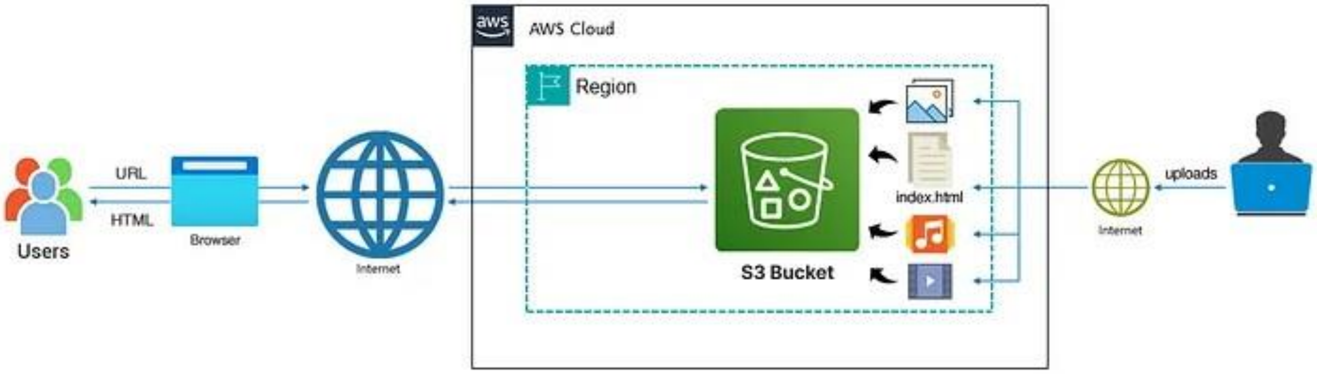
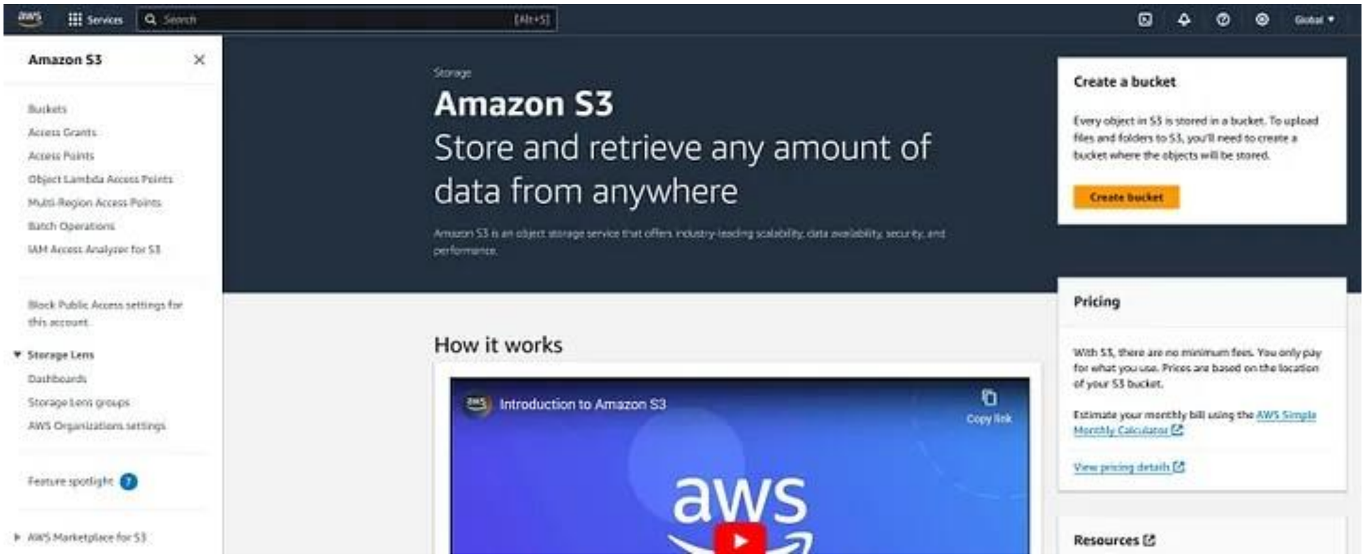


Step 1: Creating a S3 bucket

The first step you need to take is to create an S3 bucket to put your website’sfiles and folders.

1. Sign in to the AWS Management Console.
2. Open the Amazon S3 console

This should display the S3 dashboard.



Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Pricing

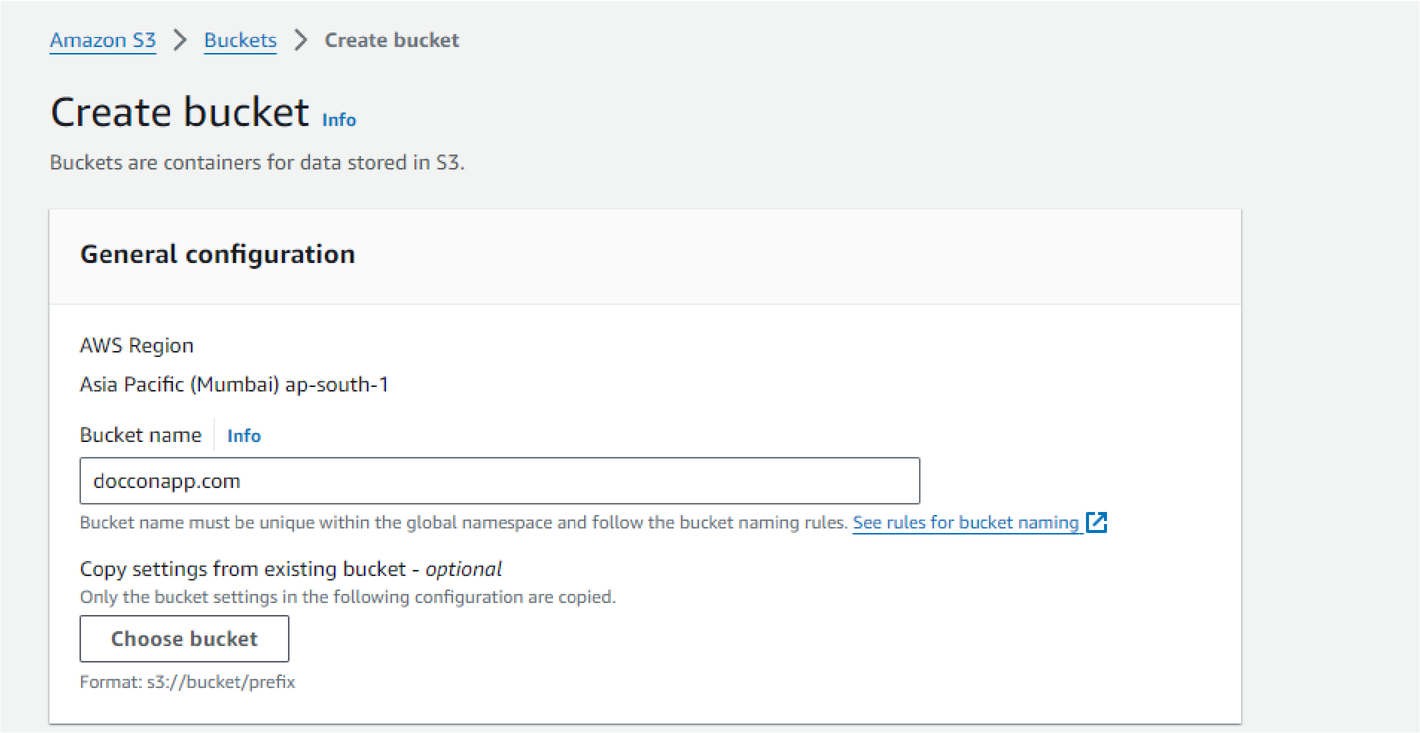
With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

3. Click on Create bucket.

4. Choose a Region that is geographically close to you to minimize latencyand costs, or to address regulatory requirements. The Region that you choose determines your Amazon S3 website endpoint.



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name Info

docconapp.com

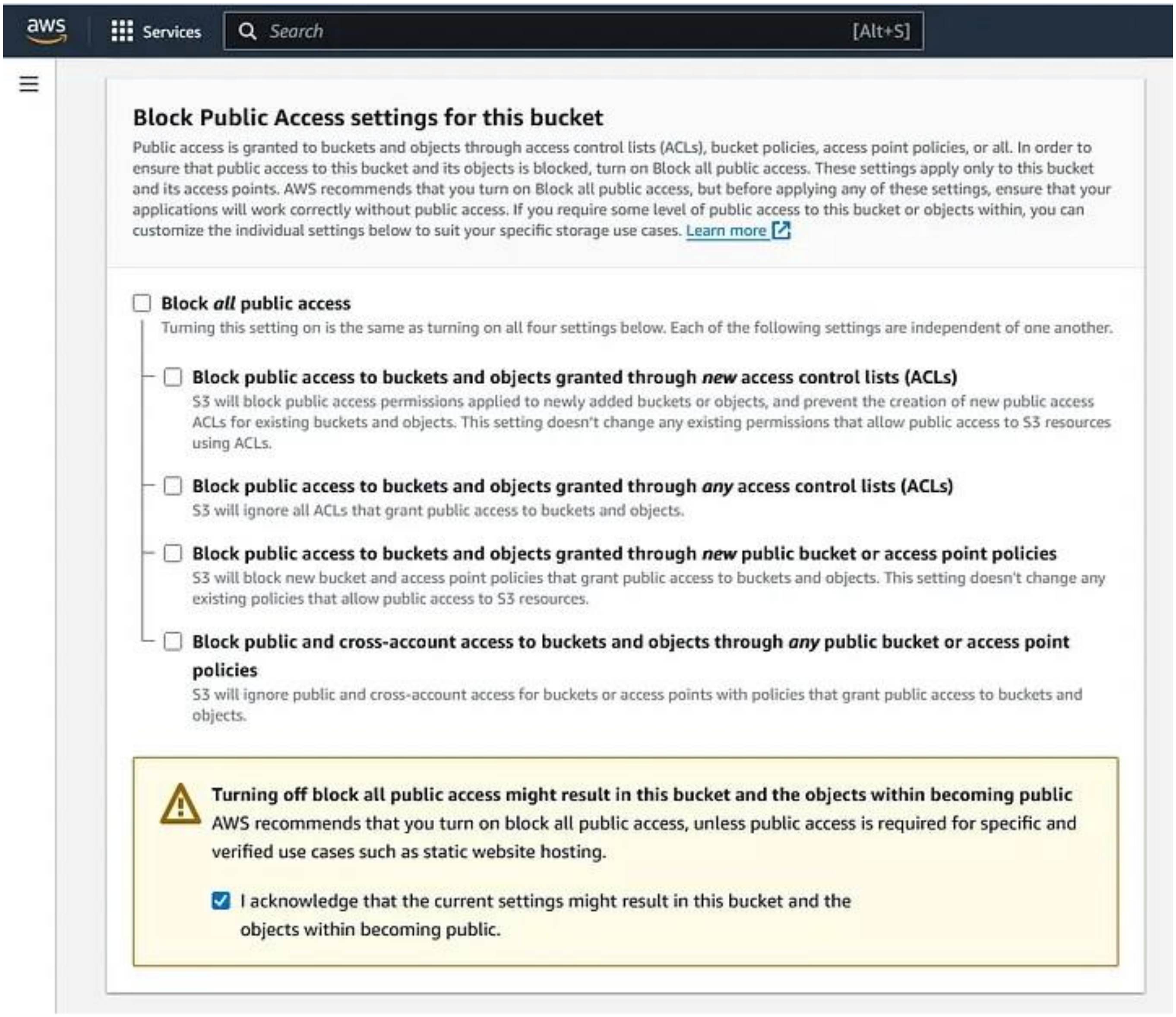
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

5. Under “Block Public Access settings for this bucket” section, uncheck the“Block all public access” checkbox and accept the acknowledgement.



