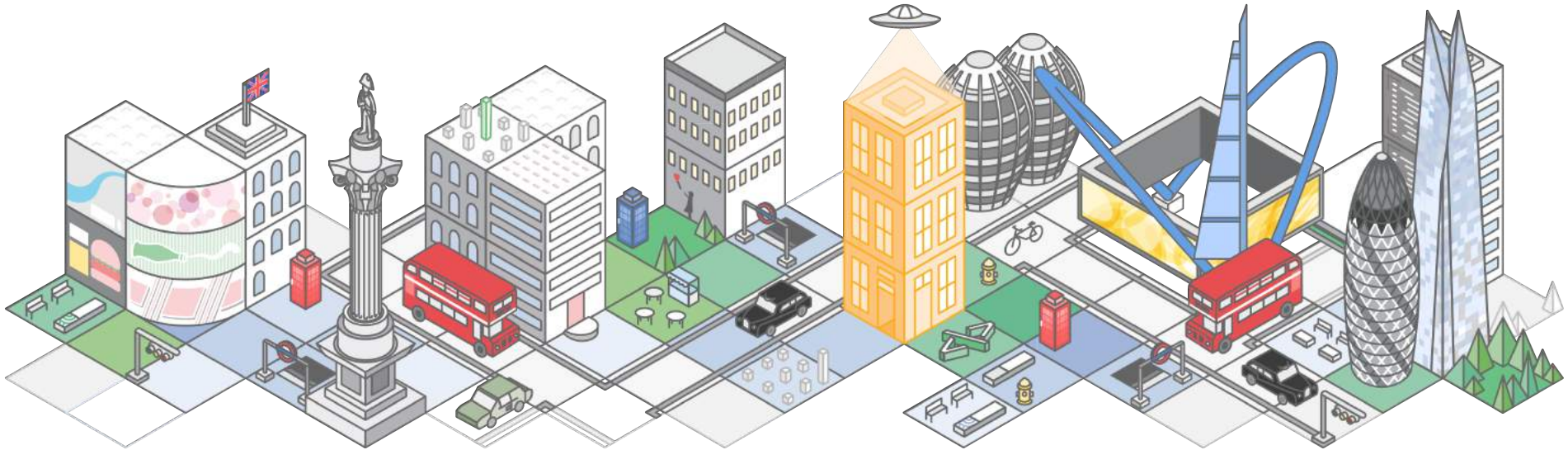


Amazon S3: Masterclass LIVE

Ian Massingham @IanMmmm
Chief Evangelist (EMEA), AWS

amazon web services | Pop-up Loft LONDON

Masterclass

1. A technical deep dive that goes beyond the basics
2. Intended to educate you on how to get the best from AWS services
3. Show you how things work and how to get things done

Amazon S3

Secure, durable, highly-scalable object storage

Accessible via a simple web services interface

Store & retrieve any amount of data

Use alone or together with other AWS services

Integrated

Low Cost

Durable

Available

Amazon S3

Easy to Use

Secure

Scalable

High Performance

Content Storage & Distribution

Backup & Archiving

Big Data Analytics

Amazon S3

Disaster Recovery

Static Website Hosting

Cloud-native Application Data

Agenda

Amazon S3 Concepts & Fundamentals

Namespaces

Access Controls

Storage Classes

Encryption & Other Security Features

Versioning & Cross-Region Replication

Lifecycle Rules

Website Hosting

AMAZON S3 CONCEPTS

BUCKETS

Containers for objects stored in S3

Serve several purposes:

- Organise the Amazon S3 namespace at the highest level
- Identify the account responsible for charges
- Play a role in access control
- Serve as the unit of aggregation for usage reporting

OBJECTS

Fundamental entities stored in Amazon S3

Consist of data & metadata

- Data portion is opaque to Amazon S3
- Metadata is a set of name-value pairs that describe the object
- Object is uniquely identified within a bucket by a key (name) and a version ID

http://doc.s3.amazonaws.com/2006-03-01/AmazonS3.wsdl

KEYS

Unique identifier for an object within a bucket.

Every object in a bucket has exactly one key

Combination of a bucket, key & version ID uniquely identify each object

REGIONS

The geographical region where Amazon S3 will store the buckets that you create

Choose a region to optimise latency, minimise costs, or address regulatory requirements.

Highly scalable data storage

A web store, not a file system

Access via APIs

AMAZON S3 FUNDAMENTALS

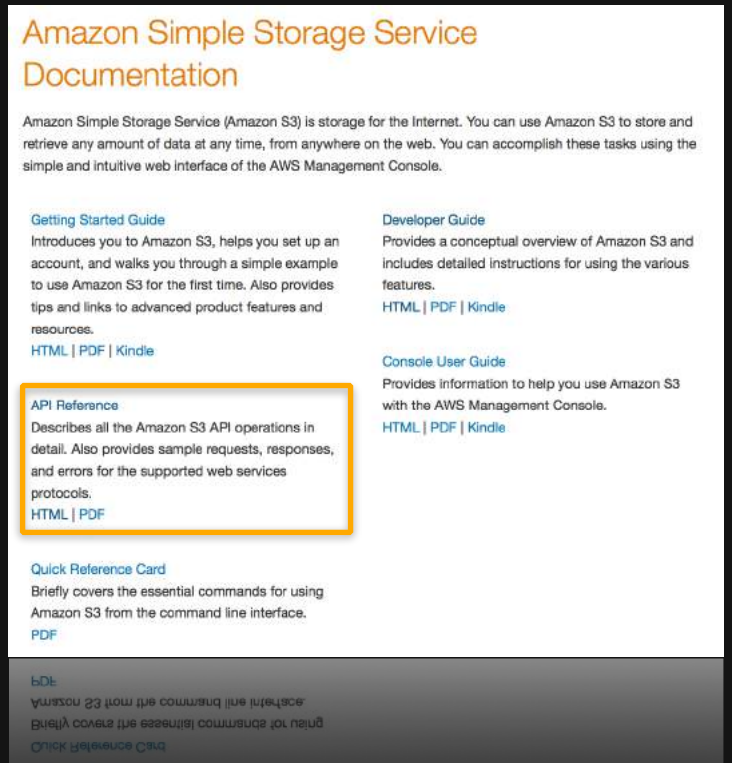
Fast

Economical

Highly available & durable

http://aws.amazon.com/documentation/s3/

Access via APIs



Amazon Simple Storage Service Documentation

Amazon Simple Storage Service (Amazon S3) is storage for the Internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web. You can accomplish these tasks using the simple and intuitive web interface of the AWS Management Console.

Getting Started Guide
Introduces you to Amazon S3, helps you set up an account, and walks you through a simple example to use Amazon S3 for the first time. Also provides tips and links to advanced product features and resources.
HTML | PDF | Kindle

Developer Guide
Provides a conceptual overview of Amazon S3 and includes detailed instructions for using the various features.
HTML | PDF | Kindle

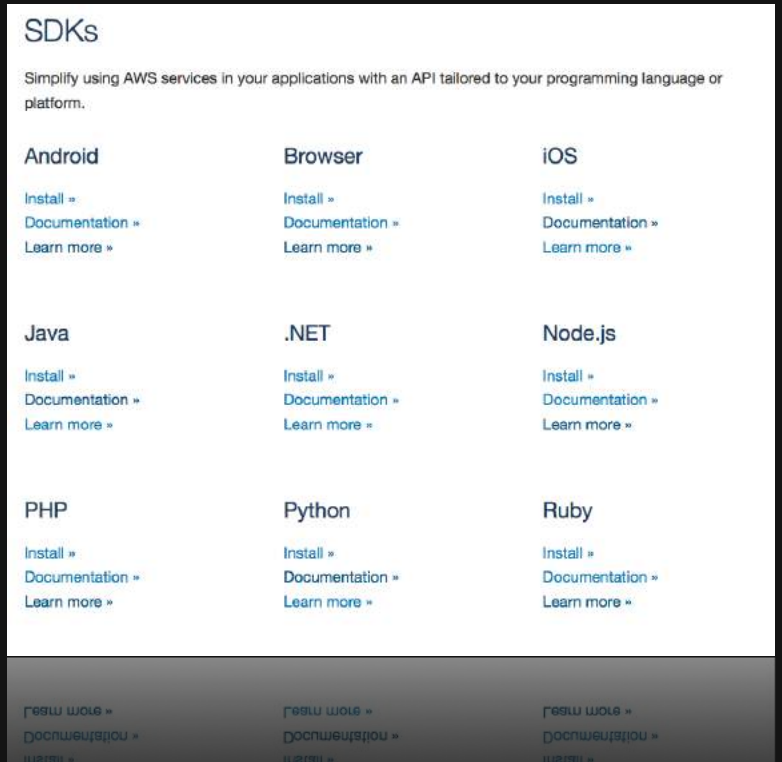
API Reference
Describes all the Amazon S3 API operations in detail. Also provides sample requests, responses, and errors for the supported web services protocols.
HTML | PDF

Console User Guide
Provides information to help you use Amazon S3 with the AWS Management Console.
HTML | PDF | Kindle

Quick Reference Card
Briefly covers the essential commands for using Amazon S3 from the command line interface.
PDF

http://aws.amazon.com/tools/

Access via SDKs



SDKs

Simplify using AWS services in your applications with an API tailored to your programming language or platform.

Android

Install »
Documentation »
Learn more »

Browser

Install »
Documentation »
Learn more »

iOS

Install »
Documentation »
Learn more »

Java

Install »
Documentation »
Learn more »

.NET

Install »
Documentation »
Learn more »

Node.js

Install »
Documentation »
Learn more »

PHP

Install »
Documentation »
Learn more »

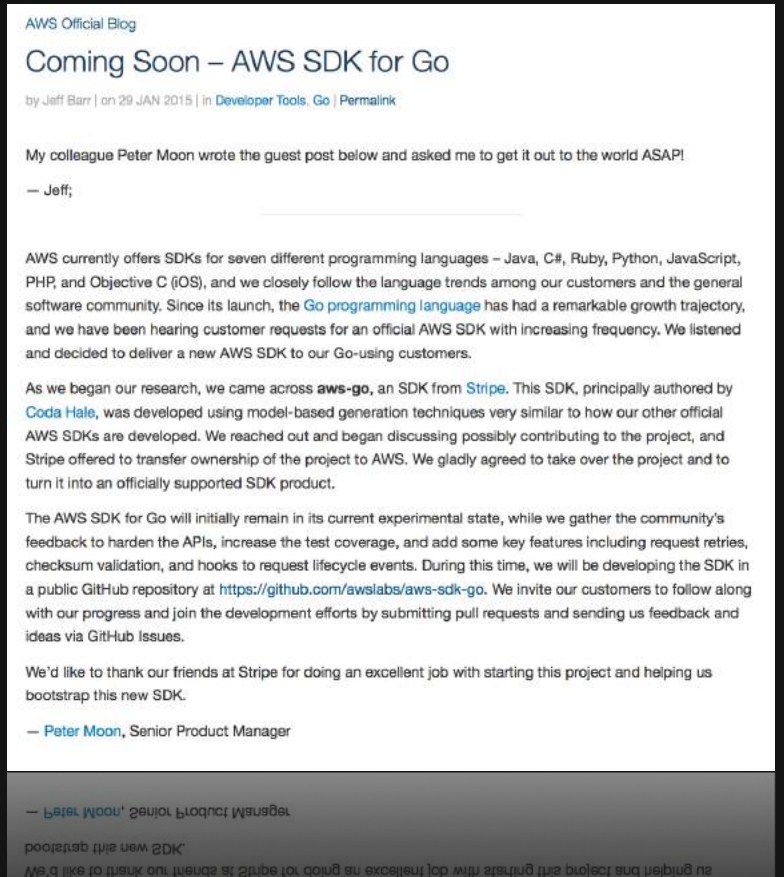
Python

Install »
Documentation »
Learn more »

Ruby

Install »
Documentation »
Learn more »

https://github.com/awslabs/aws-sdk-go



AWS Official Blog

Coming Soon – AWS SDK for Go

by Jeff Barr | on 29 JAN 2015 | in Developer Tools, Go | Permalink

My colleague Peter Moon wrote the guest post below and asked me to get it out to the world ASAP!

— Jeff;

AWS currently offers SDKs for seven different programming languages – Java, C#, Ruby, Python, JavaScript, PHP, and Objective C (iOS), and we closely follow the language trends among our customers and the general software community. Since its launch, the Go programming language has had a remarkable growth trajectory, and we have been hearing customer requests for an official AWS SDK with increasing frequency. We listened and decided to deliver a new AWS SDK to our Go-using customers.

As we began our research, we came across **aws-go**, an SDK from Stripe. This SDK, principally authored by Coda Hale, was developed using model-based generation techniques very similar to how our other official AWS SDKs are developed. We reached out and began discussing possibly contributing to the project, and Stripe offered to transfer ownership of the project to AWS. We gladly agreed to take over the project and to turn it into an officially supported SDK product.

The AWS SDK for Go will initially remain in its current experimental state, while we gather the community's feedback to harden the APIs, increase the test coverage, and add some key features including request retries, checksum validation, and hooks to request lifecycle events. During this time, we will be developing the SDK in a public GitHub repository at https://github.com/awslabs/aws-sdk-go. We invite our customers to follow along with our progress and join the development efforts by submitting pull requests and sending us feedback and ideas via GitHub Issues.

We'd like to thank our friends at Stripe for doing an excellent job with starting this project and helping us bootstrap this new SDK.

