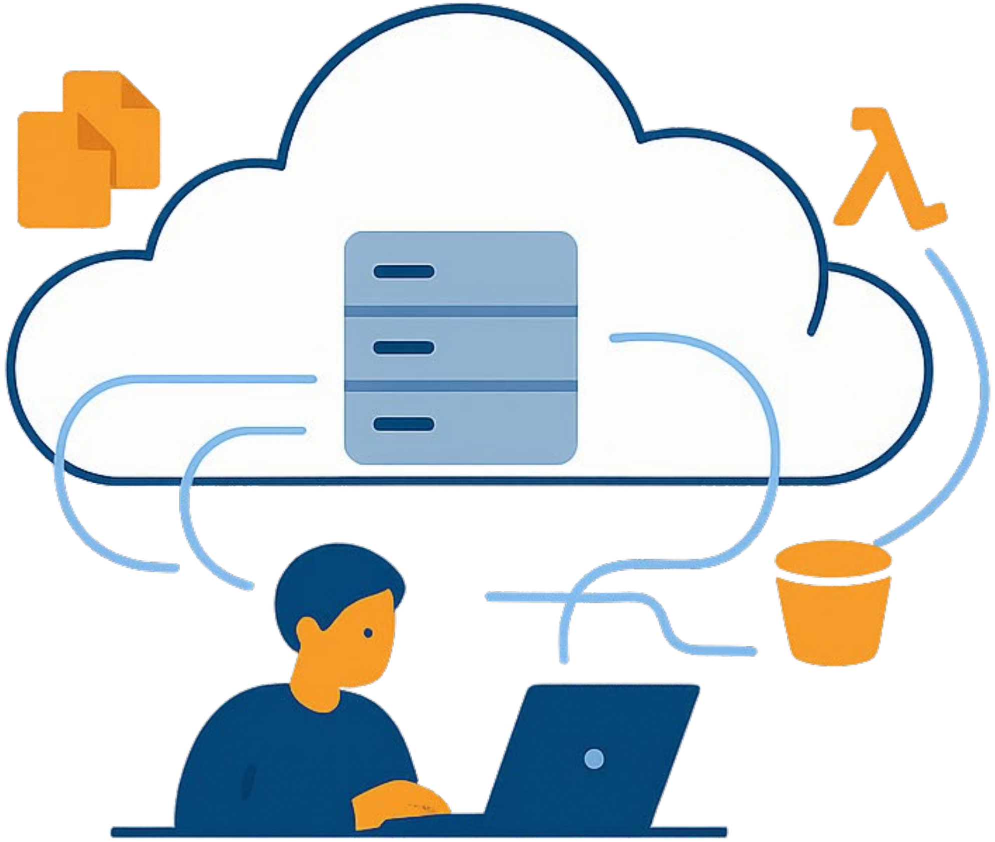
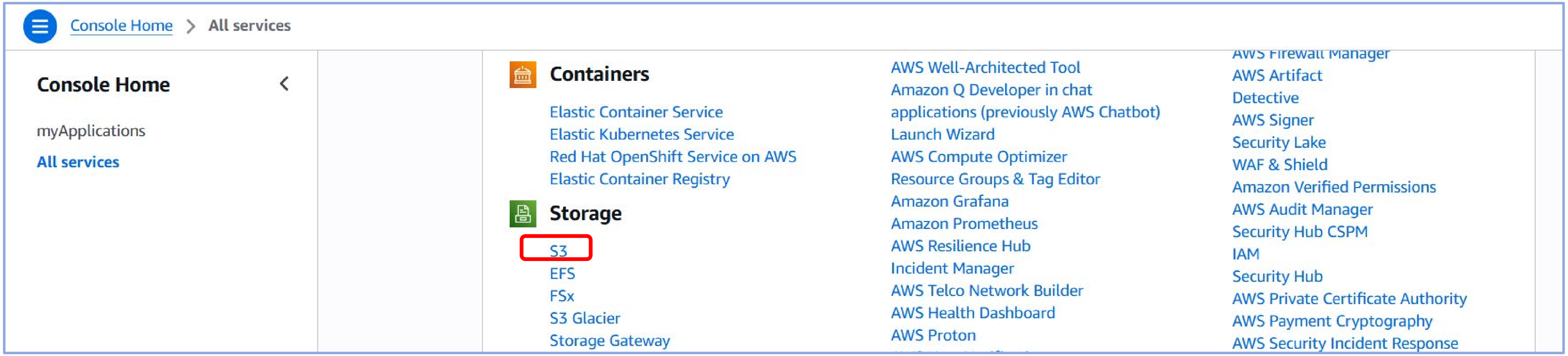


The cloudCraft

From Clicks to Cloud Confidence

BY ASHAN DISSANAYAKE



Console Home > All services

Console Home

myApplications

All services

Containers

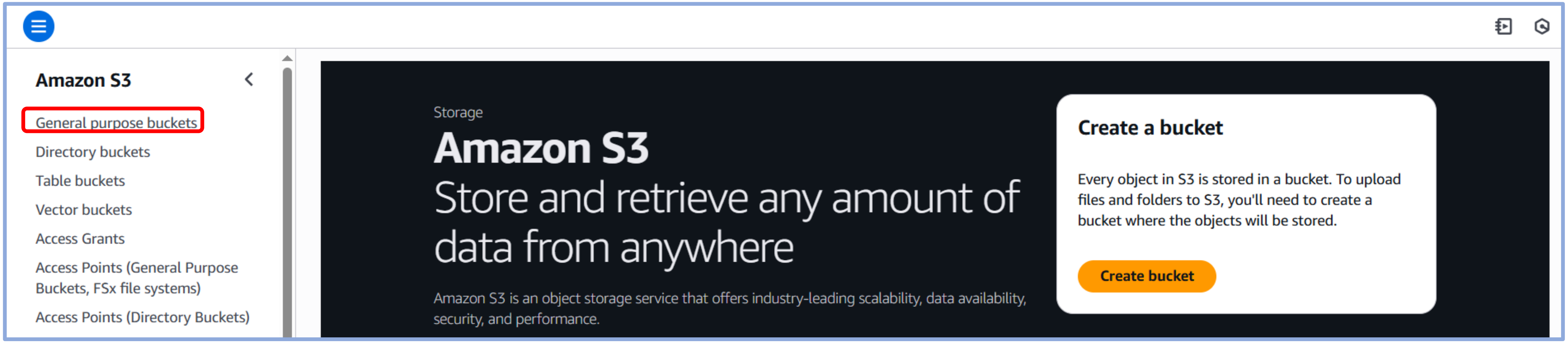
Elastic Container Service
Elastic Kubernetes Service
Red Hat OpenShift Service on AWS
Elastic Container Registry

Storage

S3
EFS
FSx
S3 Glacier
Storage Gateway

AWS Well-Architected Tool
Amazon Q Developer in chat applications (previously AWS Chatbot)
Launch Wizard
AWS Compute Optimizer
Resource Groups & Tag Editor
Amazon Grafana
Amazon Prometheus
AWS Resilience Hub
Incident Manager
AWS Telco Network Builder
AWS Health Dashboard
AWS Proton

AWS Firewall Manager
AWS Artifact
Detective
AWS Signer
Security Lake
WAF & Shield
Amazon Verified Permissions
AWS Audit Manager
Security Hub CSPM
IAM
Security Hub
AWS Private Certificate Authority
AWS Payment Cryptography
AWS Security Incident Response



Amazon S3

General purpose buckets
Directory buckets
Table buckets
Vector buckets
Access Grants
Access Points (General Purpose Buckets, FSx file systems)
Access Points (Directory Buckets)