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

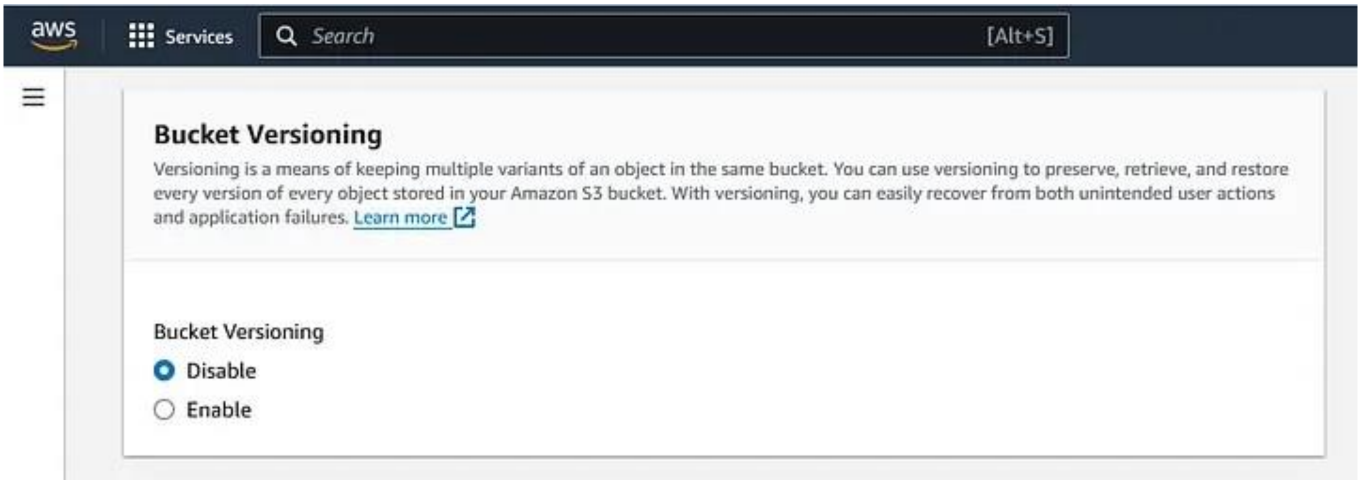
□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **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 objects.

⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

6. Select “Disable” for Bucket Versioning.

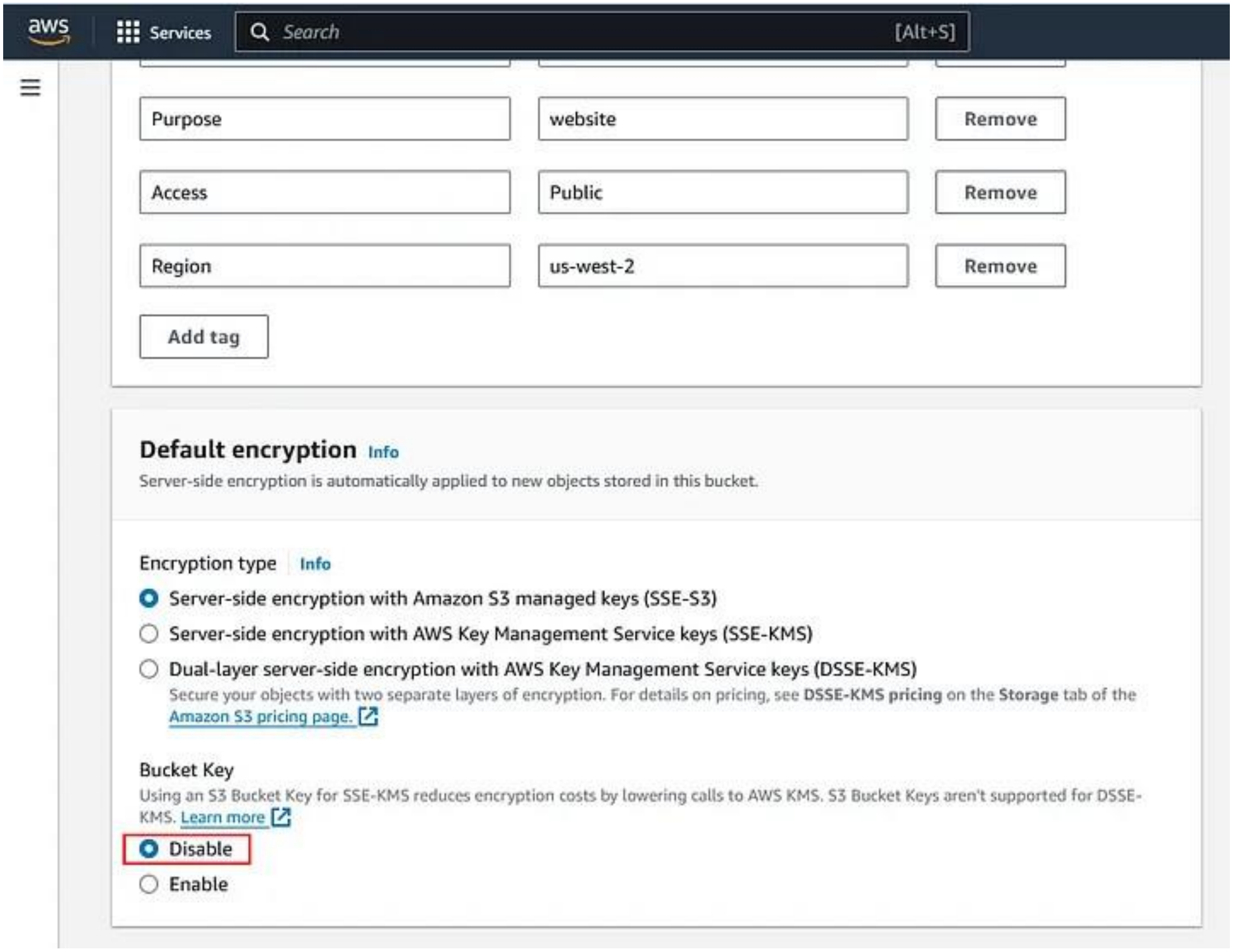


Bucket Versioning

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

7. Under “Default encryption” section, click on disable for Server-sideencryption.



Purpose	website	Remove
Access	Public	Remove
Region	us-west-2	Remove

Add tag

Default encryption Info

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

Encryption type Info

● Server-side encryption with Amazon S3 managed keys (SSE-S3)

○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

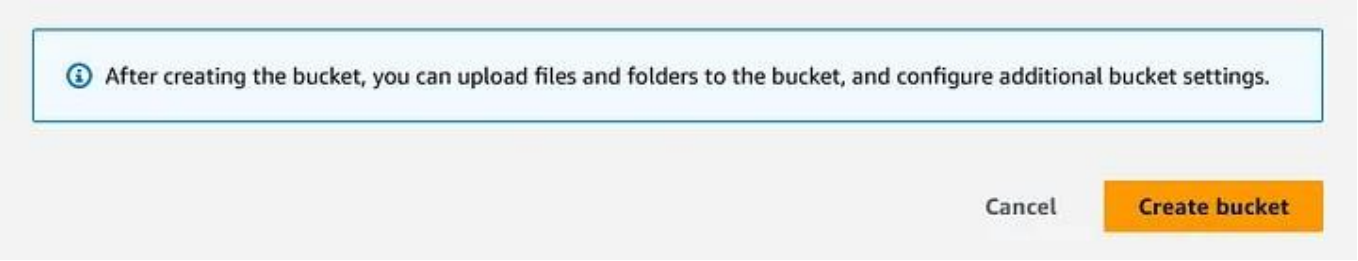
Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

● Disable

○ Enable

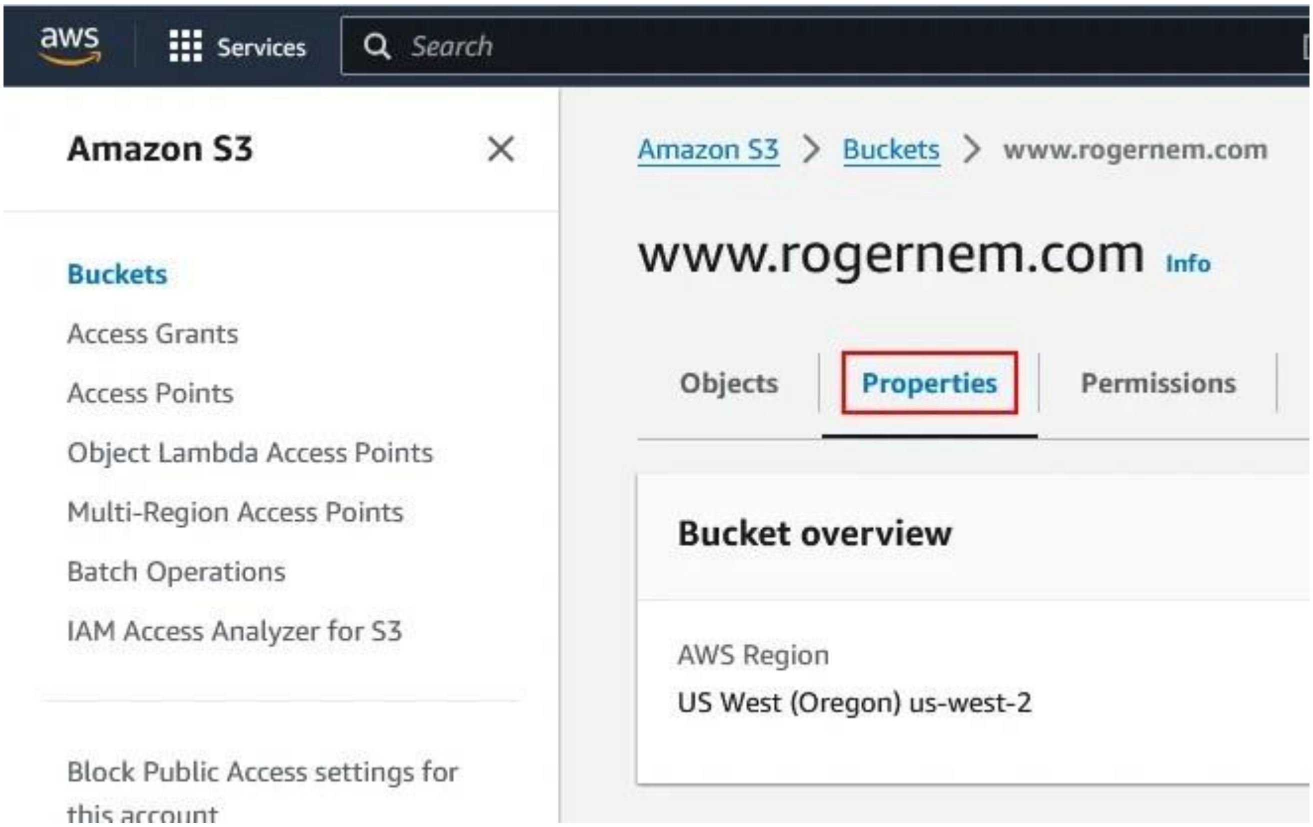
8. Click on “Create bucket”.