— Peter Moon, Senior Product Manager

Access via SDKs

AWS CLI

Access via AWS CLI

List buckets

Copy a file to an object

List buckets contents

Stream the contents of an object to STDOUT

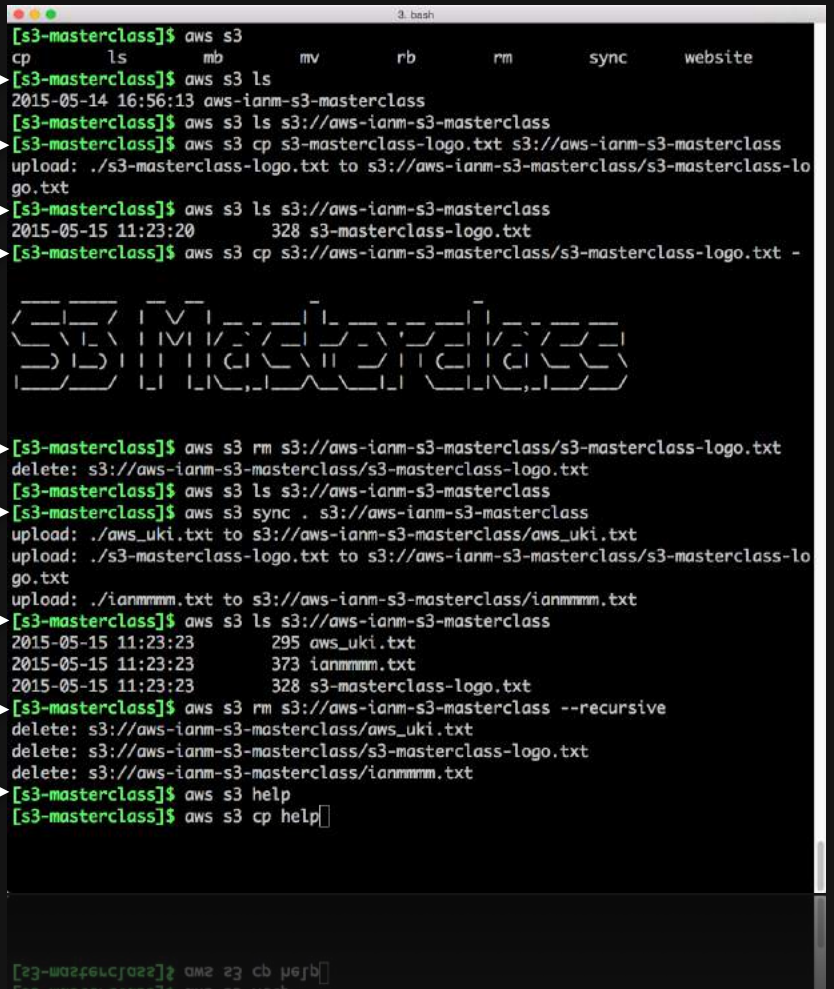
Delete an object

Sync a directory with a bucket

List buckets contents

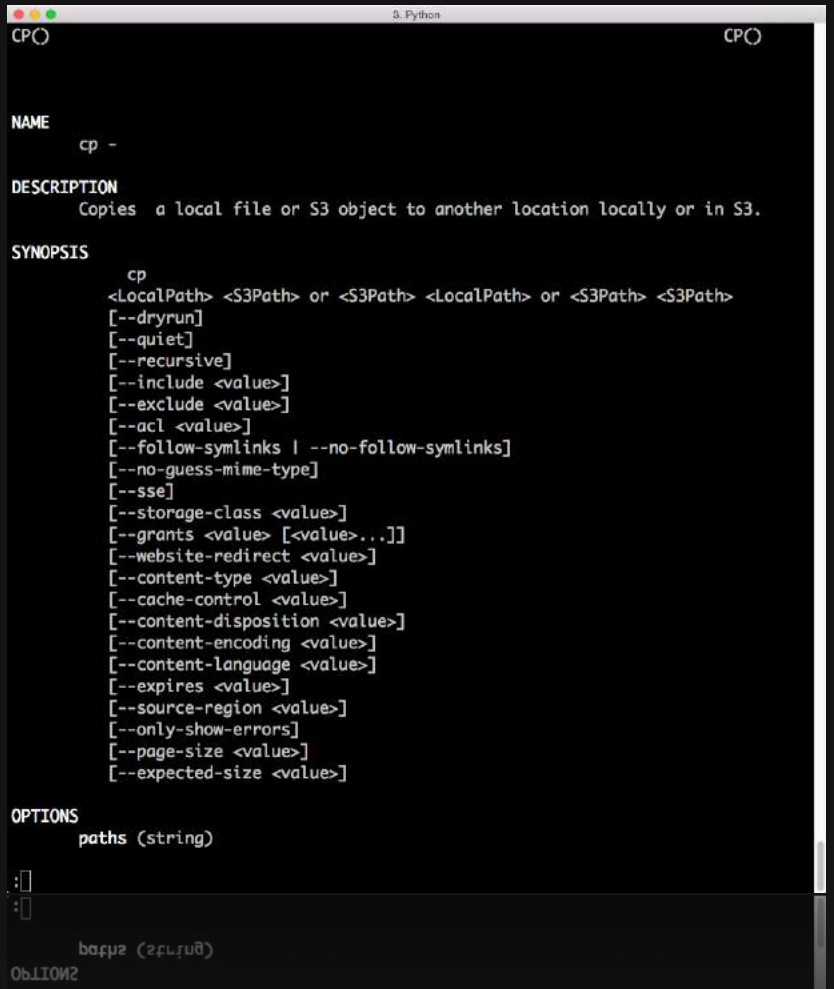
Delete buckets contents

AWS S3 CLI help



AWS CLI

Detailed help on a specific command



Access via AWS CLI

Highly scalable data storage

A web store, not a file system

Access via APIs

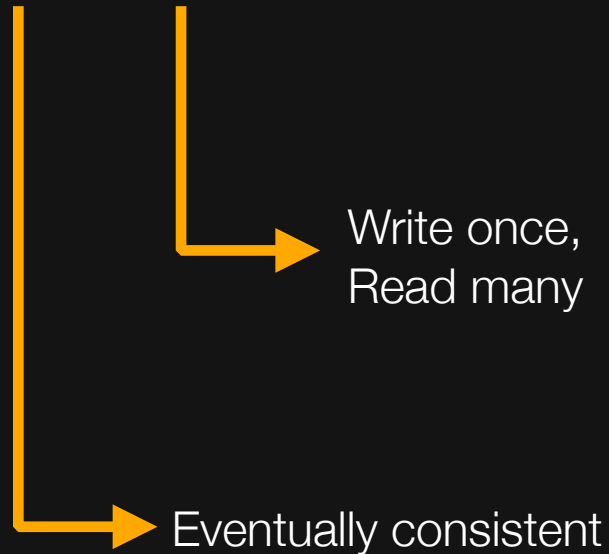
AMAZON S3 FUNDAMENTALS

Fast

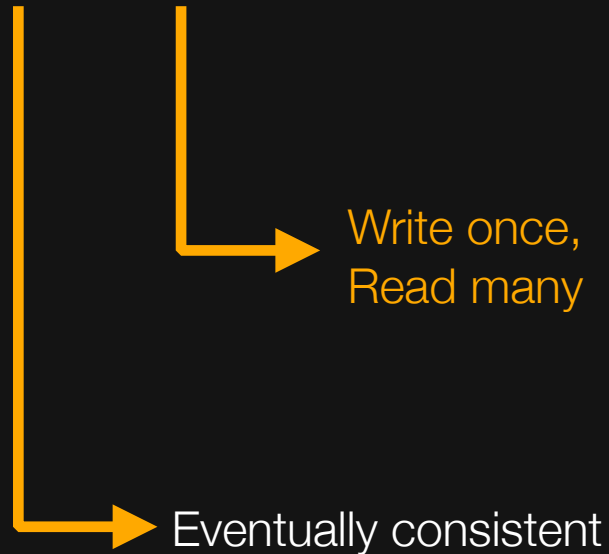
Economical

Highly available & durable

A web store, not a file system



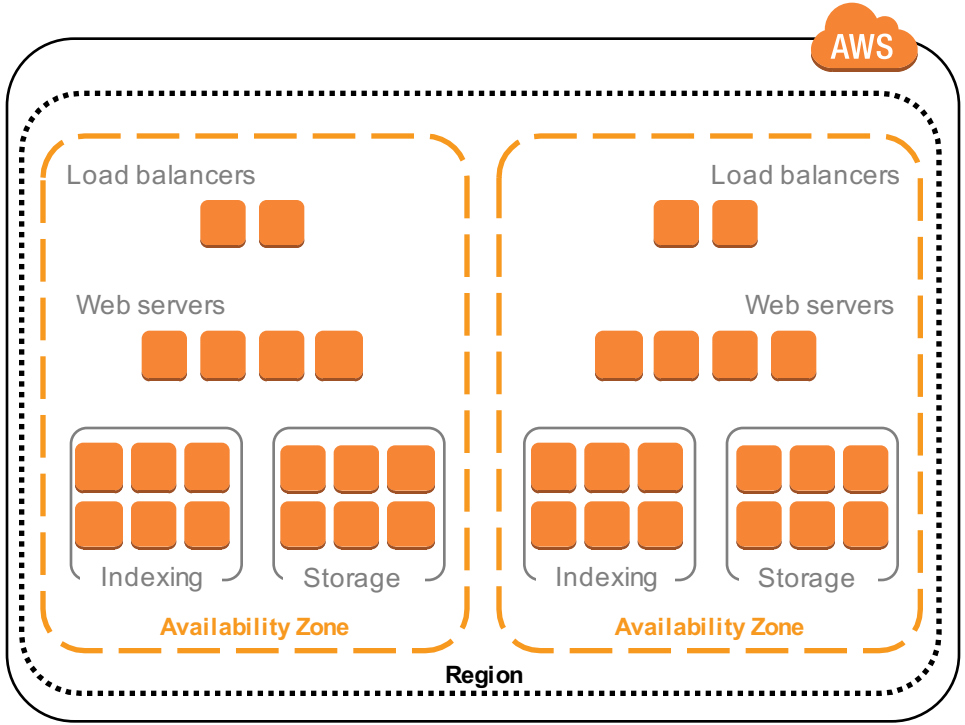
A web store, not a file system



A web store, not a file system

Write once,
Read many

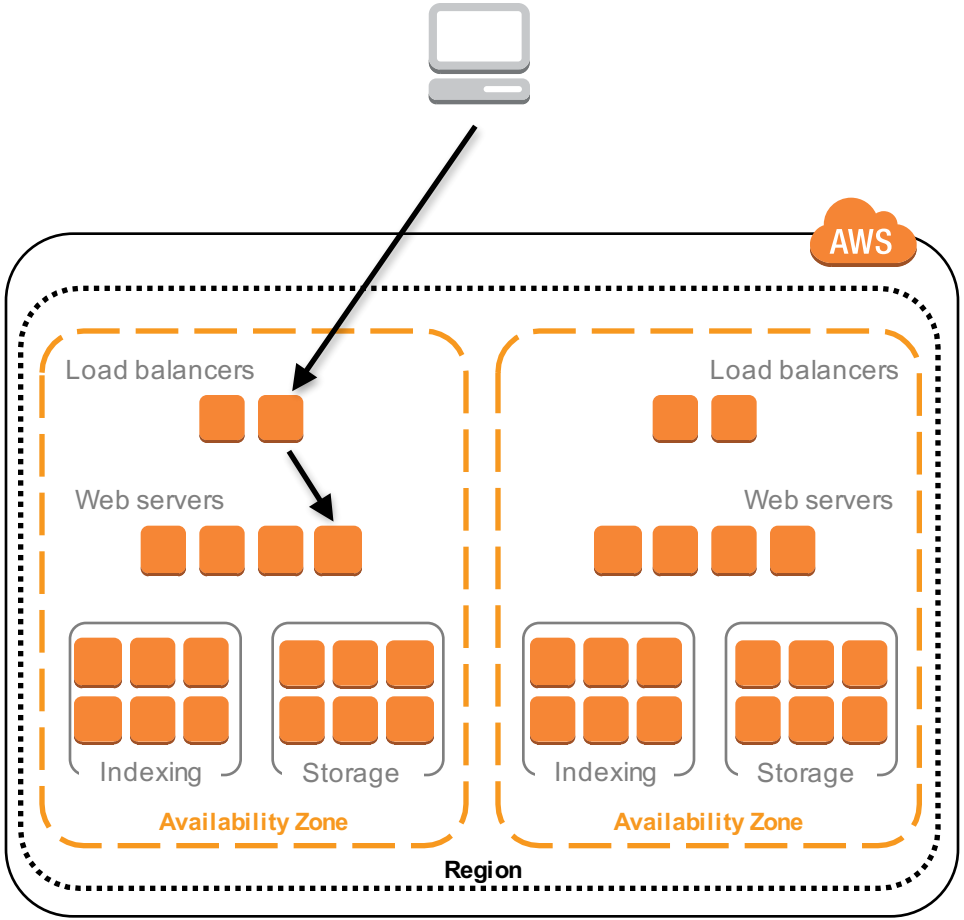
Eventually consistent



A web store, not a file system

Write once,
Read many

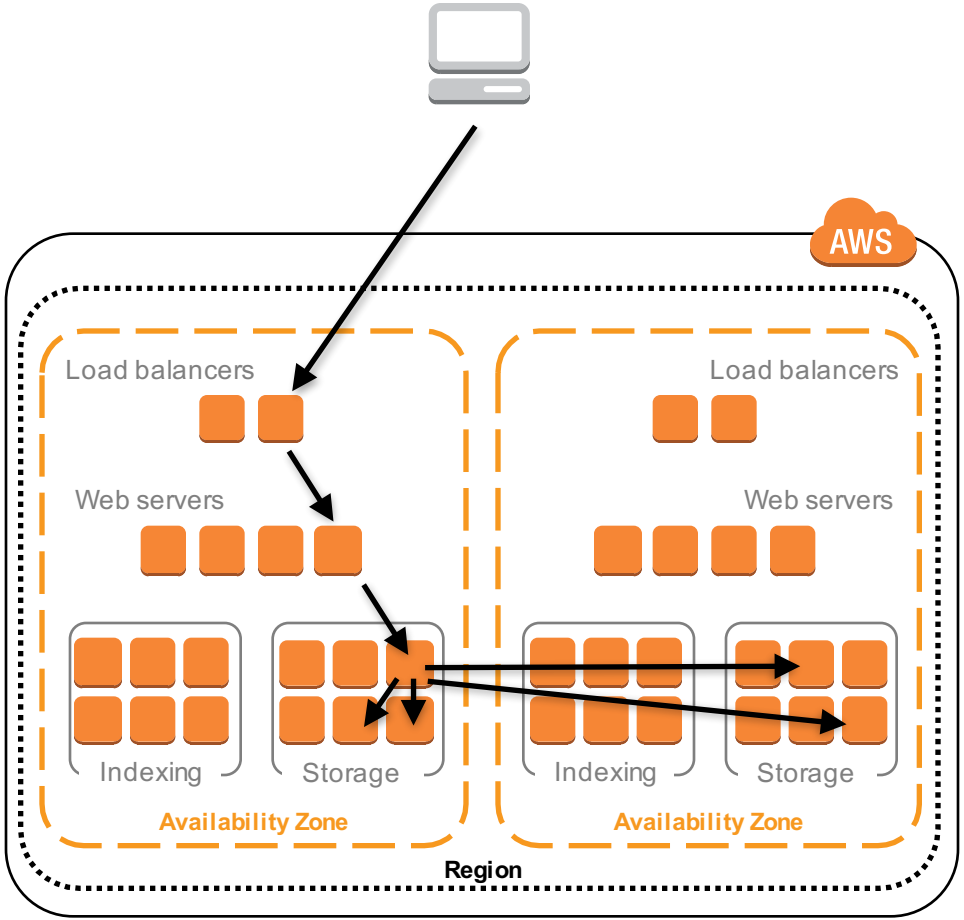
Eventually consistent



A web store, not a file system

Write once,
Read many

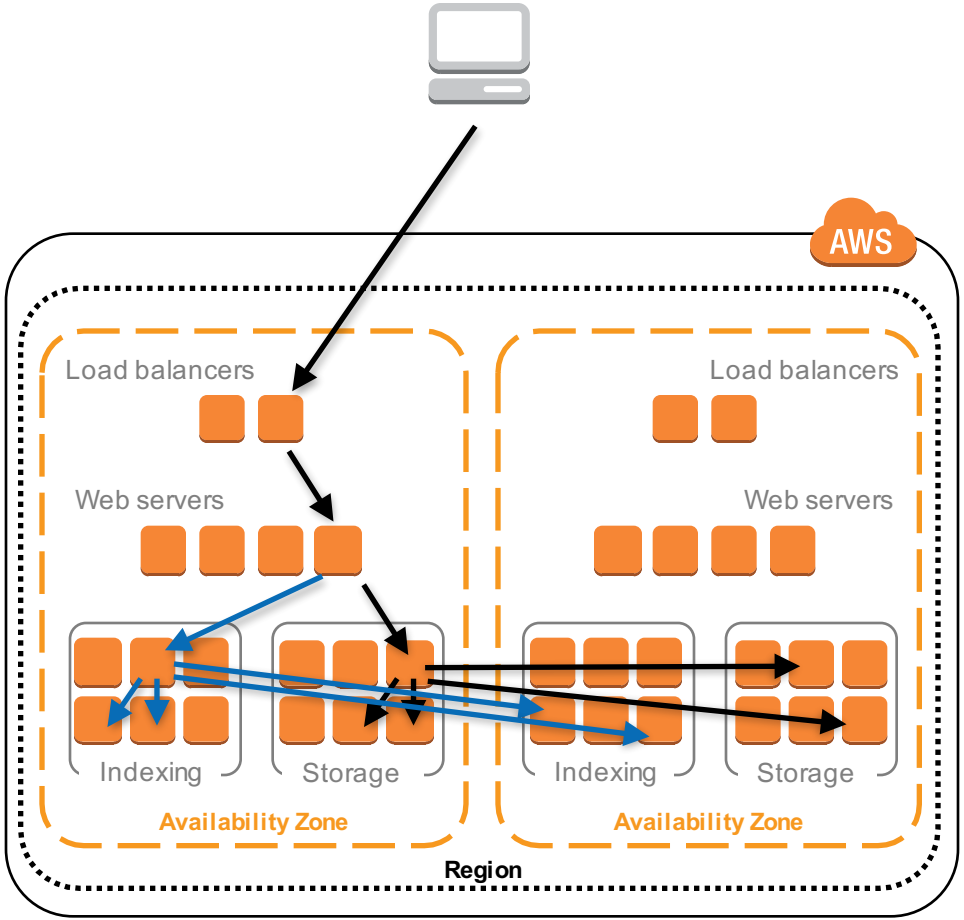
Eventually consistent



A web store, not a file system

Write once,
Read many

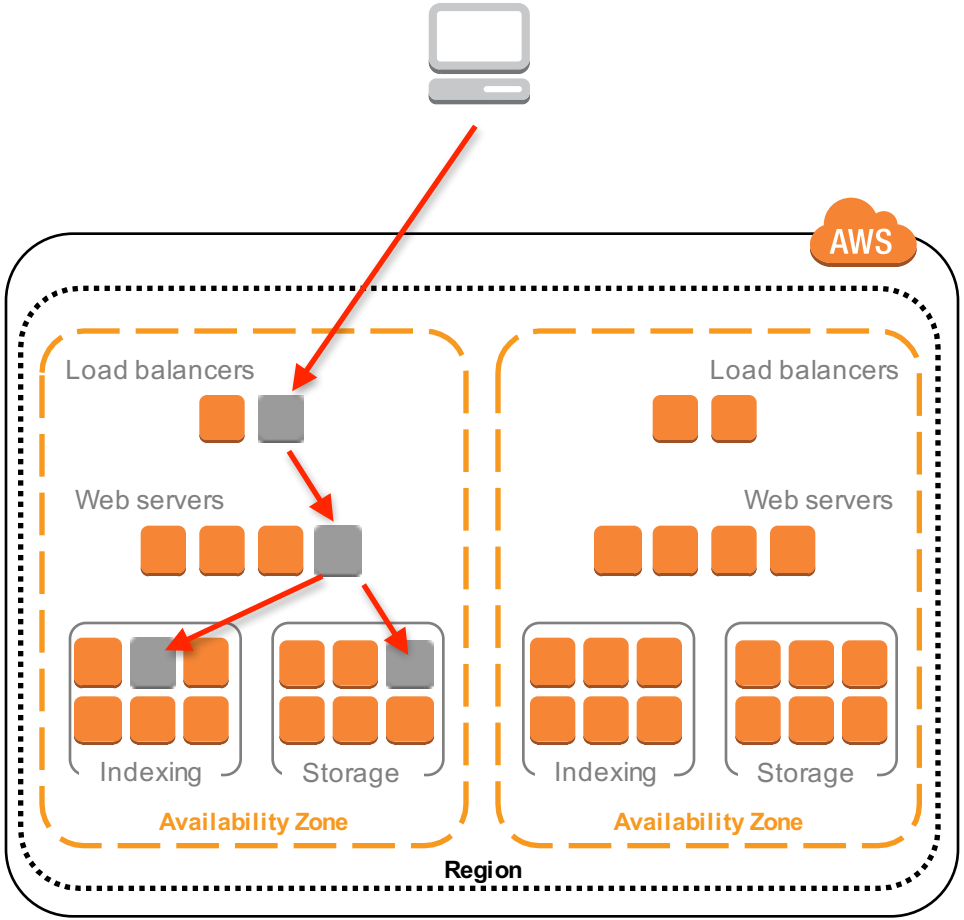
Eventually consistent



A web store, not a file system

Write once,
Read many

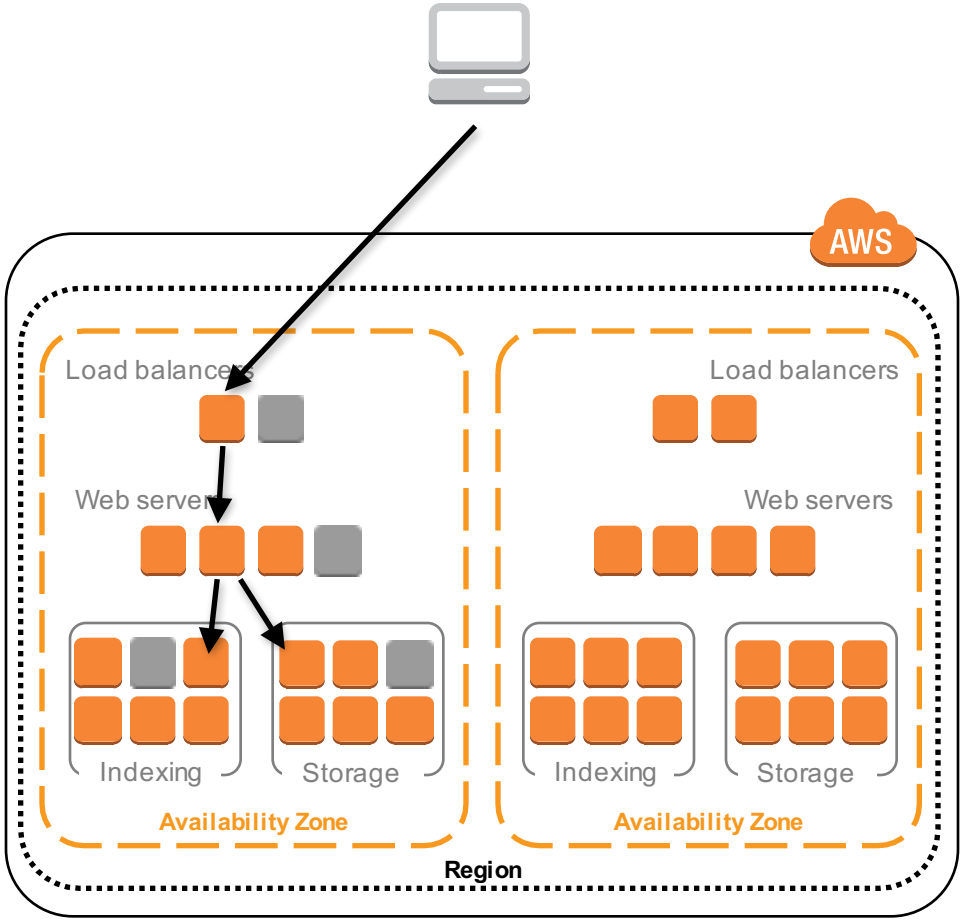
Eventually consistent



A web store, not a file system

Write once,
Read many

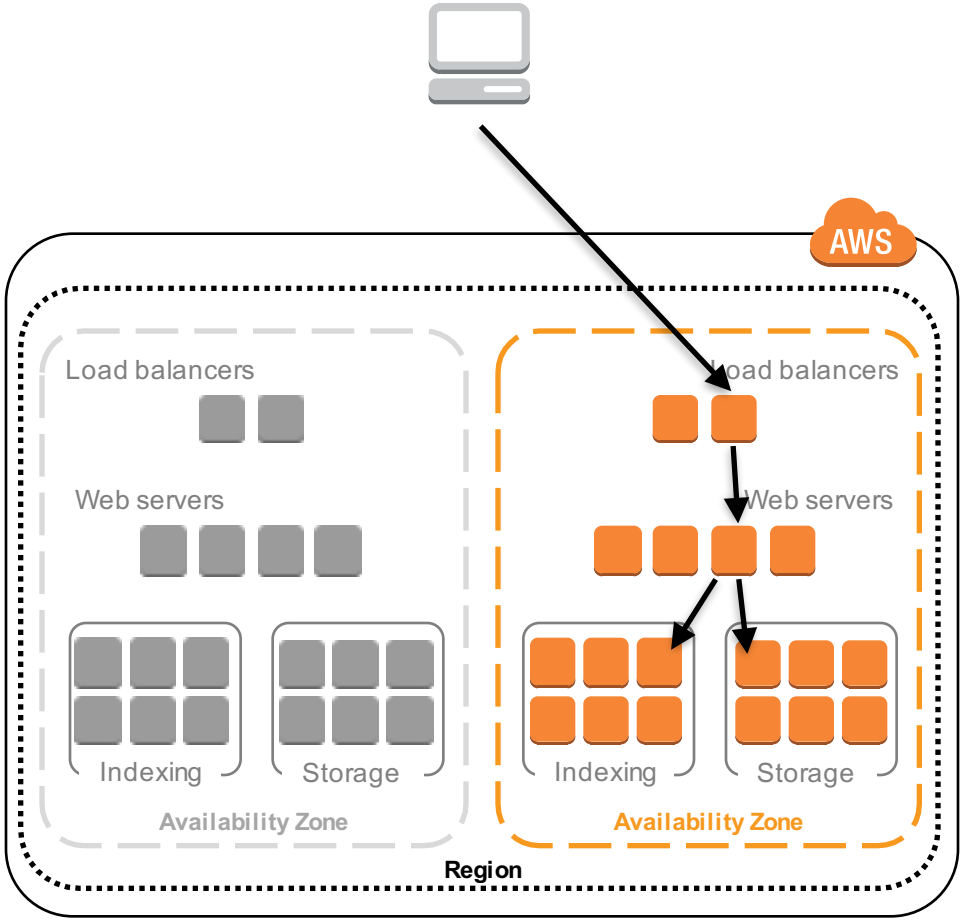
Eventually consistent



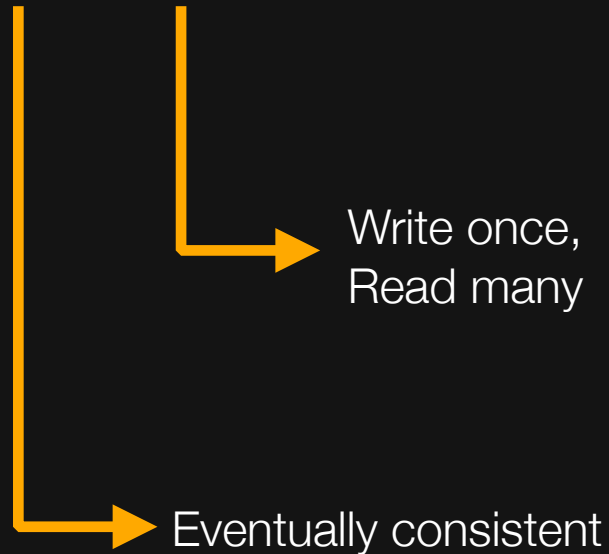
A web store, not a file system

Write once,
Read many

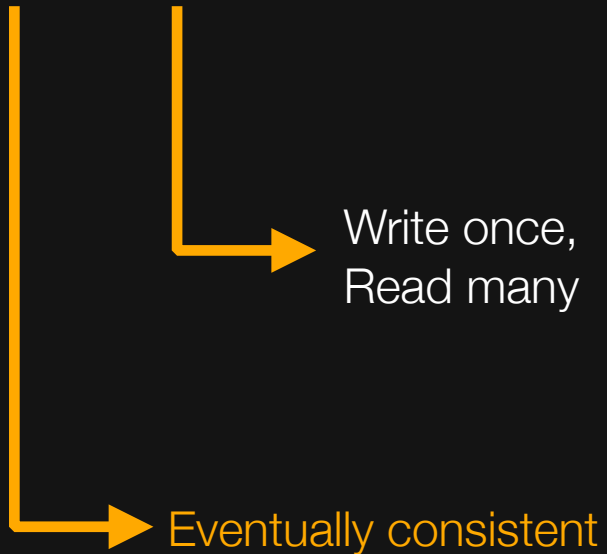
Eventually consistent



A web store, not a file system



A web store, not a file system



New Objects

Synchronously stores your data across multiple facilities before returning SUCCESS

Updates

Write then read: could report key does not exist
Write then list: might not include key in list
Overwrite then read: old data could be returned

Deletes

Delete then read: could still get old data
Delete then list: deleted key could be included in list

Find out more here: docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html

NAMESPACES

Globally Unique

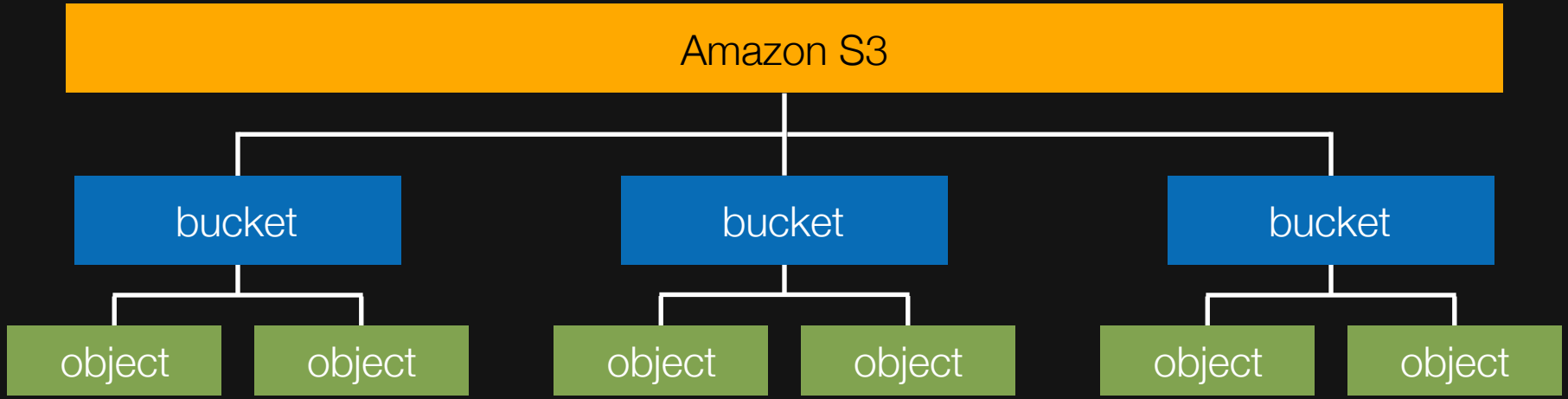
↓

Bucket Name + Object Name (key)

Globally Unique

↓

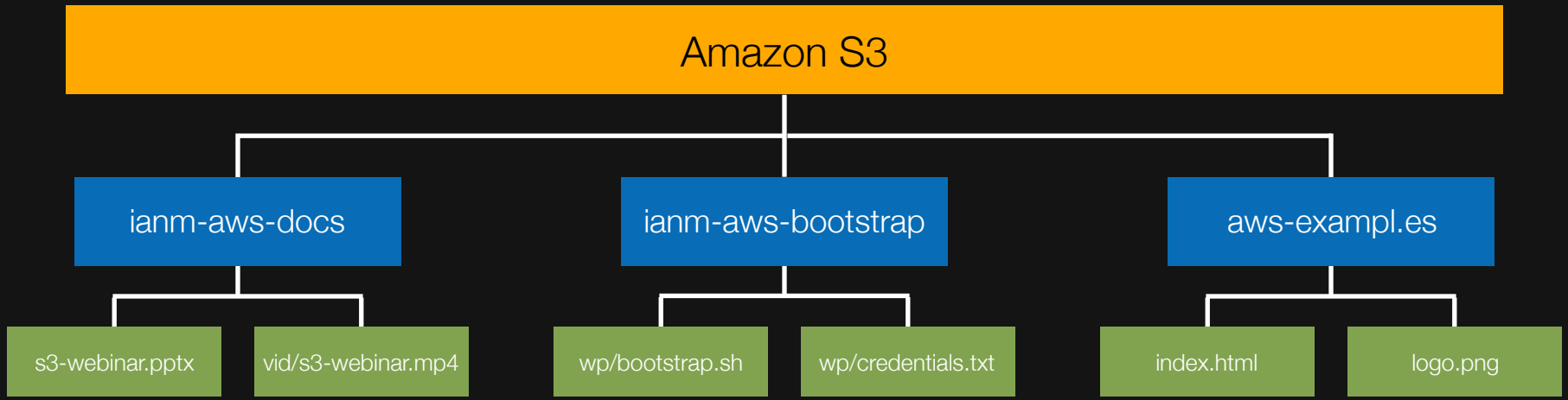
Bucket Name + Object Name (key)



Globally Unique

↓

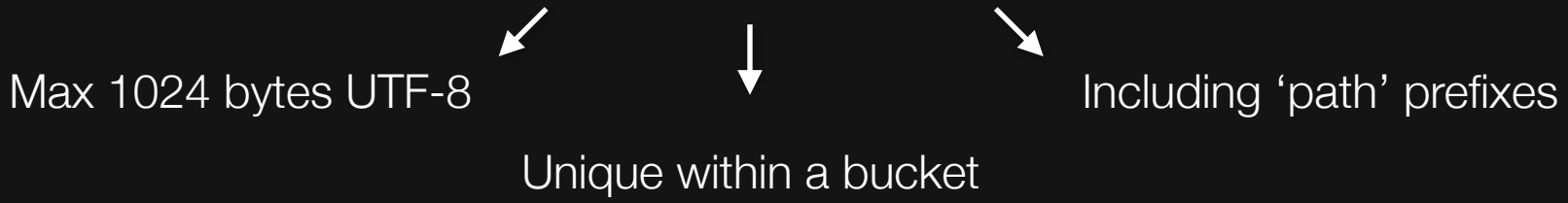
Bucket Name + Object Name (key)



Object key

Unique within a bucket

Object key


Max 1024 bytes UTF-8
Unique within a bucket
Including ‘path’ prefixes

Object key

Max 1024 bytes UTF-8

Unique within a bucket

Including ‘path’ prefixes

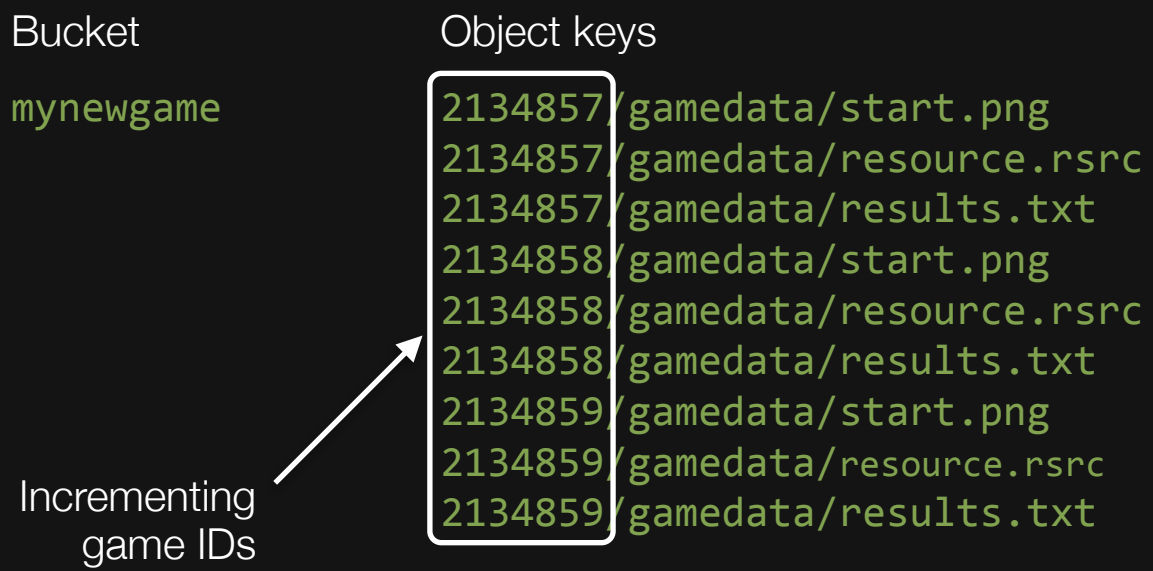
Throughput Optimisation

S3 automatically partitions based upon key prefix:

Bucket	Object keys
mynewgame	2134857/gamedata/start.png 2134857/gamedata/resource.rsrc 2134857/gamedata/results.txt 2134858/gamedata/start.png 2134858/gamedata/resource.rsrc 2134858/gamedata/results.txt 2134859/gamedata/start.png 2134859/gamedata/resource.rsrc 2134859/gamedata/results.txt

Throughput Optimisation

S3 automatically partitions based upon key prefix:



Throughput Optimisation

S3 automatically partitions based upon key prefix:

Throughput Optimisation

S3 automatically partitions based upon key prefix:

Throughput Optimisation

S3 automatically partitions based upon key prefix:

ACCESS CONTROLS

You decide what to share

Apply policies to buckets and objects

SECURE BY DEFAULT

Policies, ACLs & IAM

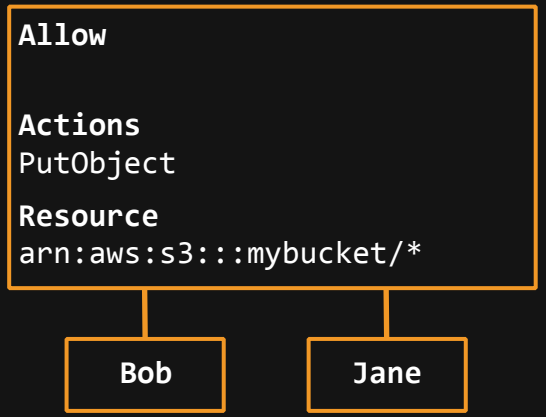
Use S3 policies, ACLs or IAM to define rules

IAM Policies

Fine grained

Administer as part of role based access

Apply policies to S3 at role, user & group level



Announcing AWS Identity and Access Management (IAM) - Preview Beta

Posted On: Sep 2, 2010

We're pleased to release today a Preview Beta of a new AWS feature: AWS Identity and Access Management (IAM). IAM enables you to create multiple Users and manage the permissions for each of these Users within your AWS Account. A User is an identity (within your AWS Account) with unique security credentials that can be used to access AWS Services. IAM eliminates the need to share passwords or access keys, and makes it easy to enable or disable a User's access as appropriate. IAM offers you greater flexibility, control and security when using AWS.

We are excited to offer you early access to this new functionality. As part of this Preview Beta, we are enabling you to programmatically add Users to your AWS Account, set groups and permissions for these Users, and enable your Users to call AWS Service APIs.

In the near future, we plan on adding support for your Users to login to the AWS Management Console. We also plan to extend the AWS Management Console to support IAM, providing a web-based interface to manage your Users, groups, and permissions.

