



lab title

# Bulletproof HTML5 Websites with AWS in a Nutshell V1.49



Course title

BackSpace Academy  
Nutshell Series



# Table of Contents

## Contents

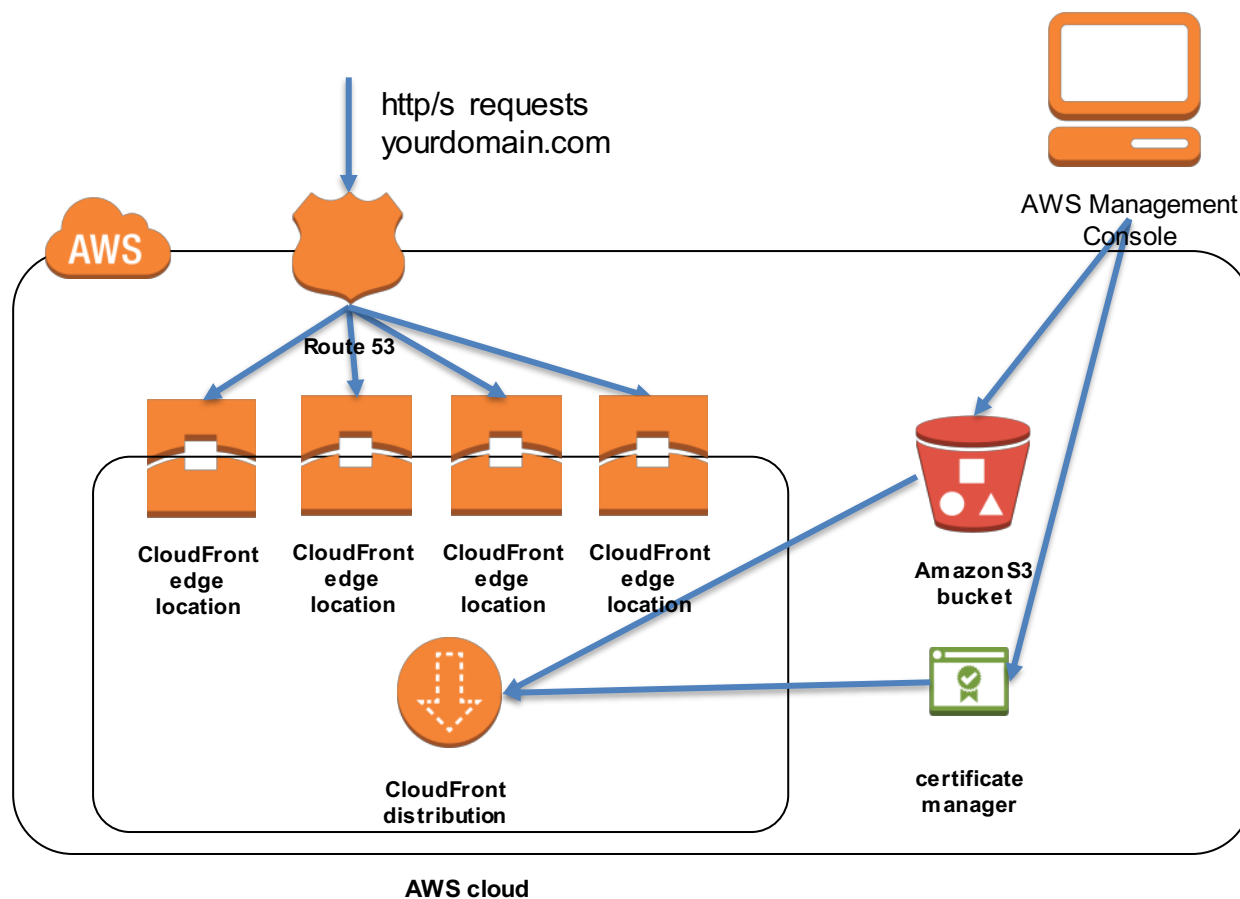
<b>Table of Contents .....</b>	<b>1</b>
<b>About the Lab.....</b>	<b>2</b>
<b>Purchasing a Custom Domain Name.....</b>	<b>3</b>
<b>Creating an S3 Bucket and Uploading our Website.....</b>	<b>5</b>
Create an S3 Bucket.....	5
Upload Website Objects.....	7
<b>Enabling S3 Website Hosting .....</b>	<b>10</b>
Troubleshooting .....	11
<b>Creating an SSL Certificate with AWS Certificate Manager.....</b>	<b>13</b>
<b>Creating a CloudFront Distribution.....</b>	<b>16</b>
Requiring HTTPS for Communication Between CloudFront and Your Amazon S3 Origin .....	20
Invalidating a CloudFront Distribution .....	21
<b>Routing Traffic with AWS Route 53 .....</b>	<b>23</b>
Routing Traffic with a Domain Name from another Registrar.....	25
Route Requests for www Subdomain .....	25
Checking DNS Propagation Status .....	26
<b>Deleting the Website .....</b>	<b>27</b>
Delete Bucket .....	27
Delete CloudFront Distribution .....	28

## ▶ About the Lab

**Please note that not all AWS services are supported in all regions. Please use the US-East-1 (North Virginia) region for this lab.**

These lab notes are to support the instructional videos on Bulletproof HTML5 Websites with AWS in a Nutshell Course.

This is a typical use case for S3 and CloudFront to deliver highly available static websites that can handle heavy traffic.



**Please note that AWS services change on a weekly basis and it is extremely important you check the version number on this document to ensure you have the latest version with any updates or corrections.**

# ▶ Purchasing a Custom Domain Name

In this section, we will purchase a domain name through AWS Route 53.

