Group member	Sisi Zhang, Harish Ram
• Step 1: Create a bucket	Amazon S3 > Create bucket **Create bucket** Info Buckets are containers for data stored in S3. Learn more ⧉ **General configuration** Bucket name www.g32408374.gwu.edu 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** **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.

● Step 2: Enable static website hosting	Amazon S3 > www.g32408374.gwu.edu > Edit static website hosting **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 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 ↗
● Step 3: Edit Block Public Access settings	Objects Properties **Permissions** Metrics Management Access Points **Permissions overview** Access Objects can be 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 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 ↗ [Edit] Block *all* public access ⚠ Off — Block public access to buckets and objects granted through *new* access control lists (ACLs) ⚠ Off — Block public access to buckets and objects granted through *any* access control lists (ACLs) ⚠ Off — Block public access to buckets and objects granted through *new* public bucket or access point policies ⚠ Off — Block public and cross-account access to buckets and objects through *any* public bucket or access point policies ⚠ Off

| ● Step 4: Add a bucket policy that makes your bucket content publicly available | **Bucket policy**<br>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** [↗]<br><br>[ Policy examples ↗ ]  [ Policy generator ↗ ]<br><br>Bucket ARN<br>⧉ arn:aws:s3:::www.g32408374.gwu.edu<br><br>**Policy**<br><br>```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::www.g32408374.gwu.edu/*"
            ]
        }
    ]
}
``` |
● Step 5: Configure an index document	# 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** (1 Total, 189.0 B) [Remove] [Add files] [Add folder] All files and folders in this table will be uploaded. 🔍 Find by name ⟨ 1 ⟩ | ☐	Name ▲	Folder ▽	Type ▽	Size ▽
☐	index.html	-	text/html	189.0 B | **Destination** Destination s3://www.g32408374.gwu.edu ▸ **Destination details** Bucket settings that impact new objects stored in the specified destination.

● Step 6: Configure an error document	Amazon S3 > www.g32408374.gwu.edu > 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 folders**. **Files and folders** (2 Total, 325.0 B) Remove Add files Add folder All files and folders in this table will be uploaded. Find by name ‹ 1 › |	Name ▲	Folder ▽	Type ▽	Size ▽
---	---	---	---	---
☐	error.html	-	text/html	136.0 B
☐	index.html	-	text/html	189.0 B	 **Destination** Destination s3://www.g32408374.gwu.edu ▶ **Destination details** Bucket settings that impact new objects stored in the specified destination.
● Step 7: Test your website endpoint	← → C ⌂ ⚠ Not Secure | www.g32408374.gwu.edu.s3-website-us-east-1.amazonaws.com ⠿ Apps ◉ 海外申请护照在线… ✎ Paraphrasing Tool… ◉ 网易云音乐 ◎ WhatsApp ◉ GroupMe 📁 GW ## Welcome to my website Now hosted on Amazon S3!
● Step 8: Clean up	Amazon S3 > www.g32408374.gwu.edu > Delete bucket **Delete bucket** Info ⊗ **This bucket is not empty** Buckets must be empty before they can be deleted. To delete all objects in the bucket, use the empty bucket configuration. **Delete bucket "www.g32408374.gwu.edu"?** To confirm deletion, enter the name of the bucket in the text input field. www.g32408374.gwu.edu

Empty bucket Info

⚠ • Emptying the bucket deletes all objects in the bucket and cannot be undone.
  • Objects added to the bucket while the empty bucket action is in progress might be deleted.
  • To prevent new objects from being added to this bucket while the empty bucket action is in progress, you might need to update your bucket policy to stop objects from being added to the bucket.

Learn more ↗

ⓘ If your bucket contains a large number of objects, creating a lifecycle rule to delete all objects in the bucket might be a more efficient way of emptying your bucket. Learn more ↗

[Go to lifecycle rule configuration]

Permanently delete all objects in bucket "www.g32408374.gwu.edu"?

To confirm deletion, type *permanently delete* in the text input field.

permanently delete