AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

STG319

Building a compliant data archive

Pablo Salazar
Senior Practice Manager
Professional Services
Amazon Web Services

Eric Bowman
Senior Storage Solutions Architect
S3 Glacier
Amazon Web Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compliant archives

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compliance

and

Cost

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is a compliant archive?

Questions customers often ask:

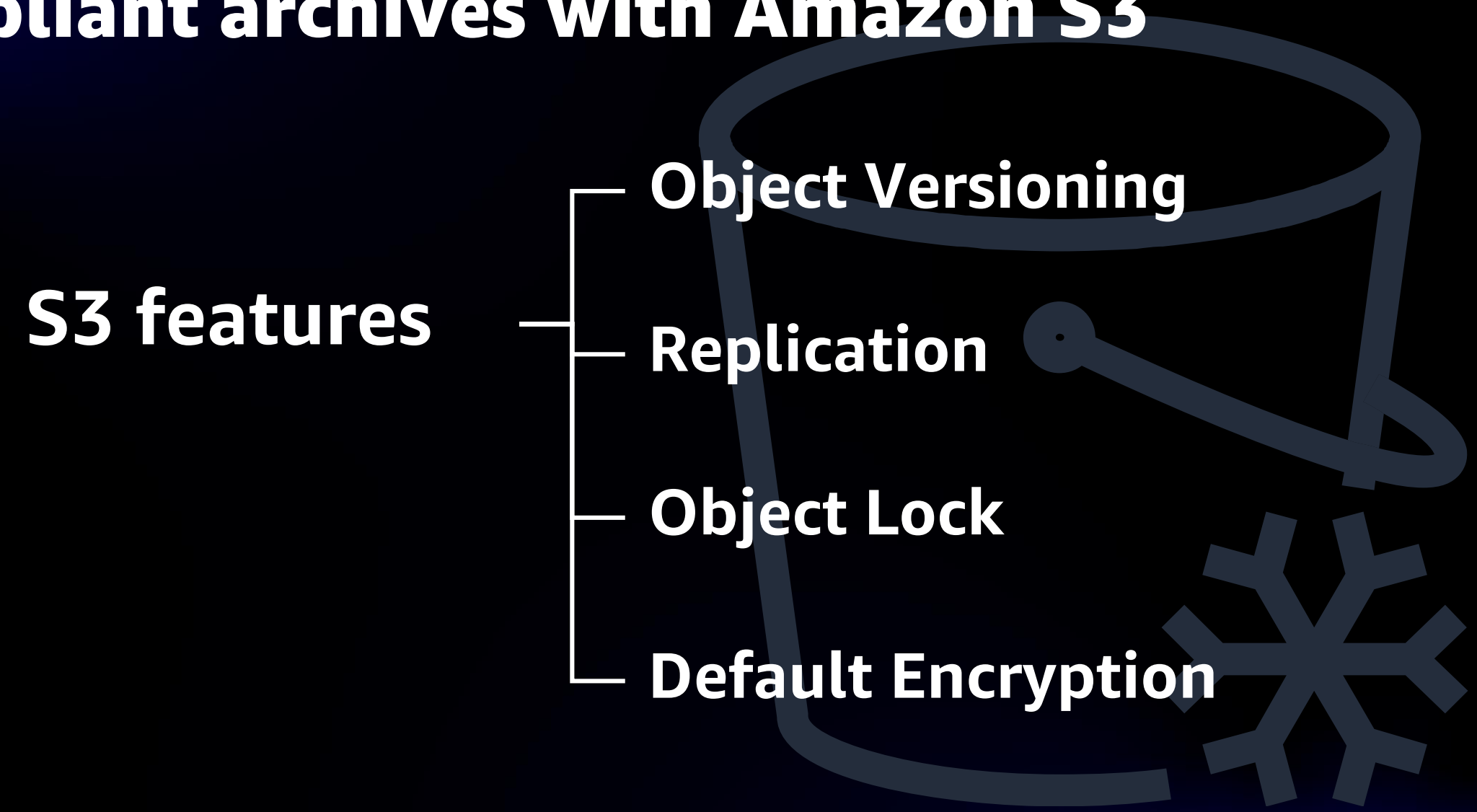
- What are the regulatory requirements for archival storage?
- How long do I need to store a data type?
- How often must I retrieve a data type during operations?
- How quickly must I retrieve a data type during operations?

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 and S3 Glacier – Control features

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compliant archives with Amazon S3