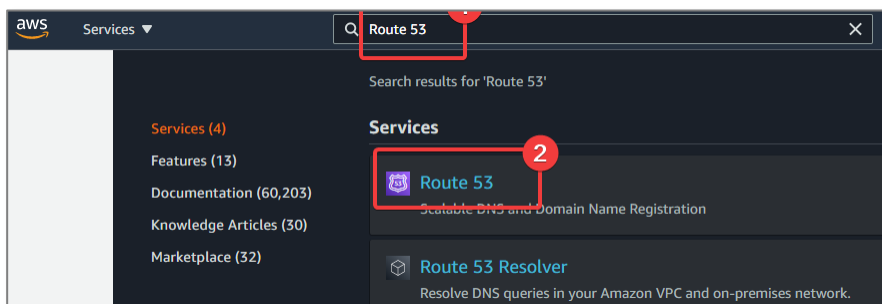
**\*Please note this process will involve paying for a domain name with AWS.**

**Although not recommended, if you would like to use another domain registrar instructions are detailed later under *Routing Traffic with a Domain Name from another Registrar*.**

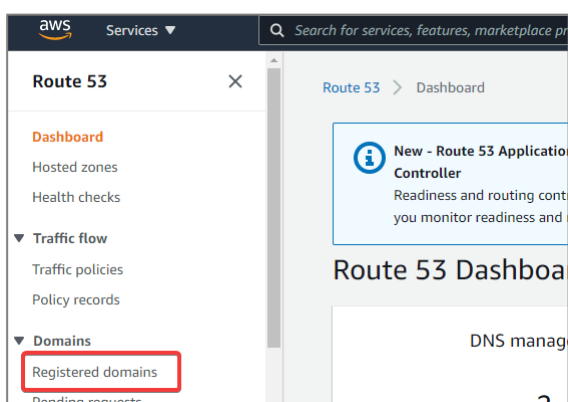
Our first task is to purchase a domain name for our website.

This part involves purchasing a domain through the Route 53 service.

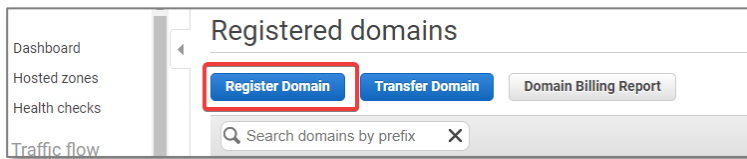
From the management console search *Route 53*.



Click on Registered Domains from the menu



Click on Register Domain



Type in the domain name you would like and click *Check* to see if it is available.

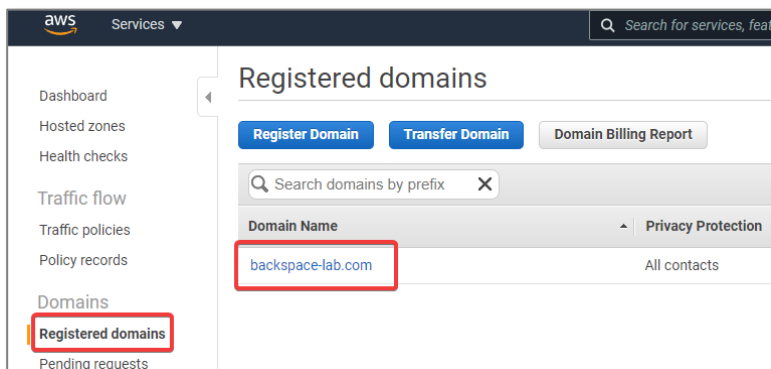
If it is available click “add to cart”

Scroll down and click on “Continue”

Complete the process making sure you use a valid email for the domain registration otherwise the process will fail.

You should receive an email with a link to verify your email. About 30 minutes after your email address has been verified you should receive an email stating the domain was successfully registered with Route 53.

After the domain has been successfully registered you will see it in the “Registered domains”

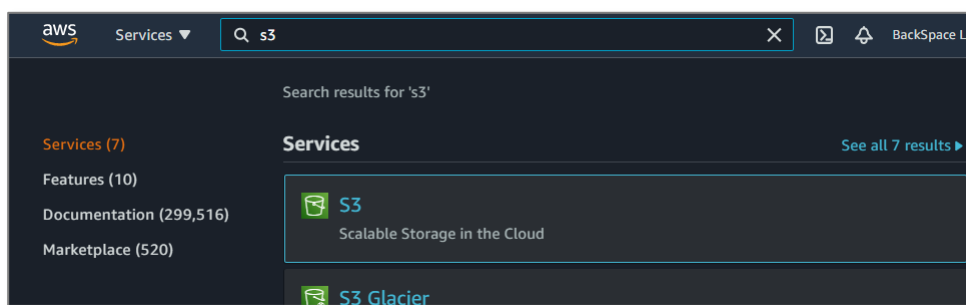


# ▶ Creating an S3 Bucket and Uploading our Website

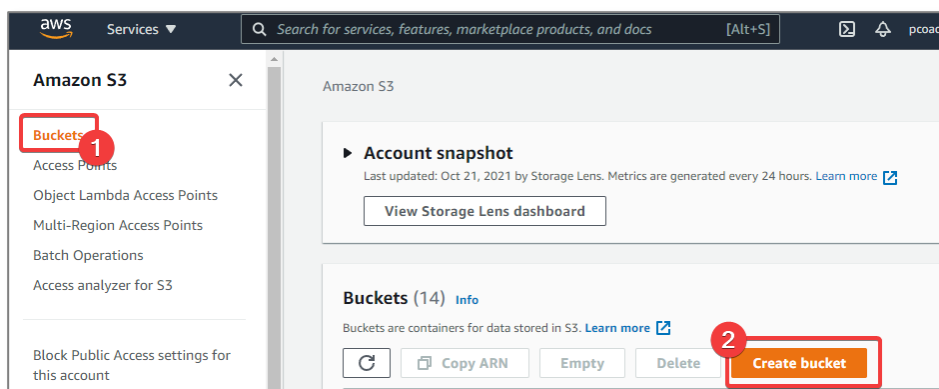
In this section we will create an S3 bucket and upload our HTML5 website.

Create an S3 Bucket

From the management console search S3.



Click on *Buckets* -> *Create Bucket*



Enter your custom domain name.

Select US East (N. Virginia).

Amazon S3 > Create bucket

## Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

### General configuration

**Bucket name**

backspace-lab.com

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

**AWS Region**

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

Copy settings from existing bucket - *optional*  
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Uncheck *Block all public access*

\*Without public access our website cannot be seen by the public. We can still restrict access to any objects as required. By default individual objects uploaded will be private.

