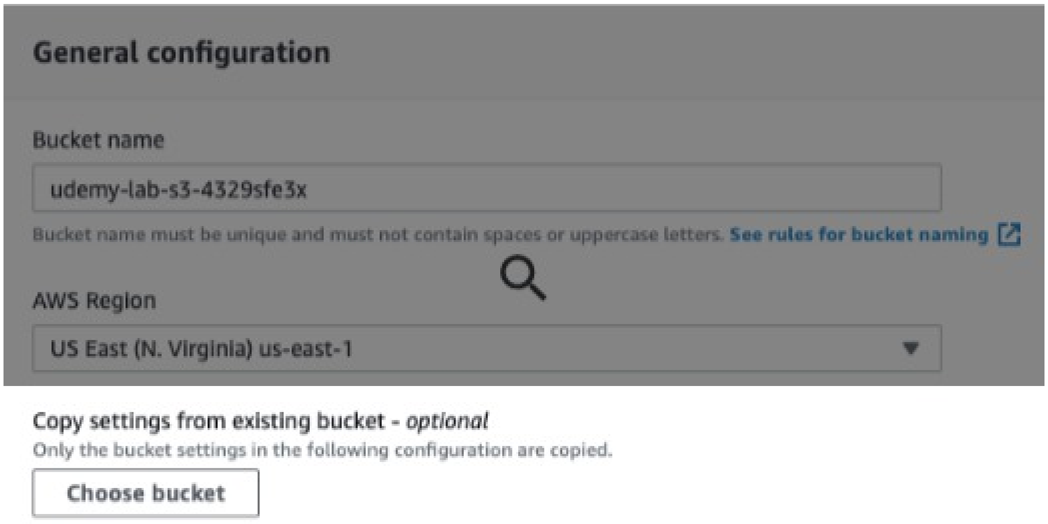
Example approach

✕

1. In the **AWS Management Console**, go to **Services** and click **S3**
2. Click **Create Bucket** and then set the bucket name to "udemy-lab-s3-" and add a random string of letters and numbers on the end to ensure uniqueness. E.g. "udemy-lab-s3-4329sfe3x9"