Learn more about AWS Identity and Access Management Preview Beta at: http://aws.amazon.com/iam

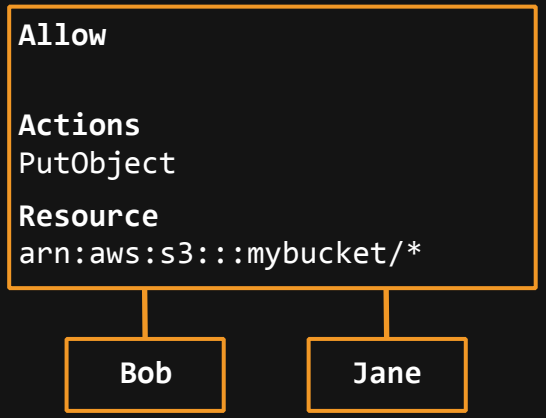
Find out more here: aws.amazon.com/iam

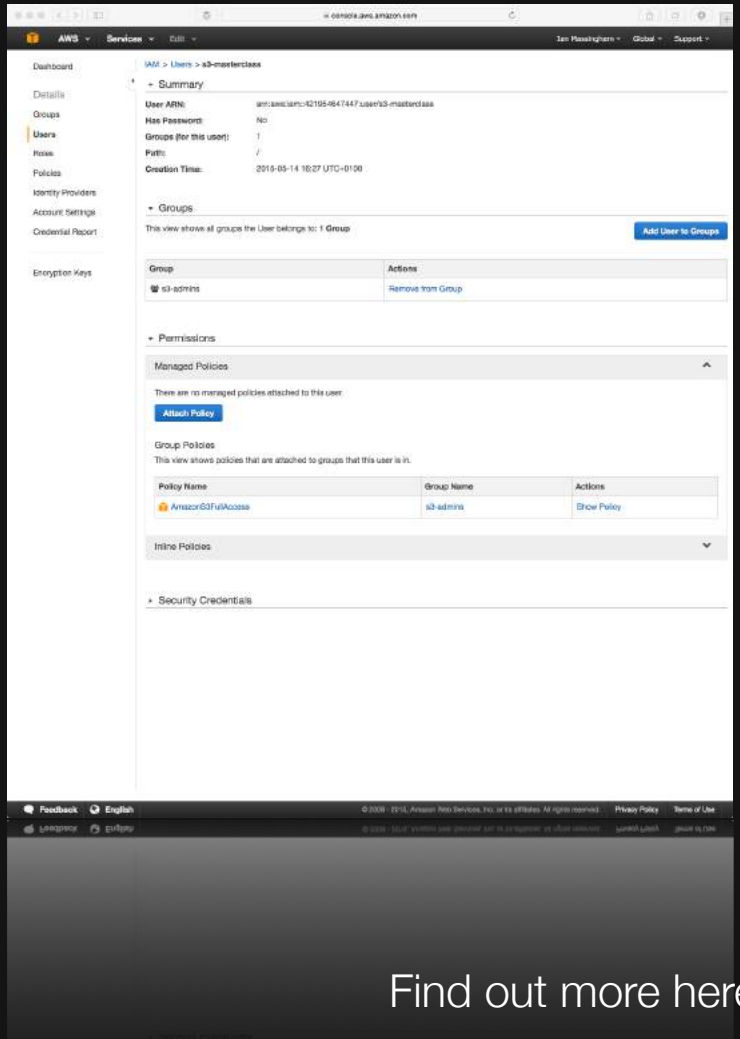
IAM Policies

Fine grained

Administer as part of role based access

Apply policies to S3 at role, user & group level





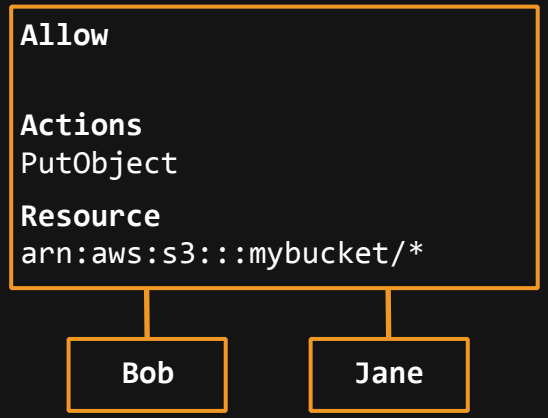
Find out more here: aws.amazon.com/iam

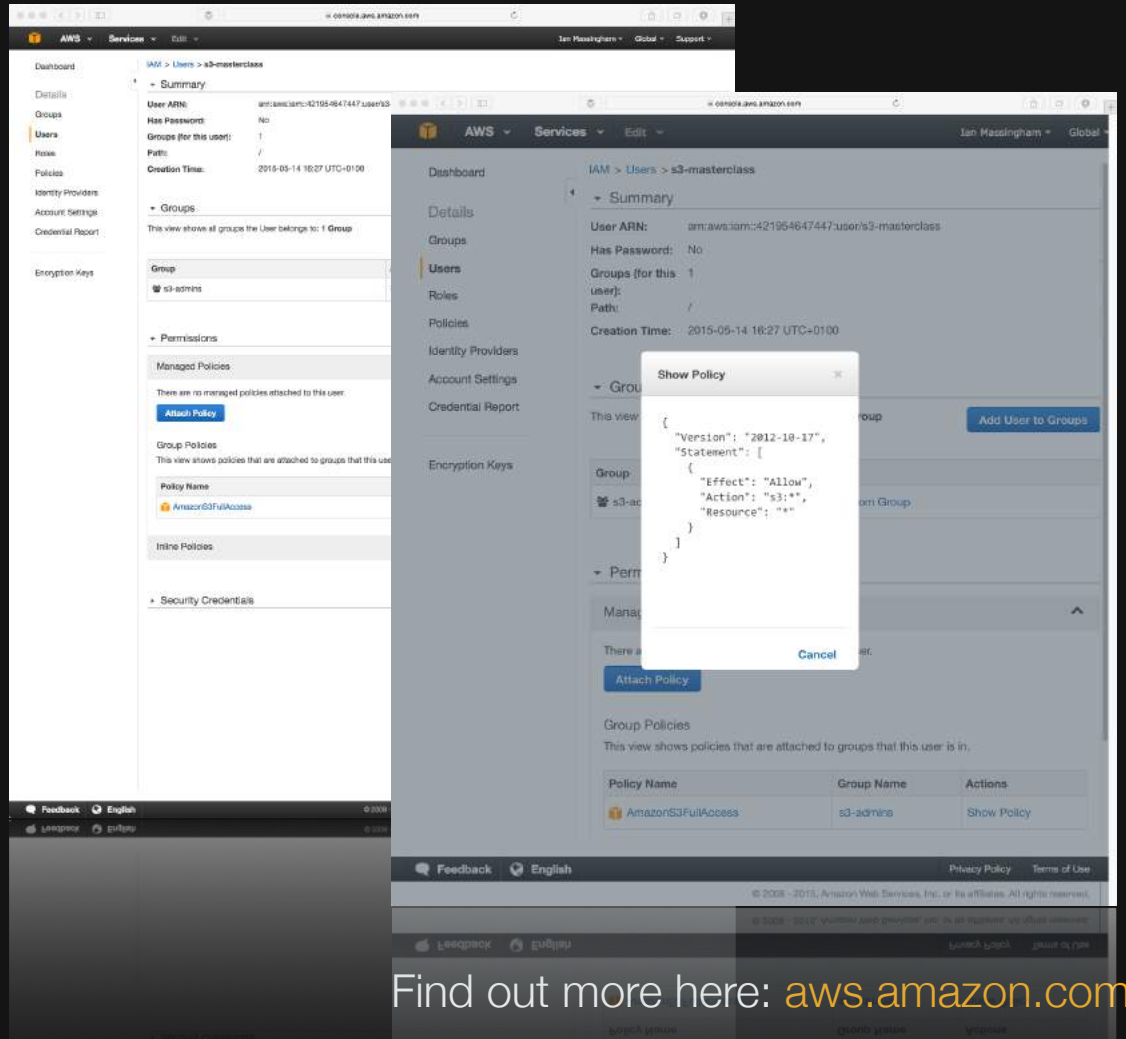
IAM Policies

Fine grained

Administer as part of role based access

Apply policies to S3 at role, user & group level





Find out more here: aws.amazon.com/iam

IAM Policies

Fine grained

Administer as part of role based access

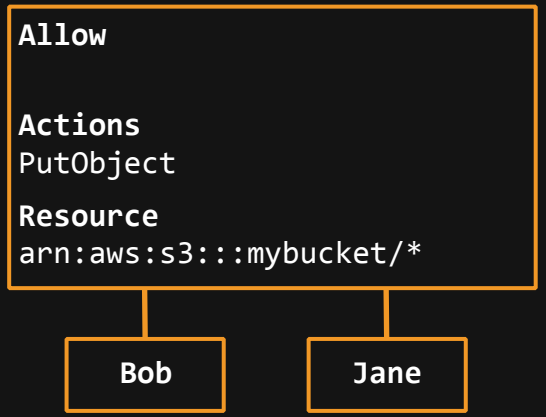
Apply policies to S3 at role, user & group level

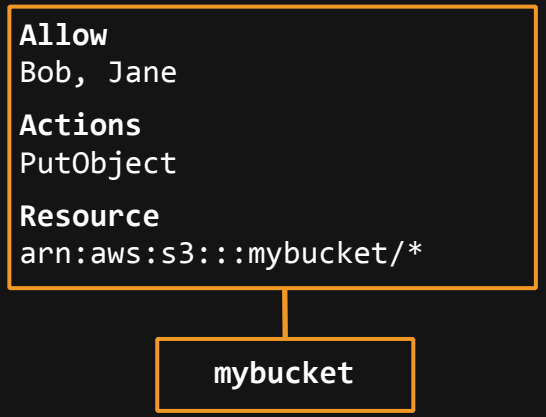
Bucket Policies

Fine grained

Apply policies at the bucket level in S3

Incorporate user restrictions without using IAM



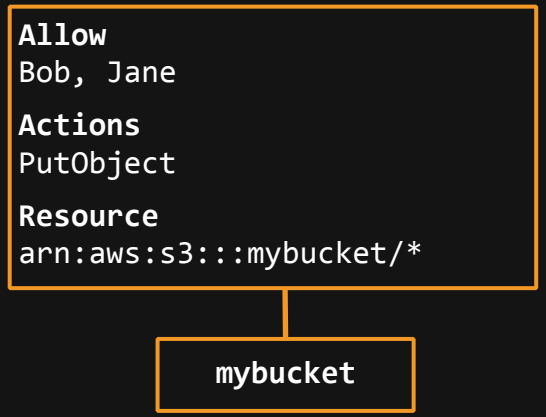


Bucket Policies

Fine grained

Apply policies at the bucket level in S3

Incorporate user restrictions without using IAM



Granting Read-Only Permission to an Anonymous User

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

Granting Read-Only Permission to an Anonymous User

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

The effect of the policy, allow or deny

Who the policy applies to. * means everyone

The actions allowed/denied by this policy

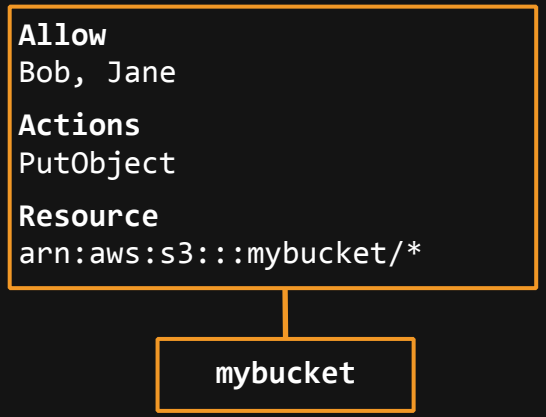
The AWS resource that this policy applies to.
In this case all objects in example bucket

Bucket Policies

Fine grained

Apply policies at the bucket level in S3

Incorporate user restrictions without using IAM



Restricting Access to Specific IP Addresses

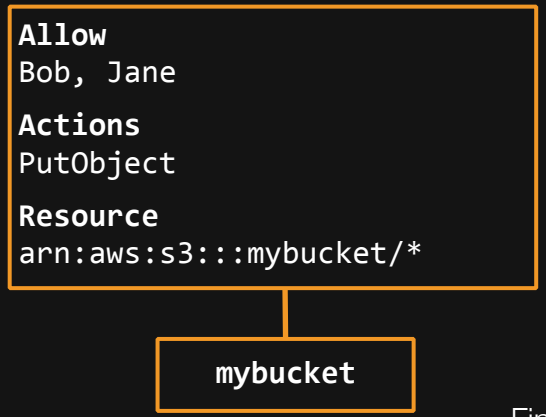
```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
         "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
         "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
      }
    }
  ]
}
```

Bucket Policies

Fine grained

Apply policies at the bucket level in S3

Incorporate user restrictions without using IAM



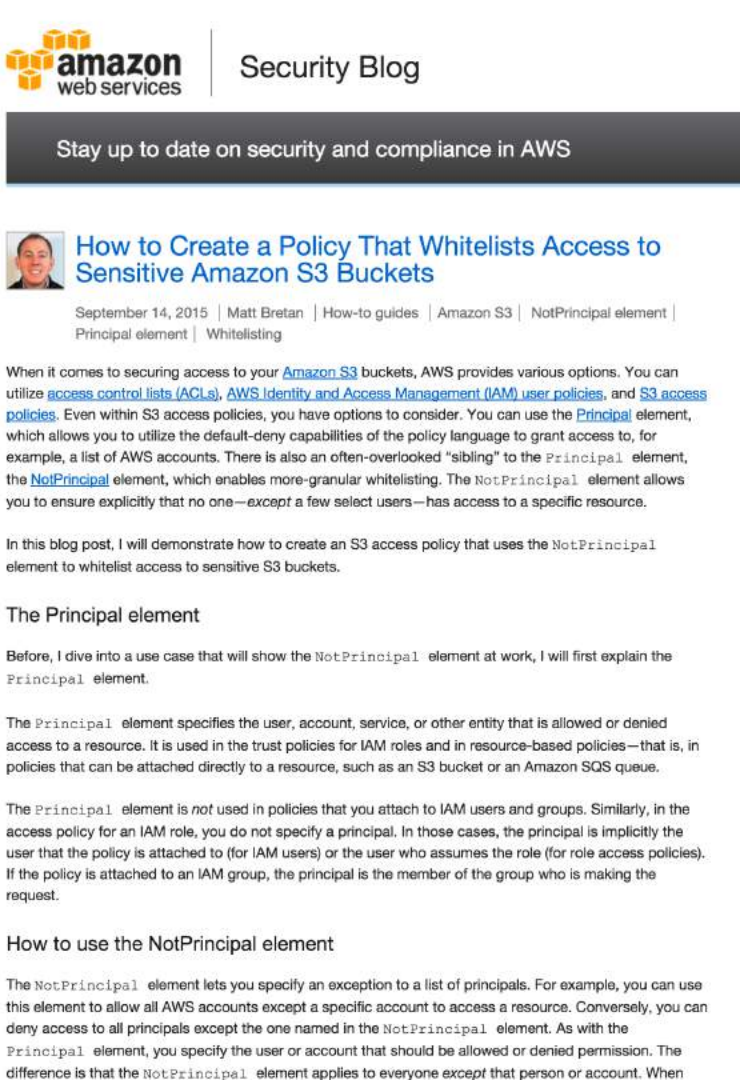
Other Example Use-Cases for Bucket Policies

- Granting Permissions to Multiple Accounts with Added Conditions
- Restricting Access to a Specific HTTP Referrer
- Granting Permission to an Amazon CloudFront Origin Identity
- Adding a Policy to Require MFA Authentication
- Granting Cross-Account Permissions to Upload Objects While Ensuring the Bucket Owner Has Full Control

Find out more here: docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html

AWS SECURITY BLOG

How to Create a Policy That Whitelists Access to Sensitive Amazon S3 Buckets



amazon web services | Security Blog

Stay up to date on security and compliance in AWS

How to Create a Policy That Whitelists Access to Sensitive Amazon S3 Buckets

September 14, 2015 | Matt Bretan | How-to guides | Amazon S3 | NotPrincipal element | Principal element | Whitelisting

When it comes to securing access to your Amazon S3 buckets, AWS provides various options. You can utilize access control lists (ACLs), AWS Identity and Access Management (IAM) user policies, and S3 access policies. Even within S3 access policies, you have options to consider. You can use the Principal element, which allows you to utilize the default-deny capabilities of the policy language to grant access to, for example, a list of AWS accounts. There is also an often-overlooked "sibling" to the `Principal` element, the NotPrincipal element, which enables more-granular whitelisting. The `NotPrincipal` element allows you to ensure explicitly that no one—*except* a few select users—has access to a specific resource.

In this blog post, I will demonstrate how to create an S3 access policy that uses the `NotPrincipal` element to whitelist access to sensitive S3 buckets.

The Principal element

Before, I dive into a use case that will show the `NotPrincipal` element at work, I will first explain the `Principal` element.

The `Principal` element specifies the user, account, service, or other entity that is allowed or denied access to a resource. It is used in the trust policies for IAM roles and in resource-based policies—that is, in policies that can be attached directly to a resource, such as an S3 bucket or an Amazon SQS queue.

The `Principal` element is *not* used in policies that you attach to IAM users and groups. Similarly, in the access policy for an IAM role, you do not specify a principal. In those cases, the principal is implicitly the user that the policy is attached to (for IAM users) or the user who assumes the role (for role access policies). If the policy is attached to an IAM group, the principal is the member of the group who is making the request.

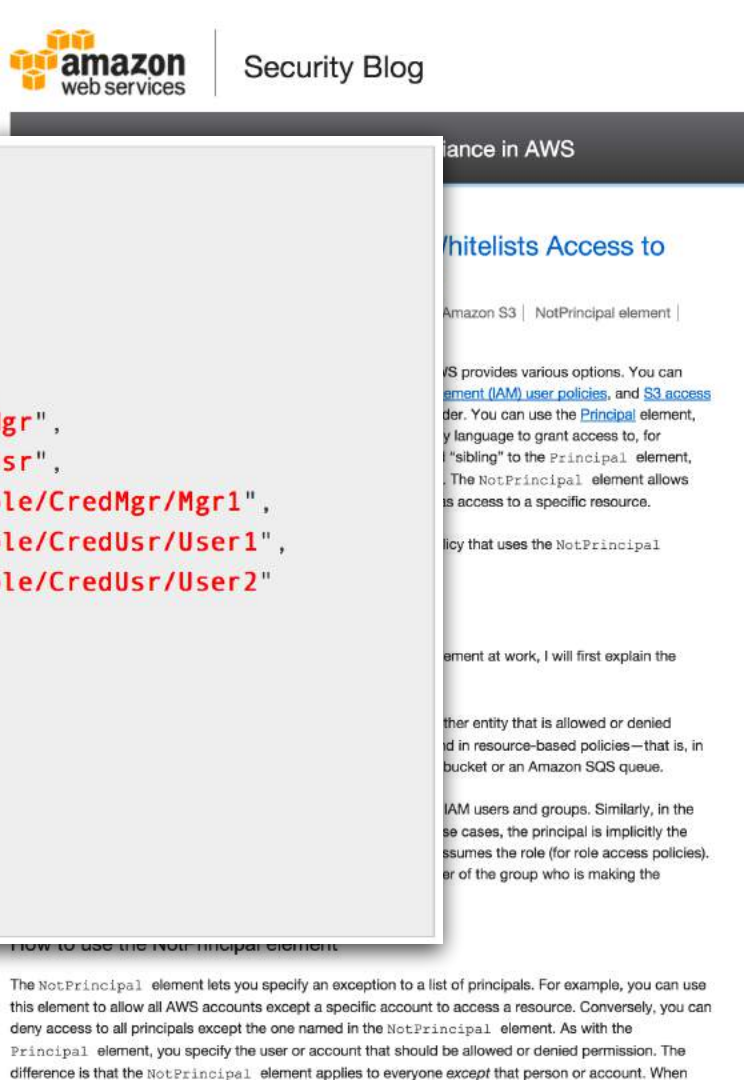
How to use the NotPrincipal element

The `NotPrincipal` element lets you specify an exception to a list of principals. For example, you can use this element to allow all AWS accounts except a specific account to access a resource. Conversely, you can deny access to all principals except the one named in the `NotPrincipal` element. As with the `Principal` element, you specify the user or account that should be allowed or denied permission. The difference is that the `NotPrincipal` element applies to everyone *except* that person or account. When

AWS

How to
Access to

```
{
     "Sid": "ListRelevantDirectories20150907",
     "Effect": "Deny",
     "NotPrincipal": {
          "AWS": [
               "arn:aws:iam::123456789012:role/CredMgr",
               "arn:aws:iam::123456789012:role/CredUsr",
               "arn:aws:sts::123456789012:assumed-role/CredMgr/Mgr1",
               "arn:aws:sts::123456789012:assumed-role/CredUsr/User1",
               "arn:aws:sts::123456789012:assumed-role/CredUsr/User2"
          ]
     },
     "Action": [
          "s3:ListBucket"
     ],
     "Resource": "arn:aws:s3:::CredentialBucket"
}
```

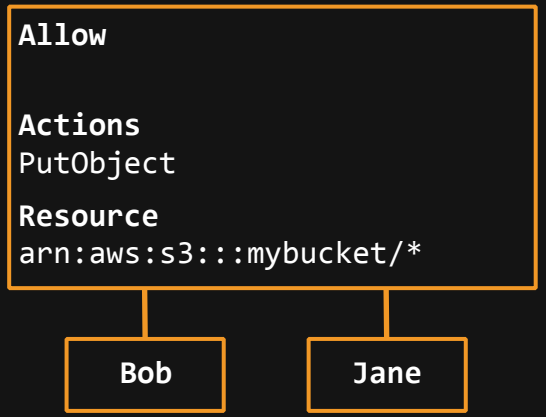


IAM Policies

Fine grained

Administer as part of role based access

Apply policies to S3 at role, user & group level

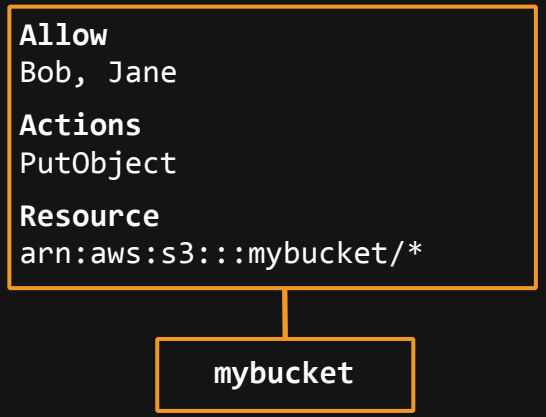


Bucket Policies

Fine grained

Apply policies at the bucket level in S3

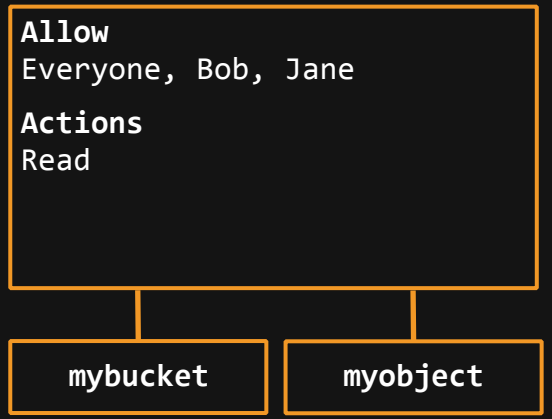
Incorporate user restrictions without using IAM



ACLs

Coarse grained

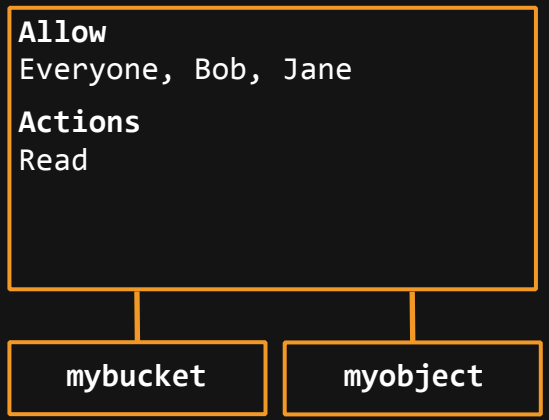
Apply access control rules at the bucket and/or object level in S3



ACLs

Coarse grained

Apply access control rules at the bucket and/or object level in S3



You can use ACLs to grant basic read/write permissions to other AWS accounts.

There are limits to managing permissions using ACLs.

For example, you can grant permissions only to other AWS accounts, you cannot grant permissions to users in your account.

STORAGE CLASSES

S3 Standard

Designed to provide 99.999999999% durability and 99.99% availability of objects over a given year

Designed to sustain the concurrent loss of data in two facilities

S3 Standard - Infrequent Access

Standard - IA offers the high durability, throughput, and low latency of Amazon S3 Standard, with a low per GB storage price and per GB retrieval fee.

Designed to provide 99.9999999999% durability and 99.9% availability of objects over a given year

---

Glacier

Suitable for archiving data, where data access is infrequent and a retrieval time of several hours is acceptable

Uses the very low-cost Amazon Glacier storage service, but managed through Amazon S3

	Standard	Standard - IA	Amazon Glacier
Designed for Durability	99.999999999%	99.999999999%	99.999999999%
Designed for Availability	99.99%	99.9%	N/A
Availability SLA	99.9%	99%	N/A
Minimum Object Size	N/A	128KB*	N/A
Minimum Storage Duration	N/A	30 days	90 days
Retrieval Fee	N/A	per GB retrieved	per GB retrieved**
First Byte Latency	milliseconds	milliseconds	4 hours
Storage Class	object level	object level	object level
Lifecycle Transitions	yes	yes	yes

* Standard - IA has a minimum object size of 128KB. Smaller objects will be charged for 128KB of storage.

Storage Pricing

Region: EU (Ireland)

	Standard Storage	Standard - Infrequent Access Storage †	Glacier Storage
First 1 TB / month	$0.0300 per GB	$0.0125 per GB	$0.007 per GB
Next 49 TB / month	$0.0295 per GB	$0.0125 per GB	$0.007 per GB
Next 450 TB / month	$0.0290 per GB	$0.0125 per GB	$0.007 per GB
Next 500 TB / month	$0.0285 per GB	$0.0125 per GB	$0.007 per GB
Next 4000 TB / month	$0.0280 per GB	$0.0125 per GB	$0.007 per GB
Over 5000 TB / month	$0.0275 per GB	$0.0125 per GB	$0.007 per GB

Amazon S3 Reduced Redundancy Storage

Enables customers to reduce their costs by storing noncritical, reproducible data at lower levels of redundancy than Amazon S3's standard storage.

