

From Google Domain Registrar to AWS S3 hosted a Static WebSite:

Given that you have already registered your domain via Google Domain Registrar, now you want to use Amazon AWS S3 to host a static website. This page highlights the needed steps to make it happen:

[AWS S3 Console: Create three S3 buckets.](#)

[S3 bucket for root domain](#)

[Optionally, S3 bucket for logging web traffic](#)

[Optionally, S3 bucket for sub domain](#)

[AWS S3 Console: Configure an index document and optionally error document](#)

[AWS S3 Console: Setting permissions for website access](#)

[Root domain bucket's Permissions setting:](#)

[If redirecting enabled, Sub domain bucket permissions:](#)

[If Log traffic enabled, Logs bucket permissions:](#)

[Optionally, AWS S3 Console: Logging web traffic](#)

[Optionally, AWS S3 Console: Configuring a web page redirecting](#)

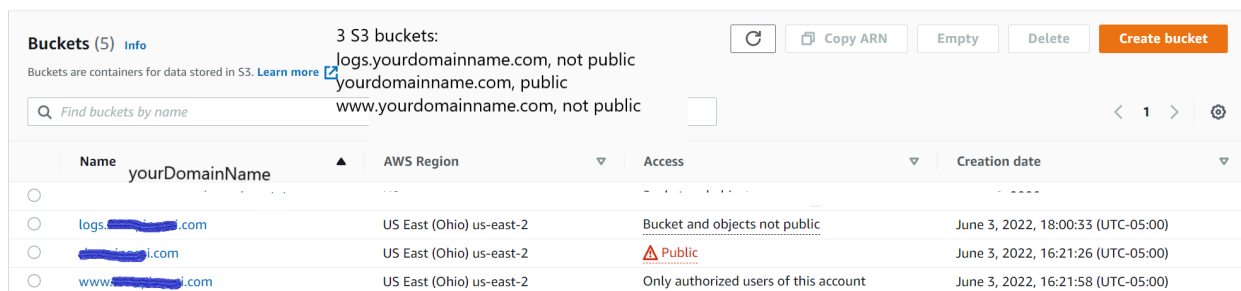
[AWS Route53 Console: Route53 to set Alias Record for root domain and sub domain](#)

[Google Domain: Define custom name servers](#)

● AWS S3 Console: Create three S3 buckets,

one mandatory S3 bucket for root domain,
optionally second one S3 bucket for redirecting subdomain,
and optionally third one for logging web traffic

3 buckets:

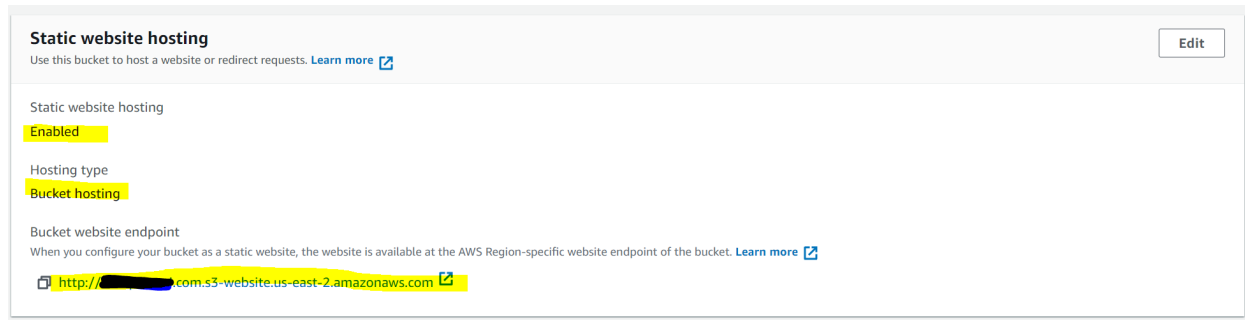


The screenshot shows the AWS S3 Console interface. At the top, it says "Buckets (5)" and "3 S3 buckets:". Below this, there are three buckets listed in a table. The first bucket is "logs.yourdomainname.com" with "not public" access. The second bucket is "yourdomainname.com" with "public" access. The third bucket is "www.yourdomainname.com" with "Only authorized users of this account" access. All buckets are in the "US East (Ohio) us-east-2" region and were created on June 3, 2022.