After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Step 2: Enabling static website hosting

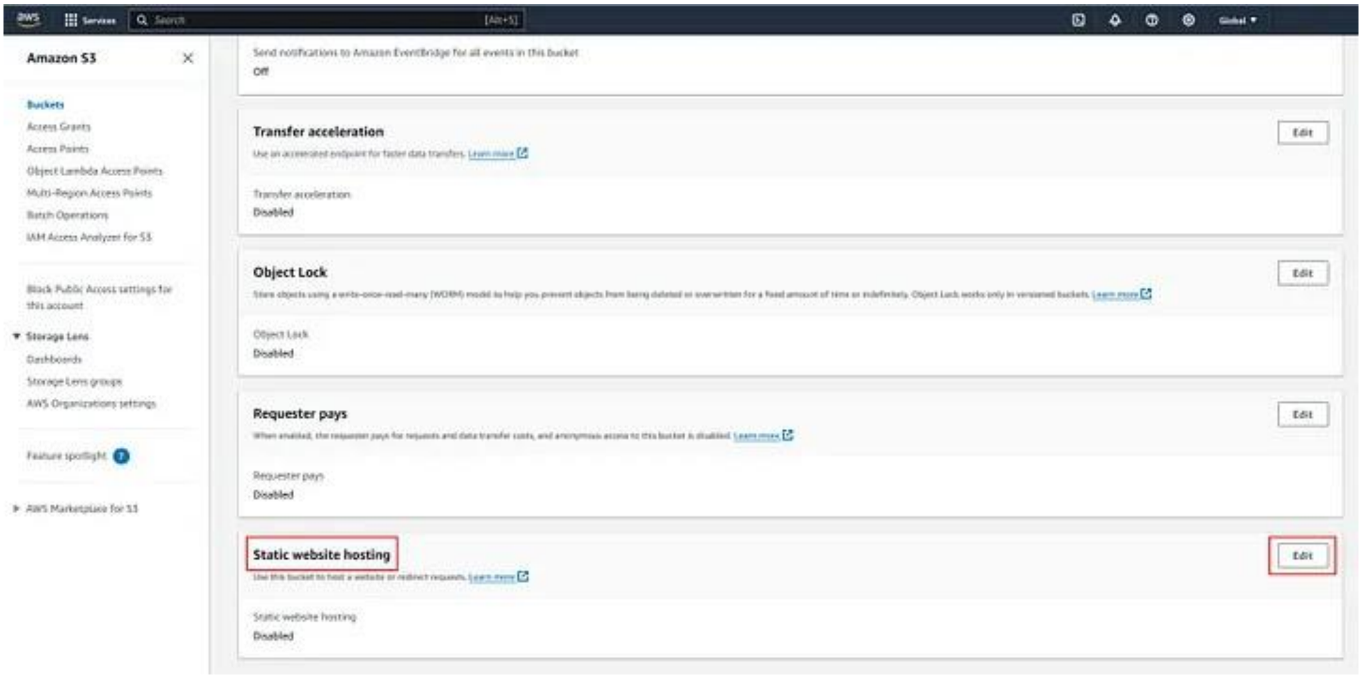
1. In the Buckets list, choose the name of the bucket that you want to enablestatic website hosting

2. Click on the “Properties” tab.


aws
Services
Search
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Amazon S3 > Buckets > www.rogernem.com
www.rogernem.com Info
Objects
Properties
Permissions
Bucket overview

AWS Region
US West (Oregon) us-west-2

3. Scroll down to the “Static website hosting” section and click on its Edit button.



Send notifications to Amazon EventBridge for all events in this bucket
Off

Transfer acceleration

Use an accelerated endpoint for faster data transfers. Learn more

Transfer acceleration
Disabled

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. Learn more

Object Lock
Disabled

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more

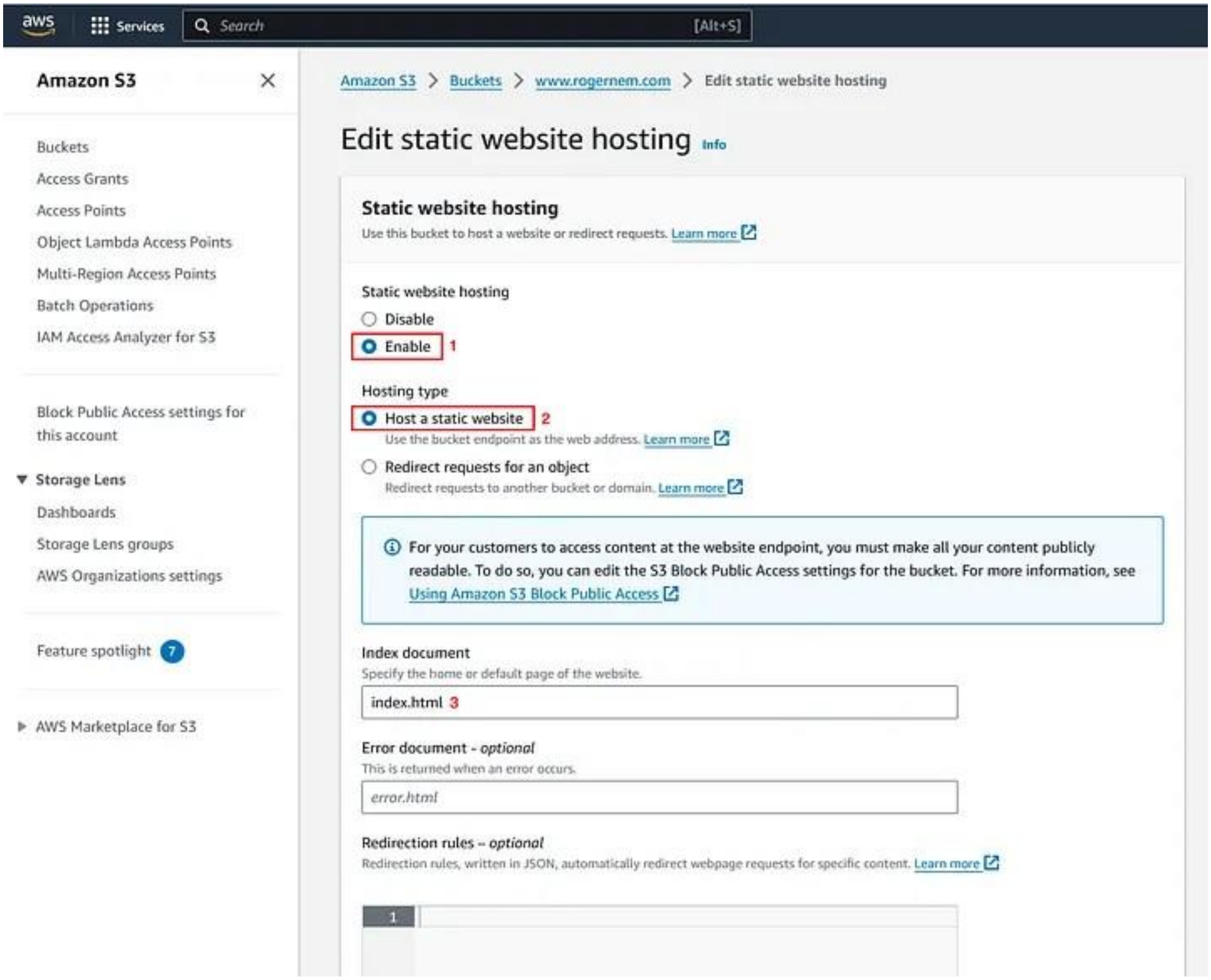
Requester pays
Disabled

Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting
Disabled

4. Under Static website hosting, choose Enable (1). Also, select Host a staticwebsite (2) for the Hosting type. In Index document, enter the file name of the index document, typically index.html (3).


aws
Services
Search
[Alt+S]
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Amazon S3 > Buckets > www.rogernem.com > Edit static website hosting
Info
1
2
3

Edit static website hosting

Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

○ Disable

● Enable

Hosting type

● Host a static website

Use the bucket endpoint as the web address. Learn more

○ Redirect requests for an object

Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

Index document

Specify the home or default page of the website.

index.html

Error document - *optional*

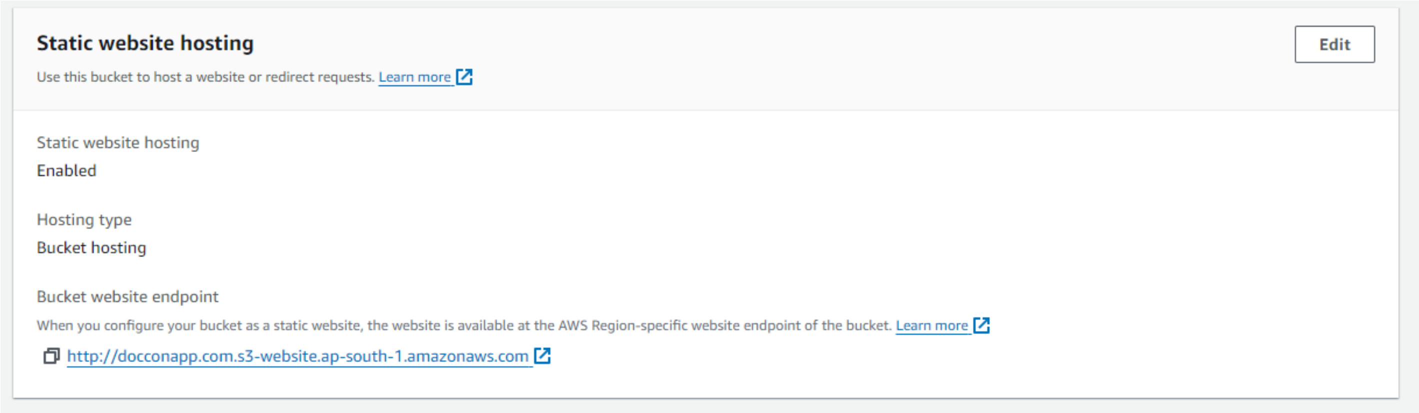
This is returned when an error occurs.

error.html

Redirection rules – *optional*

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more

5. Click on “Save Changes”. You should see the following next.



Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

Enabled

Hosting type

Bucket hosting

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more

http://docconapp.com.s3-website.ap-south-1.amazonaws.com

Under Static website hosting, note the Endpoint which is the Amazon S3website endpoint for your bucket.