	Reduced Redundancy Storage
First 1 TB / month	$0.0240 per GB

AWS CLI

Moving Objects between S3 storage classes

You can specify the storage class of an object when uploading or creating it

```
$ aws s3 cp aws_uki.txt s3://aws-ianm-s3-masterclass/ --storage-class REDUCED_REDUNDANCY
```

AWS CLI

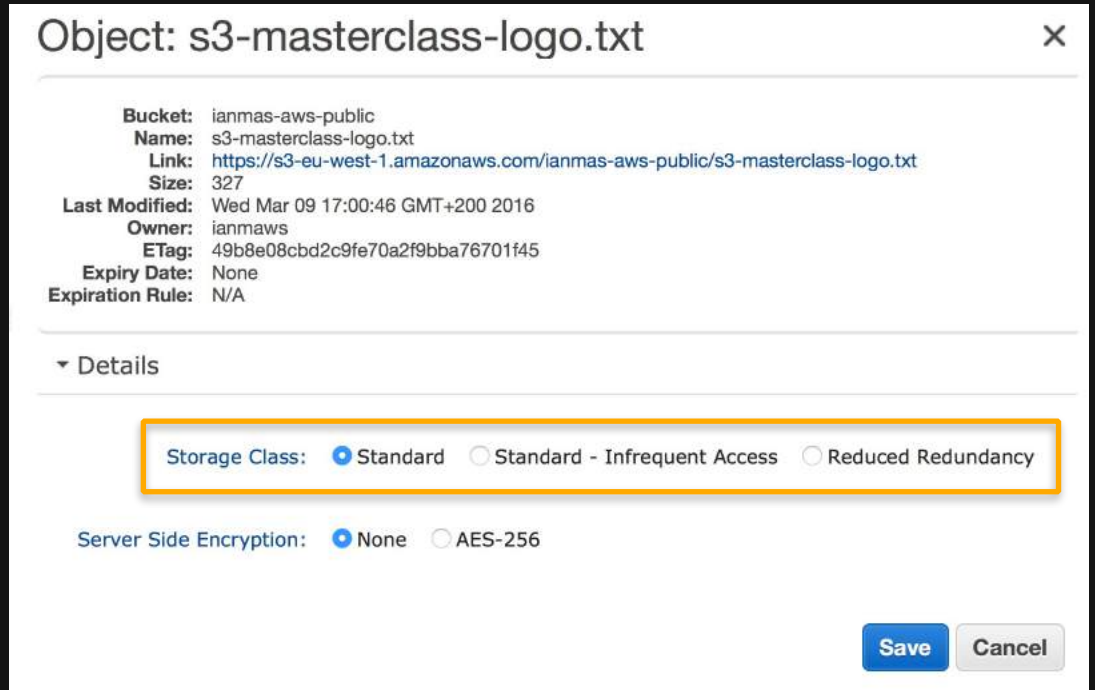
Moving Objects between S3 storage classes

You can change the storage class of an object that is already stored in Amazon S3 by copying it to the same key name in the same bucket

```
$ aws s3 cp s3://aws-ianm-s3-masterclass/aws_uki.txt s3://aws-ianm-s3-masterclass/aws_uki.txt --storage-class STANDARD
```

AWS Console

Moving Objects between storage classes



Python

Moving Objects between storage classes

```
$ python

>>> import boto

>>> conn = boto.connect_s3()

>>> mybucket = conn.get_bucket(‘aws-ianm-s3-masterclass’)

>>> mybucket.copy_key('aws_uki.txt','aws-ianm-s3-
masterclass','aws_uki.txt',storage_class='REDUCED_REDUNDANCY')
```

What about Amazon Glacier?

We will come to this when we talk about Lifecycle Management

ENCRYPTION

Securing Data in Transit

Securely upload or download your data via SSL-encrypted endpoints using HTTPS

Alternatively, use a client encryption library such as the Amazon S3 Encryption Client to encrypt your data before uploading to Amazon S3

http://docs.aws.amazon.com/AWSJavaSDK/latest/javadoc/com/amazonaws/services/s3/AmazonS3EncryptionClient.html

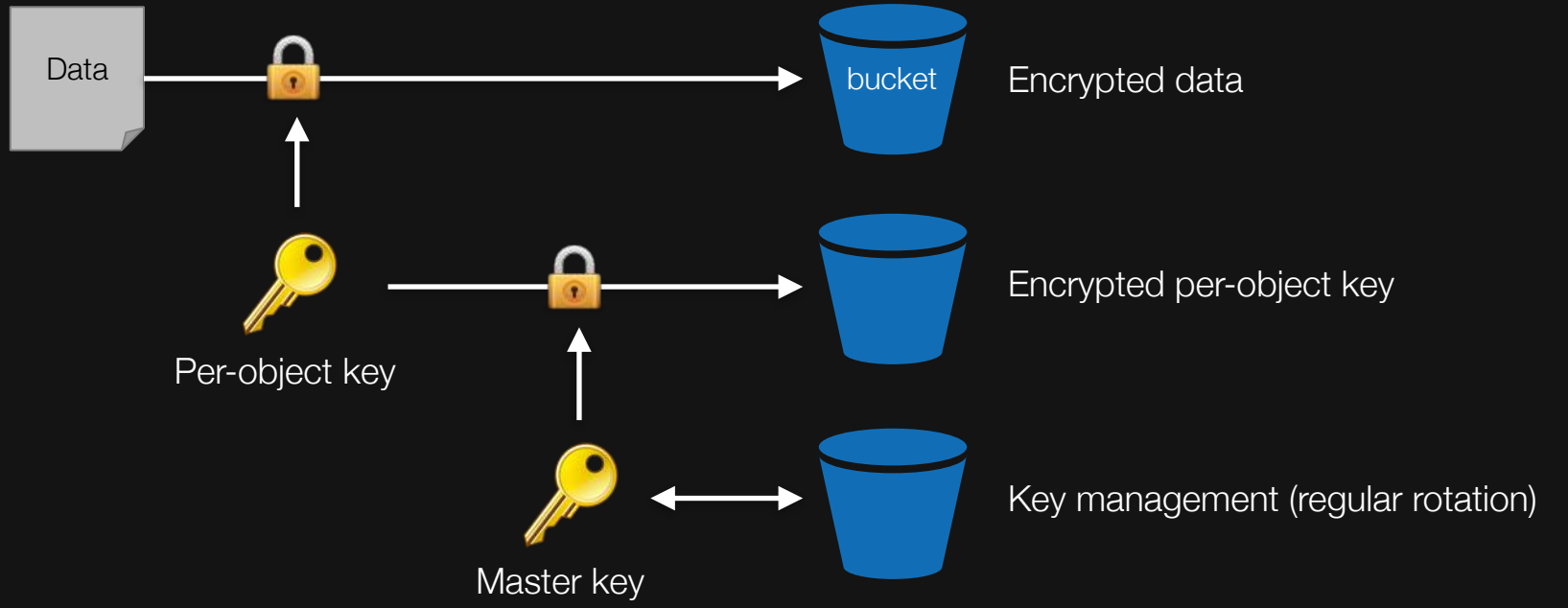
SECURING DATA AT REST

Amazon S3 Server Side Encryption (SSE)

- Amazon S3 will automatically encrypt your data on write and decrypt your data on retrieval
- Uses Advanced Encryption Standard (AES) 256-bit symmetric keys
- There are three different ways to mange encryption keys:

SSE with Amazon S3 Key Management (SSE-SE)

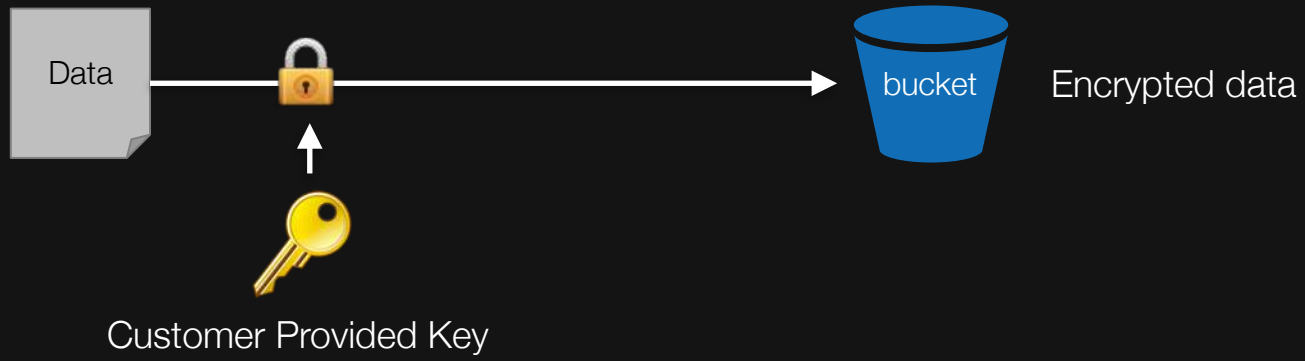
With SSE-S3, Amazon S3 will encrypt your data at rest and manage the encryption keys for you



SSE with Customer-Provided Keys (SSE-C)

With SSE-C, Amazon S3 will encrypt your data at rest using the custom encryption keys that you provide

Amazon S3 doesn't store your encryption key anywhere; the key is immediately discarded after Amazon S3 completes your requests



SSE with AWS KMS (SSE-KMS)

With SSE-KMS, Amazon S3 will encrypt your data at rest using keys that you manage in the AWS Key Management Service (KMS)

AWS KMS provides an audit trail so you can see who used your key to access which object and when

ADDITIONAL SECURITY FEATURES

OBJECT ACCESS & AUDIT LOGS

AWS Official Blog

Amazon S3 Update – CloudTrail Integration

by Jeff Barr | on 02 SEP 2015 | in Amazon S3, CloudTrail | Permalink | Comments

You can now use AWS CloudTrail to track bucket-level operations on your Amazon Simple Storage Service (S3) buckets. The tracked operations include creation and deletion of buckets, modifications to access controls, changes to lifecycle policies, and changes to cross-region replication settings.

AWS CloudTrail records API activity in your AWS account and delivers the resulting log files to a designated S3 bucket. You can look up API activity related to creating, deleting and modifying your S3 resources using the CloudTrail Console, including access to 7 days of historical data. You can also create Amazon CloudWatch Alarms to look for specific API activities and receive email notifications when they occur.

MULTI-FACTOR AUTHENTICATION DELETE

TIME-LIMTED ACCESS TO OBJECTS

Signed URLs

Provide time-limited access to specific objects that expires after a set period

Access Permissions

Use on objects in non-public buckets to prevent access once the signed URL has expired

```
https://ianmas-aws.testbucket.s3.amazonaws.com/testfile.txt
    ?Signature=JHCa39GV1fKRKkEnAWzI88lH7f8%3D
    &Expires=1391425438
    &AWSAccessKeyId=AKIAIRBKBJ3ZAYAXFC2Q
```

Generating time-limited signed links

Python

```
>>> import boto
>>> conn = boto.connect_s3()
>>> conn.generate_url(3600, 'GET', bucket='aws-ianm-s3-masterclass',
key=‘aws_uki.txt')
'https://aws-ianm-s3-masterclass.s3.amazonaws.com/aws_uki.txt?
Signature=hEBUPczy8DXCyqTz1JHgEaihvMo%3D&Expires=1431697820&AWSAcces
sKeyId=AKIAI65L23YDGKGQTRFA'

>>> import boto
>>> conn = boto.connect_s3()
>>> conn.generate_url(30, 'GET', bucket='aws-ianm-s3-masterclass',
key=‘aws_uki.txt’, force_http=True)
'http://aws-ianm-s3-masterclass.s3.amazonaws.com/aws_uki.txt?
Signature=yIYPyn0DMXk2cOcZkWPRuSHoKPA%3D&Expires=1431694649&AWSAcces
sKeyId=AKIAI65L23YDGKGQTRFA'
```

Generating time-limited signed links

Python

1st parameter is link lifetime in seconds

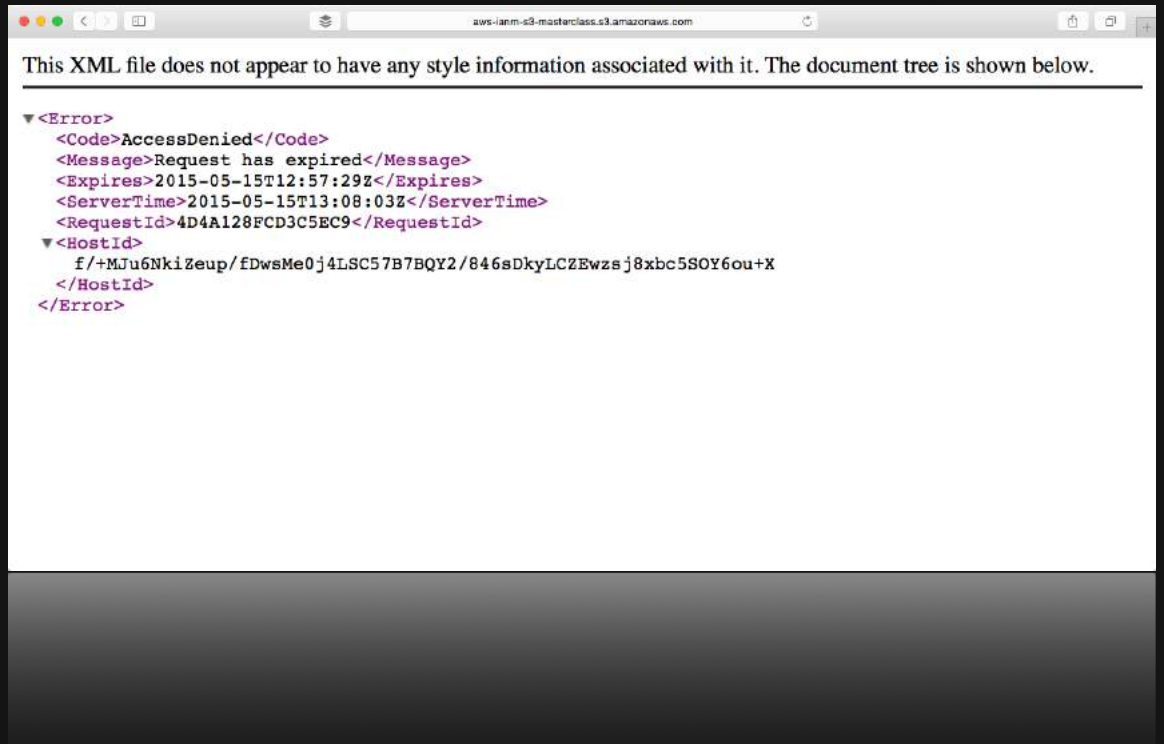
```
>>> import boto
>>> conn = boto.connect_s3()
>>> conn.generate_url(3600, 'GET', bucket='aws-ianm-s3-masterclass',
key='aws_uki.txt')
'https://aws-ianm-s3-masterclass.s3.amazonaws.com/aws_uki.txt?
Signature=hEBUPczy8DXCyqTz1JHgEaihvMo%3D&Expires=1431697820&AWSAcces
sKeyId=AKIAI65L23YDGKGQTRFA'
```

Force a non-SSL link

```
>>> import boto
>>> conn = boto.connect_s3()
>>> conn.generate_url(30, 'GET', bucket='aws-ianm-s3-masterclass',
key='aws_uki.txt', force_http=True)
'http://aws-ianm-s3-masterclass.s3.amazonaws.com/aws_uki.txt?
Signature=yIYPyn0DMXk2cOcZkWPRuSHoKPA%3D&Expires=1431694649&AWSAcces
sKeyId=AKIAI65L23YDGKGQTRFA'
```

Generating time-limited signed links

Error response: link expired



VERSIONING &
CROSS REGION REPLICATION

Bucket level

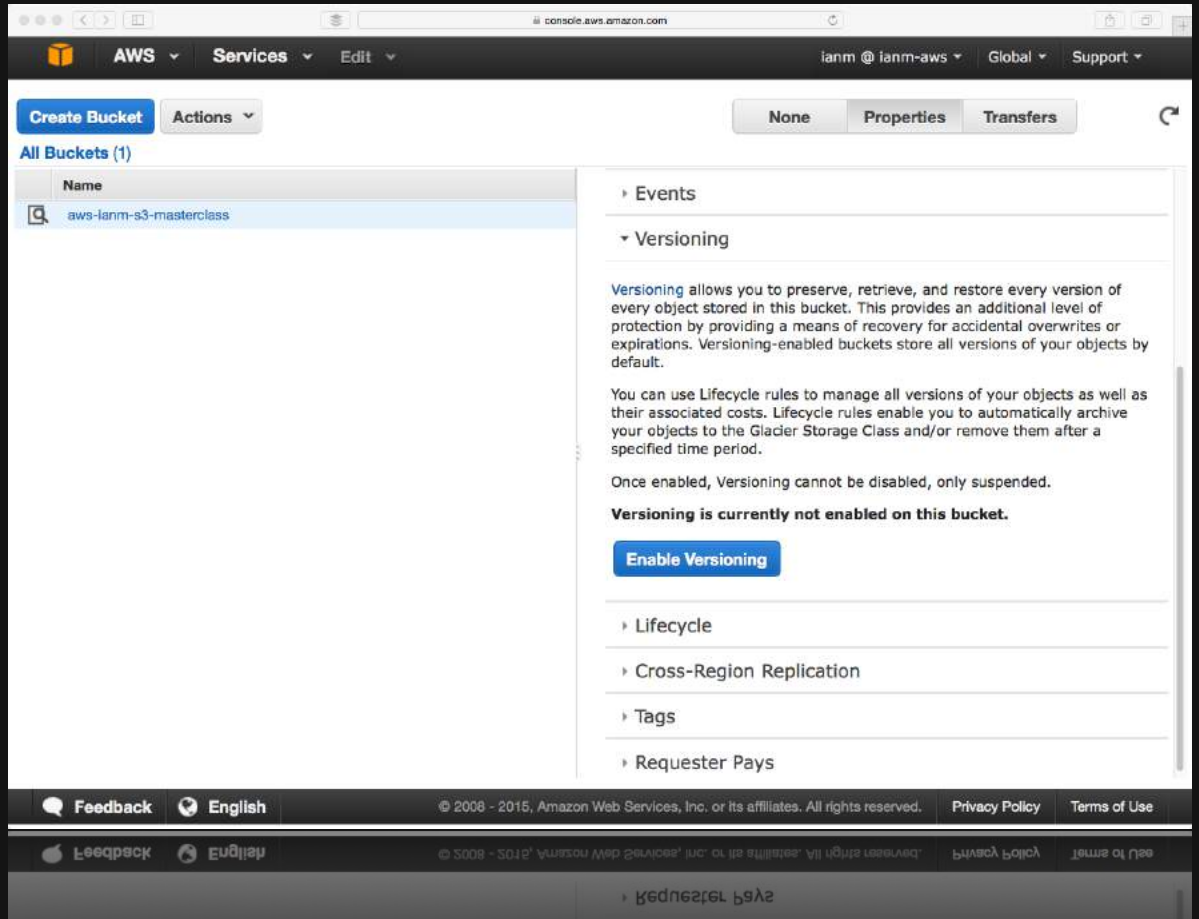
Automatically preserves all copies of objects

Persistent

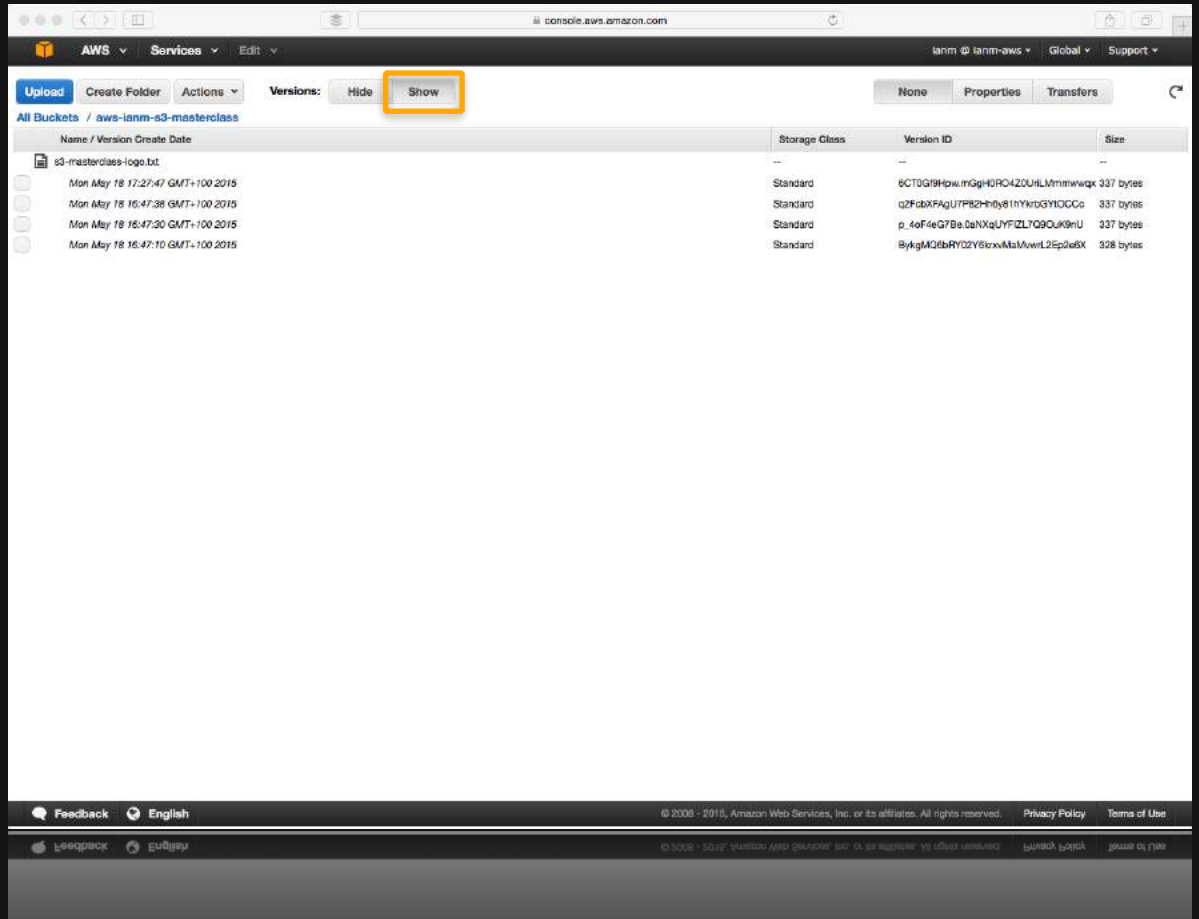
Even deleted object history is held

VERSIONING

AWS Console


console.aws.amazon.com
AWS
Services
Edit
ianm @ ianm-aws
Global
Support
Create Bucket
Actions
None
Properties
Transfers
All Buckets (1)
Name
aws-ianm-s3-masterclass
Events
Versioning
Versioning allows you to preserve, retrieve, and restore every version of every object stored in this bucket. This provides an additional level of protection by providing a means of recovery for accidental overwrites or expirations. Versioning-enabled buckets store all versions of your objects by default.
You can use Lifecycle rules to manage all versions of your objects as well as their associated costs. Lifecycle rules enable you to automatically archive your objects to the Glacier Storage Class and/or remove them after a specified time period.
Once enabled, Versioning cannot be disabled, only suspended.
Versioning is currently not enabled on this bucket.
Enable Versioning
Lifecycle
Cross-Region Replication
Tags
Requester Pays
Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

AWS Console


console.aws.amazon.com
AWS
Services
Edit
ianm @ ianm-aws
Global
Support
Upload
Create Folder
Actions
Versions:
Hide
Show
None
Properties
Transfers
All Buckets / aws-ianm-s3-masterclass
Name / Version Create Date
Storage Class
Version ID
Size
s3-masterclass-logo.txt
Mon May 18 17:27:47 GMT+100 2015
Standard
337 bytes
Mon May 18 16:47:38 GMT+100 2015
Standard
337 bytes
Mon May 18 16:47:30 GMT+100 2015
Standard
337 bytes
Mon May 18 16:47:10 GMT+100 2015
Standard
328 bytes
Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

AWS CLI

Working with versioned objects via the CLI

uses the ‘aws s3api’ CLI command, which has additional functionality over ‘aws s3’

```
$ aws s3api list-object-versions --bucket aws-ianm-s3-masterclass
```

http://docs.aws.amazon.com/cli/latest/reference/s3api/index.html#cli-aws-s3api

AWS CLI

```
$ aws s3api list-object-versions --bucket aws-ianm-s3-masterclass
```

```
None   None
VERSIONS     "36bc67941830bb388c9bf201440683a4"     True   s3-masterclass-logo.txt   2015-05-18T15:47:38.000Z
337    STANDARD     q2FcbXFAgU7P82Hh6y81hYkrbGYtOCCc
OWNER  ianm   4ee381d180ee58aa815e7d4a3a5f739b20bb8980a568947384e59c8d0ff8379b
VERSIONS     "e0253c9354f61097cbf6ce239afd0464"     False  s3-masterclass-logo.txt   2015-05-18T15:47:30.000Z
337    STANDARD     p_4oF4eG7Be.0aNXqUYFlZL7Q9OuK9nU
OWNER  ianm   4ee381d180ee58aa815e7d4a3a5f739b20bb8980a568947384e59c8d0ff8379b
VERSIONS     "84defb05031845e8b0616a9b70b2ae93"     False  s3-masterclass-logo.txt   2015-05-18T15:47:10.000Z
328    STANDARD     BykgMQ6bRY02Y6krxvMaMvwrL2Ep2e6X
OWNER  ianm   4ee381d180ee58aa815e7d4a3a5f739b20bb8980a568947384e59c8d0ff8379b
```

AWS CLI

```
$ aws s3api get-object --bucket aws-ianm-s3-masterclass --key s3-masterclass-logo.txt --version-id q2FcbXFAgU7P82Hh6y81hYkrbGYtOCCc version.txt
```

```
bytes 337    text/plain    "36bc67941830bb388c9bf201440683a4"     Mon, 18 May 2015 15:47:38 GMT
q2FcbXFAgU7P82Hh6y81hYkrbGYtOCCc
```

```
$ more version.txt
```

```
Version 3
```

http://docs.aws.amazon.com/cli/latest/reference/s3api/index.html#cli-aws-s3api

Listing object versions

Python

```
>>> import boto
>>> conn = boto.connect_s3()
>>> bucket=conn.get_bucket('aws-ianm-s3-masterclass')
>>> versions = bucket.list_versions()
>>> for version in versions:
...   print version.name + ' ' + version.version_id
...
s3-masterclass-logo.txt q2FcbXFAgU7P82Hh6y81hYkrbGYtOCCc
s3-masterclass-logo.txt p_4oF4eG7Be.0aNXqUYFlZL7Q9OuK9nU
s3-masterclass-logo.txt BykgMQ6bRY02Y6krxvMaMvwrL2Ep2e6X
```