Name	AWS Region	Access	Creation date
logs.yourdomainname.com	US East (Ohio) us-east-2	Bucket and objects not public	June 3, 2022, 18:00:33 (UTC-05:00)
yourdomainname.com	US East (Ohio) us-east-2	Public	June 3, 2022, 16:21:26 (UTC-05:00)
www.yourdomainname.com	US East (Ohio) us-east-2	Only authorized users of this account	June 3, 2022, 16:21:58 (UTC-05:00)

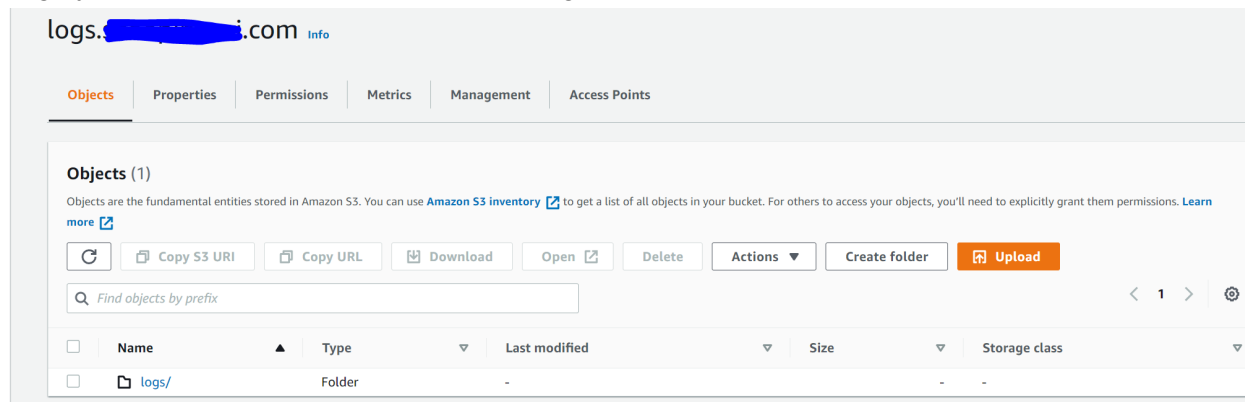
1. S3 bucket for root domain

Root domain bucket with enabled web hosting:



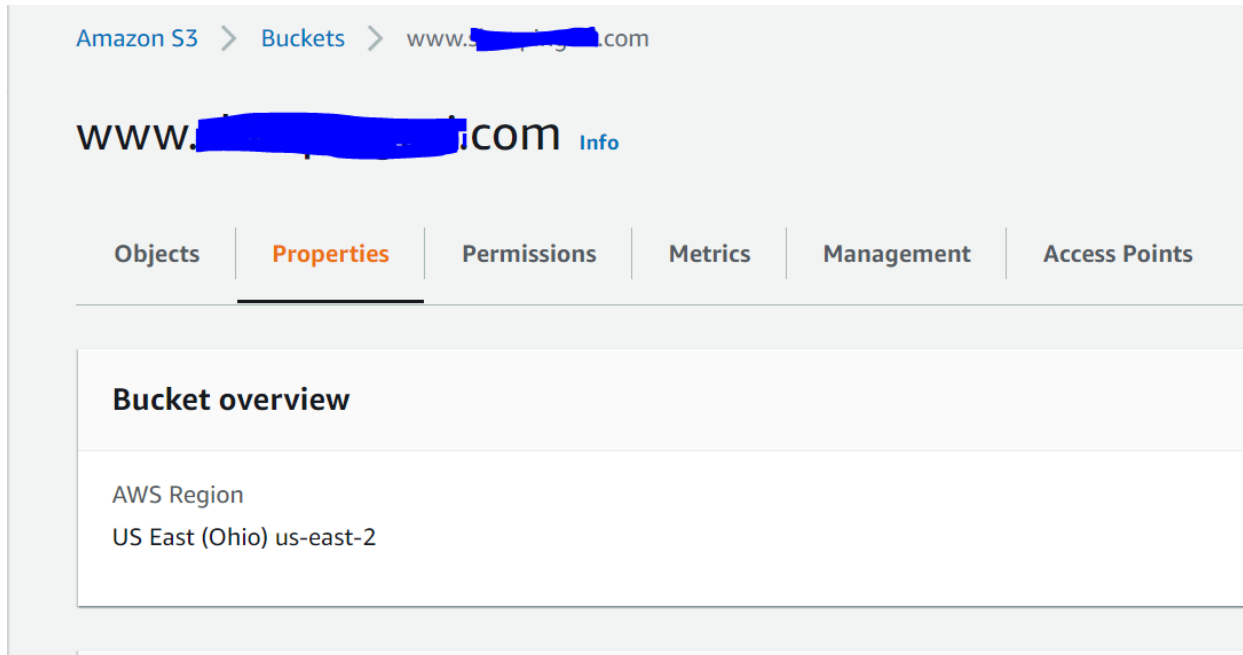
2. Optionally, S3 bucket for logging web traffic