General configuration

Bucket name

udemy-lab-s3-4329sfe3x

Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

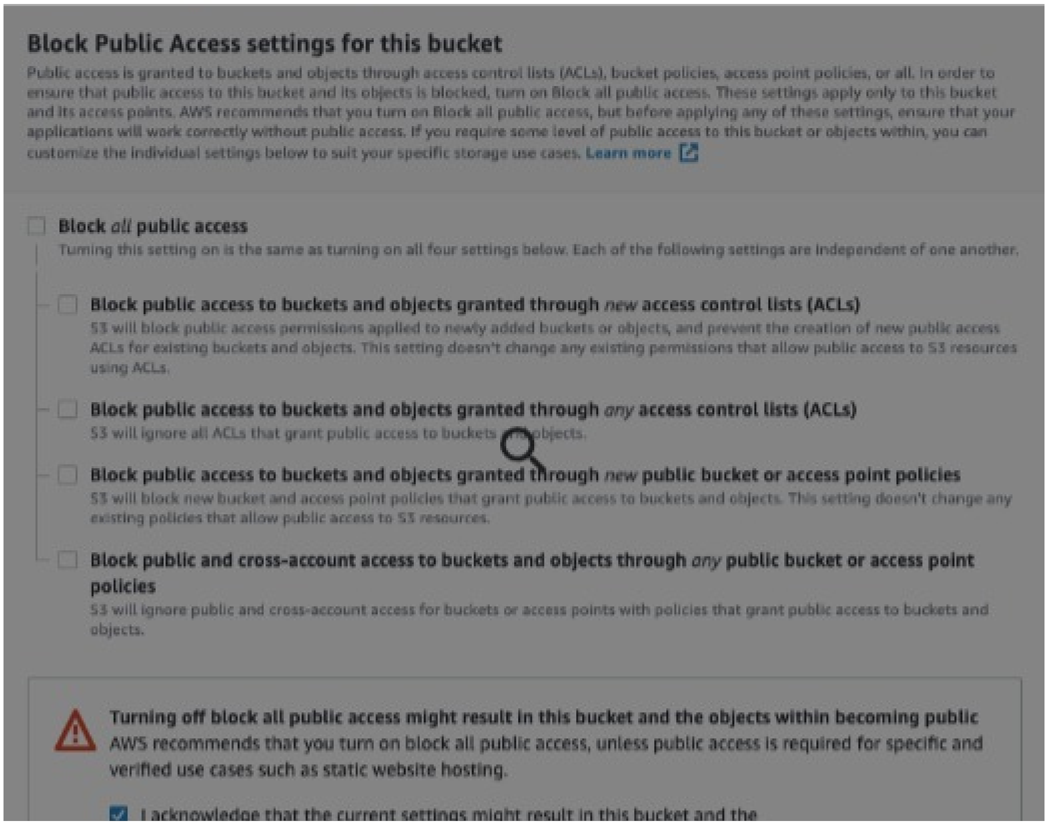
AWS Region

US East (N. Virginia) us-east-1 ▼

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

3. Change the **AWS Region** to "US-East (N. Virginia) us-east-1"
4. Deselect the option to "Block all public access" and select the checkbox to acknowledge the change



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.

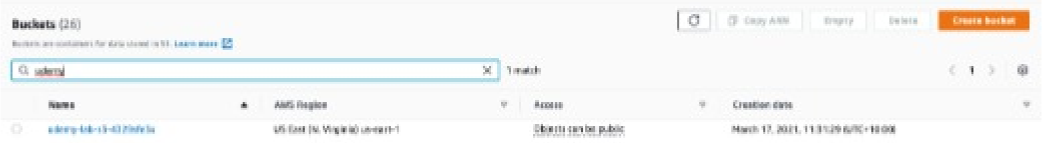
⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the

objects within becoming public.

5. Click **Create Bucket**

6. You should now see the new bucket in the S3 Management Console


Buckets (26)

udemy

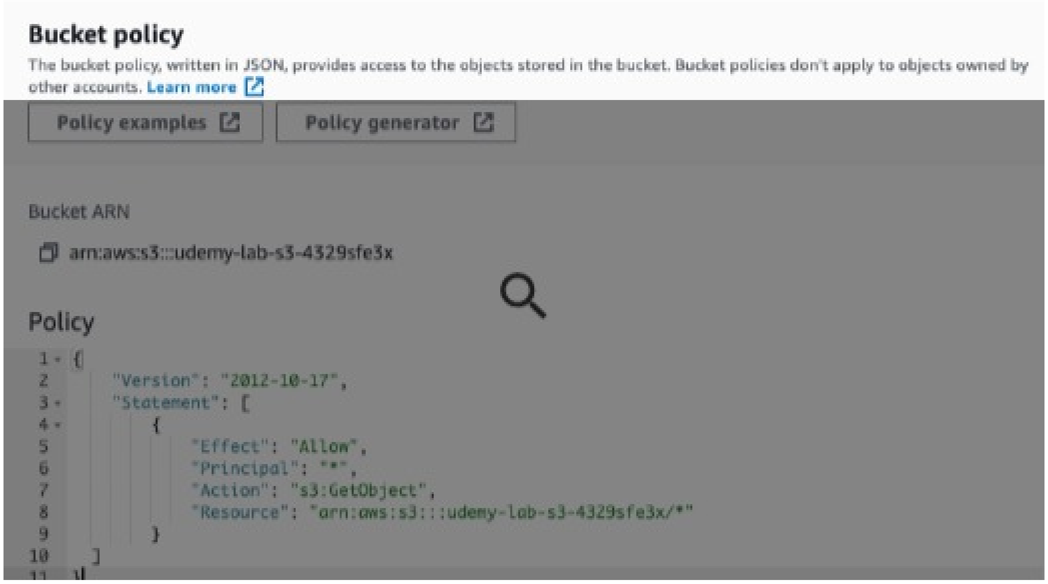
1 match

Name	AWS Region	Access	Creation date
udemy-lab-s3-4329sfe3x	US East (N. Virginia) us-east-1	Objects can be public	March 17, 2021, 11:31:29 (UTC+10:00)

7. Click the name of the bucket and then select the **Permissions** tab. Under **Bucket Policy** click **Edit** and copy and paste the code below into the policy editor

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

8. Copy the **Bucket ARN** and paste it over the ARN next to **Resource** (make sure you keep the /* at the end). It should now look like this:


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

Bucket ARN

arn:aws:s3:::udemy-lab-s3-4329sfe3x

Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::udemy-lab-s3-4329sfe3x/*"
        }
    ]
}
```

9. Click **Save changes**

10. On the **Objects** tab, click **Upload**, select the index.txt file from the resources, and click **Upload**