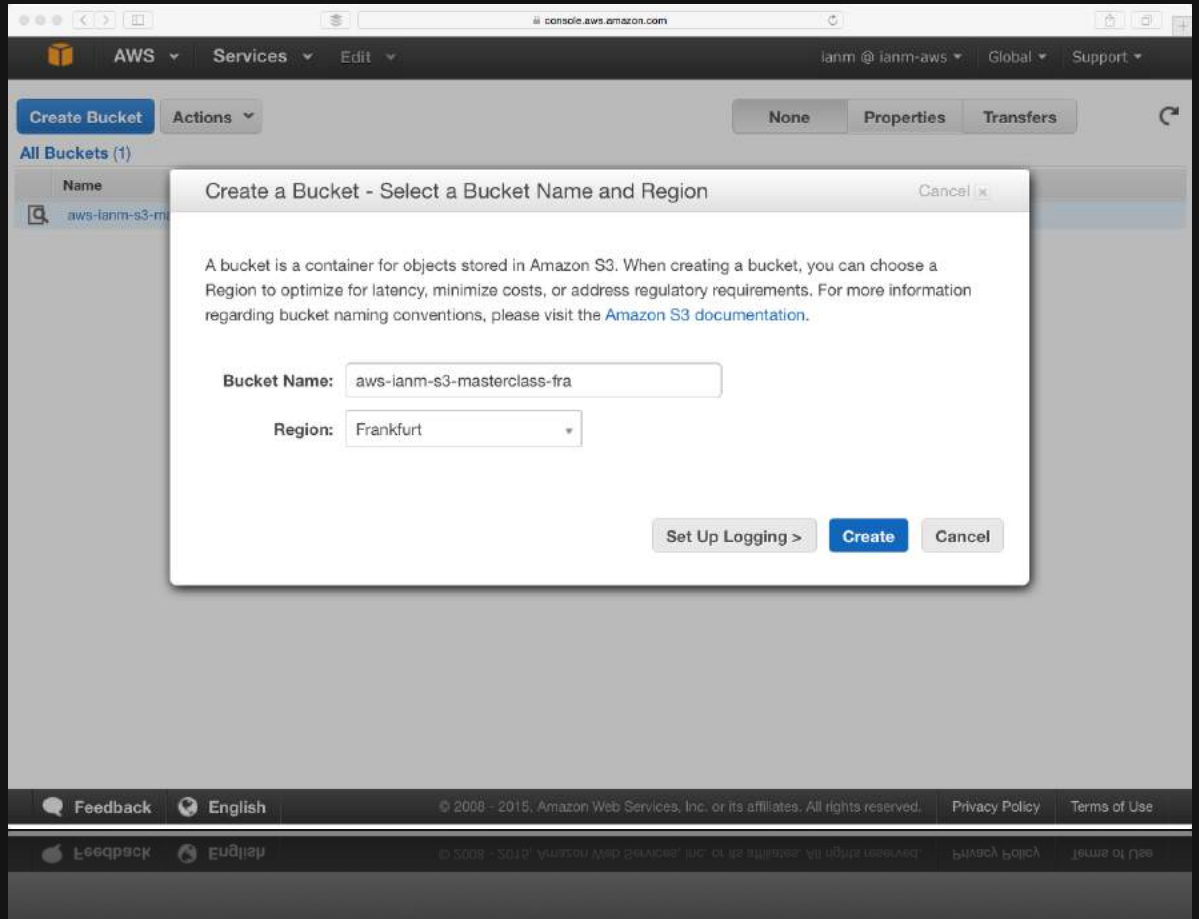
Getting a specific object version

Python

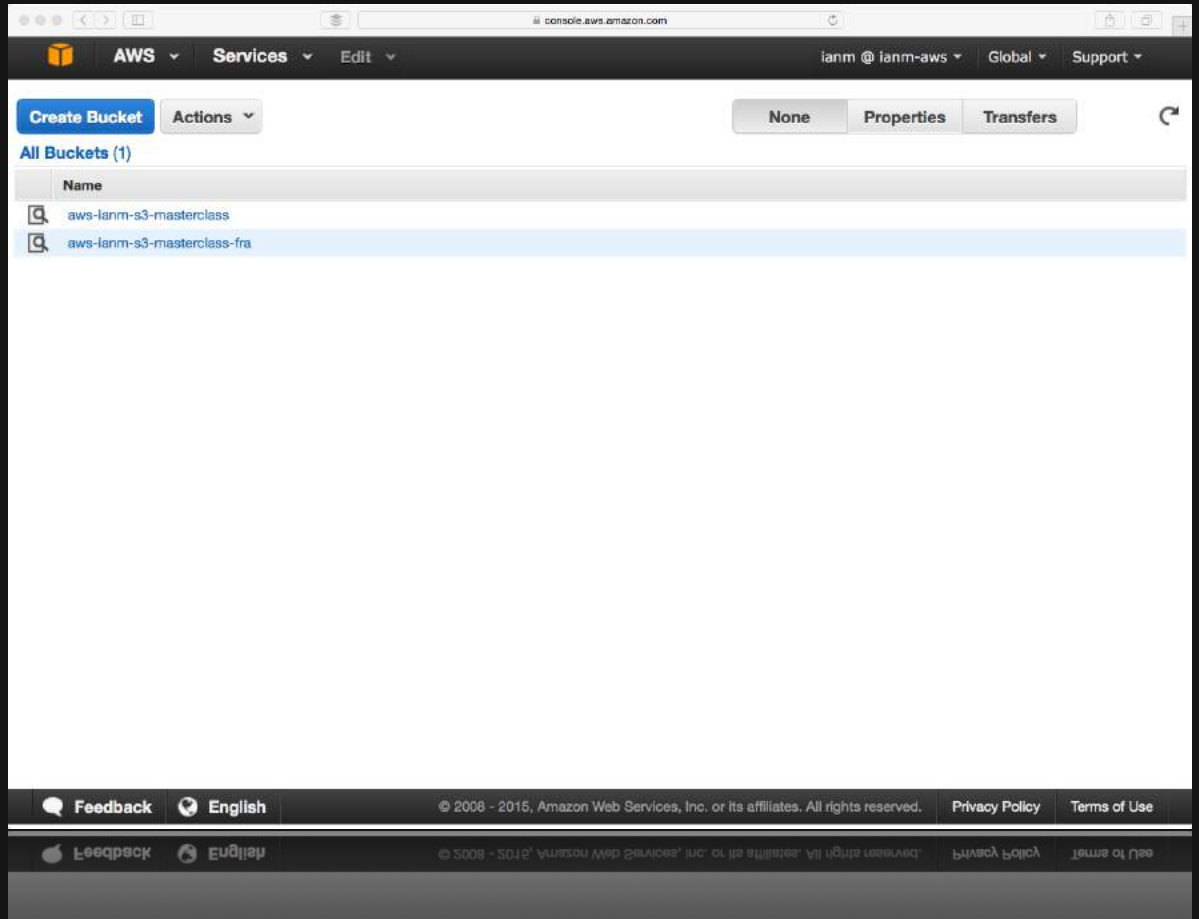
```
>>> key = bucket.get_key('s3-masterclass-logo.txt',
version_id='p_4oF4eG7Be.0aNXqUYFlZL7Q9OuK9nU')
>>> key.get_contents_as_string()
"\n ____ _____   __  __          _                _                \n/ ___|___ /  |
\\/  | __ _ ___| |_ ___ _ __ ___| | __ _ ___ ___ \n\\___ \\ |_ \\  | |\\/| |/ _` /
__| __/ _ \\ '__/ __| |/ _` / __/ __|\n ___) |__) | | |  | | (_| \\__ \\ ||  __/ | |
(__| | (_| \\__ \\__ \\\n|____/____/  |_|  |_|\\__,_|___/\\__\\___|_|  \\___|_|\
\__,_|___/___/\n\nVersion 2\n”
>>> key.generate_url(300)
'https://aws-ianm-s3-masterclass.s3.amazonaws.com/s3-masterclass-logo.txt?
Signature=c%2BjgGY5EZ4tDuI0xcKg572qL%2B9Y%3D&Expires=1431965853&AWSAccessKeyId=AKIAI
65L23YDGKGQTRFA&versionId=p_4oF4eG7Be.0aNXqUYFlZL7Q9OuK9nU'
>>>
```

CROSS REGION REPLICATION

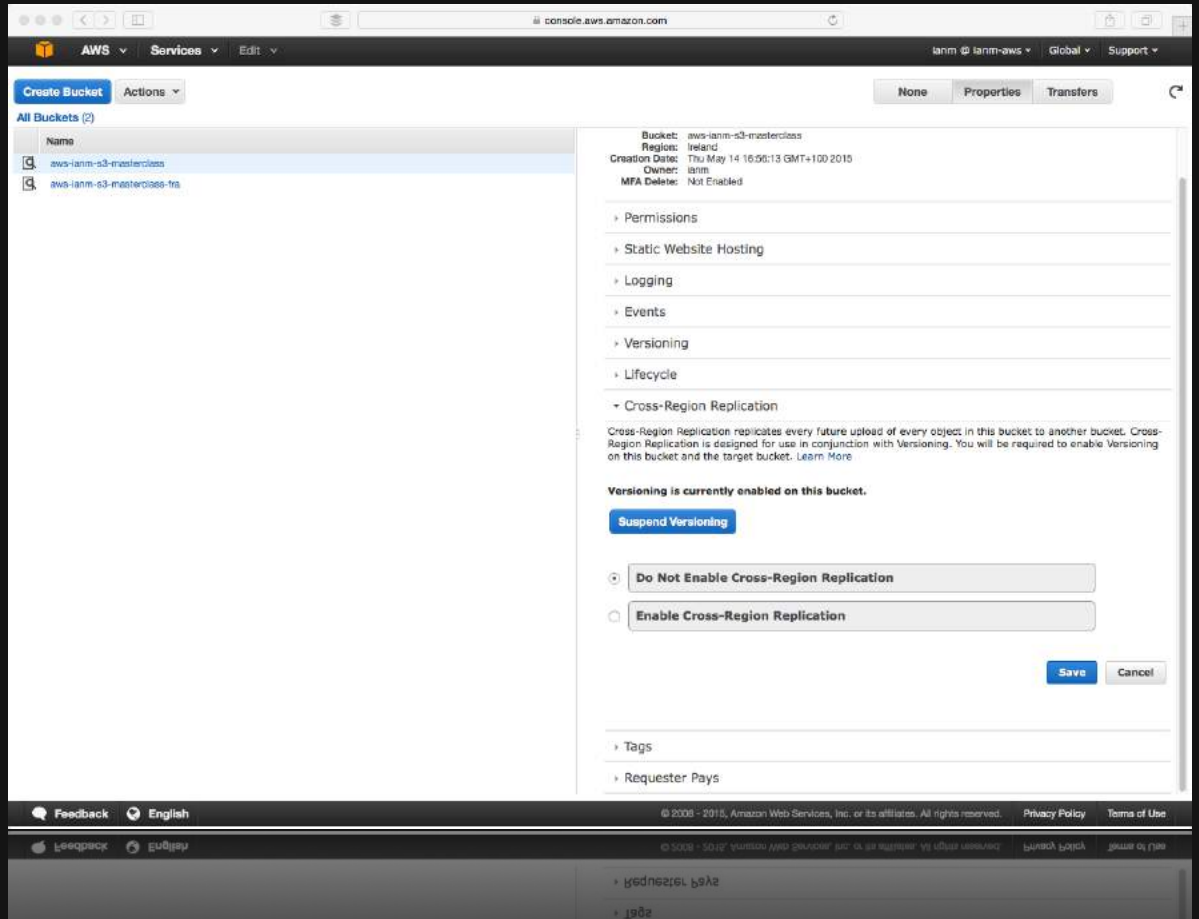
AWS Console


console.aws.amazon.com
AWS
Services
Edit
ianm @ ianm-aws
Global
Support
Create Bucket
Actions
None
Properties
Transfers
All Buckets (1)
Name
aws-ianm-s3-m
Create a Bucket - Select a Bucket Name and Region
Cancel
A bucket is a container for objects stored in Amazon S3. When creating a bucket, you can choose a Region to optimize for latency, minimize costs, or address regulatory requirements. For more information regarding bucket naming conventions, please visit the Amazon S3 documentation.
Bucket Name:
aws-ianm-s3-masterclass-fra
Region:
Frankfurt
Set Up Logging >
Create
Cancel
Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

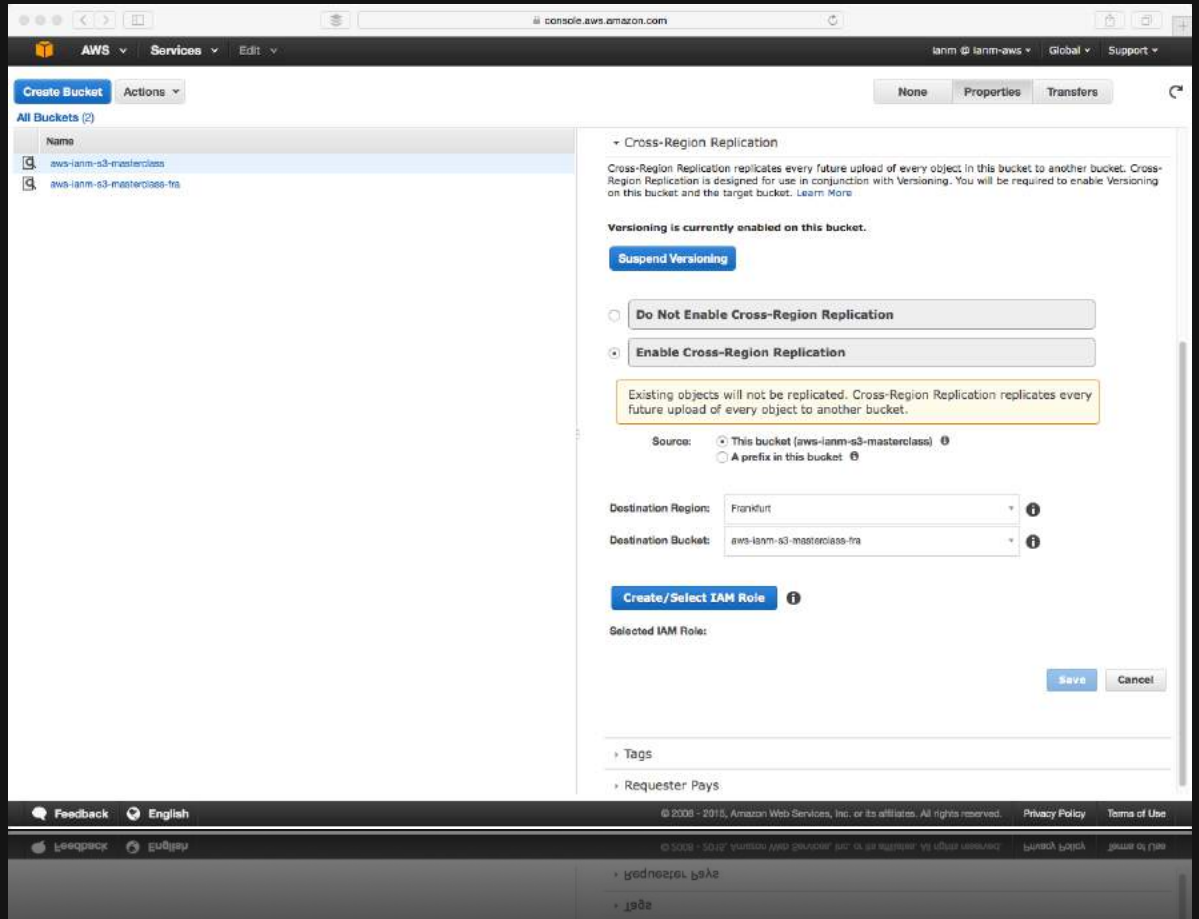
AWS Console


console.aws.amazon.com
AWS
Services
Edit
ianm @ ianm-aws
Global
Support
Create Bucket
Actions
None
Properties
Transfers
All Buckets (1)
Name
aws-ianm-s3-masterclass
aws-ianm-s3-masterclass-fra
Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

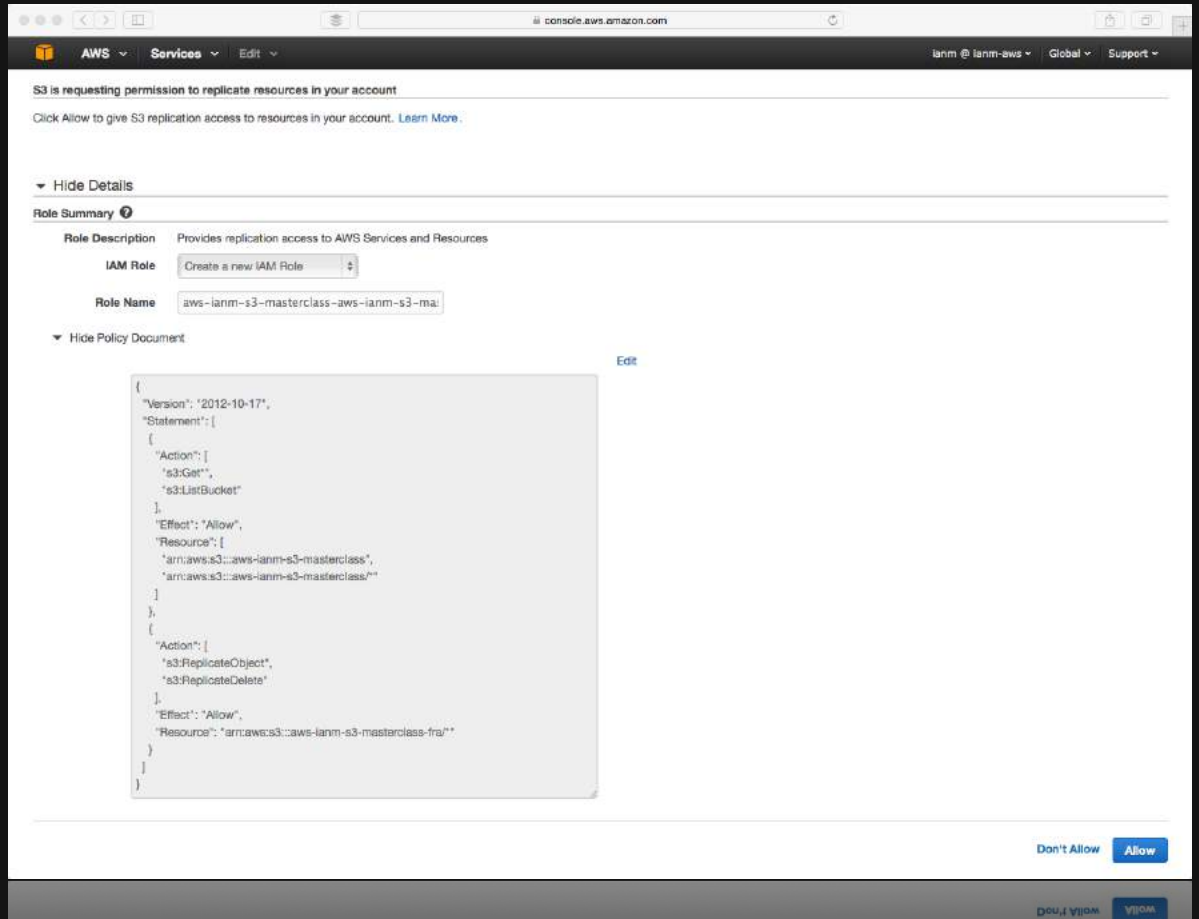
AWS Console


console.aws.amazon.com
AWS
Services
Edit
ianm @ ianm-aws
Global
Support
Create Bucket
Actions
None
Properties
Transfers
All Buckets (2)
Name
aws-ianm-s3-masterclass
aws-ianm-s3-masterclass-fra
Bucket: aws-ianm-s3-masterclass
Region: Ireland
Creation Date: Thu May 14 16:56:13 GMT+100 2015
Owner: ianm
MFA Delete: Not Enabled
Permissions
Static Website Hosting
Logging
Events
Versioning
Lifecycle
Cross-Region Replication
Cross-Region Replication replicates every future upload of every object in this bucket to another bucket. Cross-Region Replication is designed for use in conjunction with Versioning. You will be required to enable Versioning on this bucket and the target bucket. Learn More
Versioning is currently enabled on this bucket.
Suspend Versioning
Do Not Enable Cross-Region Replication
Enable Cross-Region Replication
Save
Cancel
Tags
Requester Pays
Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

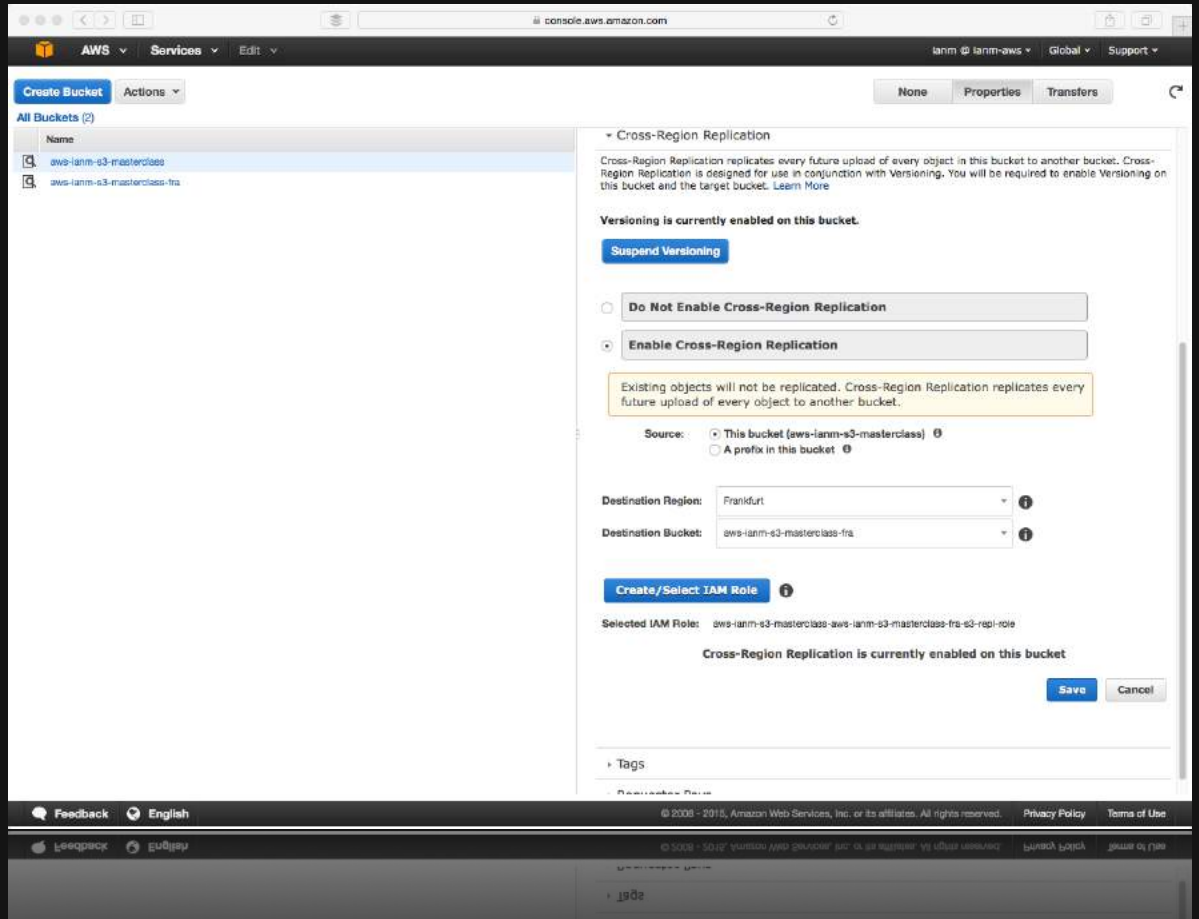
AWS Console


console.aws.amazon.com
AWS
Services
Edit
ianm @ ianm-aws
Global
Support
Create Bucket
Actions
None
Properties
Transfers
All Buckets (2)
Name
aws-ianm-s3-masterclass
aws-ianm-s3-masterclass-fra
Cross-Region Replication
Cross-Region Replication replicates every future upload of every object in this bucket to another bucket. Cross-Region Replication is designed for use in conjunction with Versioning. You will be required to enable Versioning on this bucket and the target bucket. Learn More
Versioning is currently enabled on this bucket.
Suspend Versioning
Do Not Enable Cross-Region Replication
Enable Cross-Region Replication
Existing objects will not be replicated. Cross-Region Replication replicates every future upload of every object to another bucket.
Source:
This bucket (aws-ianm-s3-masterclass)
A prefix in this bucket
Destination Region:
Frankfurt
Destination Bucket:
aws-ianm-s3-masterclass-fra
Create/Select IAM Role
Selected IAM Role:
Save
Cancel
Tags
Requester Pays
Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

AWS Console


console.aws.amazon.com
AWS
Services
Edit
ianm @ ianm-aws
Global
Support
S3 is requesting permission to replicate resources in your account
Click Allow to give S3 replication access to resources in your account. Learn More.
Hide Details
Role Summary
Role Description
Provides replication access to AWS Services and Resources
IAM Role
Create a new IAM Role
Role Name
aws-ianm-s3-masterclass-aws-ianm-s3-ma
Hide Policy Document
Edit
{
"Version": "2012-10-17",
"Statement": [
{
"Action": [
"s3:Get*",
"s3:ListBucket"
],
"Effect": "Allow",
"Resource": [
"arn:aws:s3:::aws-ianm-s3-masterclass",
"arn:aws:s3:::aws-ianm-s3-masterclass/*"
]
},
{
"Action": [
"s3:ReplicateObject",
"s3:ReplicateDelete"
],
"Effect": "Allow",
"Resource": "arn:aws:s3:::aws-ianm-s3-masterclass-fra/*"
}
]
}
Don't Allow
Allow

AWS Console


console.aws.amazon.com
AWS
Services
Edit
iannm @ iannm-aws
Global
Support
Create Bucket
Actions
None
Properties
Transfers
All Buckets (2)
Name
aws-iannm-s3-masterclass
aws-iannm-s3-masterclass-fra
Cross-Region Replication
Cross-Region Replication replicates every future upload of every object in this bucket to another bucket. Cross-Region Replication is designed for use in conjunction with Versioning. You will be required to enable Versioning on this bucket and the target bucket. Learn More
Versioning is currently enabled on this bucket.
Suspend Versioning
Do Not Enable Cross-Region Replication
Enable Cross-Region Replication
Existing objects will not be replicated. Cross-Region Replication replicates every future upload of every object to another bucket.
Source:
This bucket (aws-iannm-s3-masterclass)
A prefix in this bucket
Destination Region:
Frankfurt
Destination Bucket:
aws-iannm-s3-masterclass-fra
Create/Select IAM Role
Selected IAM Role:
aws-iannm-s3-masterclass-aws-iannm-s3-masterclass-fra-s3-repl-role
Cross-Region Replication is currently enabled on this bucket
Save
Cancel
Tags
Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

AWS CLI

```
$ aws s3 cp s3-masterclass-logo.txt s3://aws-ianm-s3-masterclass
upload: ./s3-masterclass-logo.txt to s3://aws-ianm-s3-masterclass/s3-masterclass-logo.txt

$ aws s3 ls s3://aws-ianm-s3-masterclass-fra --region=eu-central-1
2015-05-18 17:27:47        337 s3-masterclass-logo.txt
```

