

Create S3 bucket in AWS

- Create Bucket: **my-assessment-bucket-1**

The screenshot shows the 'Create bucket' page in the AWS console. The browser address bar indicates the URL: `us-east-2.console.aws.amazon.com/s3/bucket/create?region=us-east-2&bucketType=general`. The page title is 'Create bucket'. The 'Bucket owner enforced' section is expanded, showing 'Block Public Access settings for this bucket'. The 'Block all public access' checkbox is checked, and the 'Block public access to buckets and objects granted through new access control lists (ACLs)' checkbox is also checked. A warning box states: '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.' The 'Bucket Versioning' section is also expanded, showing 'Bucket Versioning' set to 'Disable'. The 'Tags - optional' section is collapsed. The bottom of the page shows the 'Cancel' and 'Create bucket' buttons.

us-east-2.console.aws.amazon.com/s3/bucket/create?region=us-east-2&bucketType=general

Amazon S3 > Buckets > Create bucket

Bucket owner enforced

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.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☒ Disable

☐ Enable

Tags - optional (0)

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

us-east-2.console.aws.amazon.com/s3/bucket/create?region=us-east-2&bucketType=general

Amazon S3 > Buckets > Create bucket

Private link

Default encryption [info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [info](#)

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)

☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable

☒ Enable

Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

☒ Disable

☐ Enable

Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

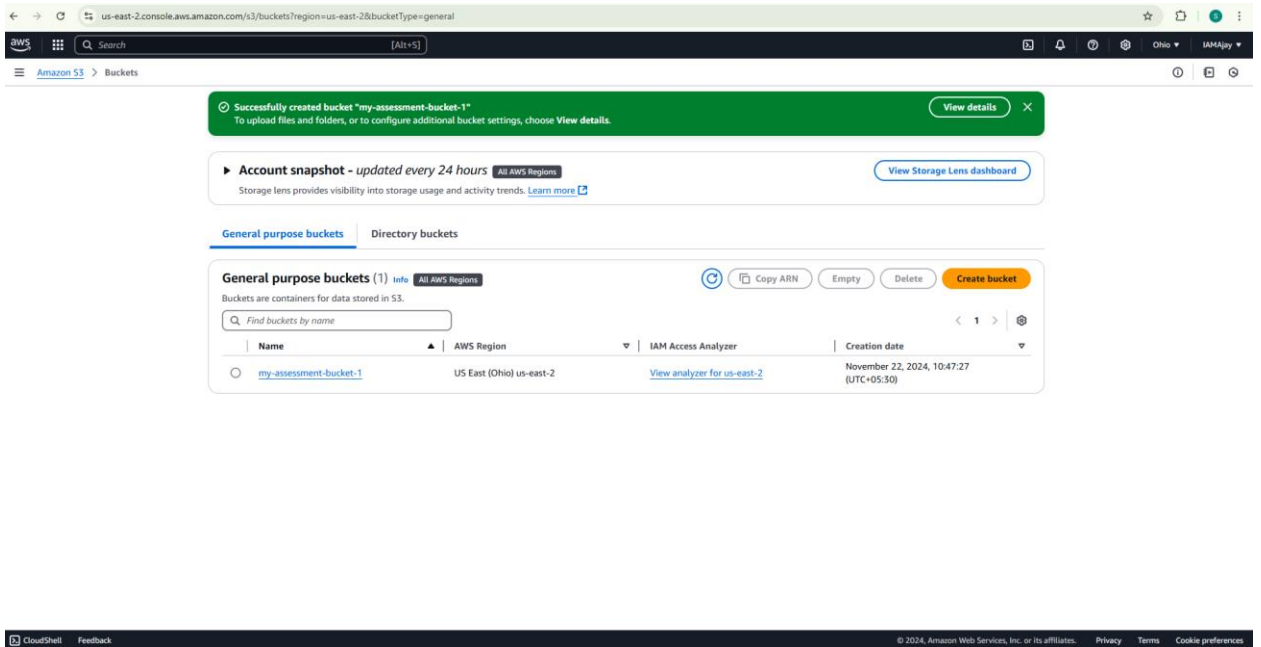
☐ Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