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

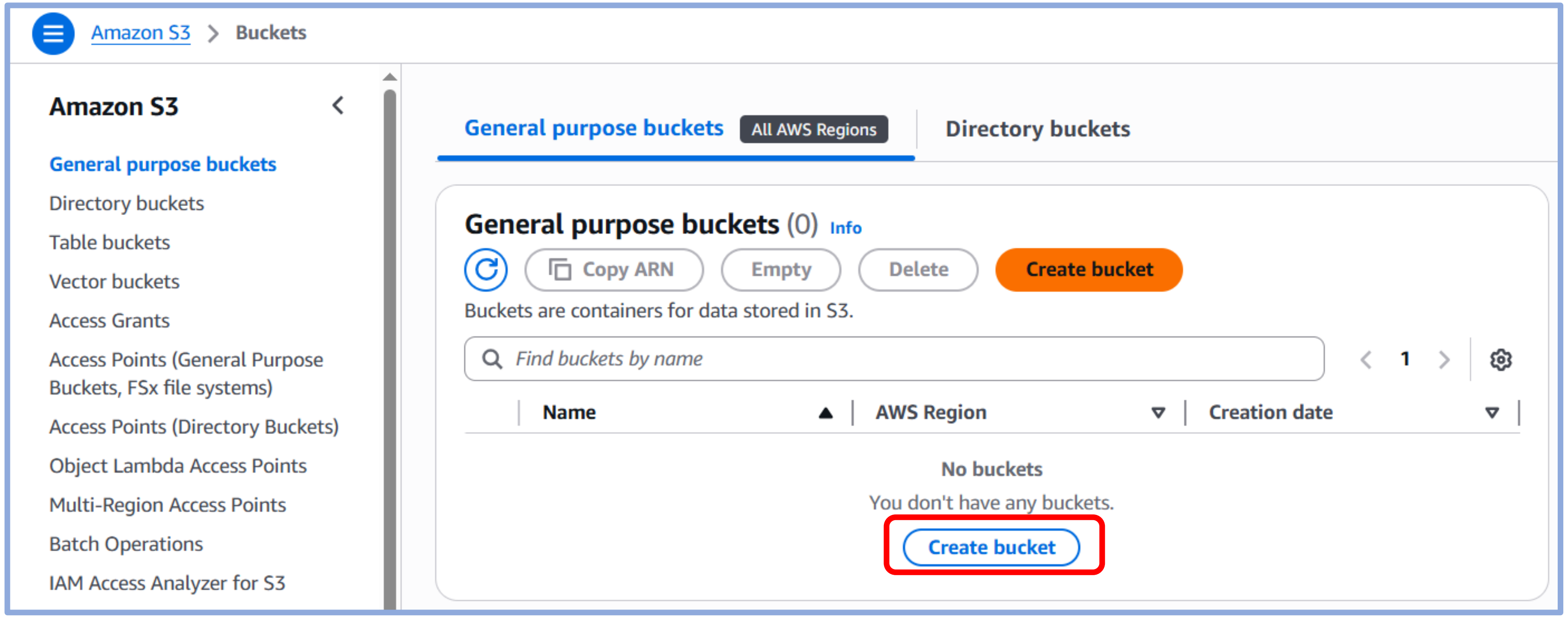
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

The cloudCraft
From Clicks to Cloud Confidence
BY ASHAN DISSANAYAKE

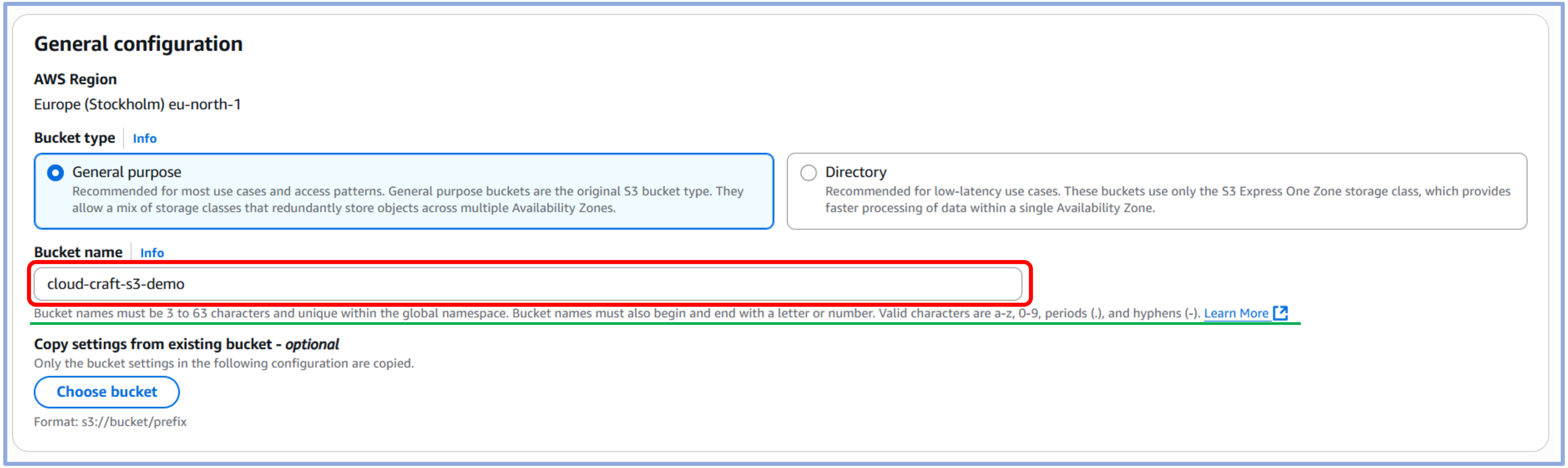


General purpose buckets (0) Info

Buckets are containers for data stored in S3.

No buckets

You don't have any buckets.



General configuration

AWS Region

Europe (Stockholm) eu-north-1

Bucket type

● 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
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