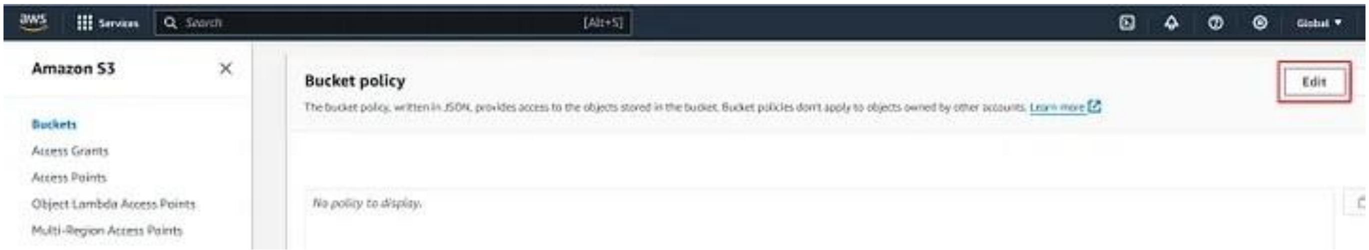
Step 3: Securing my S3 bucket through IAM policies

To allow users to access your website and to secure your S3 bucket and blockuploads and/or deletions, you will need to add a bucket policy.

1. Under Buckets, click on the name of your website bucket.

2. Click on the “Permissions” tab.

3. Under Bucket Policy, choose Edit.



Bucket policy

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. Learn more

No policy to display.

4. To grant public read access for your website, copy the following bucket policy, and paste it in the Bucket policy editor. Make sure to replace bucket-name with the name of your bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. Scroll down and click on “Save changes”. You should see the followingnext.

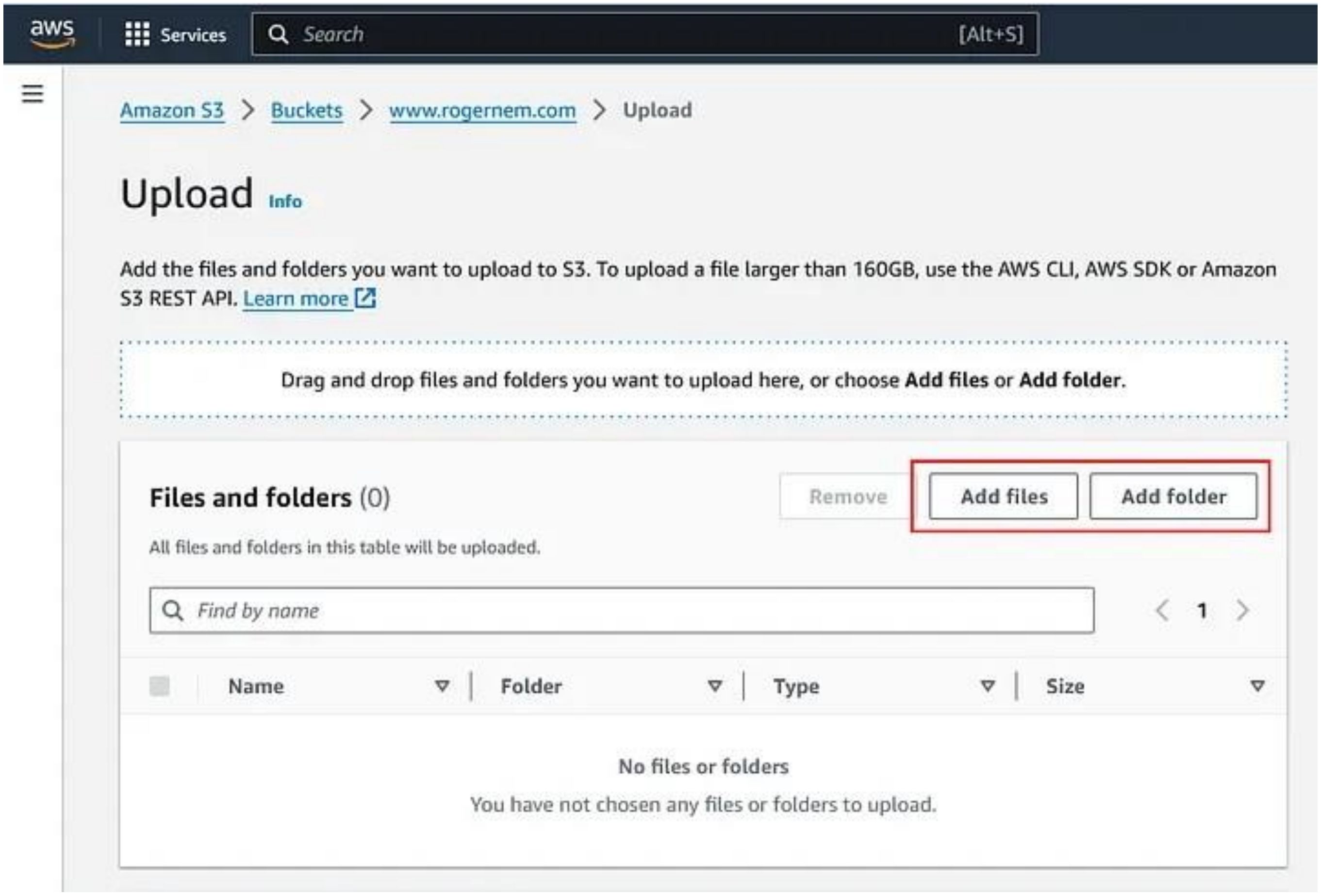
Step 4: Uploading web files to my S3 bucket

After completing all the previous steps, you need to upload your website’sfiles and folders to your website S3 bucket.

1. Under Buckets, click on the name of your website bucket.

2. On the Objects tab, you can see that the bucket is currently empty, click onthe Upload button.

3. This should take you to the Upload page. Click Add files to add the websitefiles and use Add folder to add the website folders.



Amazon S3 > Buckets > www.rogernem.com > Upload

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 folder**.

Files and folders (0)

All files and folders in this table will be uploaded.

	Name	Folder	Type	Size

No files or folders

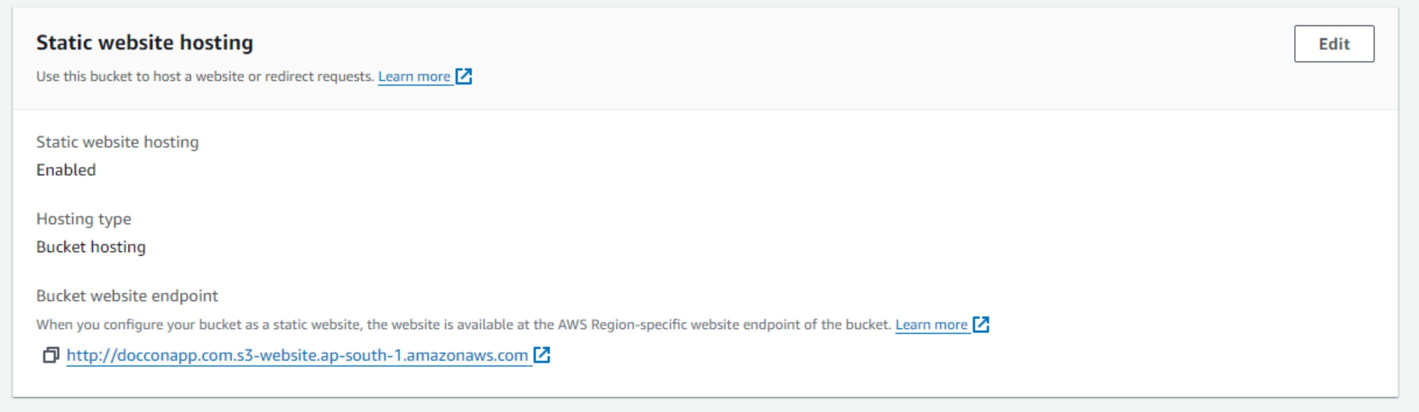
You have not chosen any files or folders to upload.

Step 5: Testing my website endpoint

1. Under Buckets, click on the name of your website bucket.

2. Click on the “Properties” tab.

3. scroll down to the “Static website hosting” section and click on yourendpoint URL.



Static website hosting

Use this bucket to host a website or redirect requests. Learn more

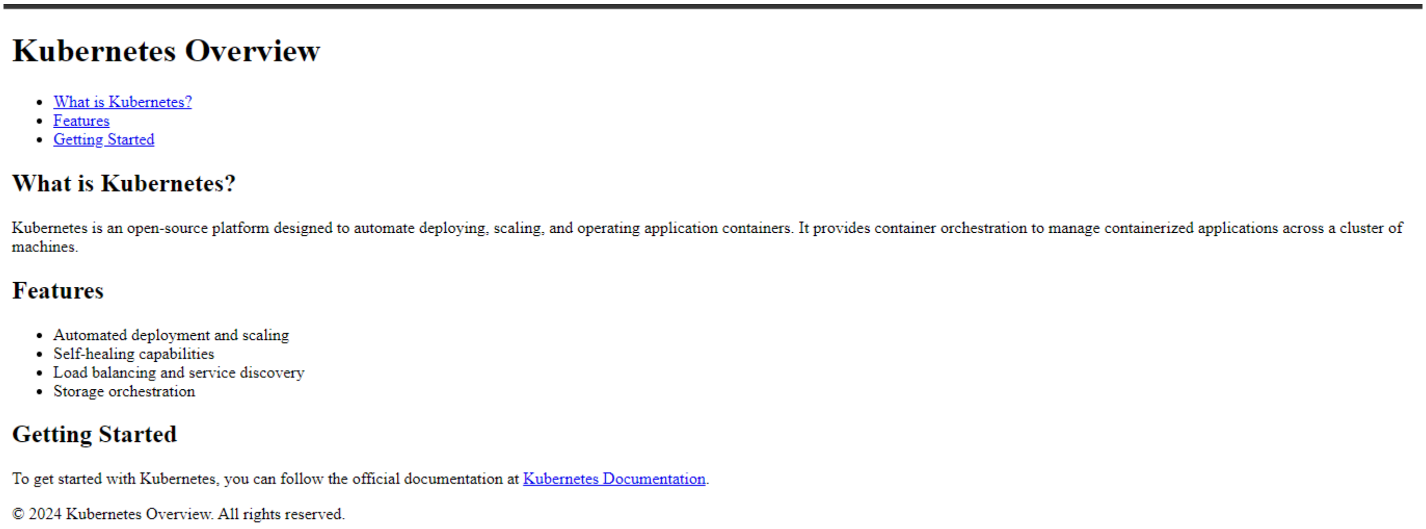
Edit

Static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more

http://docconapp.com.s3-website.ap-south-1.amazonaws.com



Kubernetes Overview

- What is Kubernetes?
- Features
- Getting Started

What is Kubernetes?

Kubernetes is an open-source platform designed to automate deploying, scaling, and operating application containers. It provides container orchestration to manage containerized applications across a cluster of machines.