### 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.

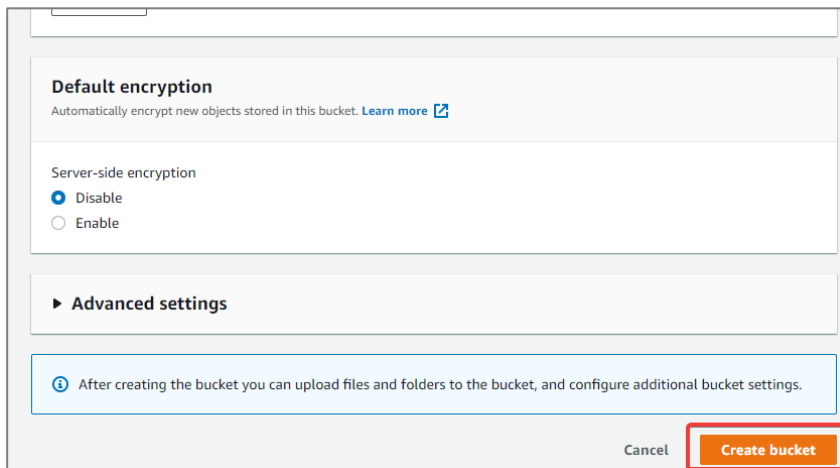
- ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any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

Leave the rest as defaults.

Scroll down and click *Create bucket*

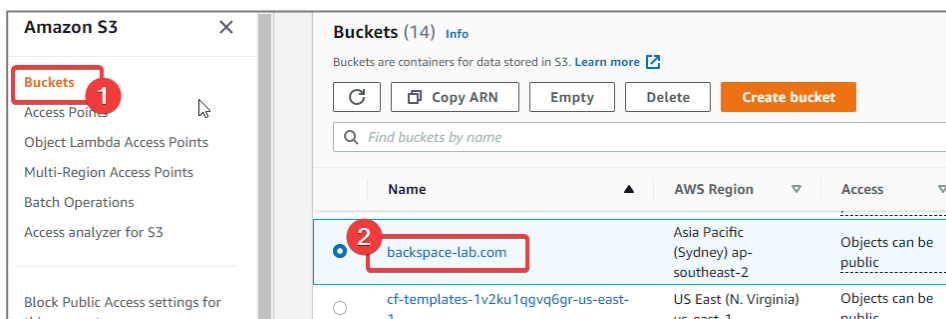


## Upload Website Objects

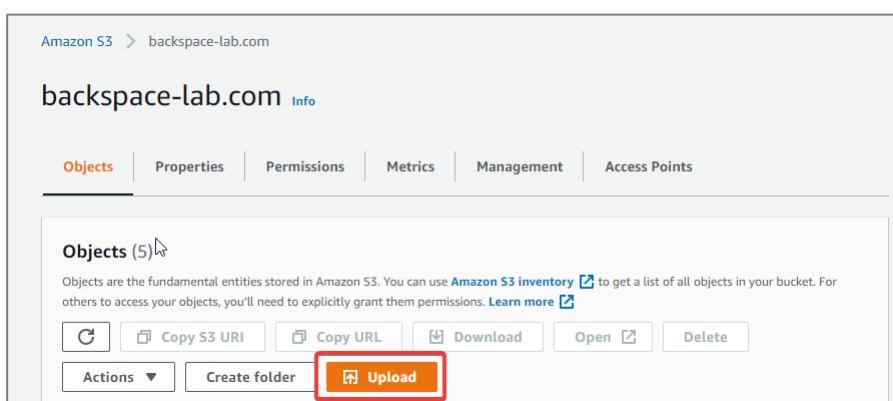
Now it is time to upload our website objects. You can find free website templates at <https://html5up.net/>

Make sure that you unzip the file before attempting to upload the files.

Click on the bucket (yourdomain.com)



Click *Upload*





You want to upload entire directories, including contents, do not Click *Add Files*. Open a Windows File Explorer window and drag the entire contents from File Explorer and drop on top of the Upload form.

## 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 (72 Total, 3.5 MB)

Remove Add files Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 2 3 4 5 6 7 8 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	01.jpg	images/gallery/fulls/	image/jpeg	62.2 KB
<input type="checkbox"/>	01.jpg	images/gallery/thumbs/	image/jpeg	20.2 KB
<input type="checkbox"/>	02.jpg	images/gallery/fulls/	image/jpeg	25.2 KB
<input type="checkbox"/>	02.jpg	images/gallery/thumbs/	image/jpeg	7.7 KB

### Expand *Permissions*

<input type="checkbox"/>	03.jpg	images/gallery/thumbs/	image/jpeg	16.1 KB
<input type="checkbox"/>	04.jpg	images/gallery/fulls/	image/jpeg	38.6 KB
<input type="checkbox"/>	04.jpg	images/gallery/thumbs/	image/jpeg	12.5 KB
<input type="checkbox"/>	05.jpg	images/gallery/fulls/	image/jpeg	43.7 KB
<input type="checkbox"/>	05.jpg	images/gallery/thumbs/	image/jpeg	14.4 KB

### Destination

Destination

[s3://backspace-lab.com](#)

► **Destination details**

Bucket settings that impact new objects stored in the specified destination.

► **Permissions**

Grant public access and access to other AWS accounts.

Scroll down to *Access Control List (ACL)*

Select *Grant public – read access*

Click the *understand* checkbox

Leave rest as defaults

Click *Upload*

1

ⓘ

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.

2

☒ 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](#)

3

1

⚠

**Granting public-read access is not recommended**  
Anyone in the world will be able to access the specified objects. [Learn more](#)

2

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

► Properties

Specify storage class, encryption settings, tags, and more.

Cancel

3

Upload

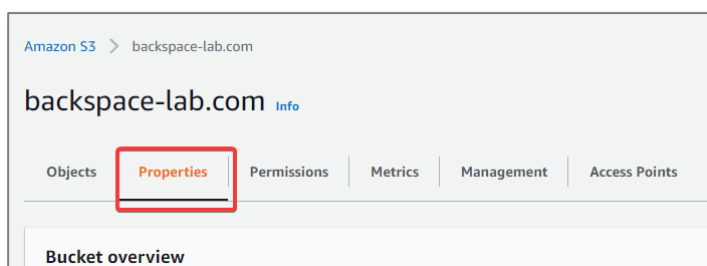
Your files will now be uploading.

A screenshot of a software interface showing an 'Uploading' dialog box. The dialog has a blue header with the title 'Uploading' and a 'Cancel' button. Below the header is a progress bar that is 60% full. Under the progress bar, the following text is displayed: 'Total remaining: 16 files: 1.4 MB(39.57%)', 'Estimated time remaining: a few seconds', and 'Transfer rate: 36.5 KB/s'. Below the dialog box, the text 'Upload: status' is visible, followed by a blurred area.

