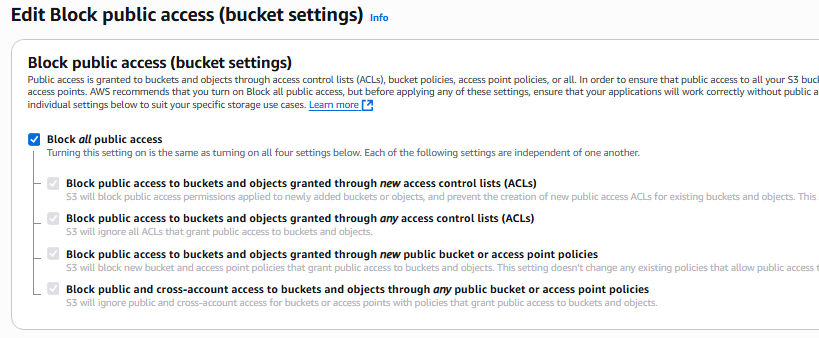
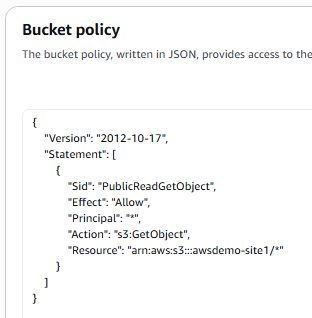
**S3**

**Scenario 1: Need to access static website with access to all (public access)**

Disable (clear Check box) **Block public access (bucket settings)**



& update in **Bucket policy**



{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "PublicReadGetObject",

"Effect": "Allow",

"Principal": "\*",

"Action": "s3:GetObject",

"Resource": "arn:aws:s3:::awsdemo-site1/\*"

}

]

}

**Scenario 2: Need to access static website with allowed IP / network (not allowed to all / not public access)**

Hosting a static website on Amazon S3 with IP-based access control involves configuring an S3 bucket for static website hosting and then applying a bucket policy to restrict access based on source IP addresses.

Steps to Host a Static Site in S3 with IP-Based Access Control:

* **Prepare Your Website Files:**

Organize your static website files (HTML, CSS, JavaScript, images, etc.) in a local directory. Ensure you have an index.html file for your homepage and an error.html file for custom error pages, if desired.

* **Create an S3 Bucket:**
  + Open the AWS S3 console and create a new bucket.
  + Choose a unique bucket name.
  + During creation, you can initially keep "Block all public access" enabled and adjust it later.
* **Upload Your Website Files:**

Upload your prepared website files to the newly created S3 bucket.

* **Enable Static Website Hosting:**
  + Go to the "Properties" tab of your S3 bucket.
  + Scroll down to "Static website hosting" and click "Edit."
  + Enable static website hosting.
  + Specify index.html as the index document and error.html (if applicable) as the error document.
  + Note the "Bucket website endpoint" URL provided, as this is how your static site will be accessed.
* **Configure Bucket Policy for IP-Based Access Control:**
  + Go to the "Permissions" tab of your S3 bucket.
  + Under "Bucket policy," click "Edit."
  + Add a bucket policy that allows s3:GetObject action only from specified IP addresses or ranges. An example policy is provided below:

Code

{  
 "Version": "2012-10-17",  
 "Id": "**IPAllow**",  
 "Statement": [  
 {  
 "Sid": "**AllowIPAccess**",  
 "Effect": "**Allow**",  
 "Principal": "\*",  
 "Action": "s3:GetObject",  
 "Resource": "arn:aws:s3:::your-bucket-name/\*",  
 "Condition": {  
 "IpAddress": {  
 "aws:SourceIp": ["XX.XX.XX.XX/32", "YY.YY.YY.YY/24"]  
 }  
 }  
 },  
 {  
 "Sid": "**DenyAllExceptIPs**",  
 "Effect": "**Deny**",  
 "Principal": "\*",  
 "Action": "s3:GetObject",  
 "Resource": "arn:aws:s3:::your-bucket-name/\*",  
 "Condition": {  
 "NotIpAddress": {  
 "aws:SourceIp": ["XX.XX.XX.XX/32", "YY.YY.YY.YY/24"]  
 }  
 }  
 }  
 ]  
 }

* Replace your-bucket-name with your actual bucket name and XX.XX.XX.XX/32, YY.YY.YY.YY/24 with your desired IP addresses or CIDR ranges. The first statement allows access from the specified IPs, and the second explicitly denies access from any other IP addresses.
* **Update Block Public Access Settings:**

If you initially blocked all public access, you will need to adjust these settings to allow public access to the bucket for static website hosting, while relying on the bucket policy for IP-based restrictions.

* **Test Your Website:**

Access your static website using the "Bucket website endpoint" URL. Verify that it is accessible only from the allowed IP addresses and inaccessible from others.