

Data Scientists use to work with notebooks like **Jupyter** and **RMarkdown**. Through notebooks, they can easily share their analysis in HTML format. But what about when there is a need to share the notebooks publicly? In this case, the most convenient way is to configure an Amazon S3 bucket to function as a static website. In this tutorial, we will provide you a walkthrough example of how you can share your notebooks as a static website with AWS S3.

Create your Report

The report should be in HTML format. Let's create a dummy report in R using RMarkdown. Let's create the Rmd report:

```
---
title: "Cars Report"
output: html_document
---

```{r setup, include=FALSE}
knitr::opts_chunk$set(echo = FALSE, warning = FALSE, message = FALSE)
```

# This is a DT datatable

```{r}
Load the libraries
library(DT)
library(tidyverse)
library(plotly)

DT::datatable(mtcars, options=list(
 pageLength = 10))
```

# This is a Plotly Chart

```{r}
my_plot <- ggplot(mtcars, aes(x=wt, y=mpg)) + geom_point() +
 ggtitle("Miles Per Gallon vs Weight") +
 xlab('Weight (x 1000lbs)') + ylab('Miles per Gallon') + geom_smooth()
ggplotly(my_plot)
```
```

Finally, we knit it as HTML and we store it locally.

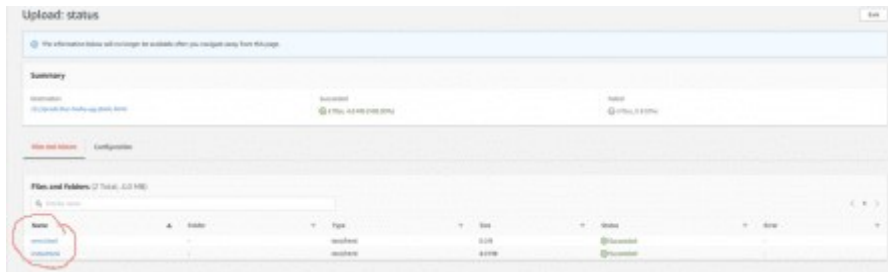
Create your S3 Bucket

Now you have to log-in to the AWS Console and to create a new bucket. In my case I created

the predictive-hacks-eg-static-html



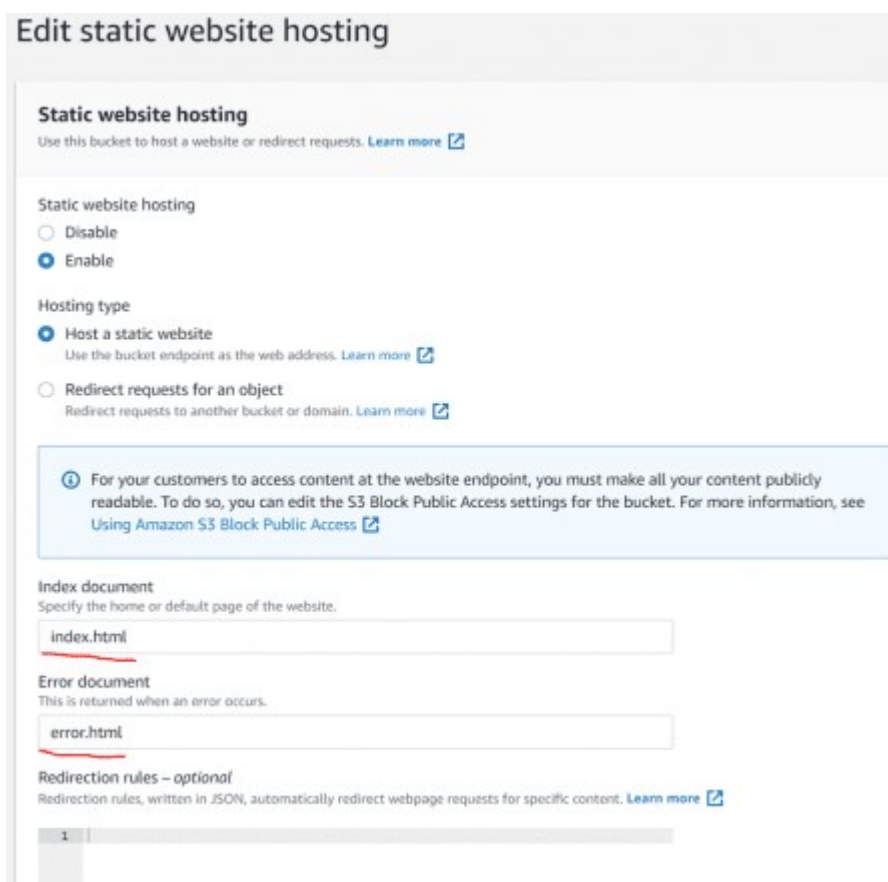
Then, you need to upload your html report, called “**index.html**” and an “error” to be returned in case there is an error. In my case, I called it “**error.html**”