# ▶ Enabling S3 Website Hosting

In this section we will enable website hosting for our root domain (yourdomain.com) and also redirect requests to the www subdomain (www.yourdomain.com) to our root domain.

Select *Properties*



Scroll down to *Static Website Hosting*

Click *Edit*



Now Select Use this bucket to host a website

Enter the Index Document (required)

Enter Error Document if available or else just leave empty

Click *Save changes*

### Edit static website hosting [Info](#)

**Static website hosting**  
Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

☐ Disable

☒ **Enable** 1

Hosting type

☒ **Host a static website** 2  
Use the bucket endpoint as a 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.

3

**Error document - optional**  
This is returned when an error occurs.

If you scroll down to Static Website Hosting you will see the public endpoint for the S3 website.

Endpoint : `http://yourdomain.com.s3-website-us-east-1.amazonaws.com`

Click on the endpoint to see your website in your browser.

### Static website hosting [Learn more](#)

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://backspace-lab.com.s3-website-ap-southeast-2.amazonaws.com>

## Troubleshooting

If you get either of the following message your object permissions are not set to public.

### 403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 3D615DF91F90446F
- HostId: VGBfqeIVfAp1LOs/1QsZzYCa3/V11o75WDkmFpJDPLrJyvqZoqYuRddGnZNaF+QUiKNNtA5nGDk=