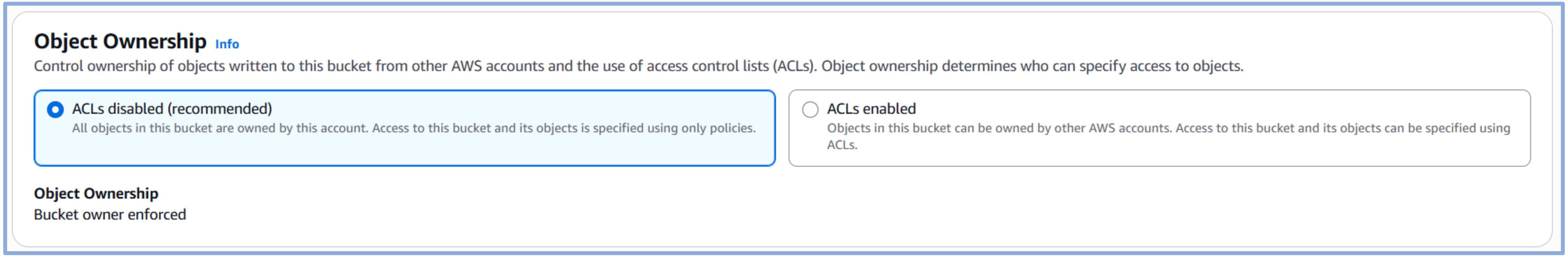
cloud-craft-s3-demo

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix



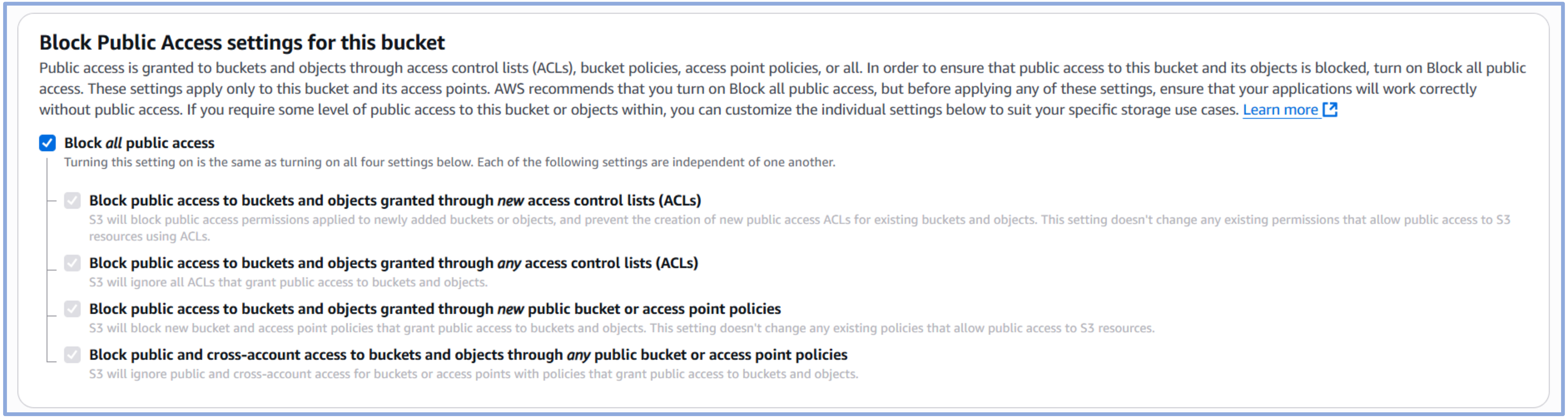
Object Ownership

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

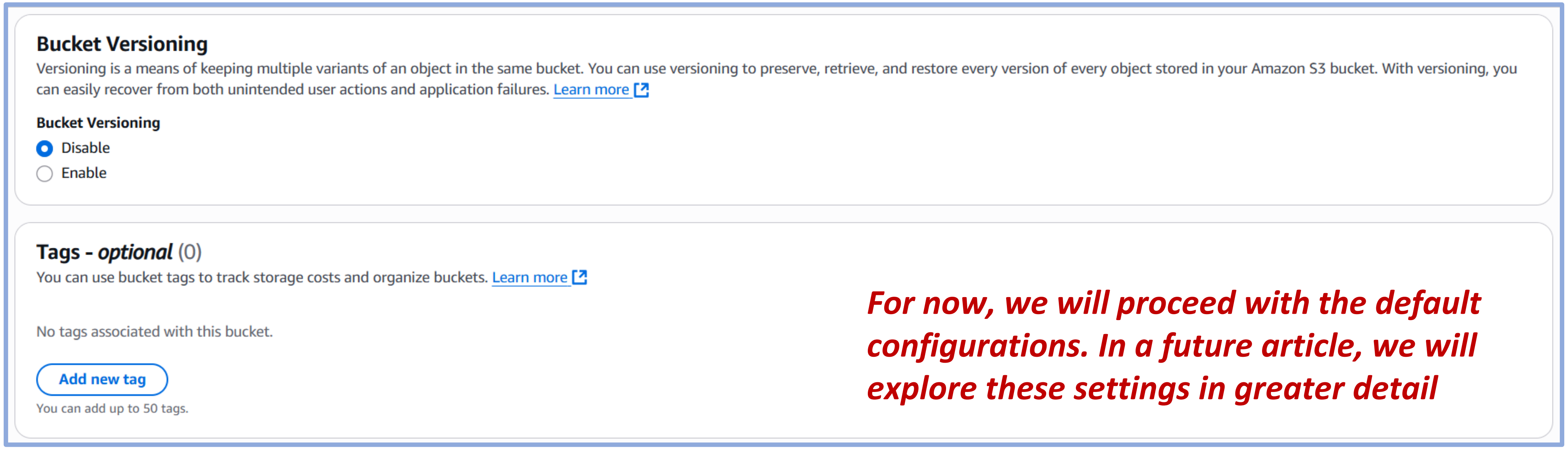


Block Public Access settings for this bucket

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.



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

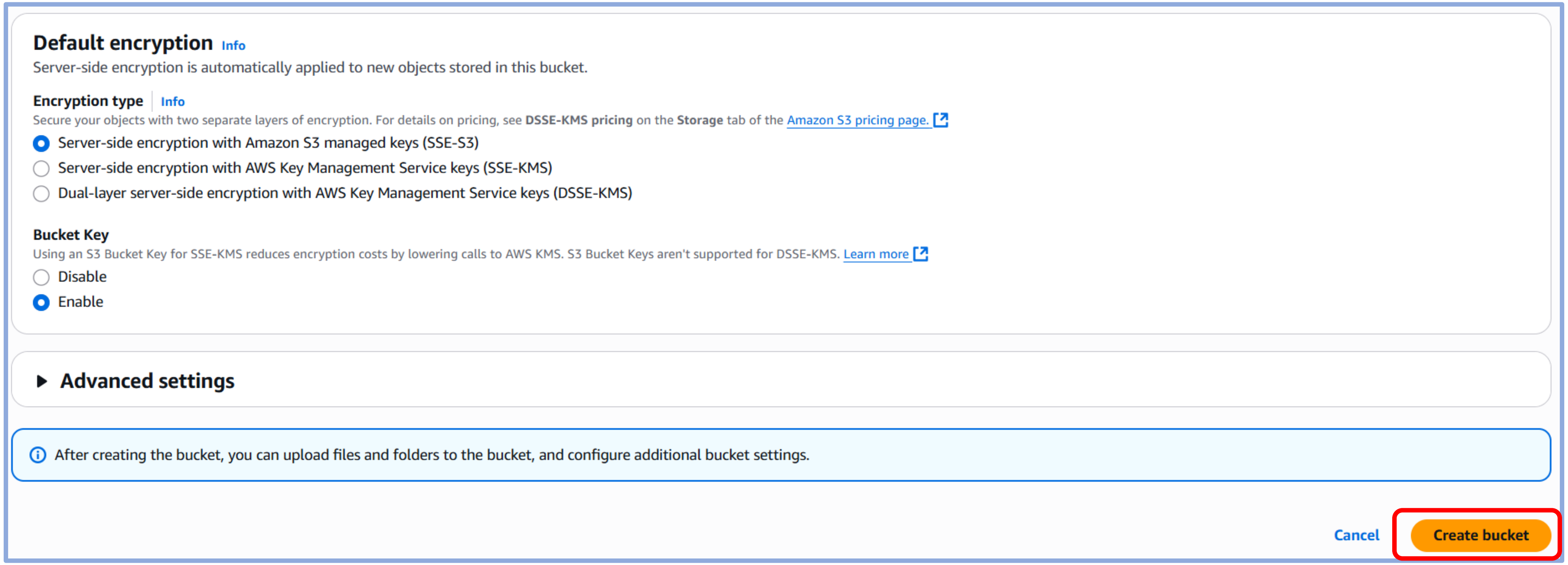
Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.

You can add up to 50 tags.

For now, we will proceed with the default configurations. In a future article, we will explore these settings in greater detail



Default encryption Info

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

Encryption type Info

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.

● 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)

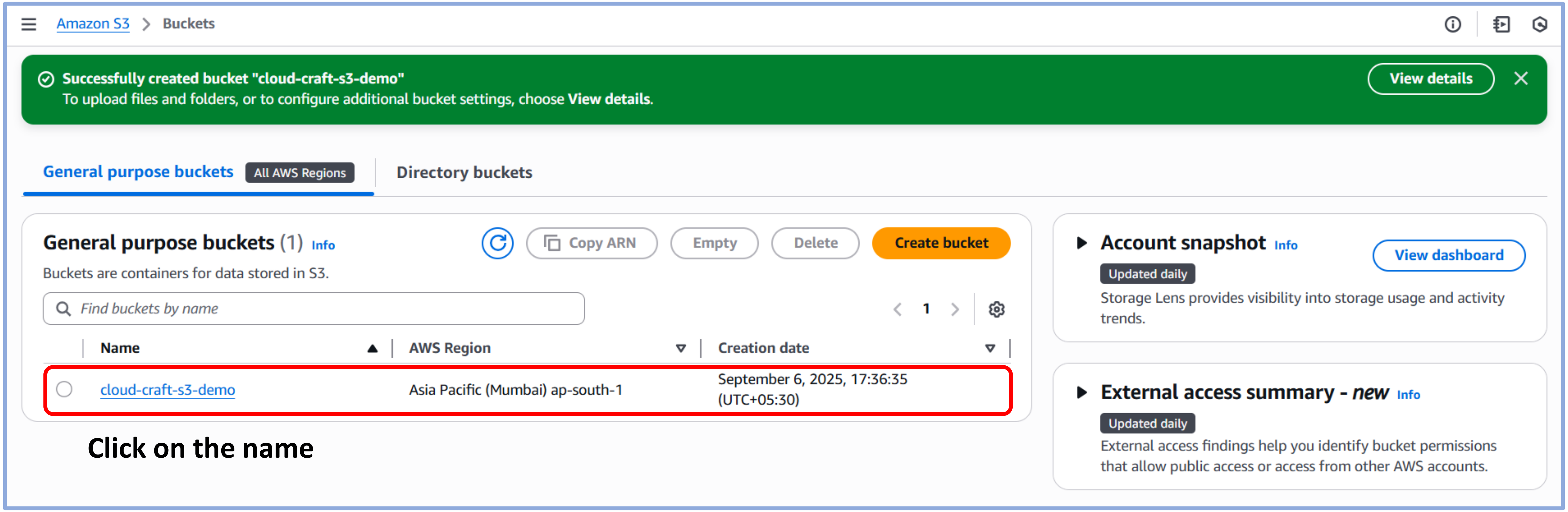
Bucket Key

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

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

The cloudCraft
From Clicks to Cloud Confidence
BY ASHAN DISSANAYAKE



Successfully created bucket "cloud-craft-s3-demo"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