Features

- Automated deployment and scaling
- Self-healing capabilities
- Load balancing and service discovery
- Storage orchestration

Getting Started

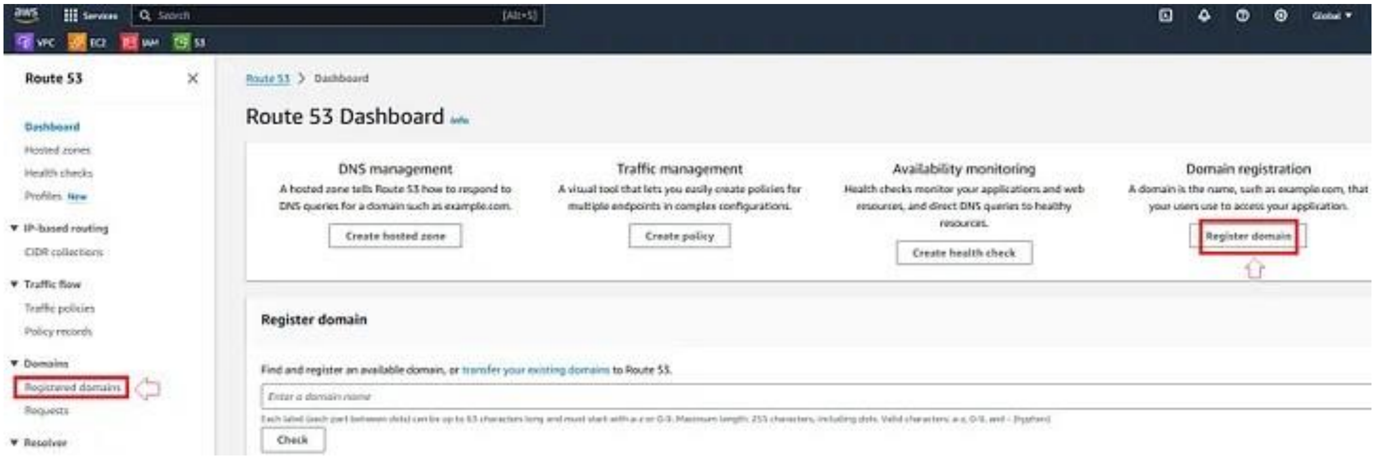
To get started with Kubernetes, you can follow the official documentation at Kubernetes Documentation.

© 2024 Kubernetes Overview. All rights reserved.

Registering a new domain using Route 53

1. Sign in to the AWS Management Console and open the Route 53 console

2. In the na~~vigation pane, choose Domains and then Registered~~ domains.



Route 53 Dashboard

DNS management
A hosted zone tells Route 53 how to respond to DNS queries for a domain such as example.com.

Traffic management
A visual tool that lets you easily create policies for multiple endpoints in complex configurations.

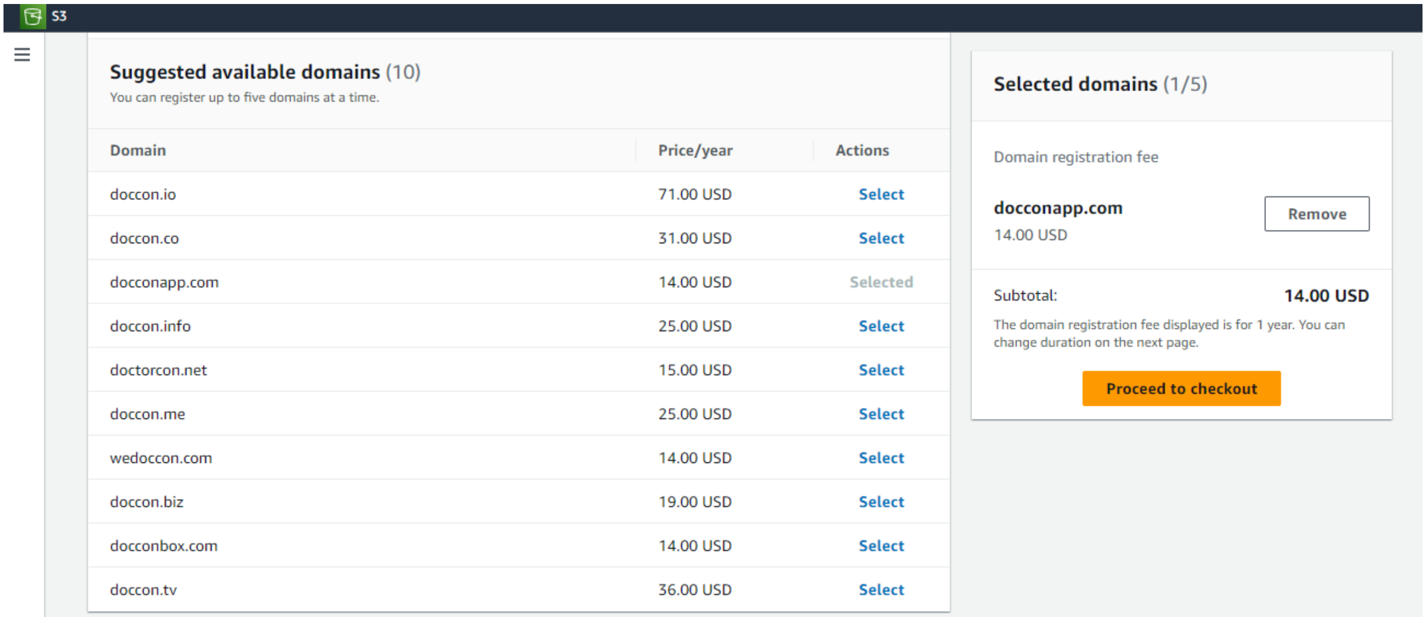
Availability monitoring
Health checks monitor your applications and web resources, and direct DNS queries to healthy resources.

Domain registration
A domain is the name, such as example.com, that your users use to access your application.

Register domain

Find and register an available domain, or transfer your existing domains to Route 53.

Each label (each part between dots) can be up to 63 characters long and must start with a-z or 0-9. Maximum length: 255 characters, including dots. Valid characters: a-z, 0-9, and - (hyphen)



Suggested available domains (10)
You can register up to five domains at a time.

Domain	Price/year	Actions
doccon.io	71.00 USD	Select
doccon.co	31.00 USD	Select
docconapp.com	14.00 USD	Selected
doccon.info	25.00 USD	Select
doctorcon.net	15.00 USD	Select
doccon.me	25.00 USD	Select
wedoccon.com	14.00 USD	Select
doccon.biz	19.00 USD	Select
docconbox.com	14.00 USD	Select
doccon.tv	36.00 USD	Select

Selected domains (1/5)

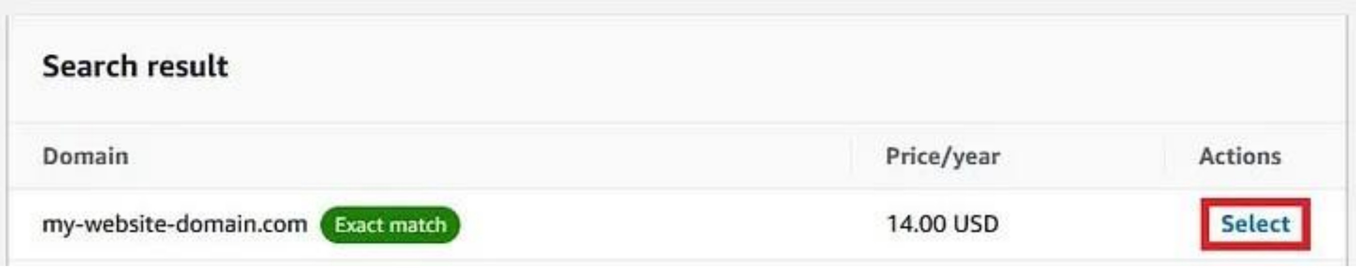
Domain registration fee

docconapp.com
14.00 USD

Subtotal: 14.00 USD

The domain registration fee displayed is for 1 year. You can change duration on the next page.

Click on “Select” to select your domain.