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

```
<?xml version="1.0" encoding="UTF-8" ?>
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>backspaceacademy.com</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>404.html</Key>
    <LastModified>2017-04-27T09:05:21.000Z</LastModified>
    <ETag>"75f1debbd9d7654a9ad312d2a9516a69"</ETag>
    <Size>29422</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

If you find svg images are not showing on your website it is most probably incorrect header information. Upload the specific files again but add Content-type "image/svg+xml" in the Metadata section (you need to expand *Additional upload options* and scroll down to see it).

**Metadata**  
Metadata is optional information provided as a name-value (key-value) pair. [Learn more](#)

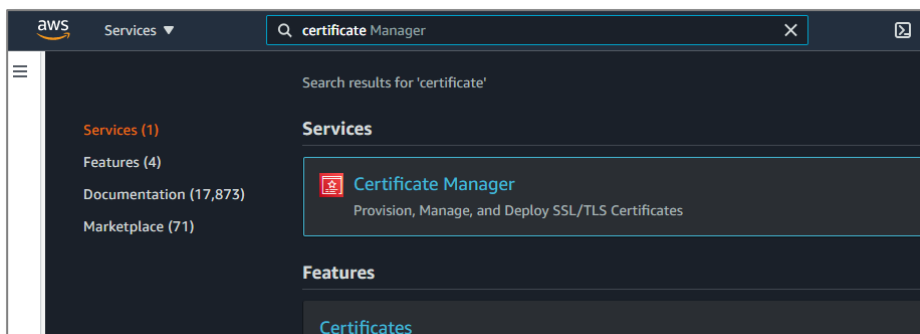
Type	Key	Value	
System defined	Content-Type	image/svg+xml	<input type="button" value="Remove"/>

# ▶ Creating an SSL Certificate with AWS Certificate Manager

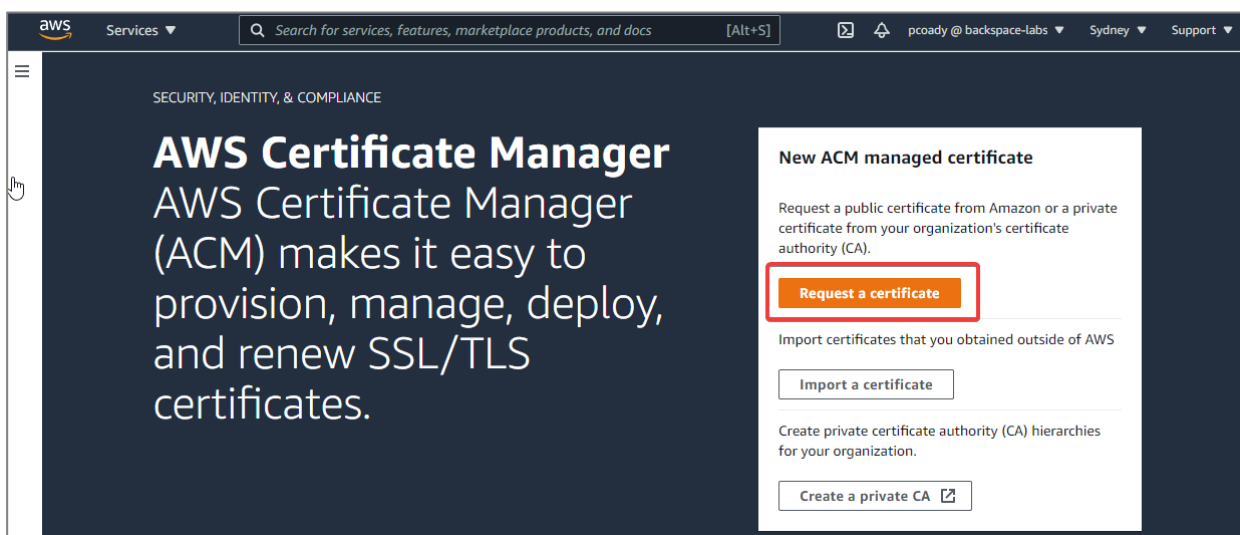
In this section we will use the **AWS Certificate Manager** to create an SSL certificate we can use to enable HTTPS with CloudFront.

Please note that to require HTTPS between viewers and CloudFront, you must change the AWS region to US East (N. Virginia) before you request or import a certificate.

From the management console search *Certificate Manager*.



Click *Request a Certificate*



Select *Request a public certificate*

Click *Next*

AWS Certificate Manager > Certificates > Request certificate

## Request certificate

**Certificate type** [Info](#)

ACM certificates can be used to establish secure communications access across the internet or within an internal network. Choose the type of certificate for ACM to provide.

- ☒ **Request a public certificate**  
Request a public SSL/TLS certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.
- ☐ Request a private certificate  
No private CAs available for issuance.

Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit [ACM Private Certificate Authority](#).

Cancel **Next**

Enter the root domain (yourdomain.com)

Click *Add another name to this certificate*

Enter the root domain prefixed with \*. (\*.yourdomain.com)

AWS Certificate Manager > Certificates > Request certificate > Request public certificate

## Request public certificate

**Domain names**

Fully qualified domain name [Info](#)

backspace-lab.com [Remove](#)

\*.backspace-lab.com [Remove](#)

[Add another name to this certificate](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

Leave default settings

Click *Request*

**Select validation method** [Info](#)  
Select a method for validating domain ownership

☒ **DNS validation - recommended**  
Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.

☐ **Email validation**  
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

**Tags** [Info](#)  
To help you manage your certificates you can optionally assign your own metadata to each resource in the form of tags.

Tag key  Tag value - optional  Remove tag

Add tag  
You can add 49 more tag(s).

Cancel Previous **Request**

After a about a minute you will see status *Pending validation*

AWS Certificate Manager > Certificates

**Certificates (1)** Refresh Delete Manage expiry events Import **Request**

< 1 > ⚙

<input type="checkbox"/>	Certificate ID	Domain name	Type	Status	In use?	Renewal eligibility