General purpose buckets (1) Info

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	Creation date
○ cloud-craft-s3-demo	Asia Pacific (Mumbai) ap-south-1	September 6, 2025, 17:36:35 (UTC+05:30)

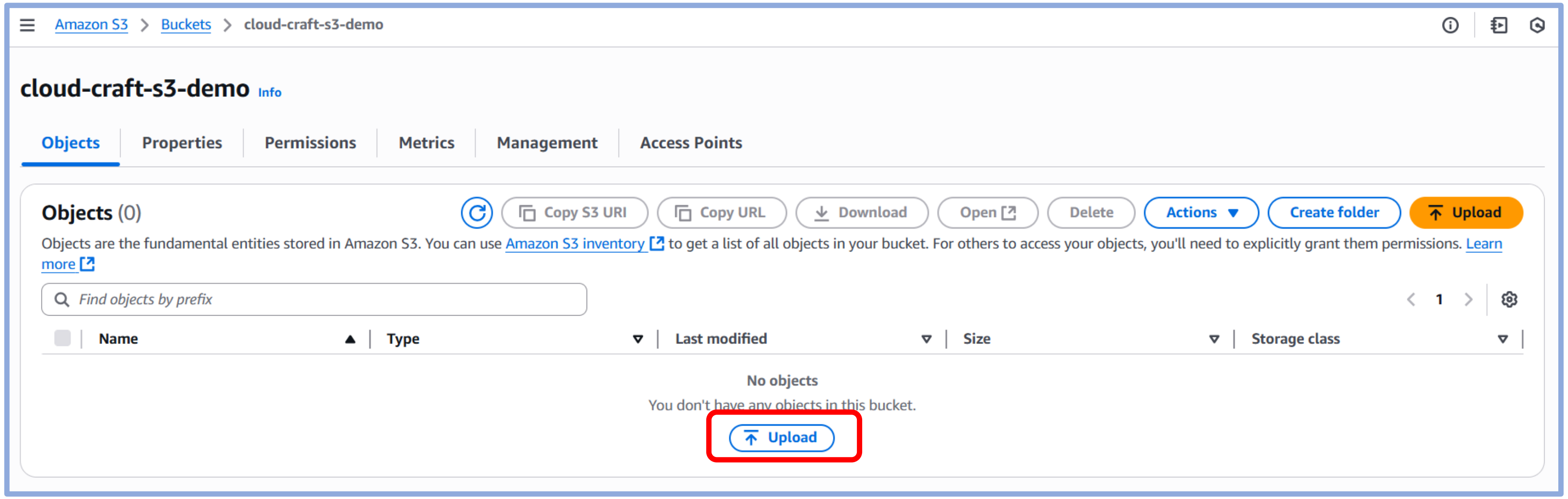
Account snapshot Info

Storage Lens provides visibility into storage usage and activity trends.

External access summary - *new* Info

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Click on the name



cloud-craft-s3-demo Info

Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

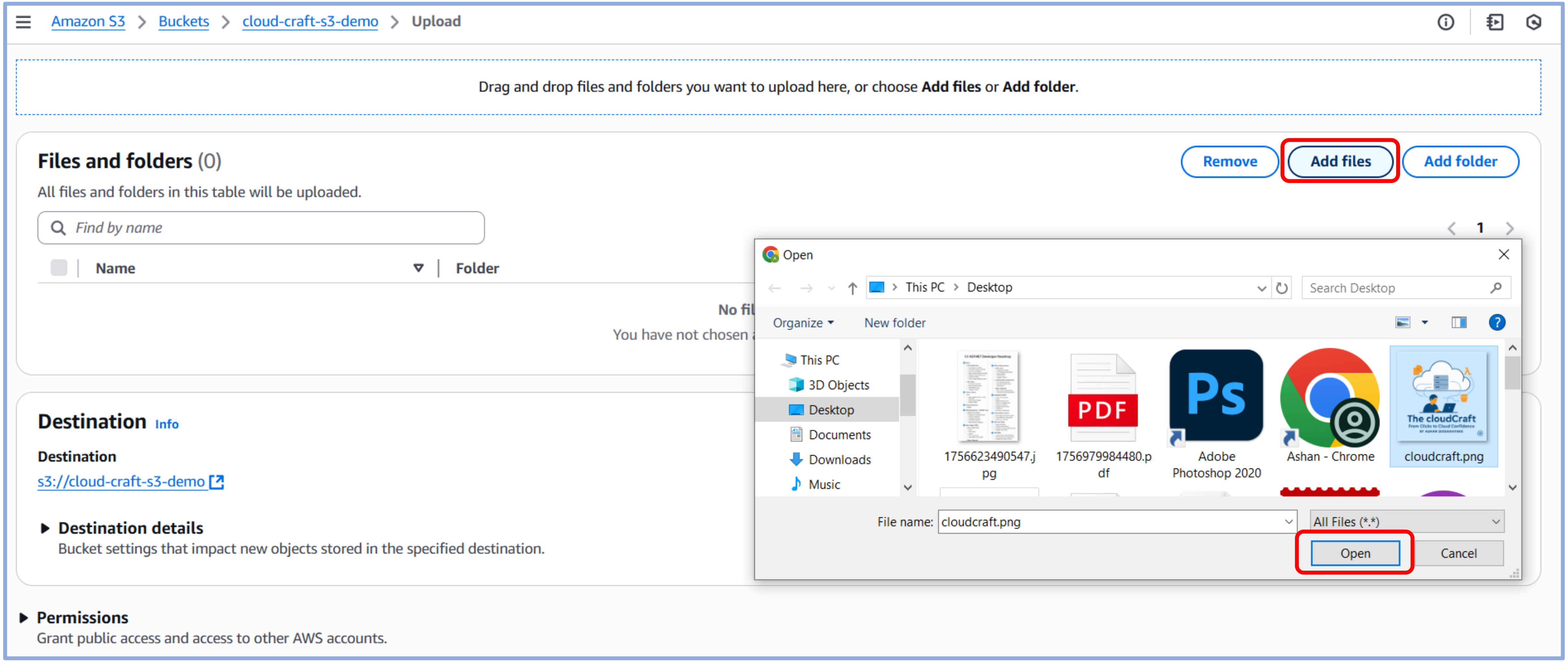
Find objects by prefix

Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

The cloudCraft
From Clicks to Cloud Confidence
BY ASHAN DISSANAYAKE



Amazon S3 > Buckets > cloud-craft-s3-demo > Upload

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (0)

All files and folders in this table will be uploaded.