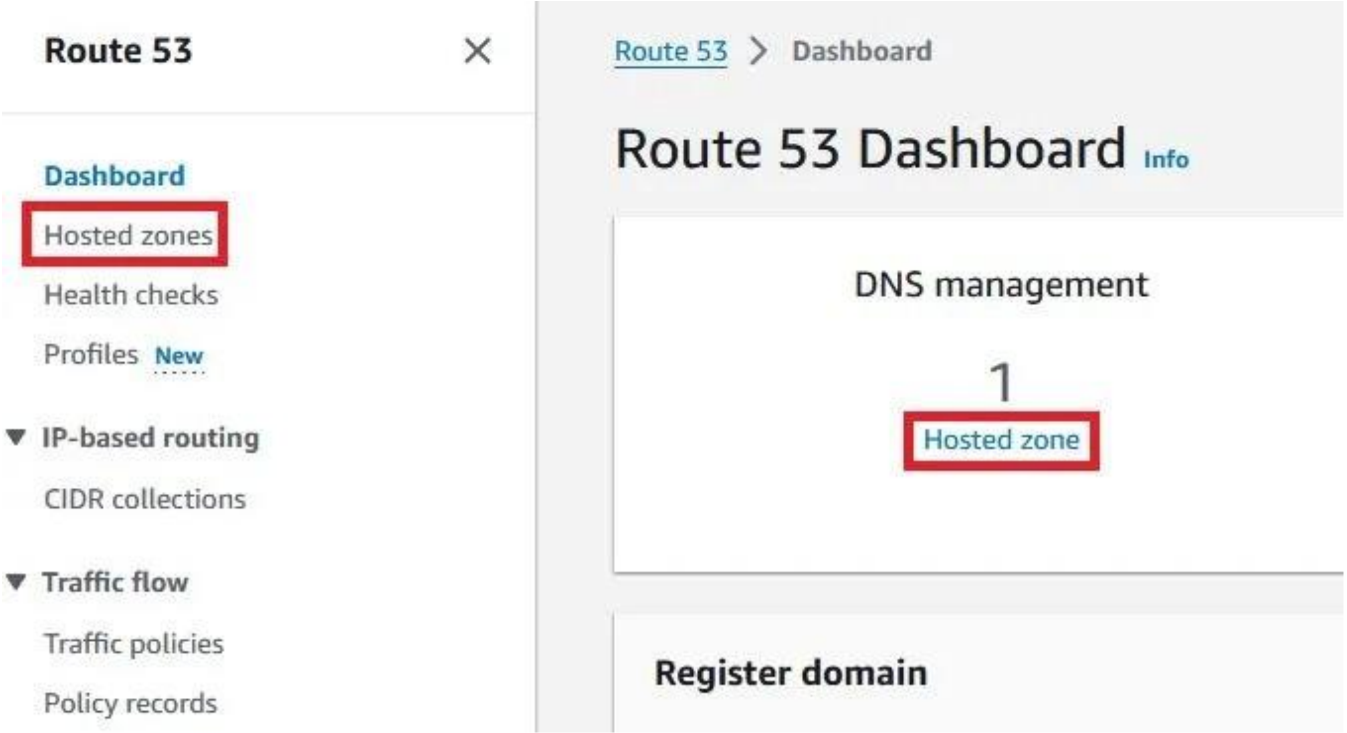
Search result

Domain	Price/year	Actions
my-website-domain.com Exact match	14.00 USD	Select

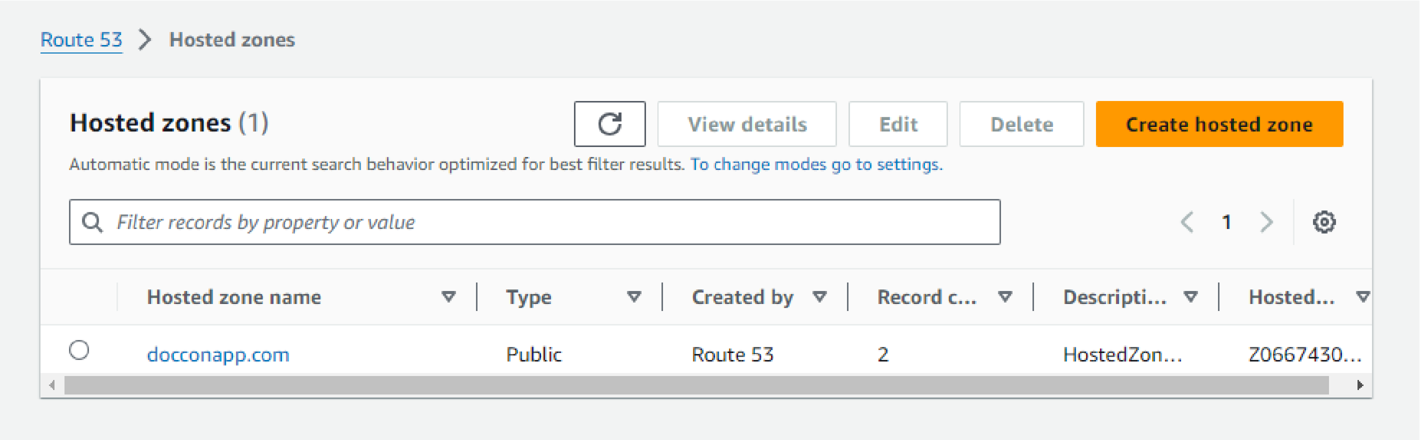
Routing traffic to our website on Amazon S3 with Route 53

1. Sign in to the AWS Management Console and open the Route 53 consoleat https://console.aws.amazon.com/route53/

2. In the navigation pane, choose Hosted zones.



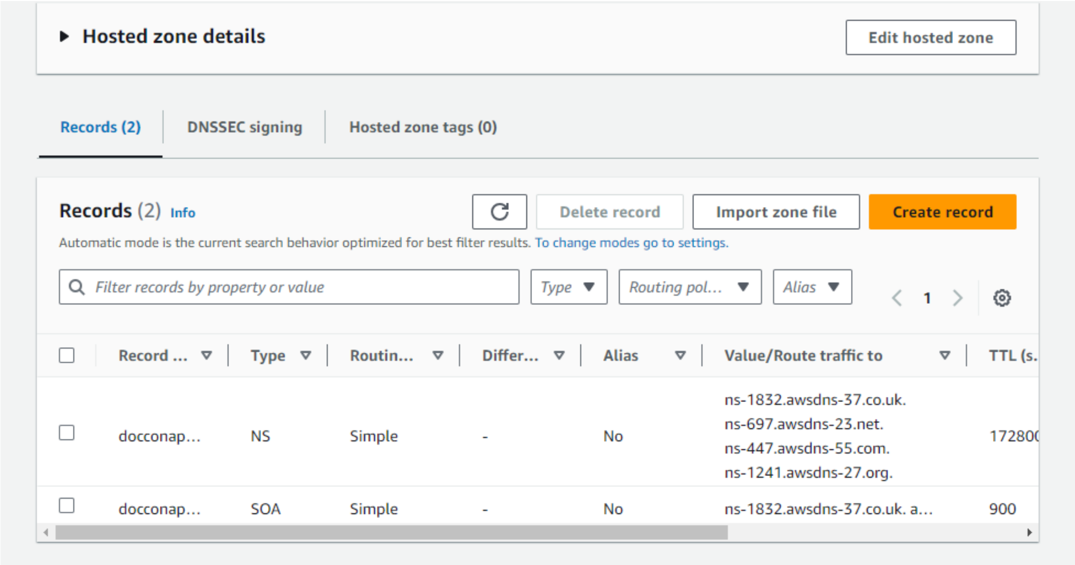
3.Choose the name of the hosted zone that has the domain name that youwant to use to route traffic to your S3 bucket



Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

	Hosted zone name	Type	Created by	Record c...	Descripti...	Hosted...
○	docconapp.com	Public	Route 53	2	HostedZon...	Z0667430...

4.Choose Create record.



Records (2) Info

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

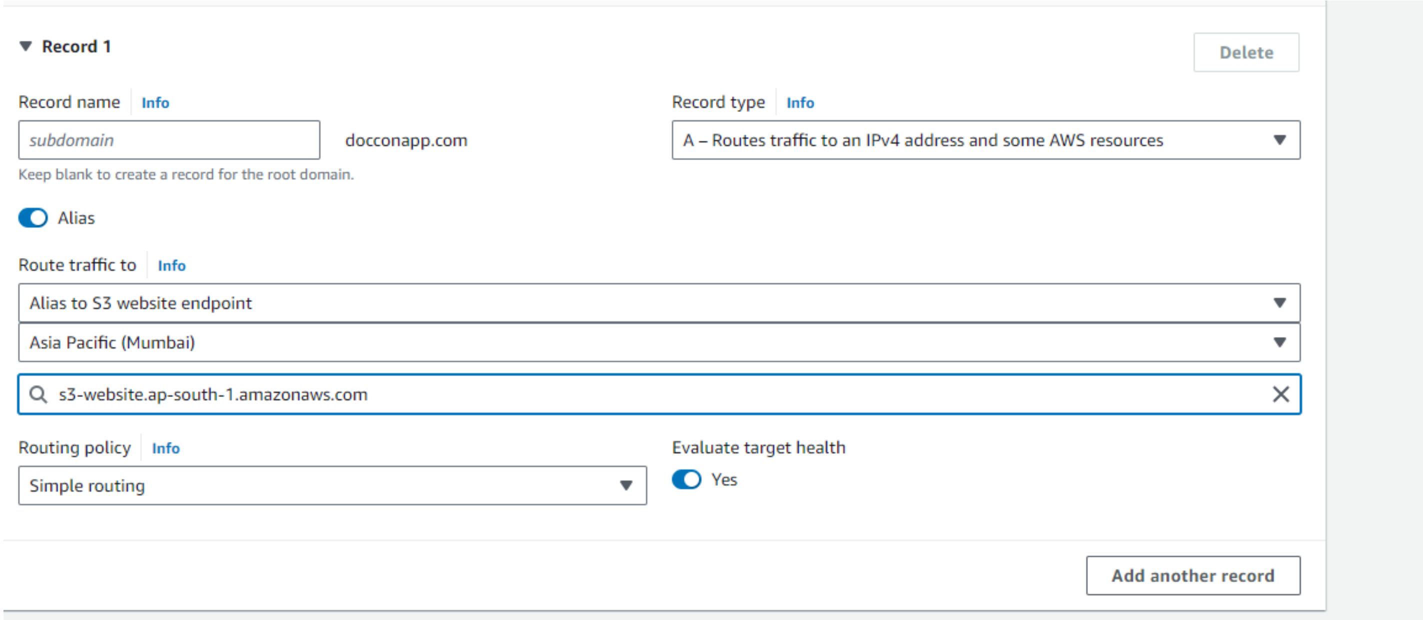
□	Record ...	Type	Routin...	Differ...	Alias	Value/Route traffic to	TTL (s.
□	docconap...	NS	Simple	-	No	ns-1832.awsdns-37.co.uk. ns-697.awsdns-23.net. ns-447.awsdns-55.com. ns-1241.awsdns-27.org.	17280(
□	docconap...	SOA	Simple	-	No	ns-1832.awsdns-37.co.uk. a...	900

On the Create record page, you will create an alias record for your Apex/root domain so that it will redirect to your S3 Bucket website. You will accomplish

this by entering the following information:Alias: toggle

the switch to “on”

- Route traffic to: Alias to S3 endpoint
- Region: Choose the Region for your S3 endpoint Enter S3 endpoint:
- Select your S3 Bucket from the listRouting Policy: Simple Routing
-



Record name: subdomain docconapp.com

Keep blank to create a record for the root domain.

Record type: A – Routes traffic to an IPv4 address and some AWS resources

Alias

Route traffic to: Alias to S3 website endpoint

Asia Pacific (Mumbai)

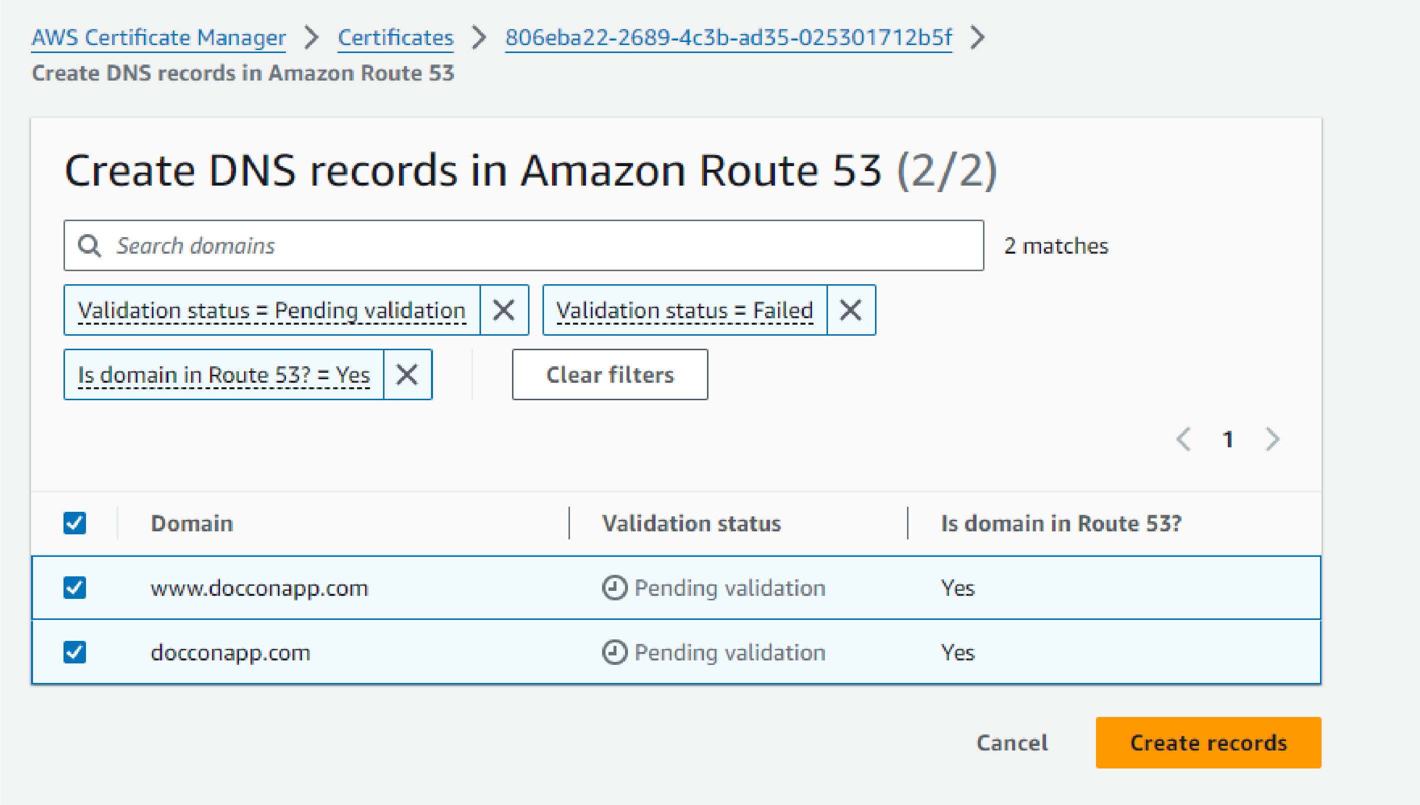
s3-website.ap-south-1.amazonaws.com

Routing policy: Simple routing

Evaluate target health: Yes

Following this, you’ll receive confirmation verifying the successful creationof the DNS record for your domain.