Now, you need to go to the S3 Bucket and to go to **properties** and to edit the Static website hosting.



You enable the website hosting and you specify the Index and Error documents respectively.



Then, you need to go to the bucket Permissions and to uncheck the “Block all public access” and then click “Save changes”

Edit Block public access (bucket settings)

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 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 your buckets 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.

Cancel [Save changes](#)

Then, you will need to edit the bucket policy by entering:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::predictive-hacks-eg-static-html/*"
      ]
    }
  ]
}
```

Where predictive-hacks-eg-static-html is my bucket. You should write yours.

Now you should be ready. If you go down to the bucket properties you will see your public URL link

Static website hosting

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

Static website hosting
Enabled

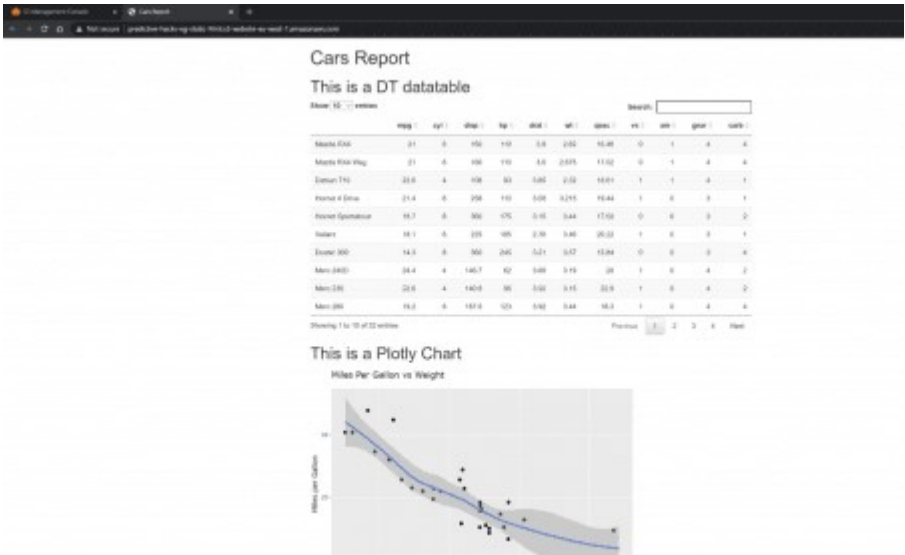
Hosting type
Bucket hosting

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://predictive-hacks-eg-static-html.s3-website-eu-west-1.amazonaws.com>

In my case it is [http://predictive-hacks-eg-static-html.s3-website-eu-](http://predictive-hacks-eg-static-html.s3-website-eu-west-1.amazonaws.com)

west-1.amazonaws.com. If you click on the link you should be able to see my report.



Finally, note that Amazon S3 does not support HTTPS access to the website. If you want to use HTTPS, you can use Amazon CloudFront to serve a static website hosted on Amazon S3.