Destination Info

Destination: s3://cloud-craft-s3-demo

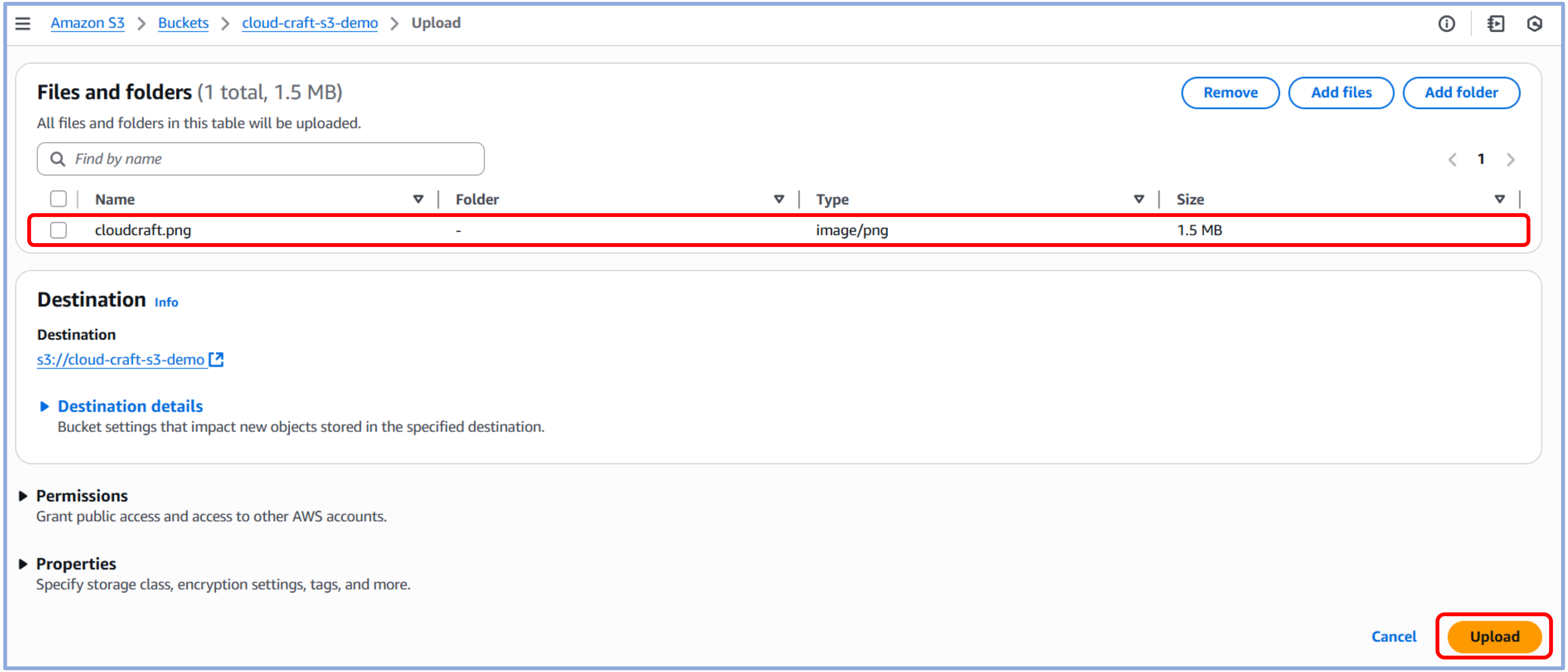
Destination details

Bucket settings that impact new objects stored in the specified destination.

Permissions

Grant public access and access to other AWS accounts.

File name: cloudcraft.png



Files and folders (1 total, 1.5 MB)

All files and folders in this table will be uploaded.

□	Name	Folder	Type	Size
□	cloudcraft.png	-	image/png	1.5 MB

Destination Info

Destination

s3://cloud-craft-s3-demo

▶ **Destination details**

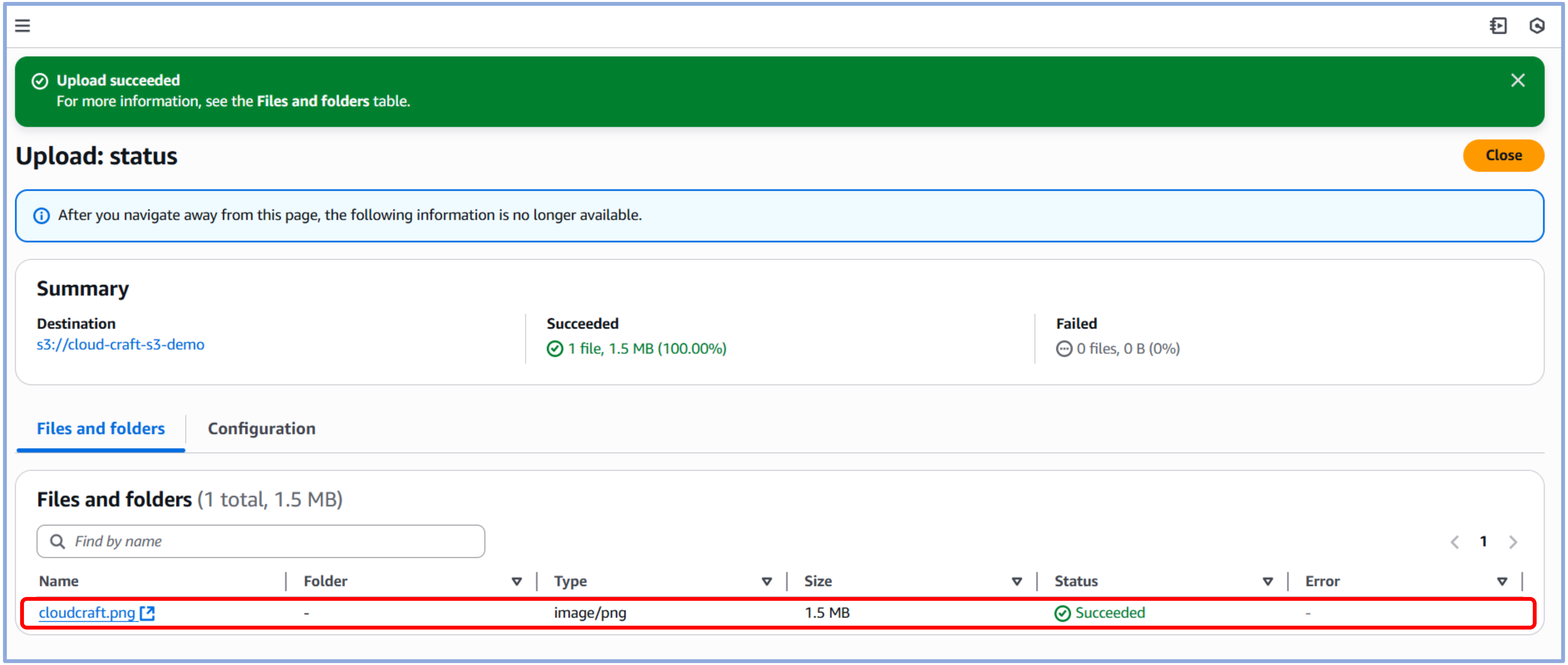
Bucket settings that impact new objects stored in the specified destination.

▶ **Permissions**

Grant public access and access to other AWS accounts.

▶ **Properties**

Specify storage class, encryption settings, tags, and more.



Upload succeeded
For more information, see the **Files and folders** table.

Upload: status

After you navigate away from this page, the following information is no longer available.

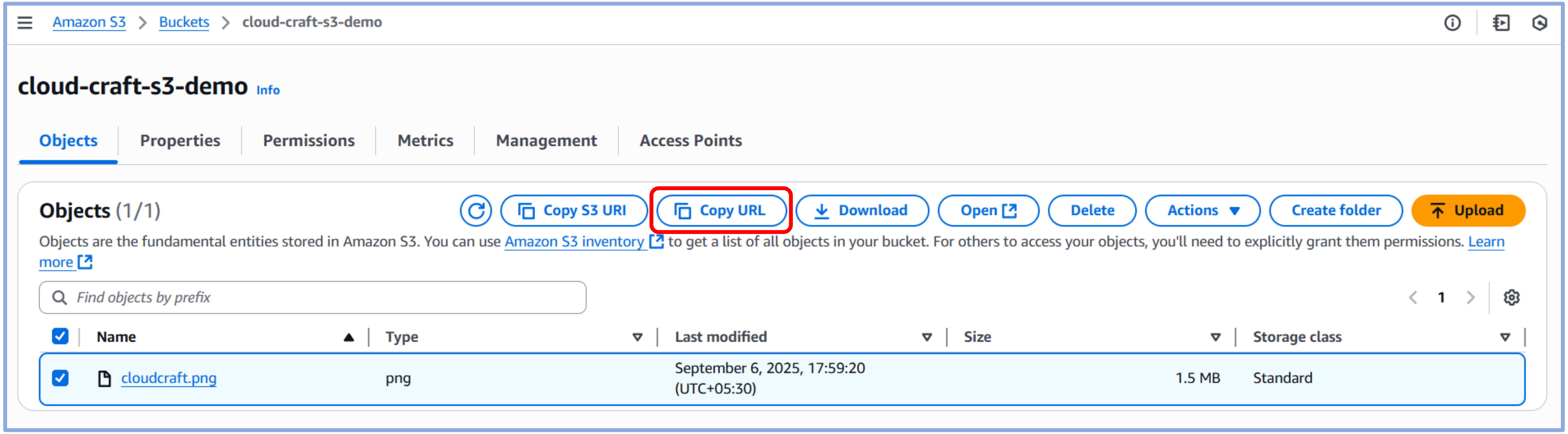
Summary

Destination	Succeeded	Failed
s3://cloud-craft-s3-demo	✓ 1 file, 1.5 MB (100.00%)	0 files, 0 B (0%)

