

# SWE 642: Assignment 1

## Urls

S3 - <http://charitha-swe-642-assignment-1.s3-website-us-east-1.amazonaws.com/>

EC2 - <http://ec2-3-91-184-96.compute-1.amazonaws.com/home-page.html>

## Documentation to deploy on S3

1. Creating the bucket - In aws S3 console, click on Create Bucket button. Provide the bucket name (charitha-swe-642-assignment-1) and select the closest aws region. Since we want the website to be publicly accessible , uncheck the Block Public Access settings option. Keep all other options to the default value. Click on the Create Button.

### Create bucket [Info](#)

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

---

#### General configuration

AWS Region

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

Bucket type [Info](#)

☒ **General purpose**  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory - New**  
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

charitha-swe-642-assignment-1

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

---

#### 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.

2. Enable Static Website Hosting - Select the bucket we have created, In the properties section, Under Static website hosting, choose Edit. Select enable option for Static website hosting, Host a static website for hosting type and Specify the home and error html files.

**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](#)

**i** 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.

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

3. Upload the files - Now click on the S3 bucket created in the above step, Click on the upload button. Click on the Add Files button and add the required html and css files and click on the upload button.

**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** (11 Total, 681.5 KB)  
All files and folders in this table will be uploaded.

< 1 2 >

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	main.css	-	text/css
<input type="checkbox"/>	bootstrap.min.css	-	text/css
<input type="checkbox"/>	cs-department-info.css	-	text/css
<input type="checkbox"/>	cs-department-info.html	-	text/html
<input type="checkbox"/>	cs-survey-page.css	-	text/css
<input type="checkbox"/>	cs-survey-page.html	-	text/html
<input type="checkbox"/>	error.html	-	text/html
<input type="checkbox"/>	home-page.css	-	text/css
<input type="checkbox"/>	home-page.html	-	text/html
<input type="checkbox"/>	Readme.txt	-	text/plain

4. Add bucket policy - Now go to the Permissions tab, In the bucket policy section, Click on the edit button and add the below code.

**Bucket policy**

EditDelete

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](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::charitha-swe-642-assignment-1/*"
    }
  ]
}
```

Copy

5. Test the website - In the properties tab of the created bucket, Under Static website hosting, choose your Bucket website endpoint.

**Static website hosting**

Edit

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://charitha-swe-642-assignment-1.s3-website-us-east-1.amazonaws.com>

## Documentation to deploy on EC2

1. Creating an EC2 Instance - In the EC2 console, click on Launch Instance button. Give the instance name (swe-642-assignment-1), Choose the Amazon Machine Image(Amazon Linux), Instance type as t2 micro, Select the key pair (selected existing pem key), In the network settings, Check Allow HTTPS traffic from the internet and Allow HTTP traffic from the internet options.

### Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

#### Name and tags [Info](#)

Name

swe-642-assignment-1

Add additional tags

#### ▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

RecentsQuick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu®

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUS

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

#### ▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-0fe92b3c24c627f71

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called 'launch-wizard-7' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere  
0.0.0.0/0

☒ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

2. Connect to your instance - Once the instance is running, Click on the connect button to see the different options. Using the below command to connect from the terminal.

```
ssh -i /path/to/your/key.pem ec2-user@your-instance-public-dns-name
```

3. Installing the Web Server - Use the below commands to update the package repository and install apache web server.

```
sudo yum update -y
```

```
sudo yum install -y httpd
```

4. Copy files and folders - Use the below command to copy the files or folder from local to EC2 instance.

```
scp -i /path/to/your/key.pem /path/to/your/zip-file.zip  
ec2-user@your-instance-public-dns-name:~/
```

```
unzip zip-file.zip
```

5. Deploying your website - Use the below commands to move the files to the web server's root directory.

```
sudo mv ~/zip-file/* /var/www/html/
```

6. Managing the Web Server Service - Use the below commands to check the status, to start, and run the web server.

```
sudo systemctl status httpd
```

```
sudo systemctl start httpd
```

```
sudo systemctl enable httpd
```

7. Verify the website - Open the web browser and enter the EC2 instance's public DNS or IP address and see if the website is live.

## REFERENCES

1. EC2 - <https://www.youtube.com/watch?v=Islmm-LMu38>
2. S3 - <https://docs.aws.amazon.com/AmazonS3/latest/userguide/HostingWebsiteOnS3Setup.html>