<input type="checkbox"/>	ba074805-b70e-4e6c-a980-19758b2be408	-	Amazon Issued	⌚ Pending validation	No	Ineligible

Wait about 15 minutes then click the refresh icon to check if it has been issued successfully.

AWS Certificate Manager > Certificates

**Certificates (1)** Refresh Delete Manage expiry events Import **Request**

⏱

< 1 > ⚙

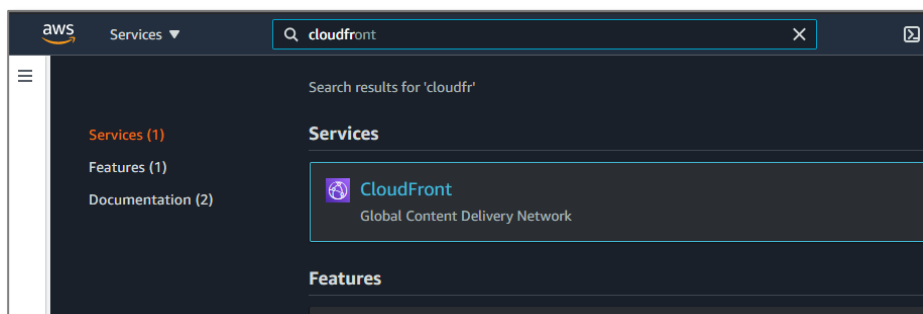
<input type="checkbox"/>	Certificate ID	Domain name	Type	Status	In use?	Renewal eligibility
<input type="checkbox"/>	ba074805-b70e-4e6c-a980-19758b2be408	backspace-lab.com	Amazon Issued	✅ Issued	No	Ineligible



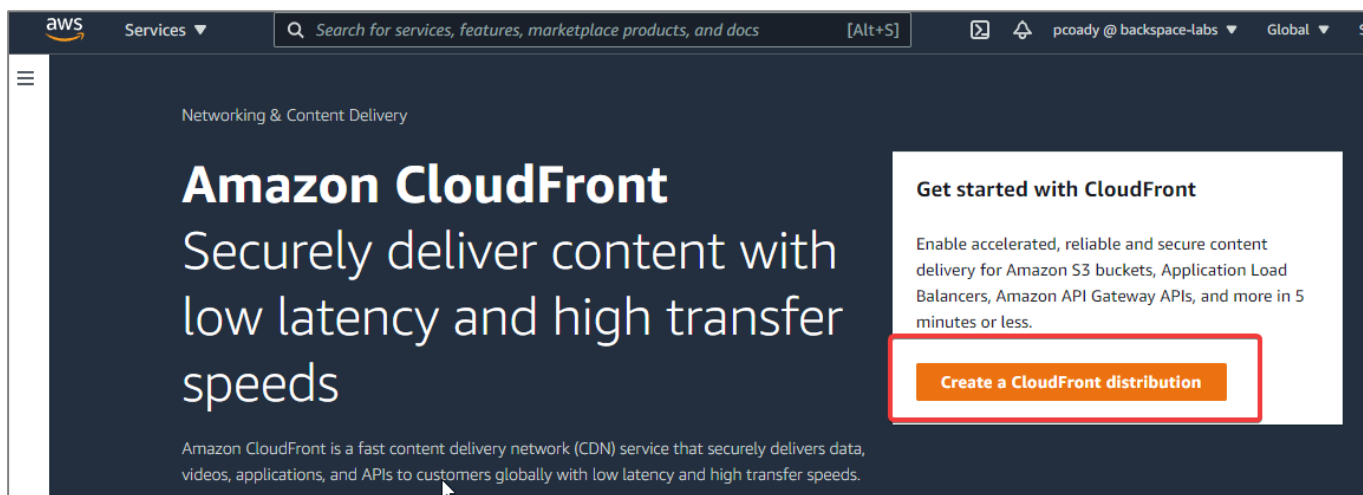
# ▶ Creating a CloudFront Distribution

In this section we will use the AWS CloudFront Content Delivery Network (CDN) to cache our site to edge locations across the Globe.

From the management console search *CloudFront*



Click on *Create a CloudFront Distribution*



In *Origin Settings* select your s3 bucket as the *Origin Domain Name*

### Origin

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

**Origin path - optional** [Info](#)  
Enter a URL path to append to the origin domain name for origin requests.

**Name**  
Enter a name for this origin.

**S3 bucket access** [Info](#)  
Use a CloudFront origin access identity (OAI) to access the S3 bucket.

☒ Don't use OAI (bucket must allow public access)

☐ Yes use OAI (bucket can restrict access to only CloudFront)

**Add custom header - optional**  
CloudFront includes this header in all requests that it sends to your origin.

**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.

☒ No

☐ Yes

► **Additional settings**

Set *Viewer Protocol Policy* to *Redirect HTTP to HTTPS*

Default cache behavior

Path pattern [Info](#)

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 policy and origin request policy (recommended)  
☐ Legacy cache settings

Cache policy  
Choose an existing cache policy or create a new one.  

CachingOptimized  
Default policy when CF compression is enabled  
Recommended for S3 origins

Create policy [↗](#)
View policy [↗](#)

Origin request policy - optional  
Choose an existing origin request policy or create a new one.  

Select origin policy

Create policy [↗](#)

Additional settings

Under *Settings* enter your domain name and subdomains (www.yourdomain.com) into *Alternate Domain Names (CNAMEs)*

Under *Distribution Settings* enter/select your custom SSL certificate

If the Custom SSL option is not available your certificate is either not issued yet or information has not propagated to CloudFront service yet. Cancel the distribution and try again after a few minutes.

### 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.

Remove  
 Remove

ⓘ 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-1** (N. Virginia) Region (us-east-1).

↻  
☒ backspace-lab.com [Request certificate](#)

Legacy clients support - \$600/month prorated charge applies. Most customers do not need this.  
CloudFront allocates dedicated IP addresses at each CloudFront edge location to serve your content over HTTPS.

☐ Enabled

Under *Default root object* enter the index.html file for your website

Set *IPv6* to Off

Put in a comment so that you easily identify the distribution.

Click *Create Distribution*

**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) that CloudFront returns when a viewer requests the root URL (/) instead of a specific object.

index.html