Files and folders (1 total, 1.5 MB)

Name	Folder	Type	Size	Status	Error
cloudcraft.png	-	image/png	1.5 MB	✓ Succeeded	-

The cloudCraft
From Clicks to Cloud Confidence
BY ASHAN DISSANAYAKE



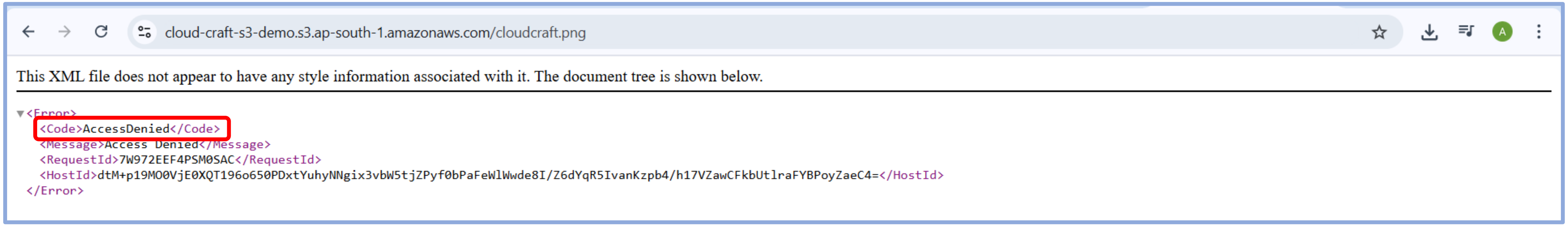
cloud-craft-s3-demo Info

Objects (1/1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

☑	Name	Type	Last modified	Size	Storage class
☑	cloudcraft.png	png	September 6, 2025, 17:59:20 (UTC+05:30)	1.5 MB	Standard

