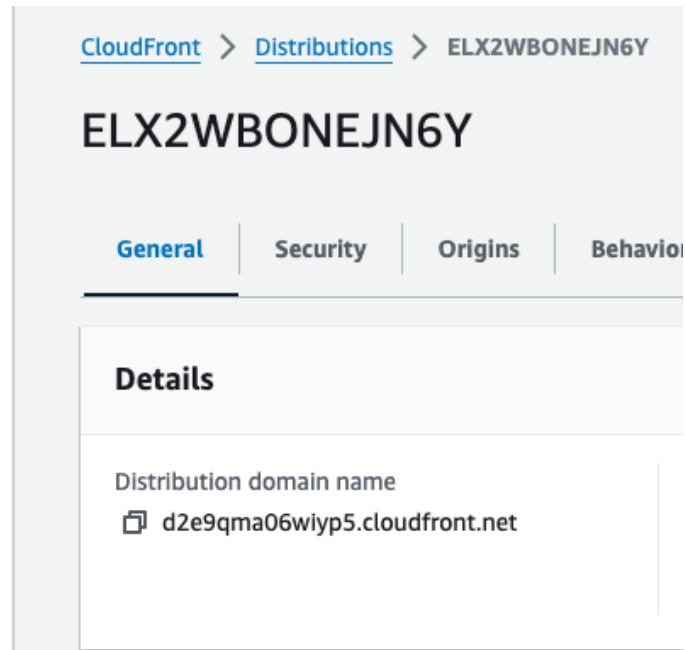
Policy

```
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:::netflux-vins/*",
13      "Condition": {
14        "StringEquals": {
15          "AWS:SourceArn": "arn:aws:cloudfront::127549748682:distribution/EKRHFXR20XIGD"
16        }
17      }
18    }
19  ]
20 }
```

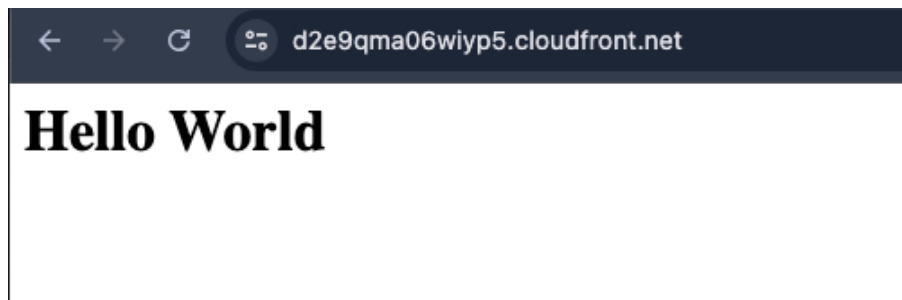
- Save changes
- At this point, CloudFront is integrated with S3 bucket.
- Go to CloudFront again. If it is “Deploying”, wait!

Distributions (1) Info							
<div> Enable Disable Delete Create distribution</div> <div><input type="text" value="Search all distributions"/></div> <div>< 1 > </div>							
ID	Descrip...	Type	Domal...	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.

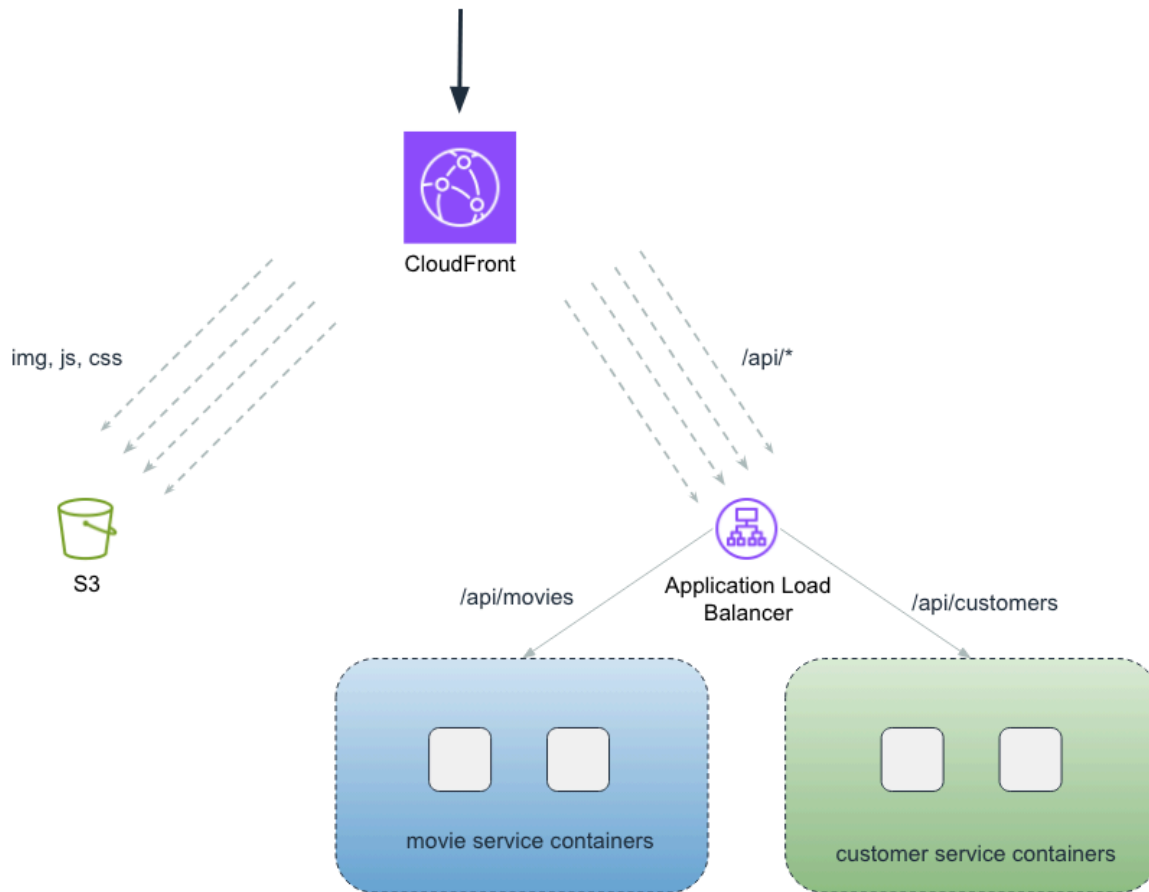


- We should be able to see our home page



CDN Distribution Origins - ALB

- 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” (That is ALB accepts HTTP)
- Create the Origin.

General	Security	Origins	Behaviors	Error pages
Origins				
<input type="text"/> 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...		

CDN Distribution Origins - Behavior

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

Settings

Path pattern
Info

Origin and origin groups

- 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.