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

☒ Off  
☐ On

**IPv6**

☒ Off  
☐ On

**Description - optional**

Pointed to backspace-lab.com

Cancel **Create distribution**

Annotations: 1 points to the Default root object field, 2 points to the IPv6 field, 3 points to the Description field, and 4 points to the Create distribution button.

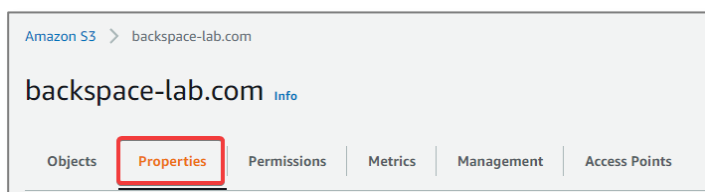
The Status of the distribution will change when it has been distributed to the edge locations.

## Requiring HTTPS for Communication Between CloudFront and Your Amazon S3 Origin

If you are creating a secure site you can also require HTTPS for communication between your S3 bucket and CloudFront. This is achieved by disabling website hosting for the S3 bucket. It will then only be possible to view the website through CloudFront.

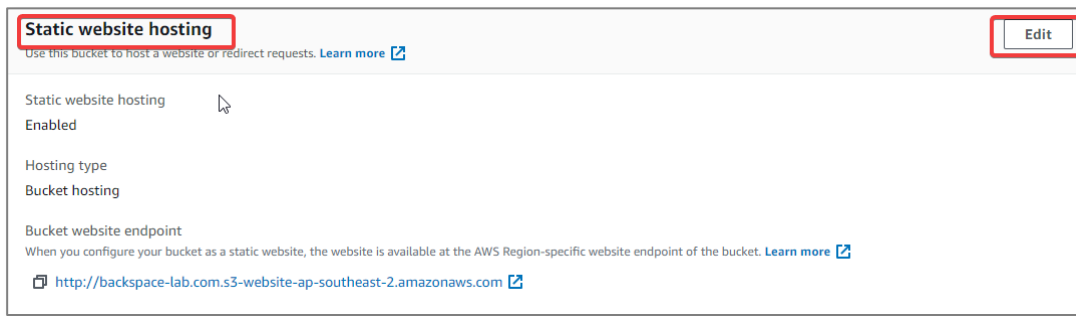
Go to the S3 management console and select the bucket.

Select the *Properties* tab

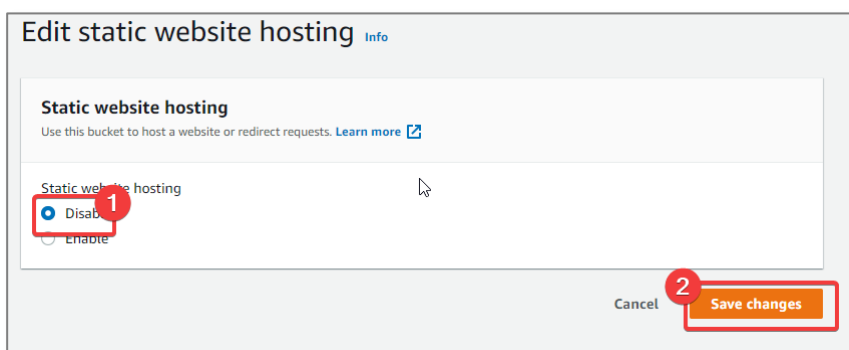


Scroll down to *Static website hosting*

Click *Edit*



Select *Disable website hosting* and then click *Save*



## Invalidating a CloudFront Distribution

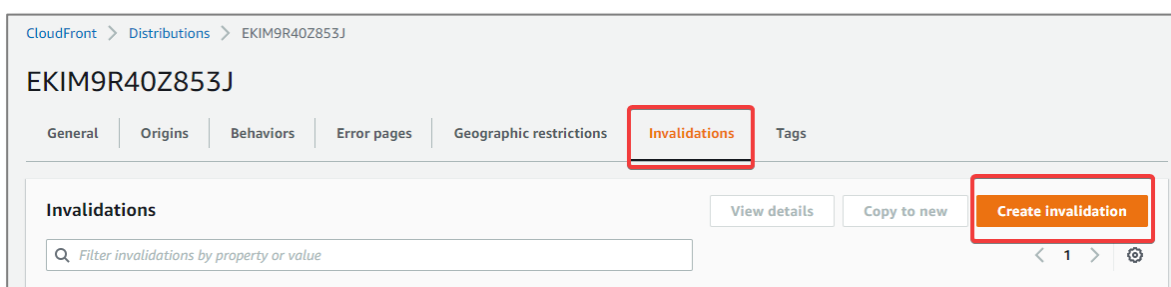
If you need to change your website and update your CloudFront distribution you can force CloudFront to fetch and update the distribution using invalidations.

To invalidate/update a CloudFront distribution:

Click on the distribution from the list of distributions

Click on the *Invalidations* tab

Click *Create Invalidation*



Enter the object path to the file you want to invalidate/update (e.g. `/index.html`) or use a wildcard symbol to invalidate all the files (e.g. `/*`)

Click *Create Invalidation*

### Create invalidation

#### Object paths

Add object paths. Add the path for each object that you want to remove from the CloudFront cache. You can use wildcards (\*).

/index.html

Remove

Add item

ⓘ To add a list of object paths, use the [bulk editor](#).

Cancel

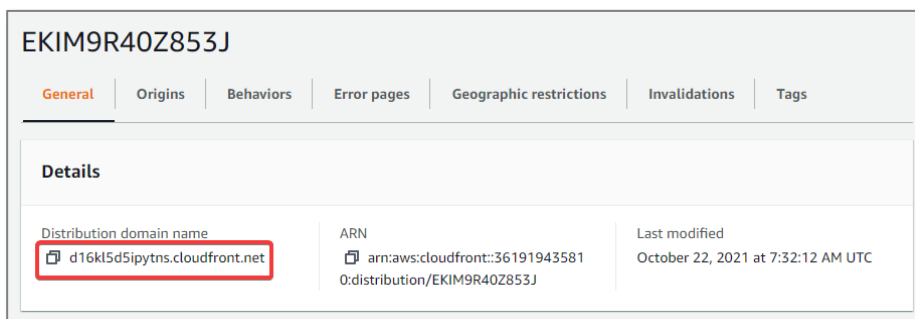
Create invalidation

This will take some time to complete.

# ▶ Routing Traffic with AWS Route 53

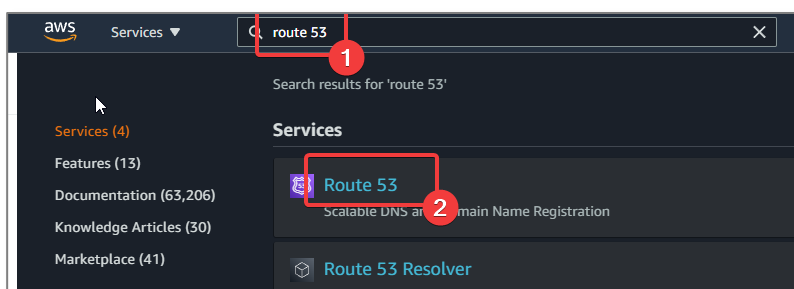
In this section we will direct all requests to our domain name and www subdomain to CloudFront using Route 53 Domain Name Service (DNS).

Go back to the CloudFront Distribution page and copy the distribution domain name



Now go back to the Route 53 Management Console:

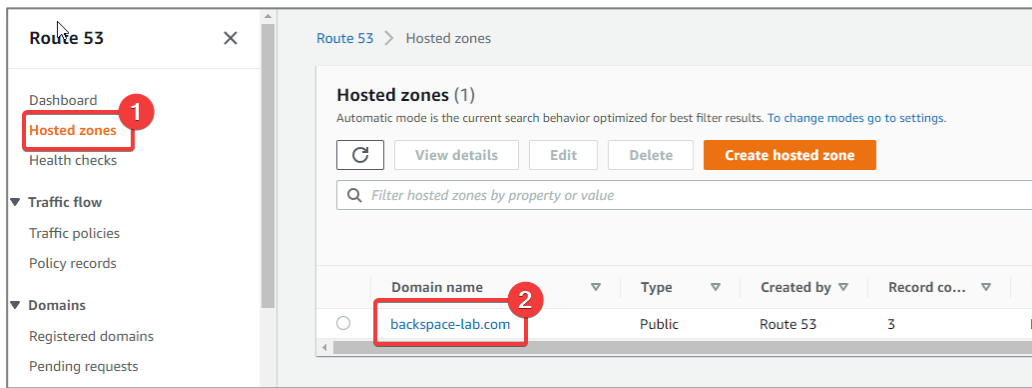
Click on the services menu and select Route 53.



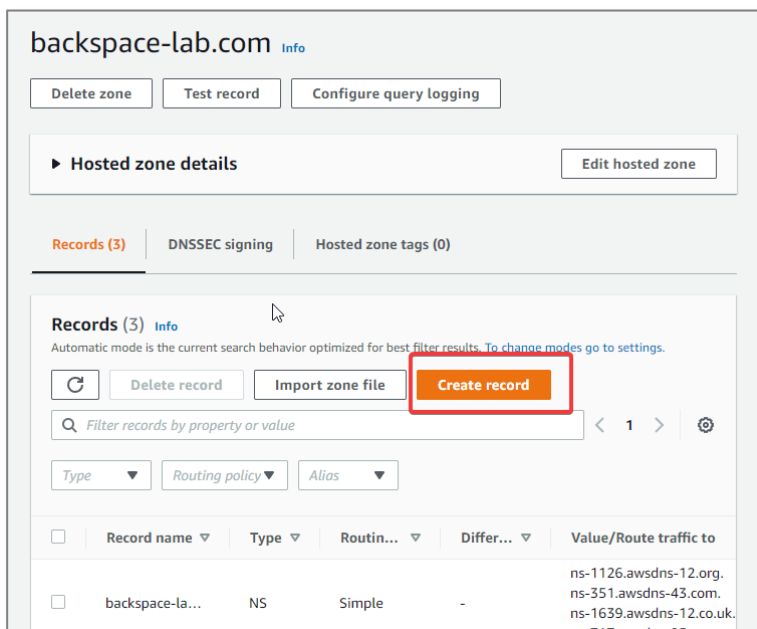
Click on Hosted Zones

Click on the hosted zone created by the Route 53 Registrar





Click on *Create Record*



Leave *Record Name* empty

Select *A-IPv4 address* as Type

Check Alias: Yes

Select *Alias to CloudFront distribution*

Select your CloudFront distribution domain name

Click *Create records*

**Quick create record** [Info](#) [Switch to wizard](#)

**Record 1**

Record name [Info](#)  backspace-lab.com

Record type [Info](#) **1**

Valid characters: a-z, 0-9, !"#\$%&'()\*+,-./:;<=>?@[ \ ] ^ \_ ` { | } . ~

Routing policy [Info](#)

Evaluate target health ☐ No

**2**

An alias to a CloudFront distribution and an alias to another record in the same hosted zone are global and available only in the US East (N. Virginia) region.