Logs.yourdomainname.com bucket with “logs” folder:



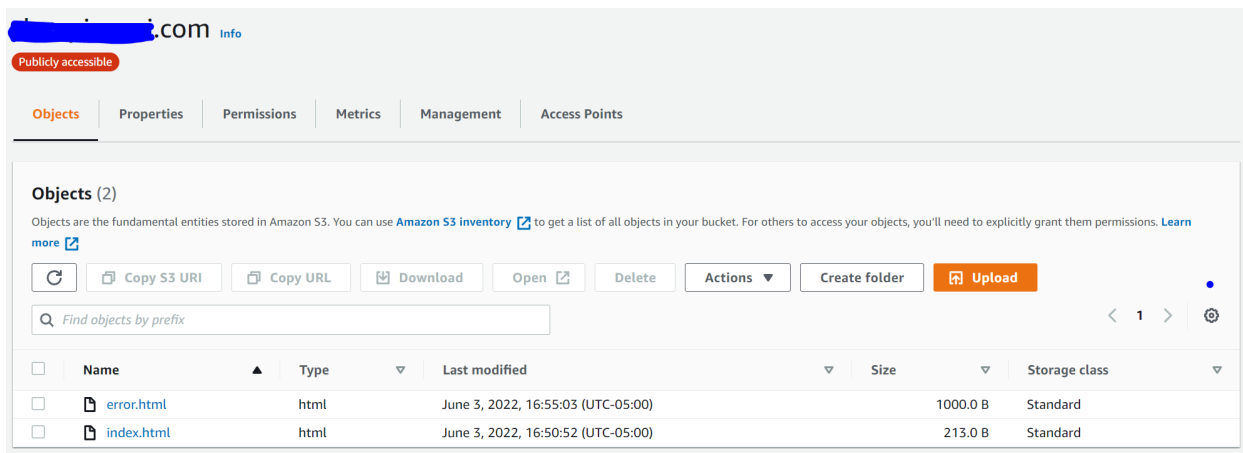
3. Optionally, S3 bucket for sub domain

Sub domain bucket for www.yourdomainname.com:



- AWS S3 Console: Configure an index document and optionally error document

Root domain bucket with index.html and error.html:



- AWS S3 Console: Setting permissions for website access

Root domain bucket's Permissions setting:

Publicly accessible

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

Public

Block public access (bucket settings)

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 all your S3 buckets and objects i of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual

Edit

Block all public access

Off

▼ Individual Block Public Access settings for this bucket

☒ 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 chang

☒ 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.