LIFECYCLE RULES

Object Deletion

Permanently delete objects from S3

LIFECYCLE RULES

Object Archiving

Move objects from S3 to Glacier

Amazon Glacier

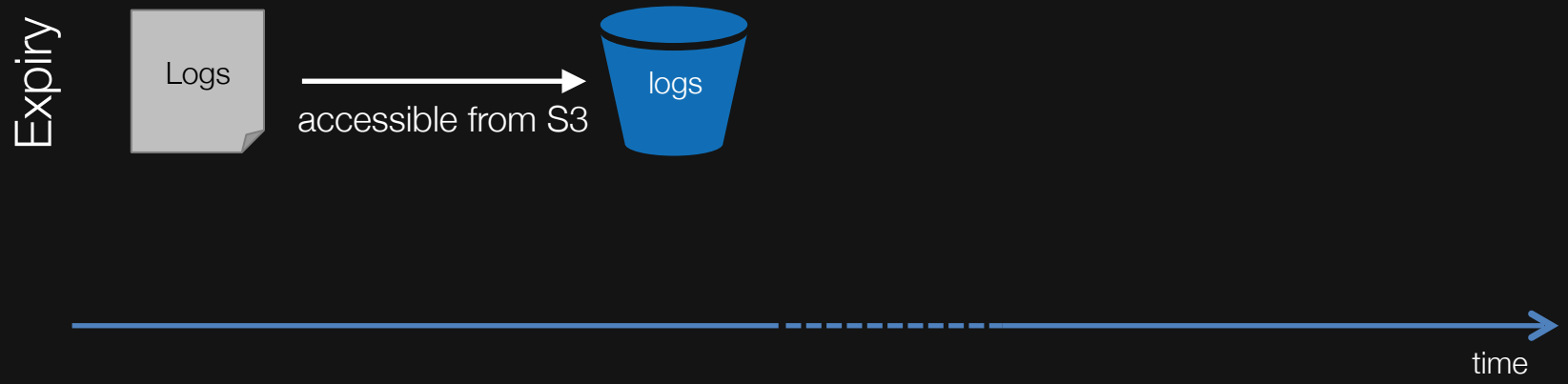
Durable

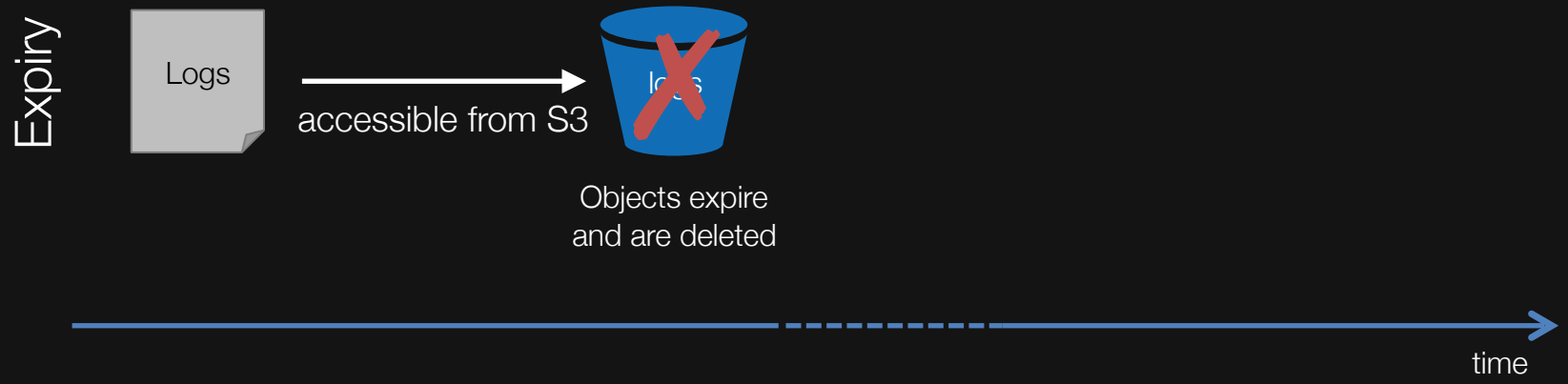
Designed for 99.999999999% durability of archives

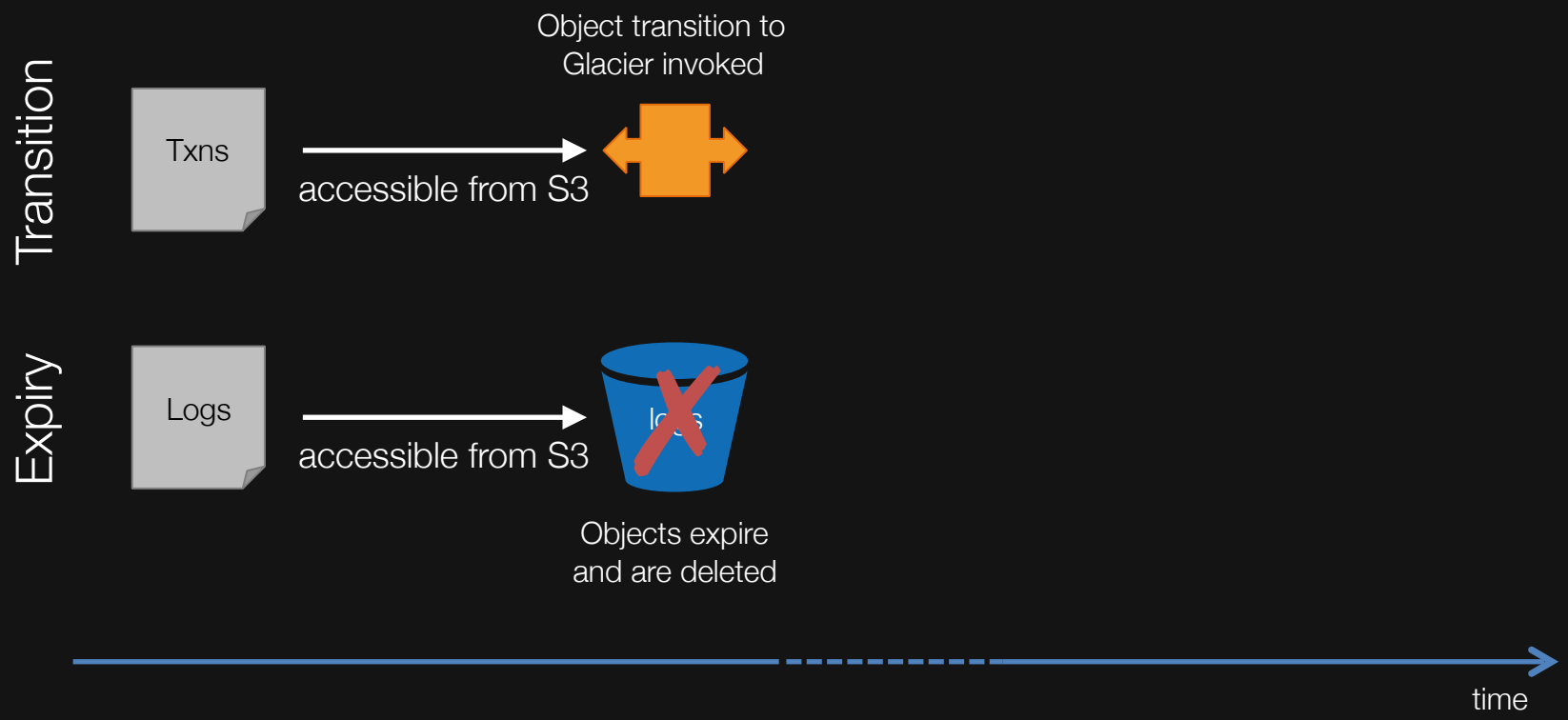
Amazon Glacier

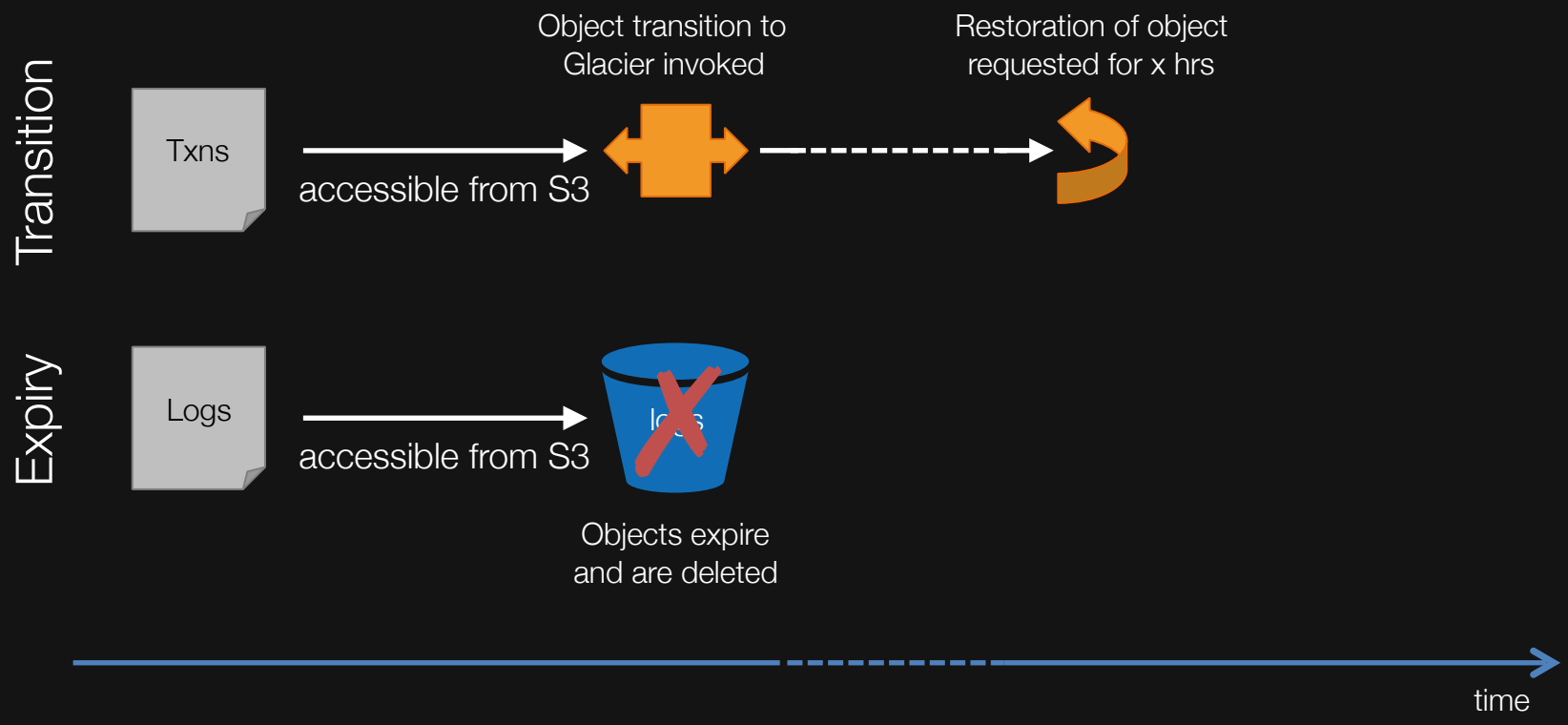
Cost Effective

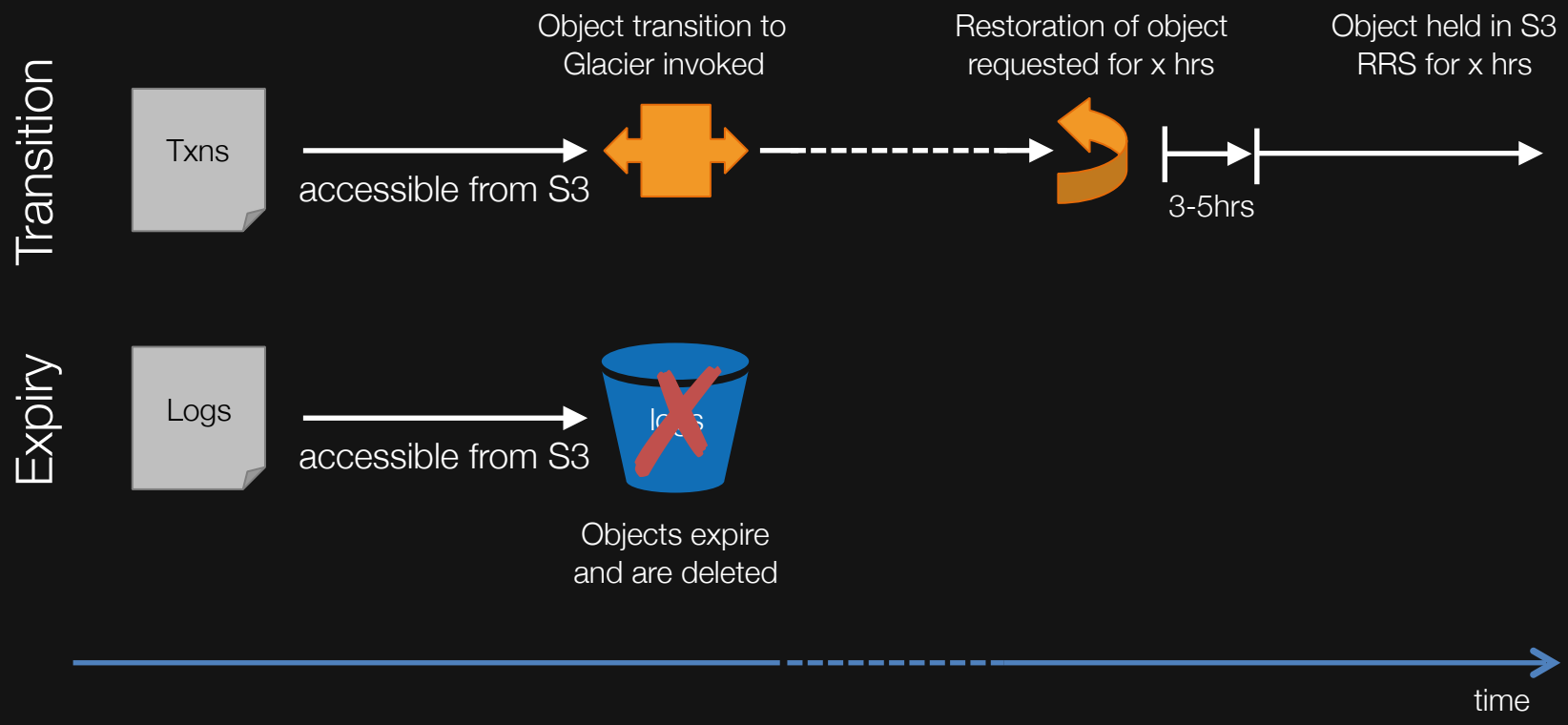
Write-once, read-never. Cost effective for long term storage. Pay for accessing data


Expiry
Logs
accessible from S3
logs
time


Expiry
Logs
accessible from S3
Objects expire
and are deleted
time

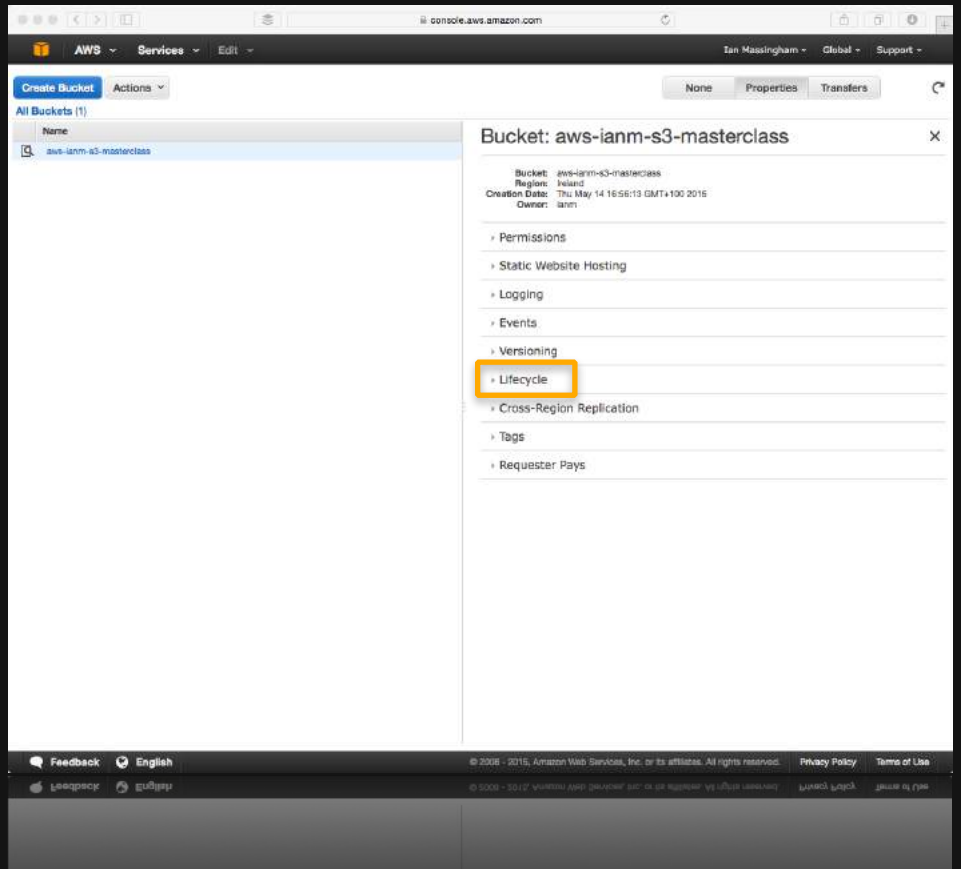

Transition
Txns
Object transition to
Glacier invoked
accessible from S3
Expiry
Logs
accessible from S3
Objects expire
and are deleted
time


Transition
Txns
accessible from S3
Object transition to
Glacier invoked
Restoration of object
requested for x hrs
Expiry
Logs
accessible from S3
Objects expire
and are deleted
time


Transition
Txns
accessible from S3
Object transition to Glacier invoked
Restoration of object requested for x hrs
3-5hrs
Object held in S3 RRS for x hrs
Expiry
Logs
accessible from S3
Objects expire and are deleted
time