**3**

## Routing Traffic with a Domain Name from another Registrar

If you have a domain name from another registrar (e.g. GoDaddy) you can still direct traffic for this domain to AWS by replacing the NS records. That way all DNS requests will be directed to AWS name servers. The process is as follows:

1. Create a Route53 hosted zone for the domain
2. Copy the NS records for the hosted zone

**Records (3)** [Info](#)

Automatic mode is the current search behavior optimized for best filter results. [To change modes go to settings.](#)

<input type="checkbox"/>	Record name ▾	Type ▾	Routin... ▾	Differ... ▾	Value/Route traffic to
<input type="checkbox"/>	backspace-la...	<b>NS</b>	Simple	-	ns-1126.awsdns-12.org. ns-351.awsdns-43.com. ns-1639.awsdns-12.co.uk. ns-717.awsdns-25.net.

3. Replace the NS records in your registrars DNS service with the NS records from your Route53 hosted zone
4. Add the A record to your Route53 hosted zone as detailed previously above.

## Route Requests for www Subdomain

Click on *Create Record*

Enter *www* for *Record Name*

Select *CNAME* as Type

Select “No” for Alias.

Enter your domain name (or the CloudFront domain, either will work) for the www subdomain as Value (without the http:// at the start)

Click on *Create Records*

**Quick create record** [Info](#) [Switch to wizard](#)

▼ Record 1 [Delete](#)

**Record name** [Info](#) **Record type** [Info](#) **Value** [Info](#) ☐ Alias

www .backspace-lab.com CNAME - Routes traffic to another domain n... backspace-lab.com

Valid characters: a-z, 0-9, ! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } . ~  
Enter multiple values on separate lines.

**TTL (seconds)** [Info](#) **Routing policy** [Info](#)

300 Simple routing

1m 1h 1d  
Recommended values: 60 to 172800 (two days)

[Add another record](#)

[Cancel](#) [Create records](#)

After some time the changes will be propagated to the Internet and you will be able to navigate to your domain name in your browser and see your website.

## Checking DNS Propagation Status

The Route 53 entries detailed above will take a while to propagate across the Internet. This could be anywhere from a couple of minutes to an hour. You can check the status of DNS propagation using the following site:

[Global DNS Propagation Checker](#)

After the records have successfully propagated you will be able to navigate to your domain name and see your website.

# ▶ Deleting the Website

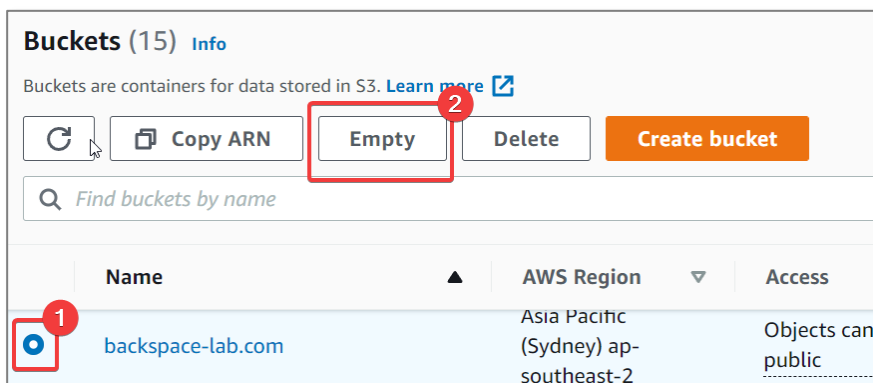
In this section we will show you how to delete all the resources if you no longer need the website.

## Delete Bucket

Go to the S3 console

Select the bucket

Click *Empty*



**Buckets (15)** [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

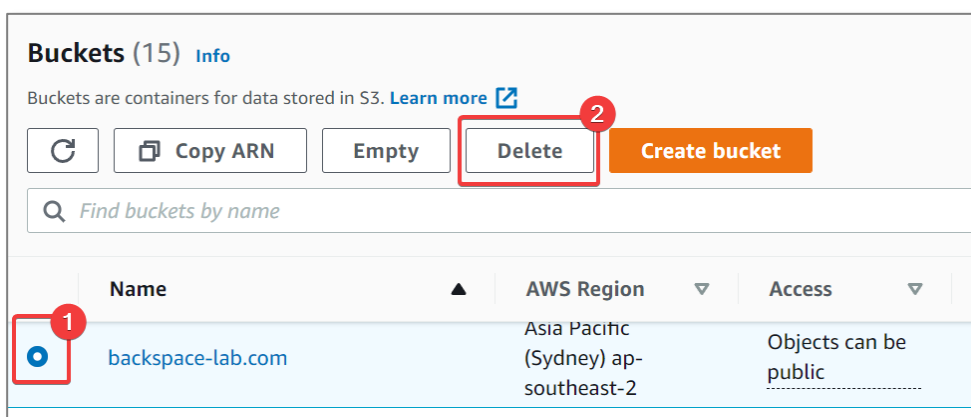
[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

	Name ▲	AWS Region ▼	Access
<a href="#">1</a>	backspace-lab.com	Asia Pacific (Sydney) ap-southeast-2	Objects can be public

Click *Exit*

Select the bucket

Click *Delete*



**Buckets (15)** [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

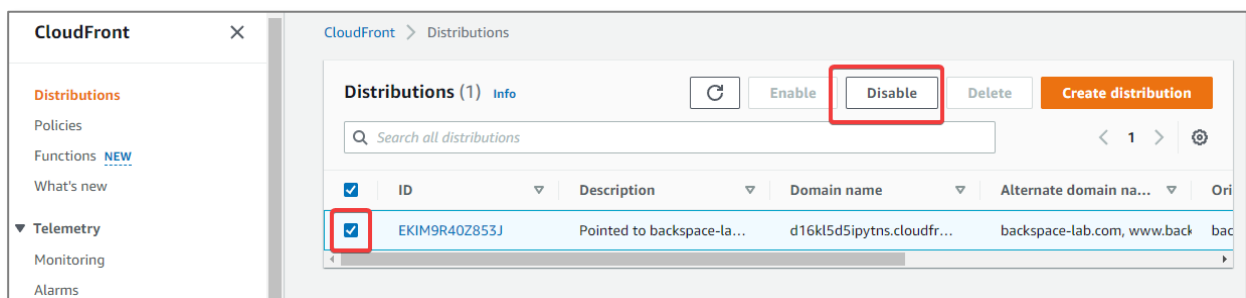
	Name ▲	AWS Region ▼	Access ▼
<a href="#">1</a>	backspace-lab.com	Asia Pacific (Sydney) ap-southeast-2	Objects can be public

## Delete CloudFront Distribution

Go to the CloudFront console

Select CloudFront Distribution

Click *Disable*



Wait for status to change to *disabled*

Click *Delete*