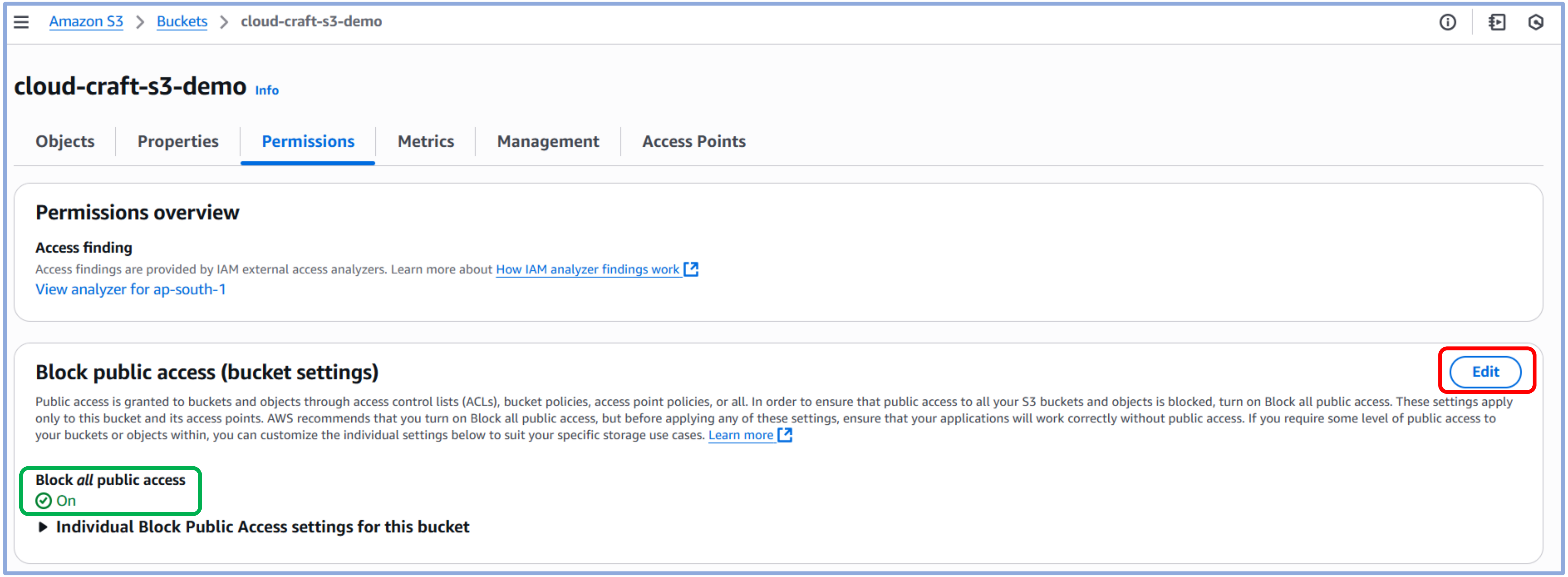

cloud-craft-s3-demo.s3.ap-south-1.amazonaws.com/cloudcraft.png

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>7W972EEF4PSM0SAC</RequestId>
  <HostId>dtM+p19MO0VjE0XQT196o650PDxtYuhyNNgix3vbW5tjZPyf0bPaFeWlWwde8I/Z6dYqR5IvanKzpb4/h17VZawCFkbUtlraFYBPoyZaeC4=</HostId>
</Error>
```

By default, AWS blocks public access on S3 buckets. This is a security safeguard to prevent accidental data leaks. If you want to share a file publicly, you’ll need to deliberately switch off this block for your bucket or object making sure you only do this for files meant to be shared.

Let's resolve the issue



Amazon S3 > Buckets > cloud-craft-s3-demo

cloud-craft-s3-demo Info

Objects | Properties | **Permissions** | Metrics | Management | Access Points

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work

View analyzer for ap-south-1

Block public access (bucket settings)

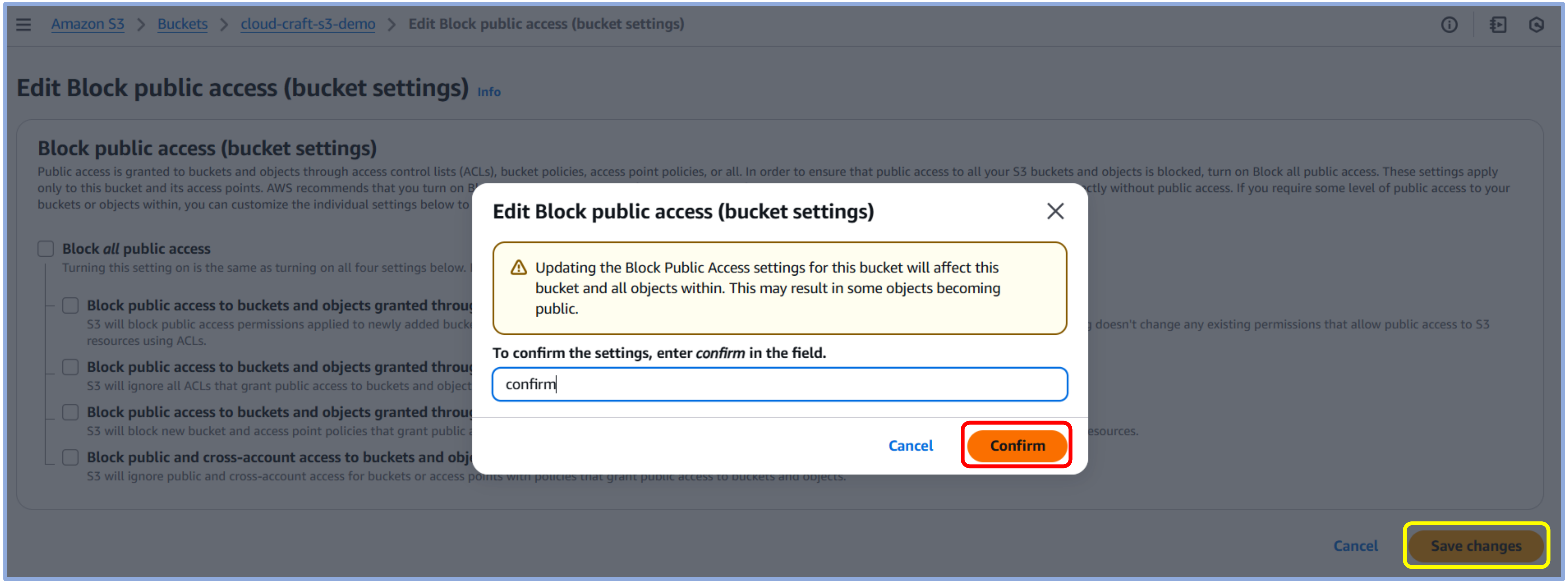
Edit

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
✓ On

▶ **Individual Block Public Access settings for this bucket**

The cloudCraft
From Clicks to Cloud Confidence
BY ASHAN DISSANAYAKE



Amazon S3 > Buckets > cloud-craft-s3-demo > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) Info

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 B… …ctly 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 …

☐ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. …

- ☐ **Block public access to buckets and objects granted throu…**
  S3 will block public access permissions applied to newly added buck… …doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted throu…**
  S3 will ignore all ACLs that grant public access to buckets and object…
- ☐ **Block public access to buckets and objects granted throu…**
  S3 will block new bucket and access point policies that grant public … …esources.
- ☐ **Block public and cross-account access to buckets and obj…**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Edit Block public access (bucket settings) ✕

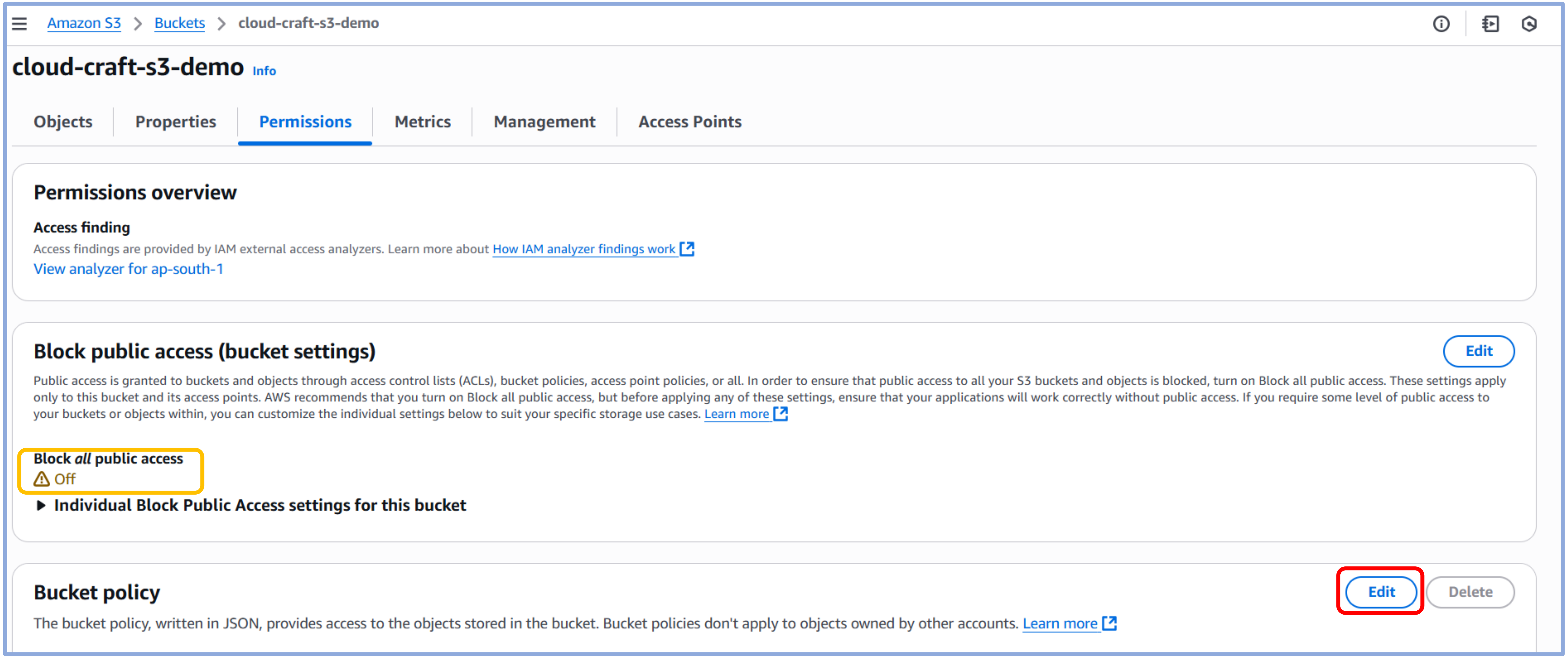
⚠ Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

confirm

Unticking all the Block Public Access options means you’re allowing this bucket and its files to be visible to anyone on the internet, if you give them the right permissions. Think of it as unlocking the door once it’s open, anyone can walk in unless you set rules to control who gets access

The cloudCraft
From Clicks to Cloud Confidence
BY ASHAN DISSANAYAKE



cloud-craft-s3-demo Info

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work

View analyzer for ap-south-1

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

Block *all* public access
⚠ Off

▶ **Individual Block Public Access settings for this bucket**

Bucket policy

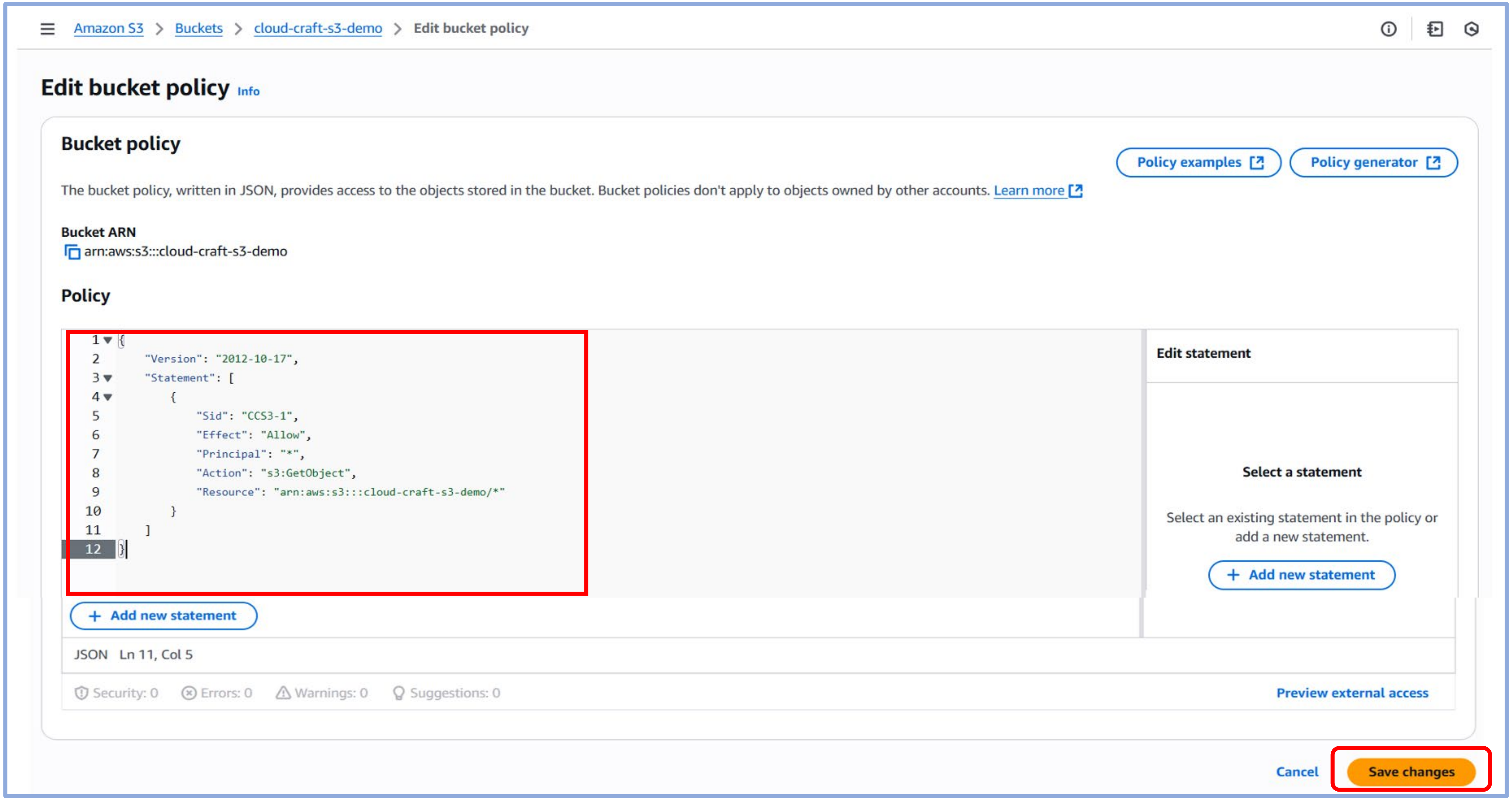
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Now that Block Public Access is off, you control accessibility through the bucket policy. The policy is like a rulebook you can decide whether only you, your team, or the whole internet can read the files inside the bucket

⚠ Warning to Add (Important for Beginners)

If you set the policy to allow public access, every object in the bucket could be visible on the internet. Always double-check you're only making the files public that you want to share.

The cloudCraft
From Clicks to Cloud Confidence
BY ASHAN DISSANAYAKE