The certificate is created, but not yet validated; let's check its configuration:
select the two FQDNs and finally Create records:

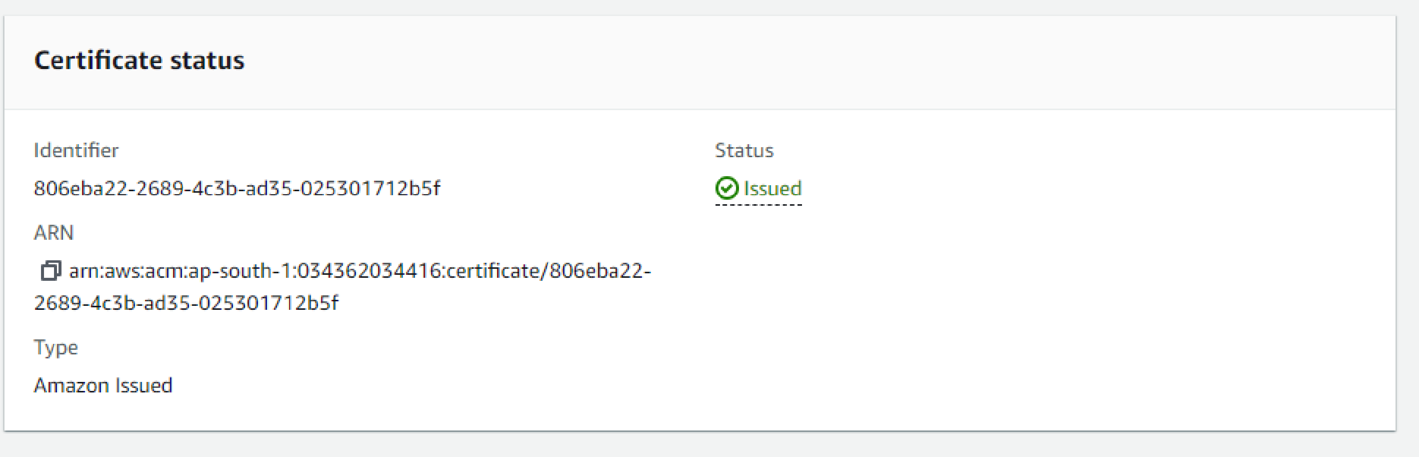

AWS Certificate Manager > Certificates > 806eba22-2689-4c3b-ad35-025301712b5f >
Create DNS records in Amazon Route 53

Create DNS records in Amazon Route 53 (2/2)

Search domains
2 matches
Validation status = Pending validation ✕
Validation status = Failed ✕
Is domain in Route 53? = Yes ✕
Clear filters
< 1 >

☑	Domain	Validation status	Is domain in Route 53?
☑	www.docconapp.com	Pending validation	Yes
☑	docconapp.com	Pending validation	Yes

All you have to do now is wait a few minutes until you see the Success status:



Certificate status

Identifier
806eba22-2689-4c3b-ad35-025301712b5f

ARN
arn:aws:acm:ap-south-1:034362034416:certificate/806eba22-2689-4c3b-ad35-025301712b5f

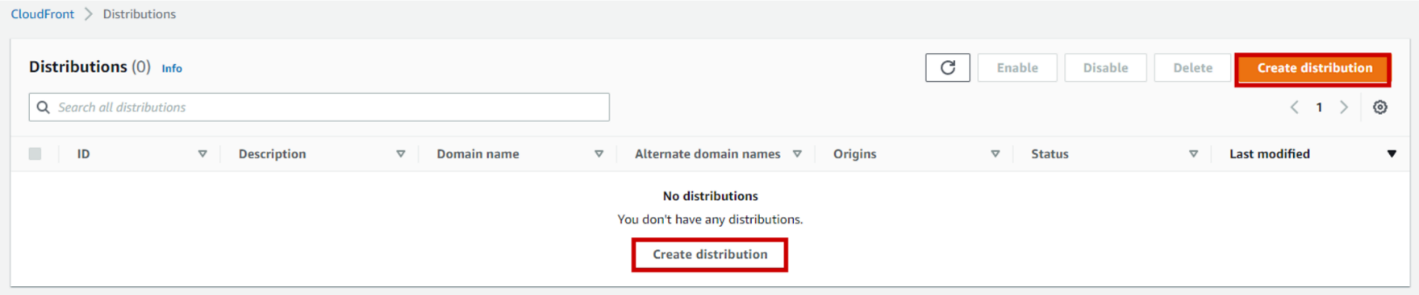
Type
Amazon Issued

Status
Issued

create and configure CloudFront distributions

By using CloudFront, you will be able to deploy your website in HTTPS, and get other benefits as using Edge locations to provide faster access to the website for the users.
CloudFront will act as a stepping stone between Route 53 and S3. In other words, the traffic from the website will be routed to a CloudFront distribution that will deliver it to the corresponding S3 Bucket. You will create a CloudFront distribution for each of your S3 Bucket, two in total.

Now, create your CloudFront distribution:



CloudFront > Distributions

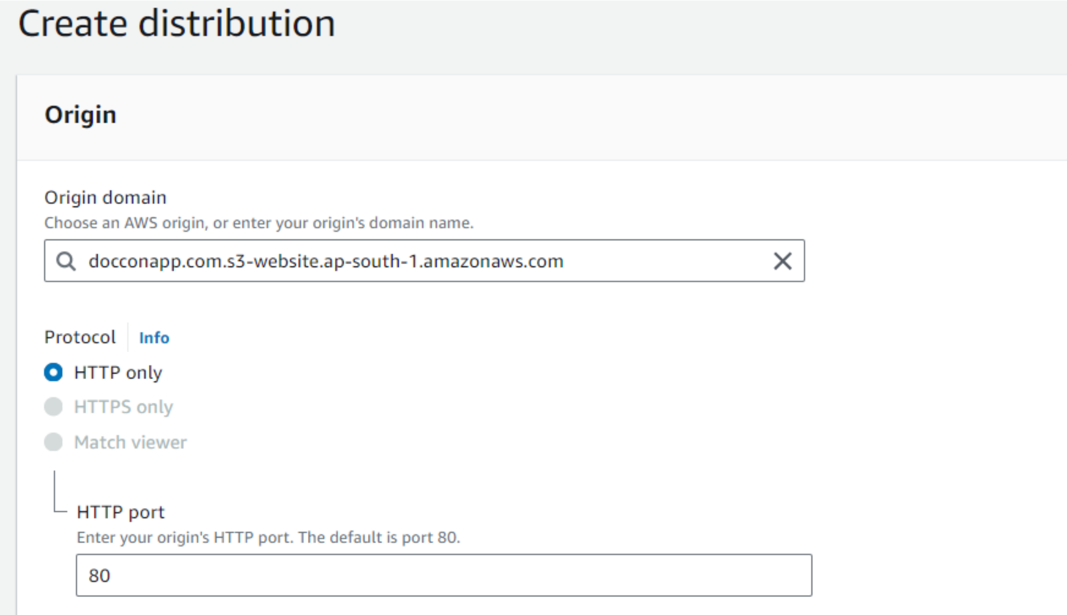
Distributions (0) Info

ID	Description	Domain name	Alternate domain names	Origins	Status	Last modified

No distributions

You don't have any distributions.

Paste the s3 endpoint url in the origin domain



Create distribution

Origin

Origin domain

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

docconapp.com.s3-website.ap-south-1.amazonaws.com

Protocol Info

● HTTP only

○ HTTPS only

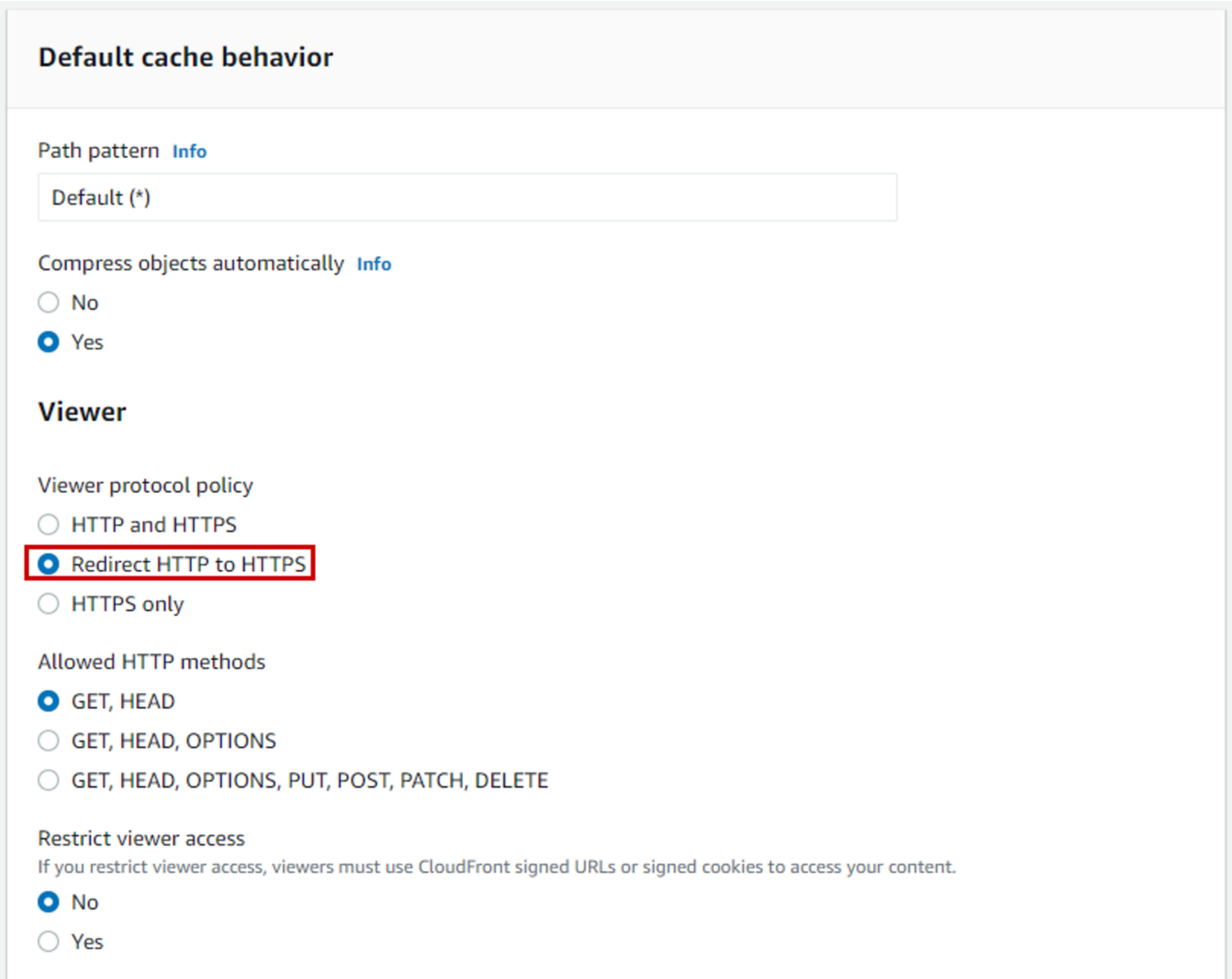
○ Match viewer

HTTP port

Enter your origin's HTTP port. The default is port 80.