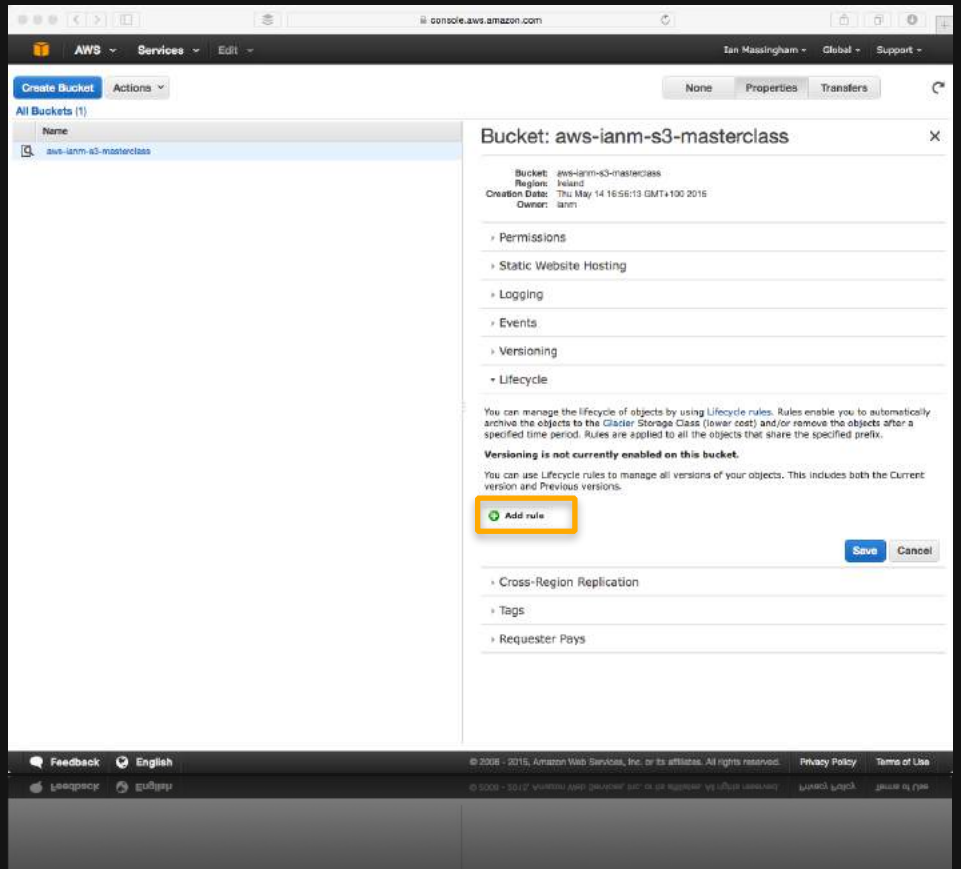
Configuring Lifecycle Rules

AWS Console



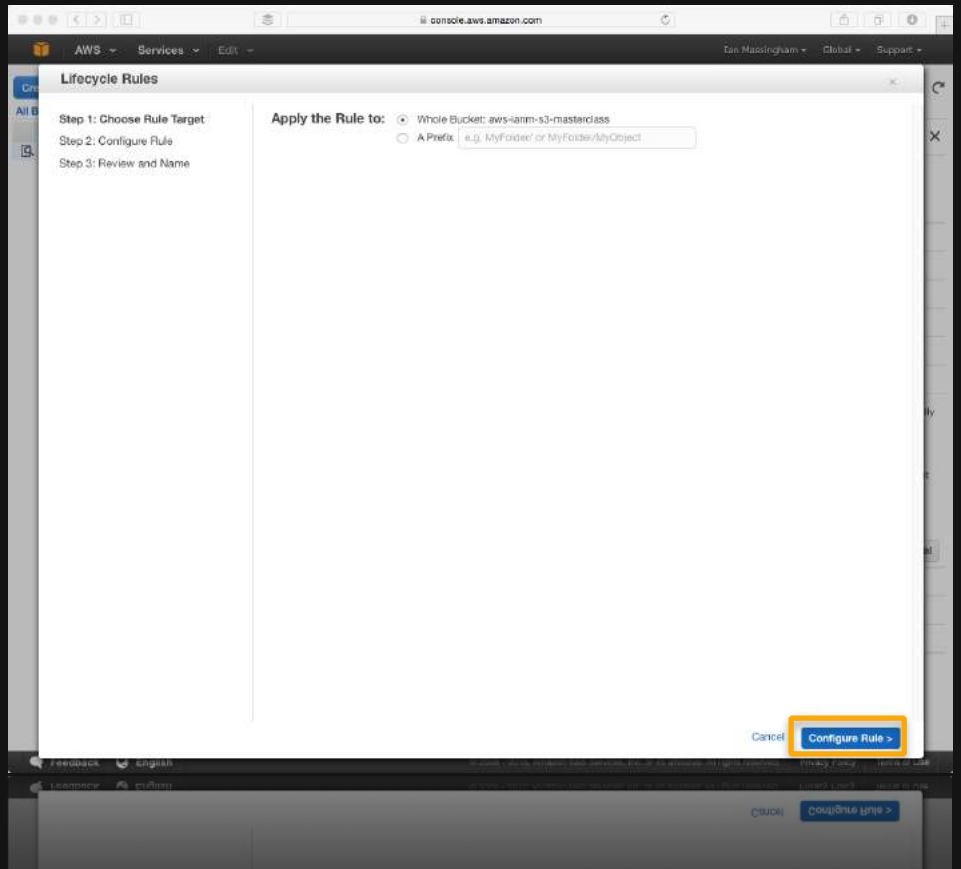
Configuring Lifecycle Rules

AWS Console



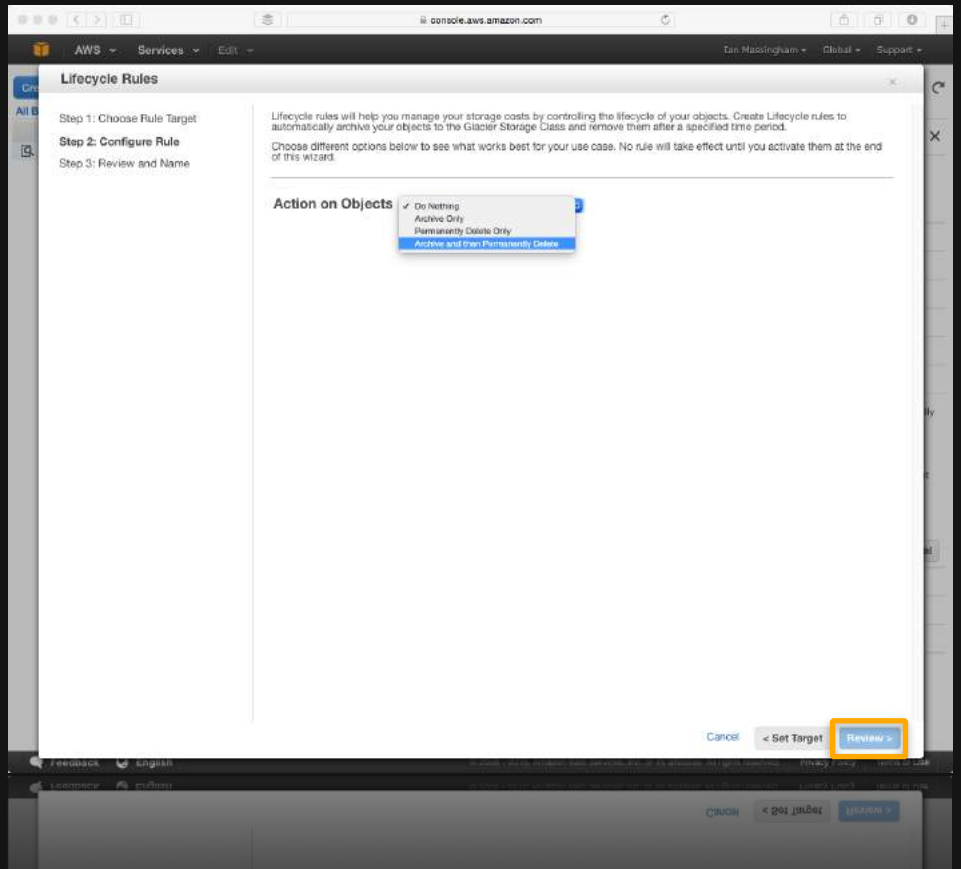
Configuring Lifecycle Rules

AWS Console



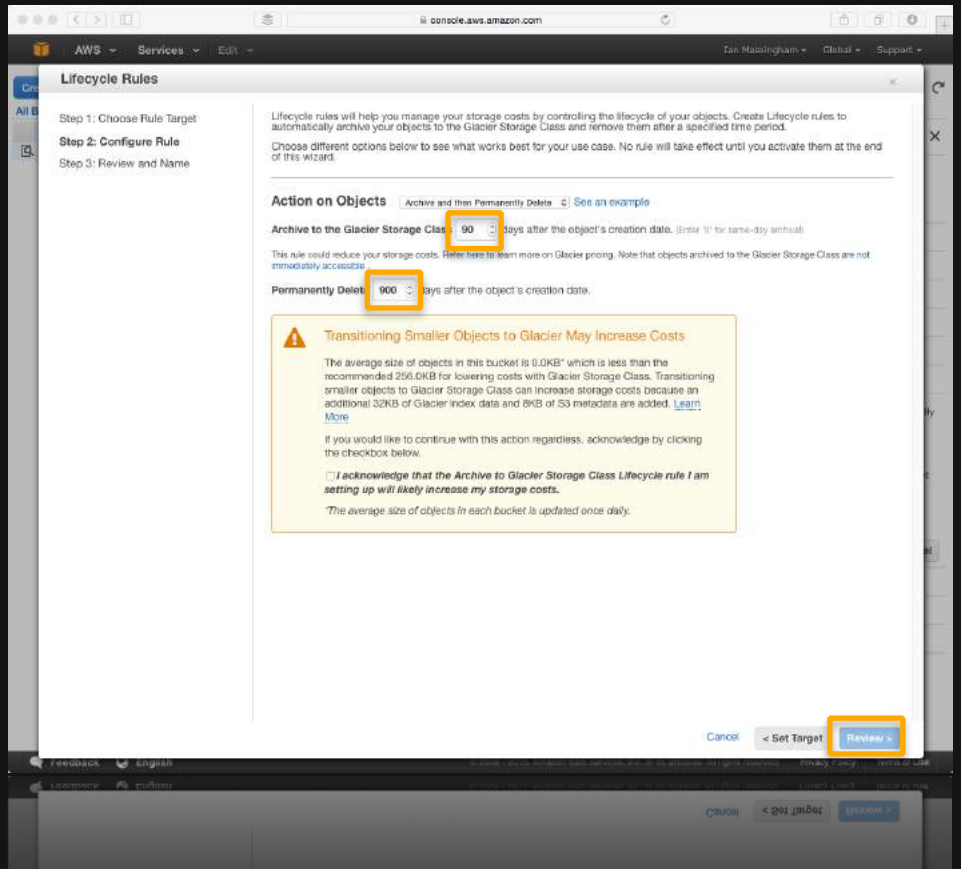
Configuring Lifecycle Rules

AWS Console



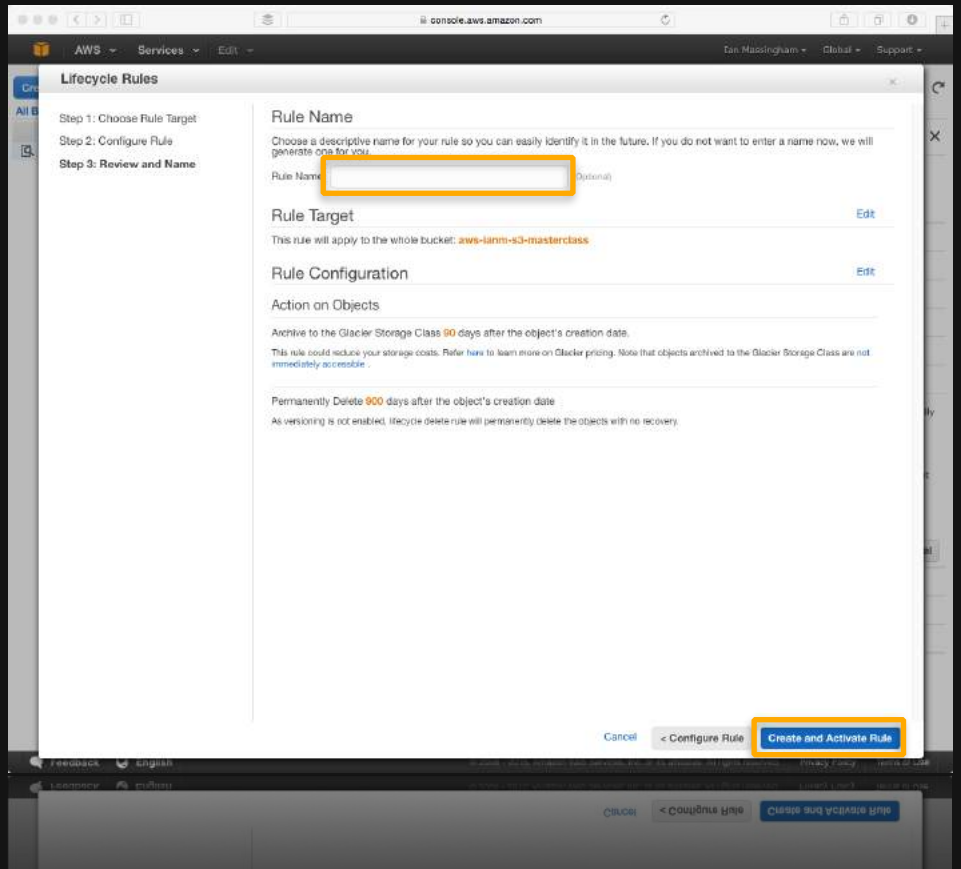
Configuring Lifecycle Rules

AWS Console



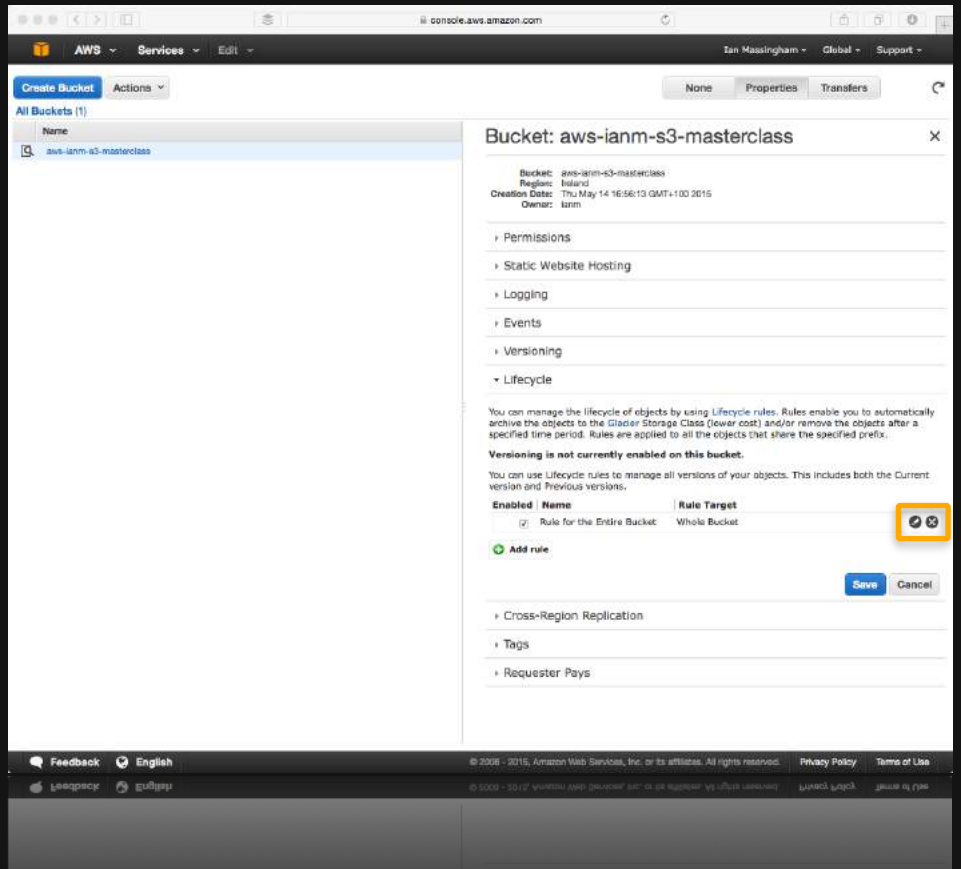
Configuring Lifecycle Rules

AWS Console



Configuring Lifecycle Rules

AWS Console



Configuring Lifecycle Rules

.Net

```
using (client = new AmazonS3Client()){
  var lifeCycleConfiguration = new LifecycleConfiguration()
  {
    Rules = new List<LifecycleRule>
    {
        new LifecycleRule
        {
             Id = "Archive and delete rule",
             Prefix = "projectdocs/",
             Status = LifecycleRuleStatus.Enabled,
              Transition = new LifecycleTransition()
              {
                   Days = 365,
                   StorageClass = S3StorageClass.Glacier
              },
              Expiration = new LifecycleRuleExpiration()
              {
                   Days = 3650
              }
        }
    }
  };
```

Configuring Lifecycle Rules

.Net

```
using (client = new AmazonS3Client()){
  var lifeCycleConfiguration = new LifecycleConfiguration()
  {
    Rules = new List<LifecycleRule>
    {
        new LifecycleRule
        {
             Id = "Archive and delete rule",
             Prefix = "projectdocs/",
             Status = LifecycleRuleStatus.Enabled,
             Transition = new LifecycleTransition()
             {
                  Days = 365,
                  StorageClass = S3StorageClass.Glacier
             },
              Expiration = new LifecycleRuleExpiration()
              {
                  Days = 3650
              }
        }
    }
  };
```

Transition to Glacier after 1 year

Configuring Lifecycle Rules

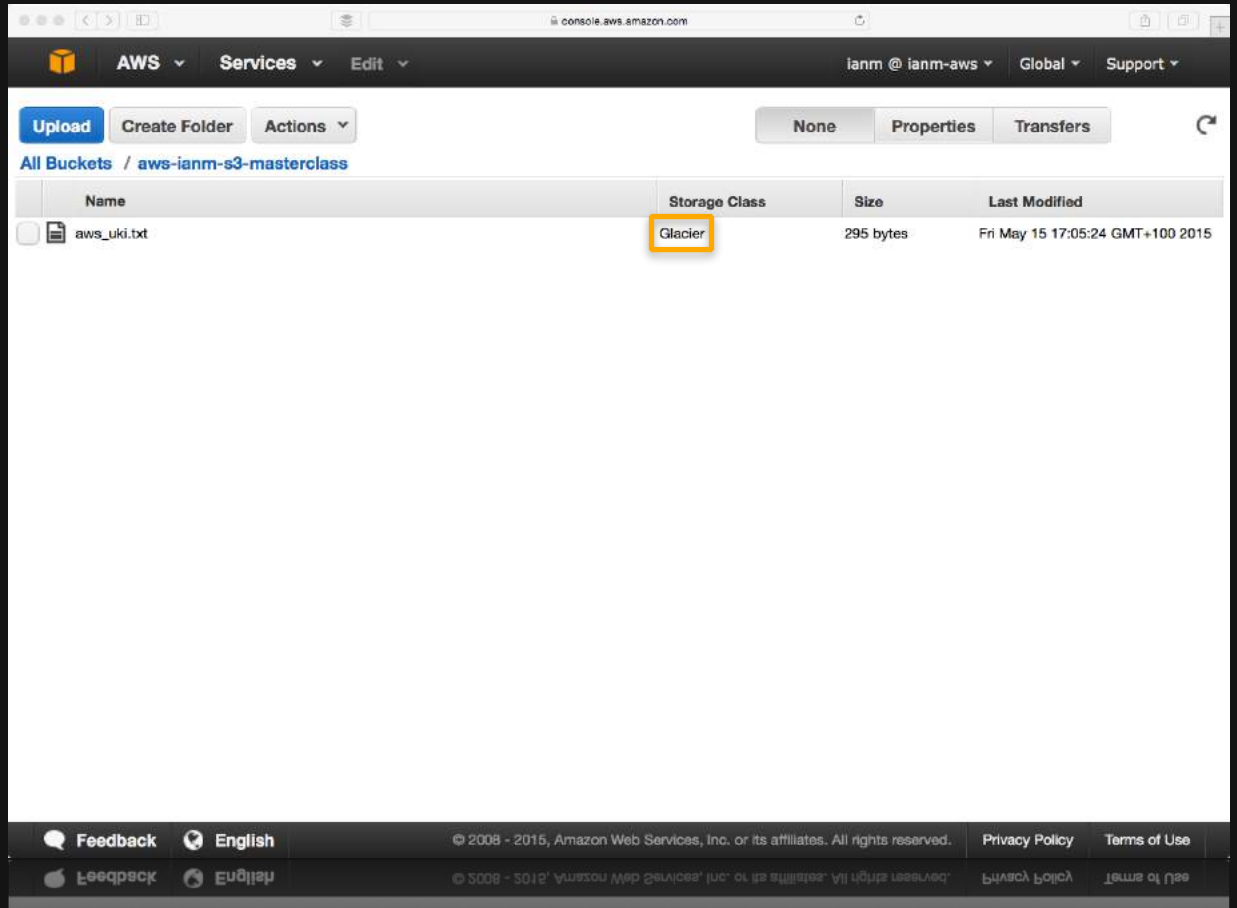
.Net

```
using (client = new AmazonS3Client()){
  var lifeCycleConfiguration = new LifecycleConfiguration()
  {
    Rules = new List<LifecycleRule>
    {
        new LifecycleRule
        {
             Id = "Archive and delete rule",
             Prefix = "projectdocs/",
             Status = LifecycleRuleStatus.Enabled,
              Transition = new LifecycleTransition()
              {
                   Days = 365,
                   StorageClass = S3StorageClass.Glacier
              },
             Expiration = new LifecycleRuleExpiration()
             {
                   Days = 3650
             }
        }
    }
  };
```

Delete object after 10 years

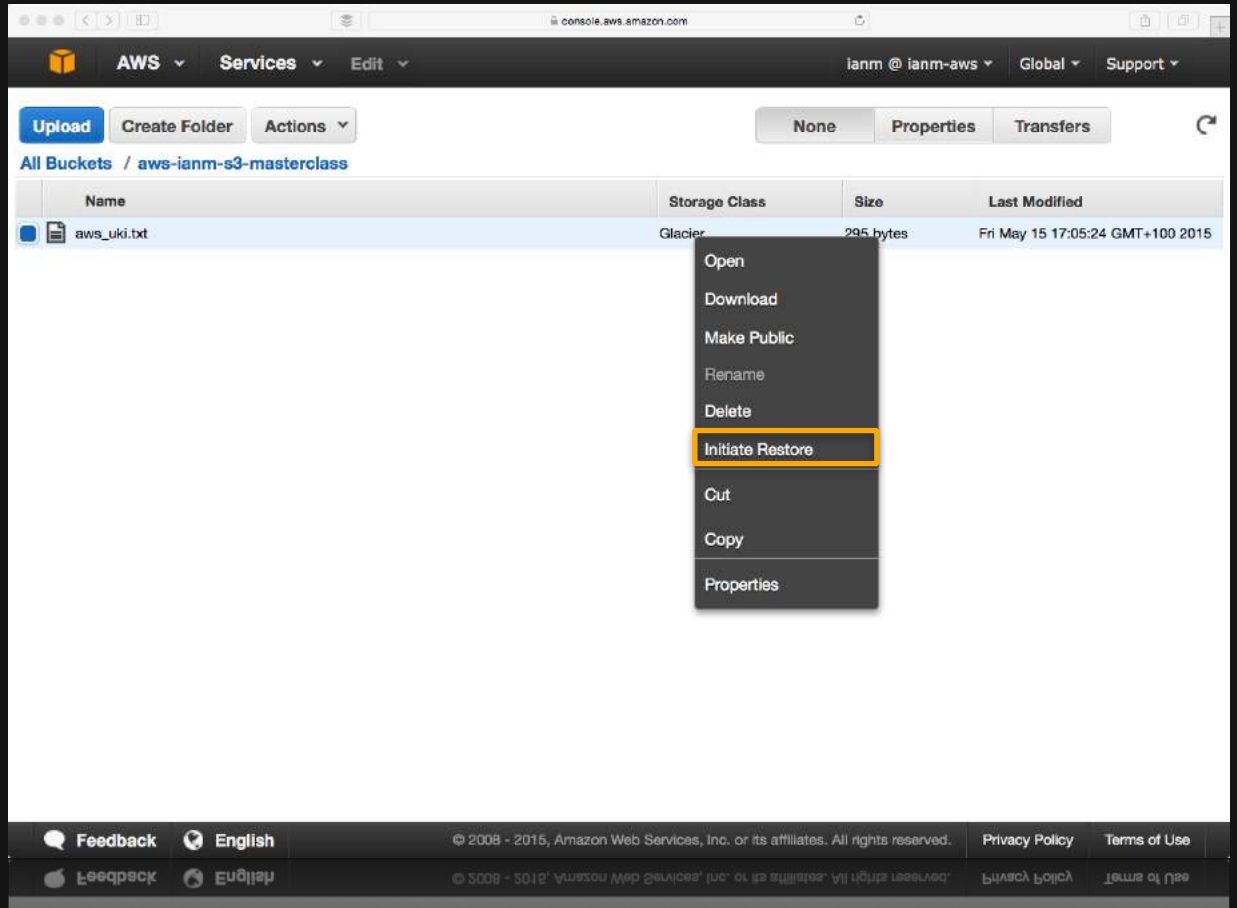
Restoring from Amazon Glacier

AWS Console



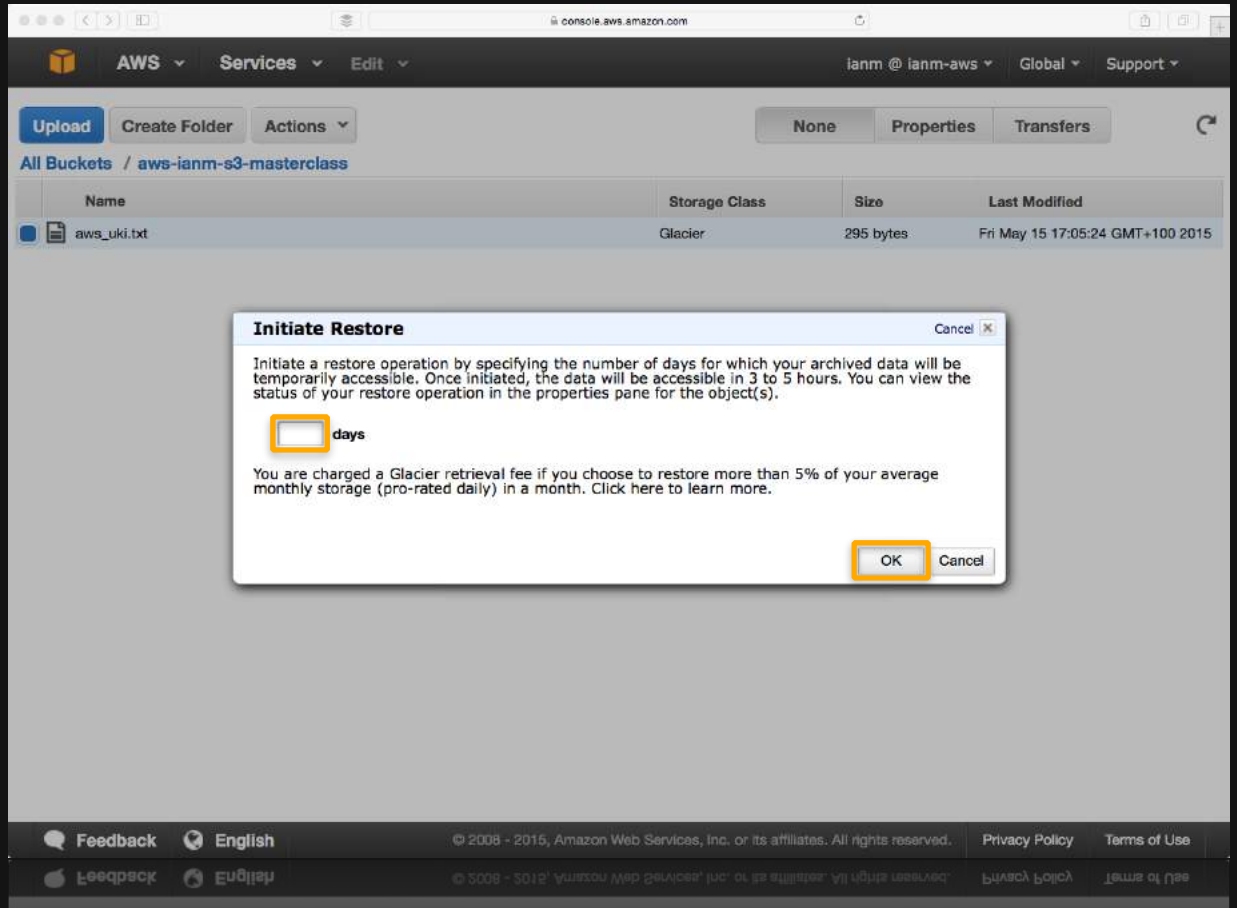
Restoring from Amazon Glacier

AWS Console



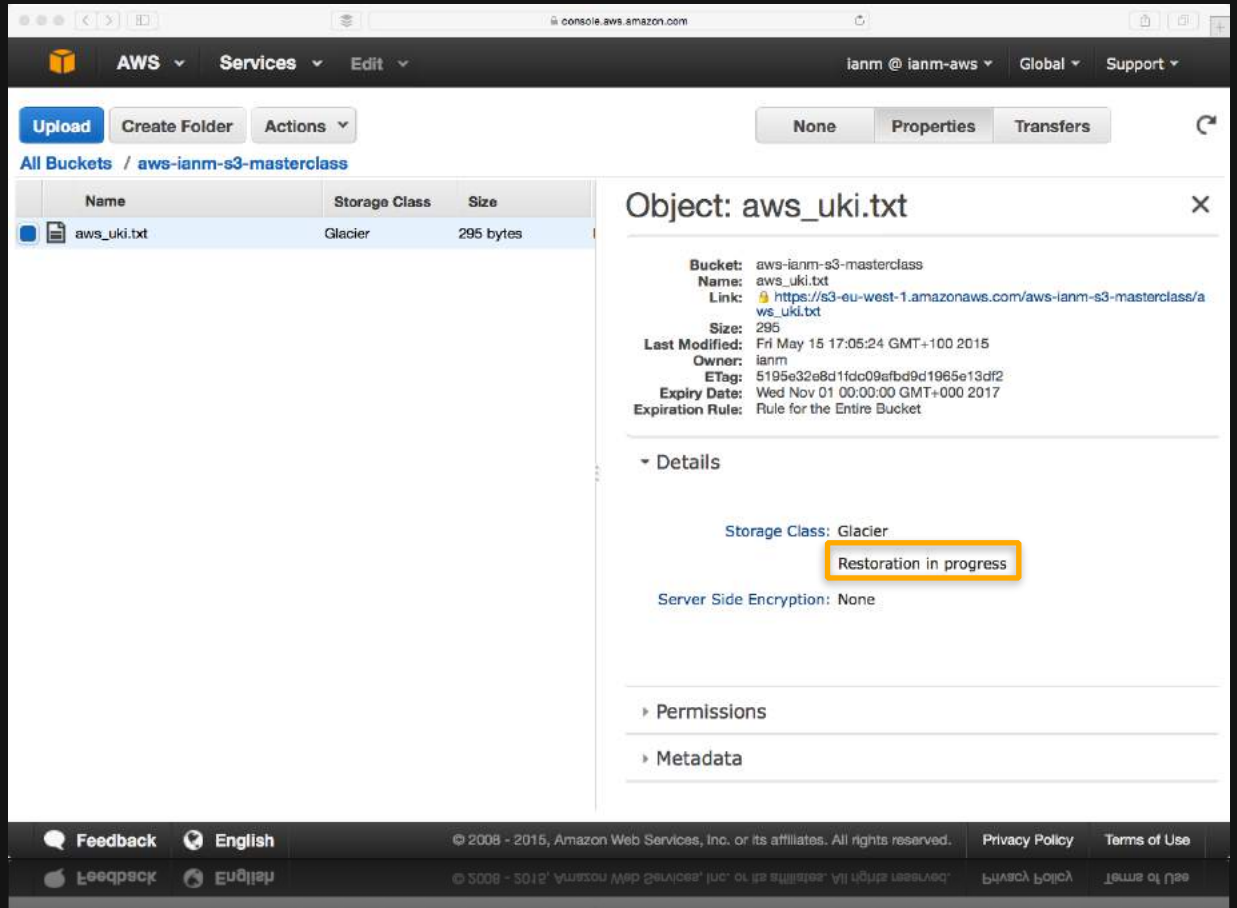
Restoring from Amazon Glacier

AWS Console



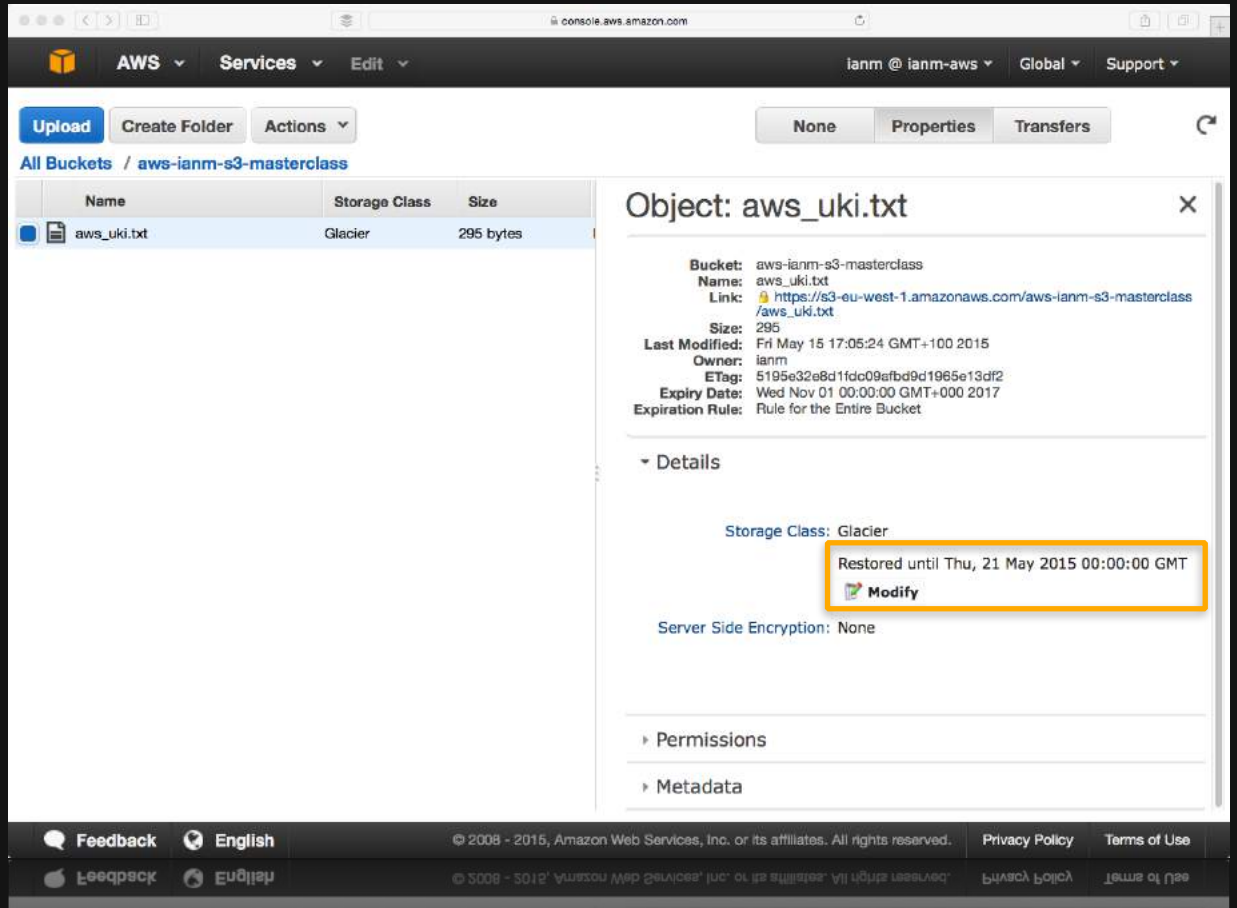
Restoring from Amazon Glacier

AWS Console



Restoring from Amazon Glacier

AWS Console



WEBSITE HOSTING

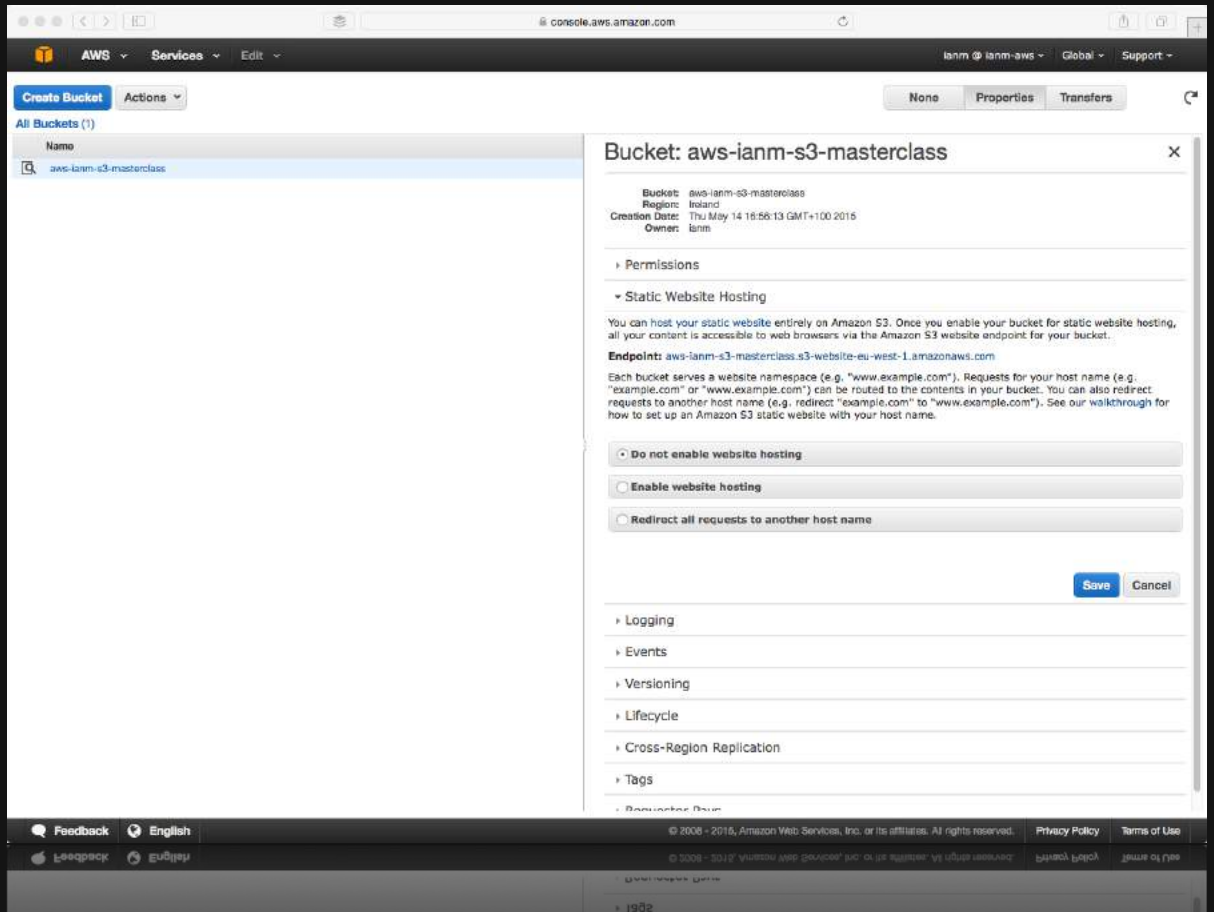
Static Website Hosting with Amazon S3

You can host your entire static website on Amazon S3 for a low-cost, highly available hosting solution that can scale automatically to meet traffic demands