☐ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

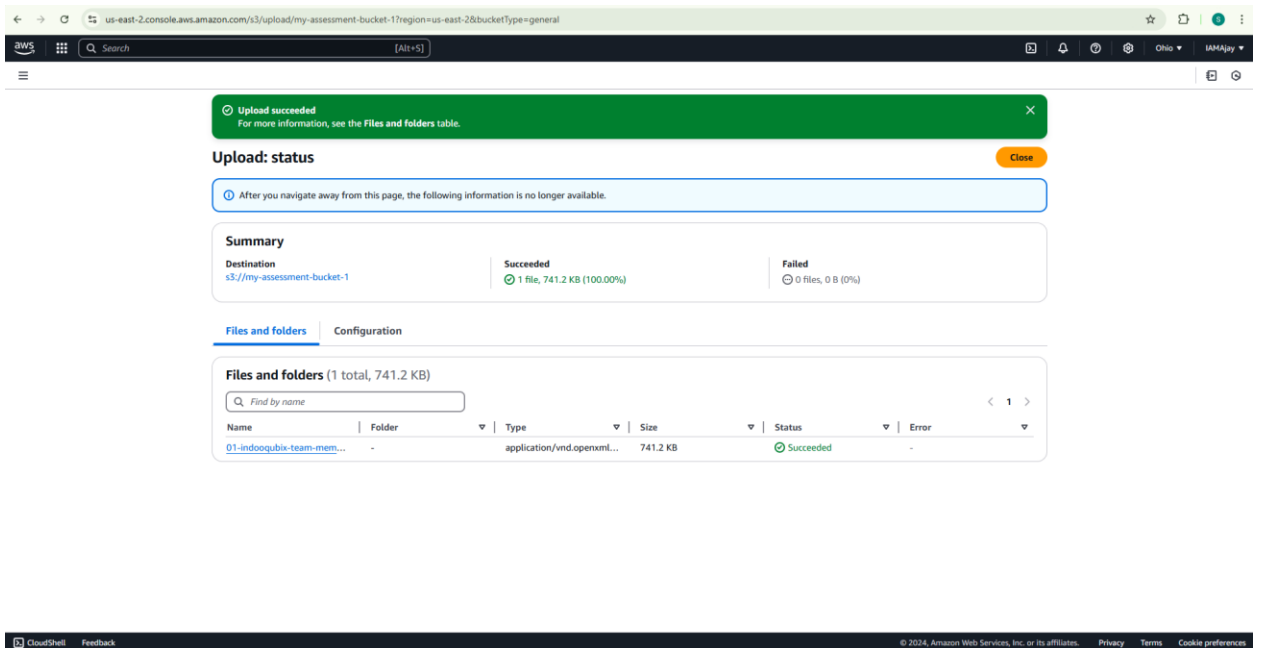
Cancel Create bucket

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



- Uploaded files in it.



- Create Policy for the bucket which I have created.

Step 1: Select Policy Type
A policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy: **S3 Bucket Policy**

Step 2: Add Statement(s)
A statement is the formal description of a single permission. See a description of [elements](#) that you can use in statements.

Effect: ☒ Allow ☐ Deny

Principal:

AWS Service: **Amazon S3** ☐ All Services (**)

Actions: **Select Actions** ☐ All Actions (**)

Amazon Resource Name (ARN):

ARN should follow the following format: `arn:aws:s3:::{BucketName}/{Keyname}`.
Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

[Add Statement](#)

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
* *	Allow	s3:GetObject	arn:aws:s3:::my-assessment-bucket-1/01-indooqubix-team-member-feature-presentation (1).pptx	None

Step 3: Generate Policy
A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

[Generate Policy](#) [Start Over](#)

This AWS Policy Generator is provided for informational purposes only; you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is, without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions associated with your use of Amazon Web Services.

Successfully edited bucket policy.

Block public access (bucket settings) [Edit](#)

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
OFF

Individual Block Public Access settings for this bucket

Bucket policy [Edit](#) [Delete](#)

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",
  "Id": "Policy173252865195",
  "Statement": [
    {
      "Sid": "Stmt173252861310",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::my-assessment-bucket-1/01-indooqubix-team-member-feature-presentation (1).pptx"
    }
  ]
}
```

[Copy](#)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- The given below URL for accessing the file which I have been uploaded.

https://my-assessment-bucket-1.s3.us-east-2.amazonaws.com/01-indooqubix-team-member-feature-presentation+(1).pptx