80

The Default cache behavior section should look like this:



Default cache behavior

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

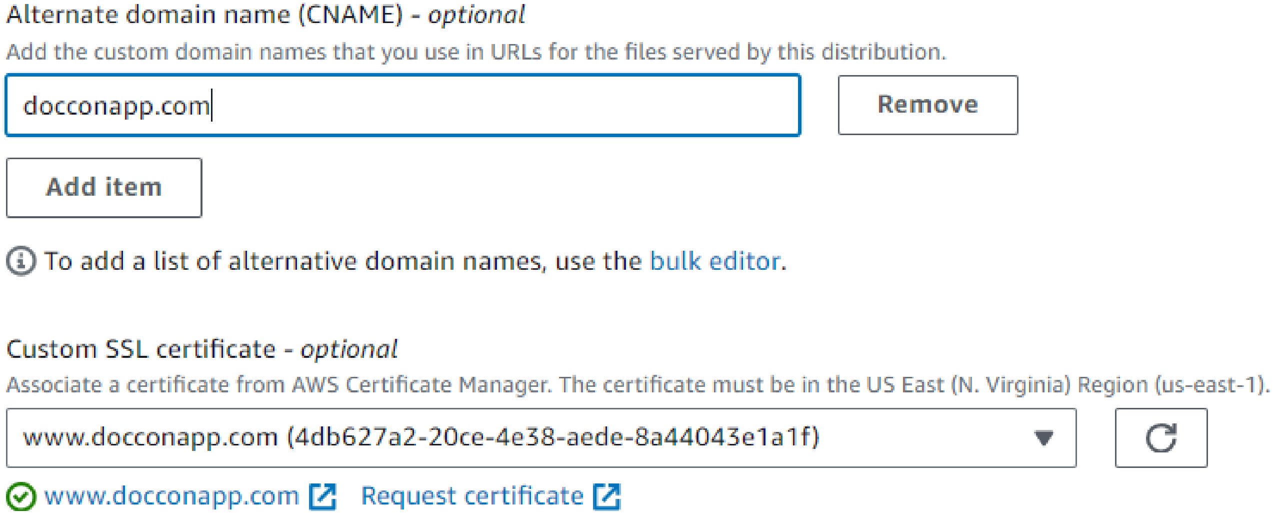
● GET, HEAD
○ GET, HEAD, OPTIONS
○ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Restrict viewer access

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

● No
○ Yes

In the custom SSL certificate field, select the newly created certificate:



Alternate domain name (CNAME) - *optional*

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

docconapp.com

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).

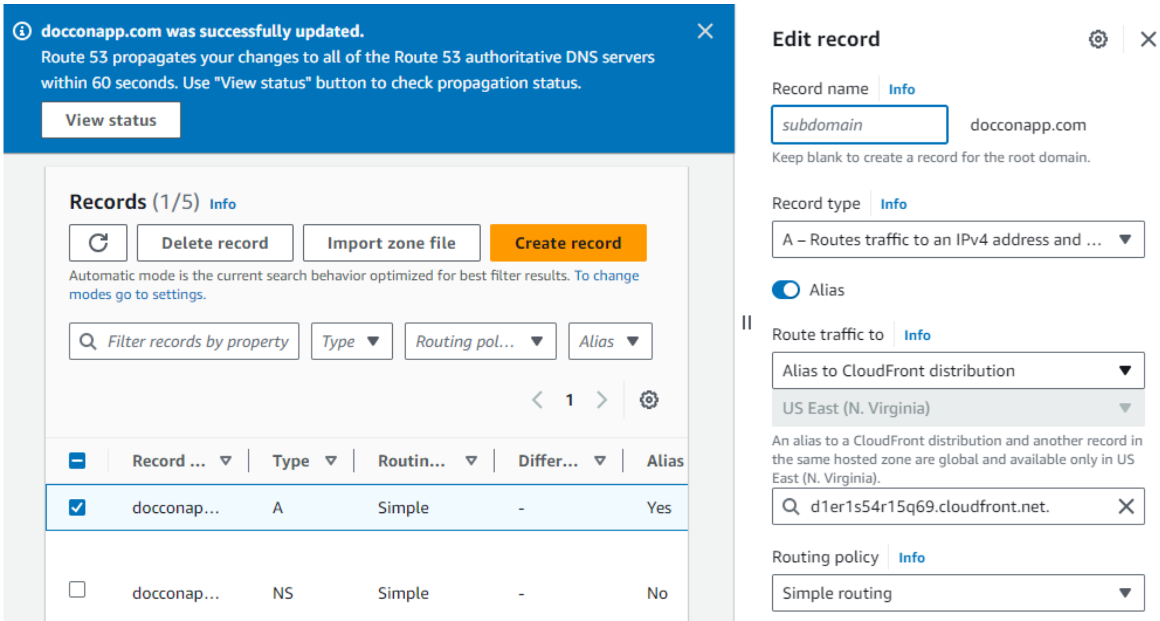
www.docconapp.com (4db627a2-20ce-4e38-aede-8a44043e1a1f)

✓ www.docconapp.com

Once all the necessary information are filled, you can now validate the creation of your main CloudFront distribution, and move on to creating the redirect CloudFront distribution

B.

select the checkbox next to your A record for your domain. Once selected, an Edit pane will open on the right. Modify the "Route traffic to" field so that the chosen option is now "**Alias to CloudFront distribution**," then proceed by clicking "Save."



ⓘ **docconapp.com was successfully updated.**
Route 53 propagates your changes to all of the Route 53 authoritative DNS servers within 60 seconds. Use "View status" button to check propagation status.

Records (1/5) Info

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

	Record ...	Type	Routin...	Differ...	Alias
☑	docconap...	A	Simple	-	Yes
□	docconap...	NS	Simple	-	No

Edit record

Record name Info: subdomain docconapp.com
Keep blank to create a record for the root domain.

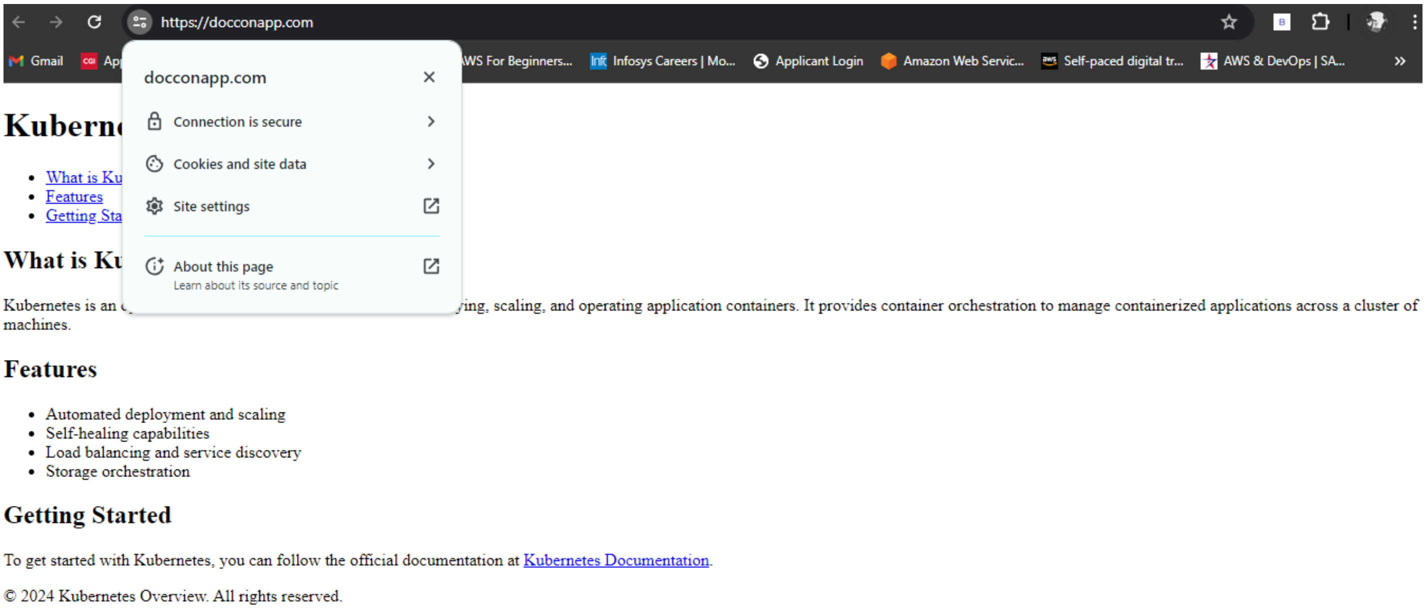
Record type Info: A – Routes traffic to an IPv4 address and ...

● Alias

Route traffic to Info: Alias to CloudFront distribution
US East (N. Virginia)
An alias to a CloudFront distribution and another record in the same hosted zone are global and available only in US East (N. Virginia).
d1er1s54r15q69.cloudfront.net.

Routing policy Info: Simple routing

The website is accessible, and in HTTPS this time



https://docconapp.com

docconapp.com
Connection is secure
Cookies and site data
Site settings
About this page
Learn about its source and topic

Kuberne

- What is Ku
- Features
- Getting Sta

What is Ku

Kubernetes is an ...ying, scaling, and operating application containers. It provides container orchestration to manage containerized applications across a cluster of machines.

Features

- Automated deployment and scaling
- Self-healing capabilities
- Load balancing and service discovery
- Storage orchestration

Getting Started

To get started with Kubernetes, you can follow the official documentation at Kubernetes Documentation.

© 2024 Kubernetes Overview. All rights reserved.

You've successfully completed all the necessary steps for deploying a secure static website on AWS, utilizing Route 53 and CloudFront.