Edit bucket policy

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.

Bucket ARN

arn:aws:s3:::cloud-craft-s3-demo

Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CCS3-1",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::cloud-craft-s3-demo/*"
        }
    ]
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

JSON Ln 11, Col 5

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0 Preview external access

The cloudCraft
From Clicks to Cloud Confidence
BY ASHAN DISSANAYAKE

Content of basic S3 Bucker policy

Version: Specifies the policy language version. 2012-10-17 is the latest and commonly used version.

- **Statement**: A list of individual permission rules.
- **Sid** ("Statement1"): Just an identifier for this statement, mainly for readability.
- **Effect**: Defines whether the action is allowed or denied.
- **Principal**: Who the policy applies to.
- **Action**: What operations are allowed.
- **Resource**: Specifies which bucket or objects this applies to.

Examples of valid S3 actions

Read actions

s3:GetObject → Download an object

s3:ListBucket → List objects inside a bucket

Write actions

s3:PutObject → Upload an object

s3:DeleteObject → Delete an object

Bucket-level actions

s3:CreateBucket

s3:DeleteBucket

s3:GetBucketPolicy

s3:PutBucketPolicy

Further more about actions

Understanding S3 Bucket Policies

Amazon S3 bucket policies are JSON-based rules that define **who can access your bucket** and **what they can do**. They are especially important when you want to allow or restrict access to objects stored in a bucket.

🔑 Structure of a Bucket Policy

A typical policy has these parts:

Version – policy language version (usually "2012-10-17")

Statement – one or more rules that define permissions

Sid – an optional identifier for the statement

Effect – Allow or Deny

Principal – who the policy applies to (* means public, everyone)

Action – what the user can do (e.g., s3:GetObject)

Resource – the bucket or objects the rule applies to

Condition – optional extra filters (like IP address or HTTPS-only access)

Bucket vs Object Resources

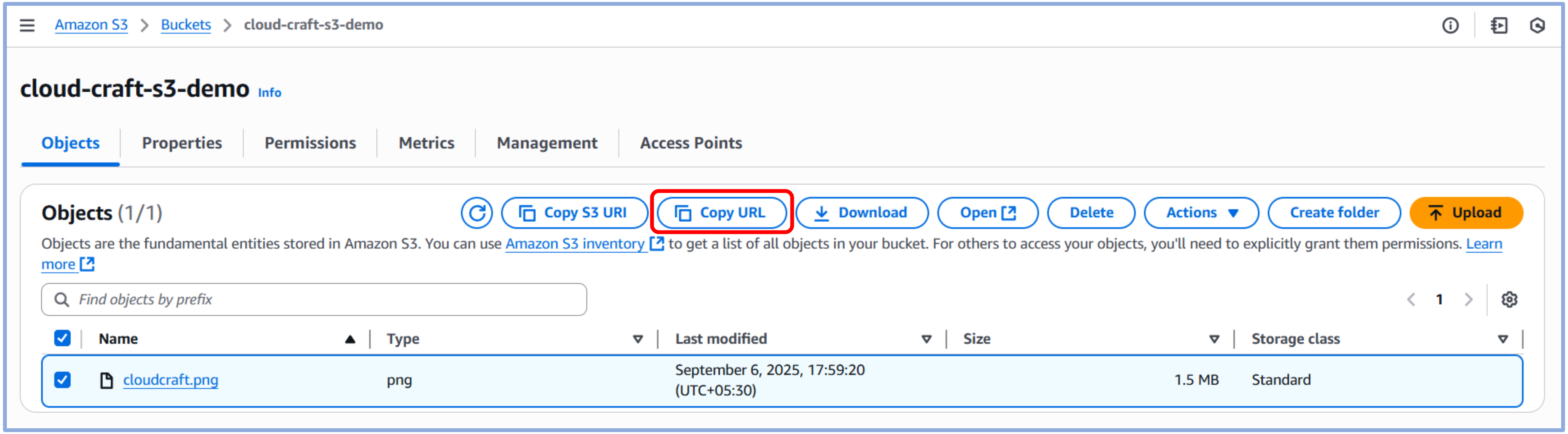
One of the most common sources of confusion is the difference between **bucket-level actions** and **object-level actions**.

- **Bucket-level actions** apply to the bucket itself (e.g., s3:ListBucket, s3:GetBucketPolicy)
  Must use bucket ARN: arn:aws:s3:::my-bucket
- **Object-level actions** apply to files inside the bucket (e.g., s3:GetObject, s3:PutObject)
  Must use object ARN: - arn:aws:s3:::my-bucket/*
- If you mix these up, you'll see the error:
  "Action does not apply to any resource(s) in statement"

Security Note

Granting public access ("Principal": "*" with "Effect": "Allow") means **anyone on the internet can read your files**. This is useful for hosting public websites or static assets.

For sensitive buckets, use IAM users, roles, or restrict access with conditions (e.g., IP address, VPC endpoint, HTTPS-only)

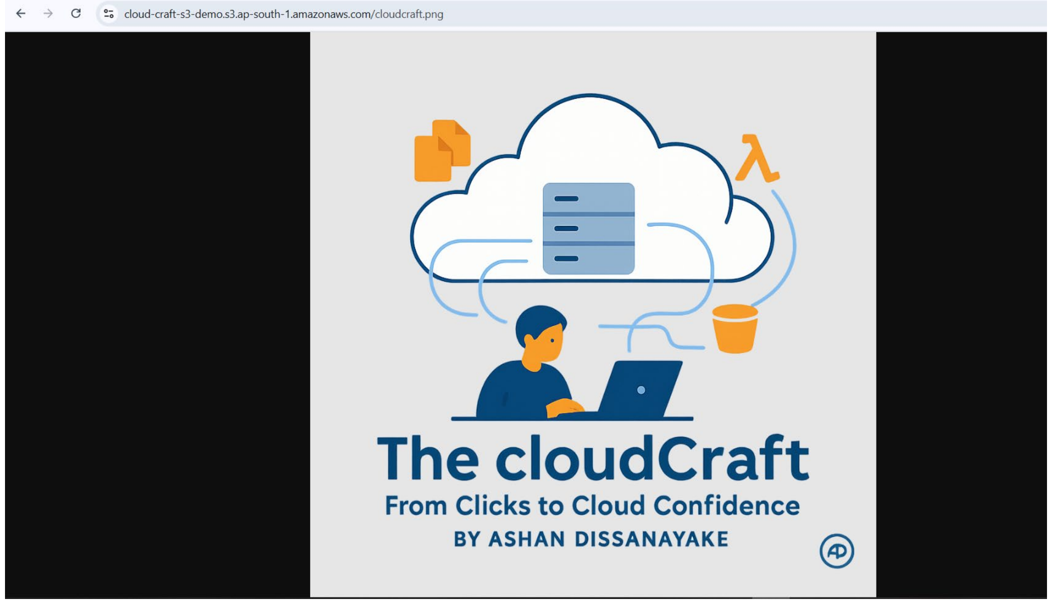


cloud-craft-s3-demo Info

Objects (1/1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

☑	Name ▲	Type	Last modified	Size	Storage class
☑	cloudcraft.png	png	September 6, 2025, 17:59:20 (UTC+05:30)	1.5 MB	Standard



cloud-craft-s3-demo.s3.ap-south-1.amazonaws.com/cloudcraft.png

Congratulations! You’ve unlocked the power of AWS S3, and this is only the beginning of your cloud journey