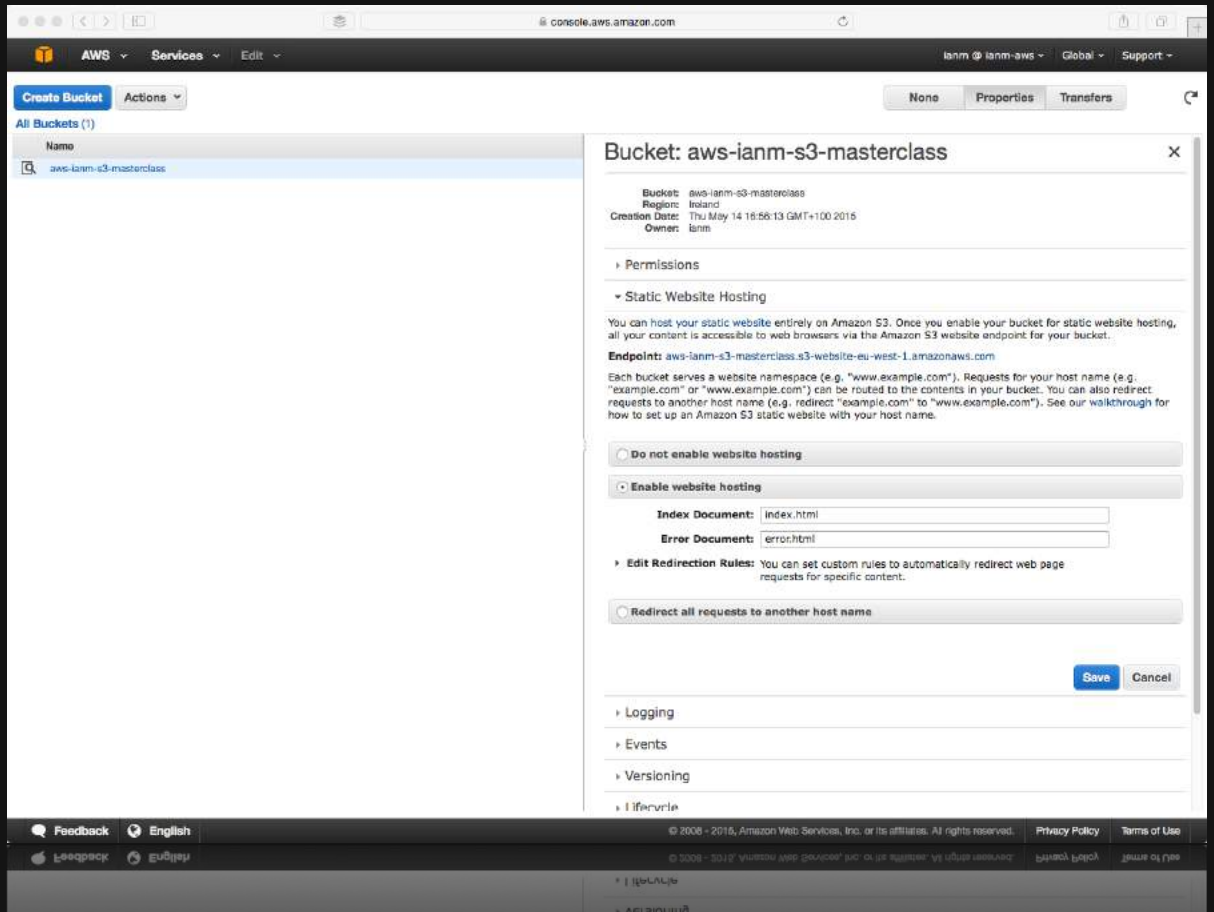
With Amazon S3, you can reliably serve your traffic and handle unexpected peaks without worrying about scaling your infrastructure

docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-custom-domain-walkthrough.html

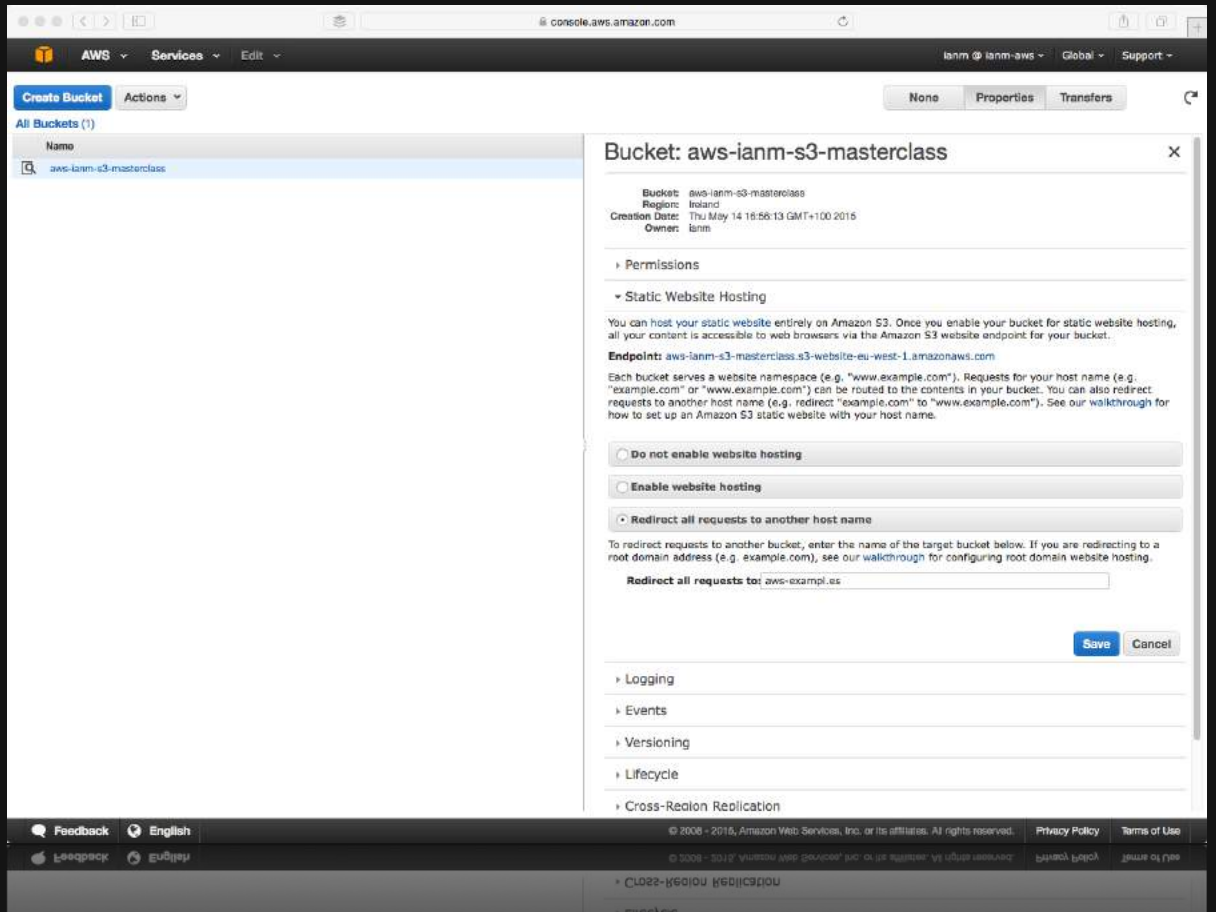
Static Website Hosting Bucket Properties



Setting Default Documents



Redirecting Requests



Bucket Policy

```
{
  "Version":"2008-10-17",
  "Statement":[{
     "Sid":"PublicReadGetObject",
       "Effect":"Allow",
      "Principal": {
          "AWS": "*"
        },
      "Action":["s3:GetObject"],
      "Resource":["arn:aws:s3:::example-bucket/*"
      ]
    }
  ]
}
```

Website Addressing

```
{bucket-name}.s3-website-{region}.amazonaws.com
e.g. mybucket.s3-website-eu-west-1.amazonaws.com
```

Normal Addressing

```
s3-{region}.amazonaws.com/{bucket-name}/{object-key}
e.g. s3-eu-west-1.amazonaws.com/mybucket/img.png

{bucket-name}.s3-{region}.amazonaws.com/{object-key}
e.g. mybucket.s3-eu-west-1.amazonaws.com/img.png
```

DNS Record set for:

`aws-exampl.es`

DNS Record set for:

`aws-exampl.es`

Website bucket name:

`www.aws-exampl.es`

Website bucket name:

`aws-exampl.es`

DNS Record set for:

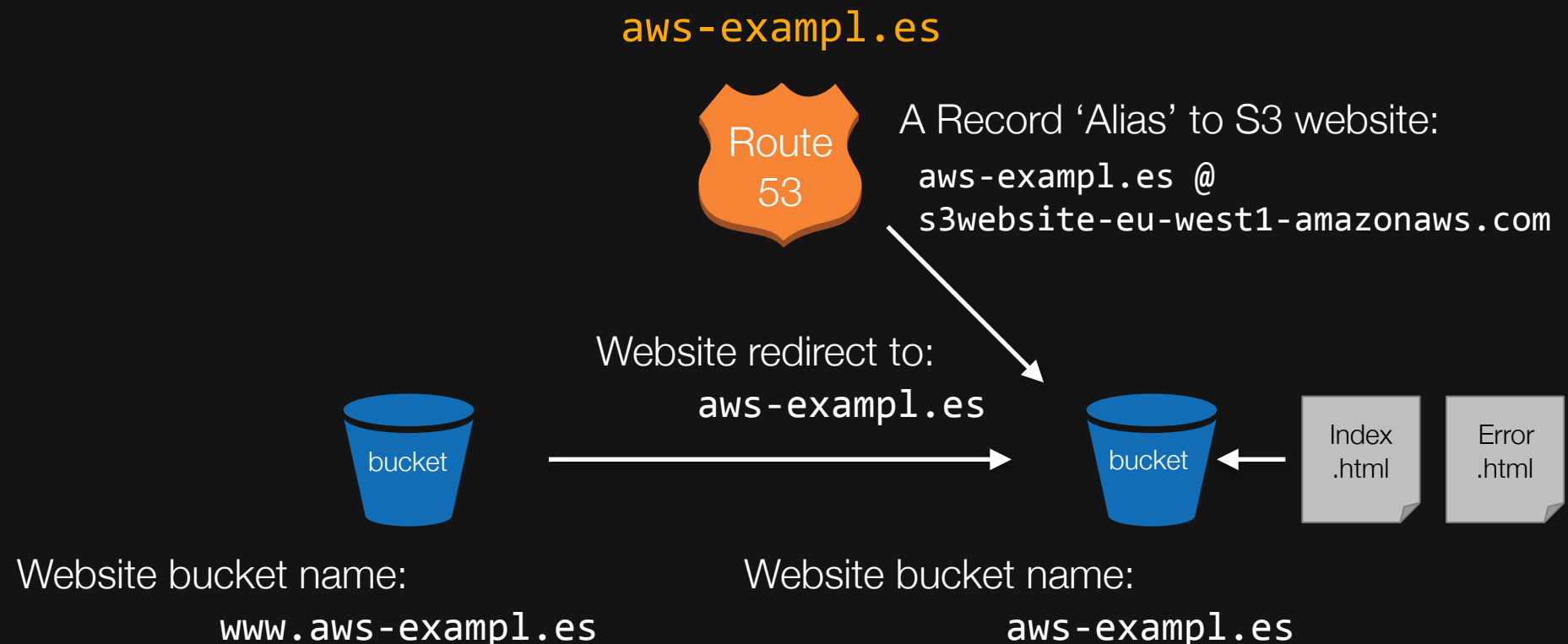
`aws-exampl.es`

Website redirect to:
`aws-exampl.es`

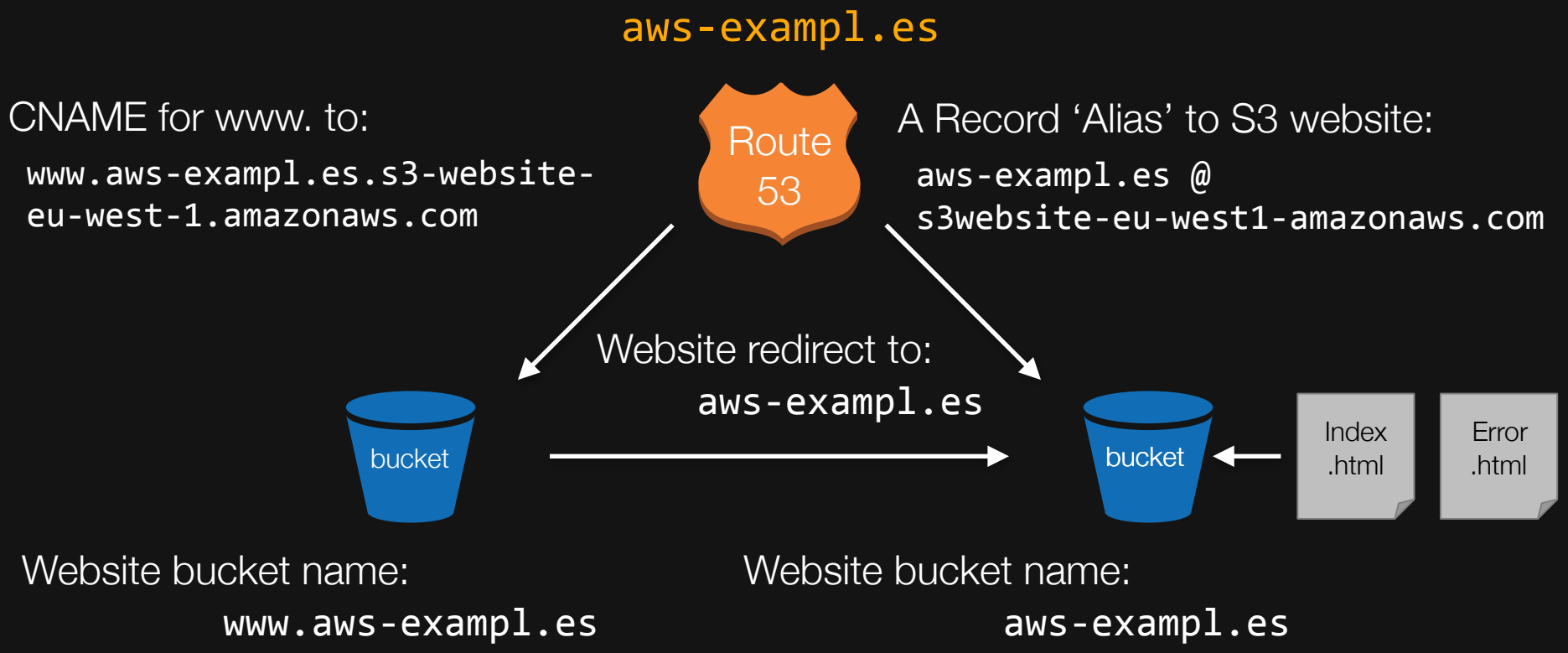
Website bucket name:
`www.aws-exampl.es`

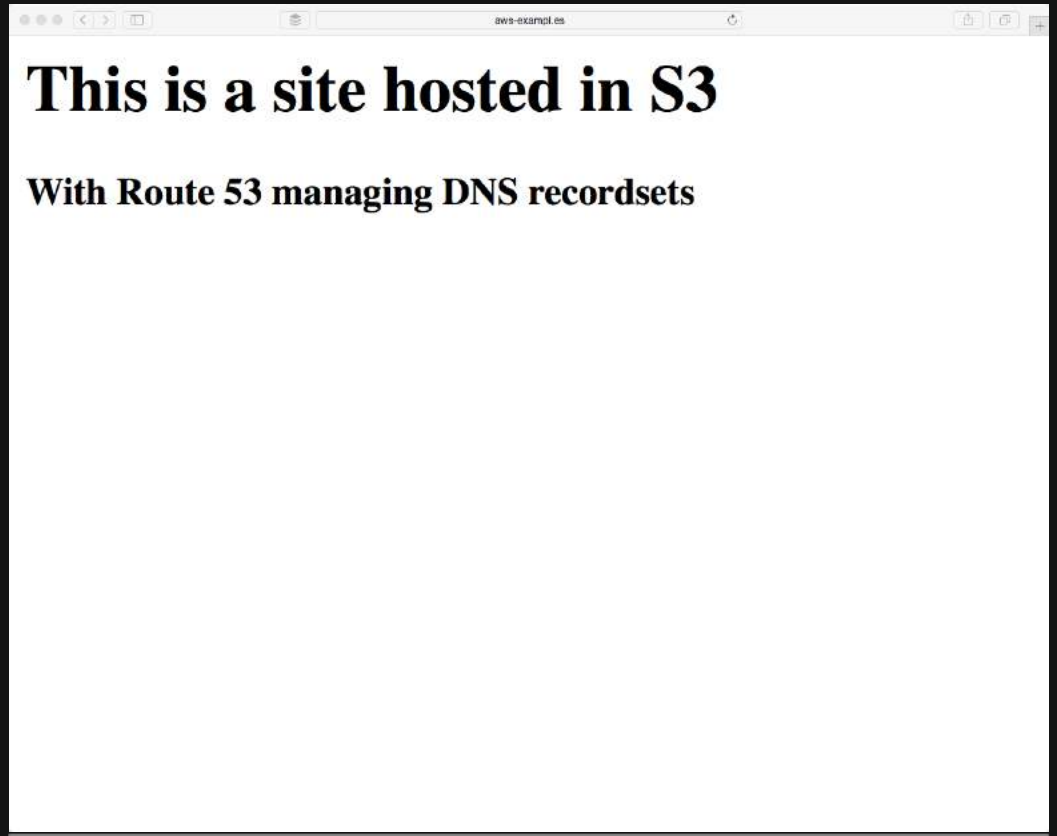
Website bucket name:
`aws-exampl.es`

DNS Record set for:



DNS Record set for:





docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-custom-domain-walkthrough.html

SUMMARY

① S3 provides developers with secure, durable & highly scalable object storage

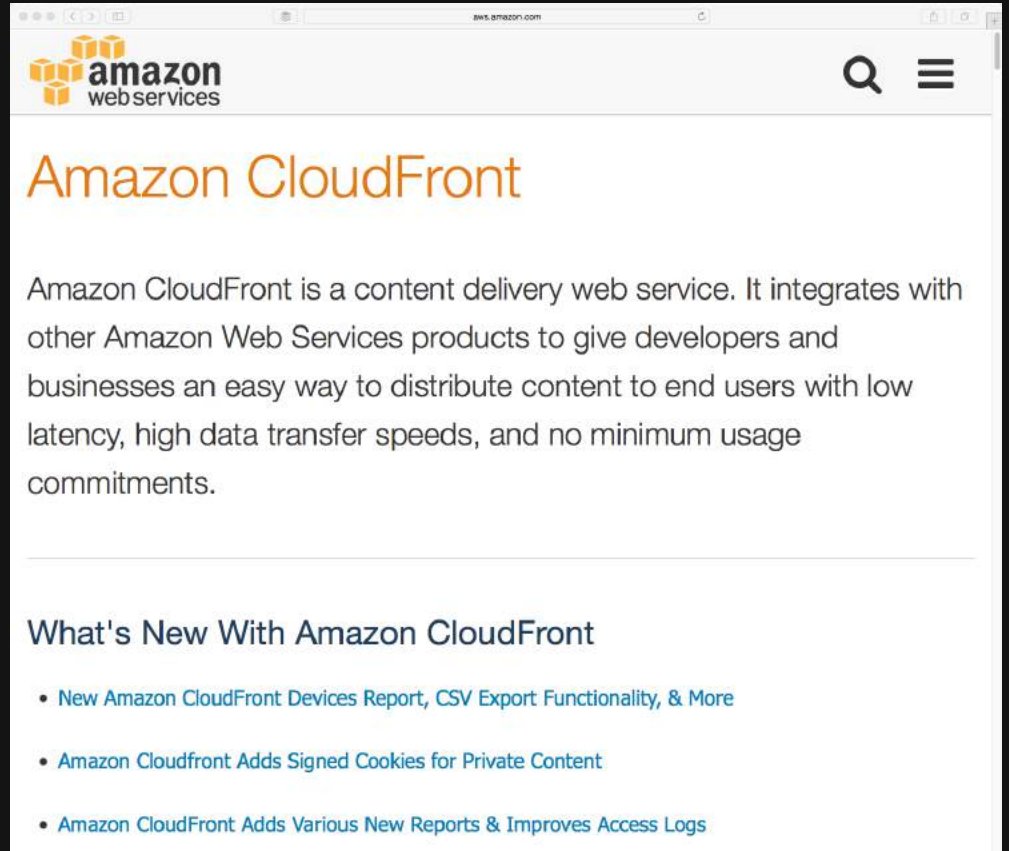
② S3 can be used alone with other AWS services or 3rd party tools & services

③ Cost effective for a wide variety of use-cases from cloud applications, content distribution, backup, archiving & disaster recovery to analytics

THINGS WE DIDN’T COVER

Amazon CloudFront

aws.amazon.com/cloudfront



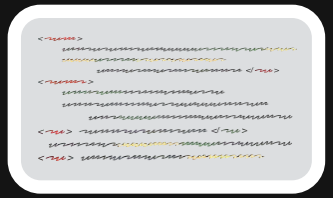
S3 EVENT NOTIFICATIONS

http://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html

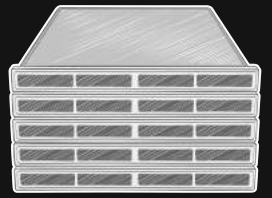
AWS Lambda

aws.amazon.com/lambda

S3 event notifications



Cloud Functions



Automatic

RESOURCES YOU CAN USE TO LEARN MORE

aws.amazon.com/s3

Getting Started with Amazon S3:

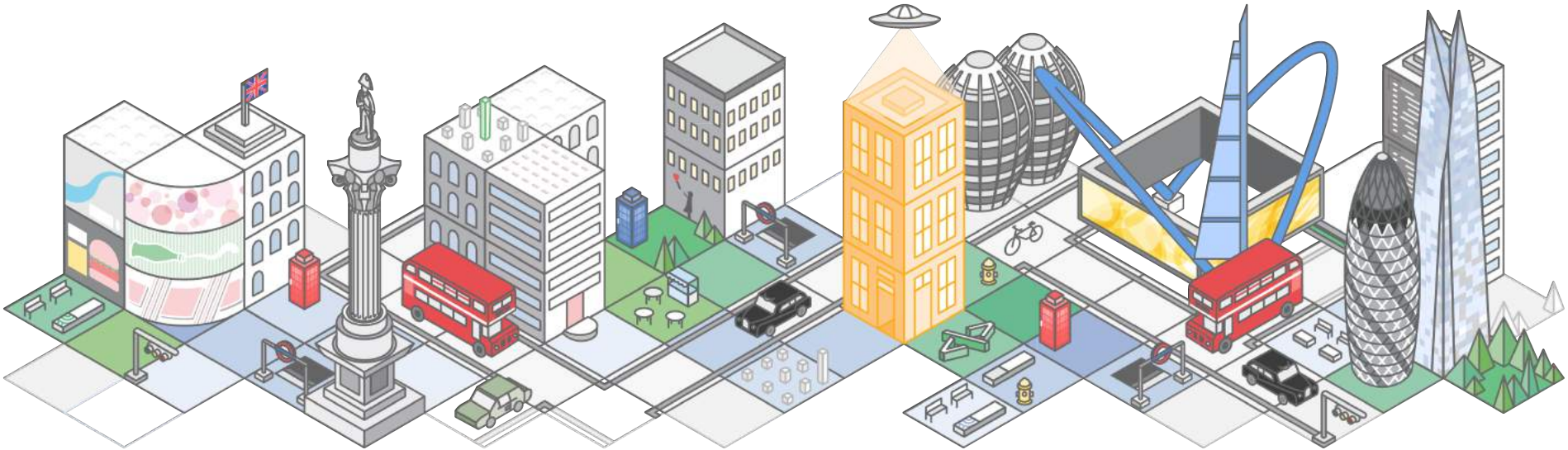
docs.aws.amazon.com/AmazonS3/latest/gsg/GetStartedWithS3.html

Amazon S3 Deep Dive & Best Practices session from AWS re:Invent 2014

https://youtu.be/2DpOS0zu8O0

Amazon S3 Documentation:

aws.amazon.com/documentation/s3/



Thank You

Ian Massingham @IanMmmm
Chief Evangelist (EMEA), AWS