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](#)

Public access is blocked because Block Public Access settings are turned on for this bucket

To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

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

If redirecting enabled, Sub domain bucket permissions:

www. [REDACTED].com

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

Only authorized users of this account

Block public access (bucket settings)

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 all of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you

Edit

Block all public access

On

Individual Block Public Access settings for this bucket

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](#)

Public access is blocked because Block Public Access settings are turned on for this bucket

To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3](#)

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

logs-**XXXXXXXXXX**.com

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

Bucket and objects not public

Block public access (bucket settings)

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 all your S3 buckets and objects is blocked, turn on Block Public Access. If you have any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your needs.

Edit

Block all public access

On

Individual Block Public Access settings for this bucket

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](#)

Public access is blocked because Block Public Access settings are turned on for this bucket

To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

```
{
  "Version": "2012-10-17",
  "Id": "S3-Console-Auto-Gen-Policy-1654297431424",
  "Statement": [
    {
      "Sid": "S3PolicyStmt-DO-NOT-MODIFY-1654297431253",
      "Effect": "Allow",
      "Principal": {
        "Service": "logging.s3.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::logs-XXXXXXXXXX.com/*"
    }
  ]
}
```

- For the root domain bucket, under Properties, choose to edit server access logging:

Amazon S3 > Buckets > [redacted].com > Edit server access logging

Edit server access logging [Info](#)


Server access logging

Log requests for access to your bucket. [Learn more](#)

Server access logging

☐ Disable

☒ Enable

 **Bucket policy will be updated**

When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery group.

Target bucket

s3://logs.[redacted].com/logs/ [Browse S3](#)

Format: s3://bucket/prefix

[Cancel](#) [Save changes](#)

After this setup, the traffic will be logged every 2 hours

- Optionally, AWS S3 Console: Configuring a web page redirecting

Sub domain bucket website hosting enabled and set as redirect request:

Static website hosting

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

Static website hosting

Enabled

Hosting type

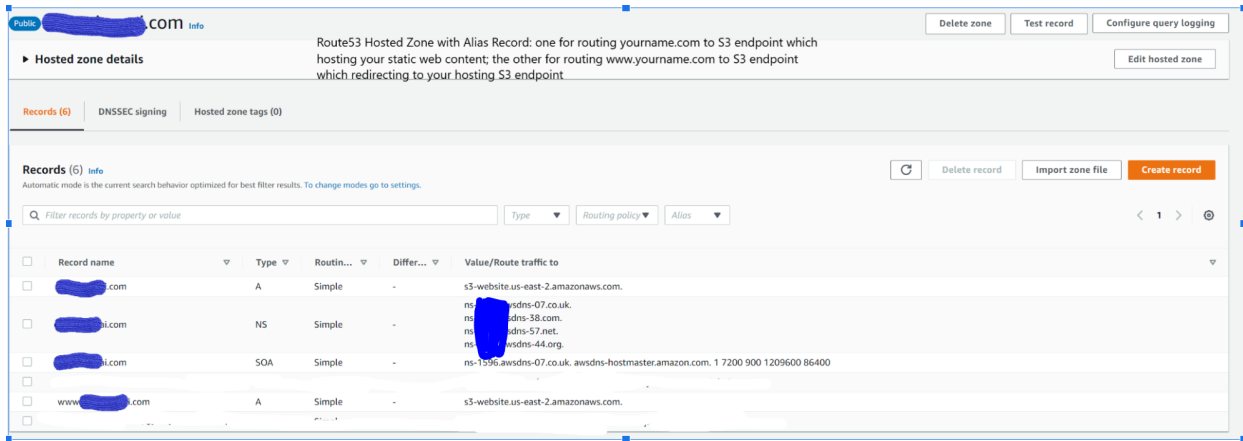
Redirect request

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://www.\[redacted\].com.s3-website.us-east-2.amazonaws.com](http://www.[redacted].com.s3-website.us-east-2.amazonaws.com)

- AWS Route53 Console: Route53 to set Alias Record for root domain and sub domain



- Google Domain: Define custom name servers

Custom name servers (Active)

Manage name servers

[Learn more about managing name servers](#)

^

?

ns-1608@redhat.com

Manage records

[Learn more](#)

No DNSSEC records have been set up

Ref:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html>