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Object versioning

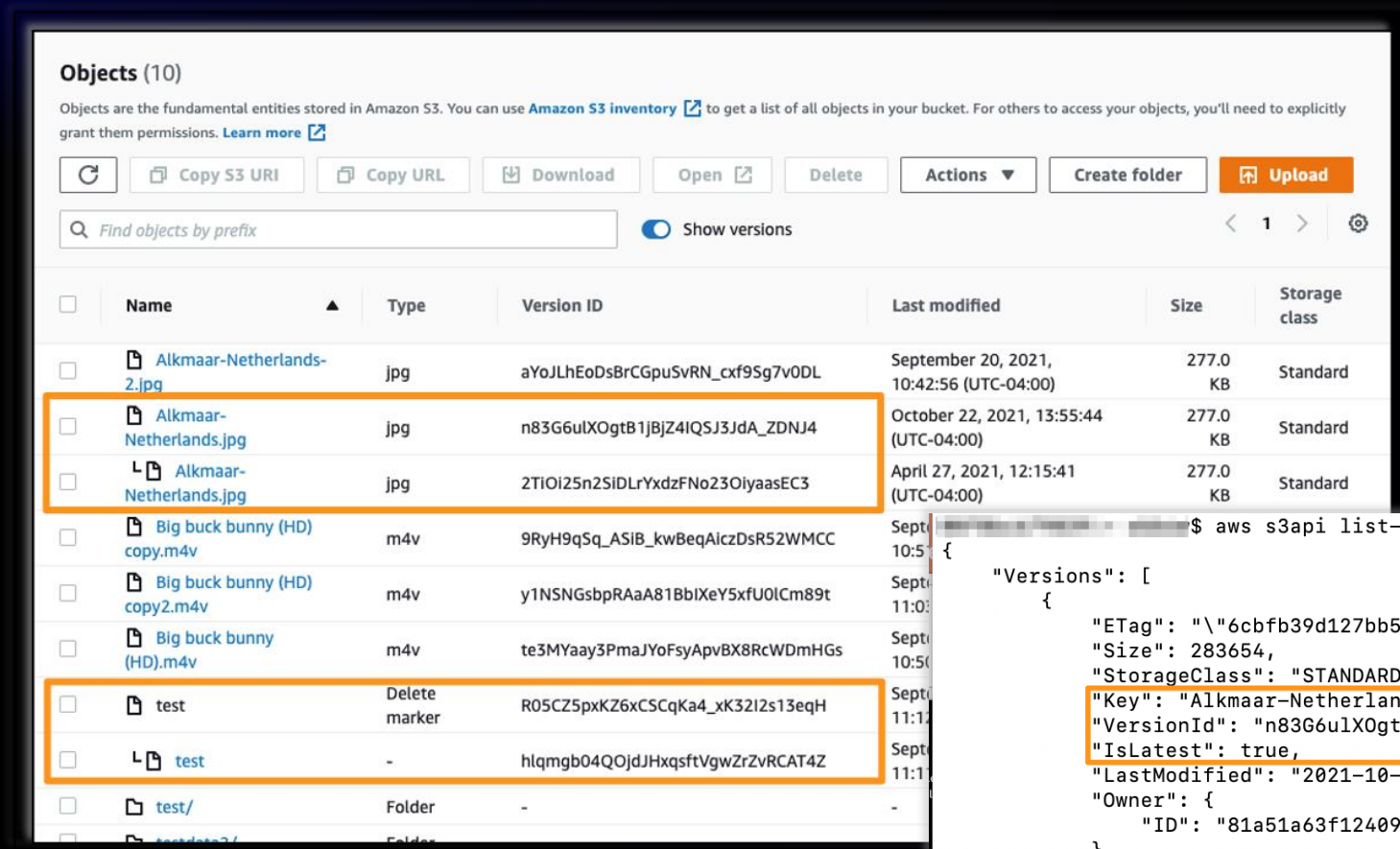
If you want to protect your data from…

- Unintended user actions leading to data overwrites or deletes
- Application code failures leading to data overwrites or deletes

…use bucket versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

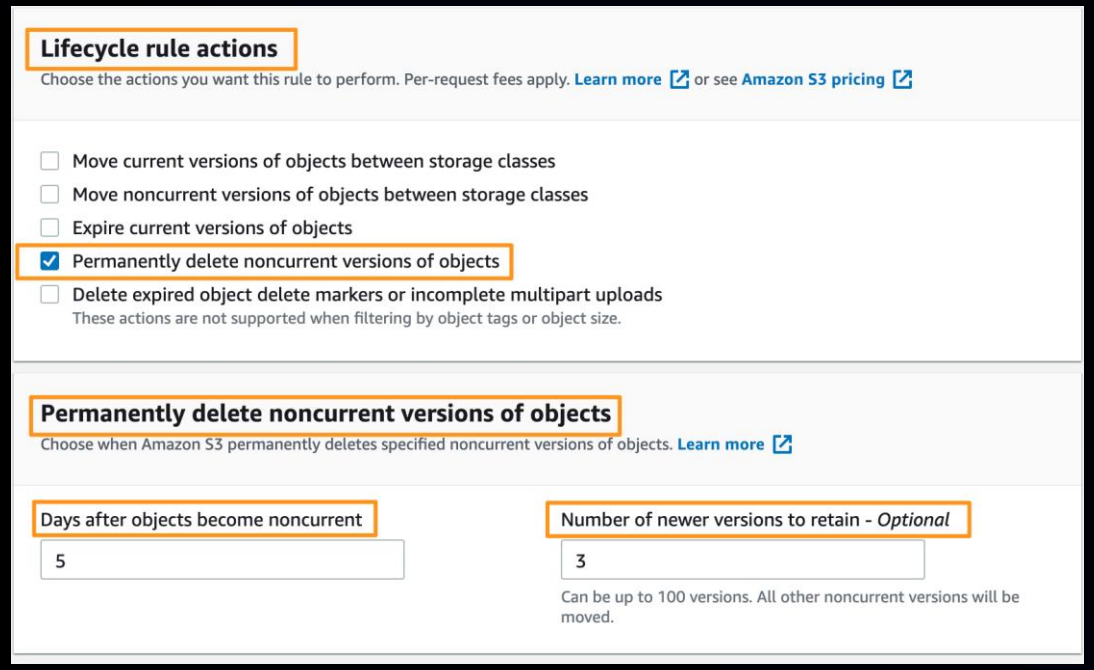
How versioning works

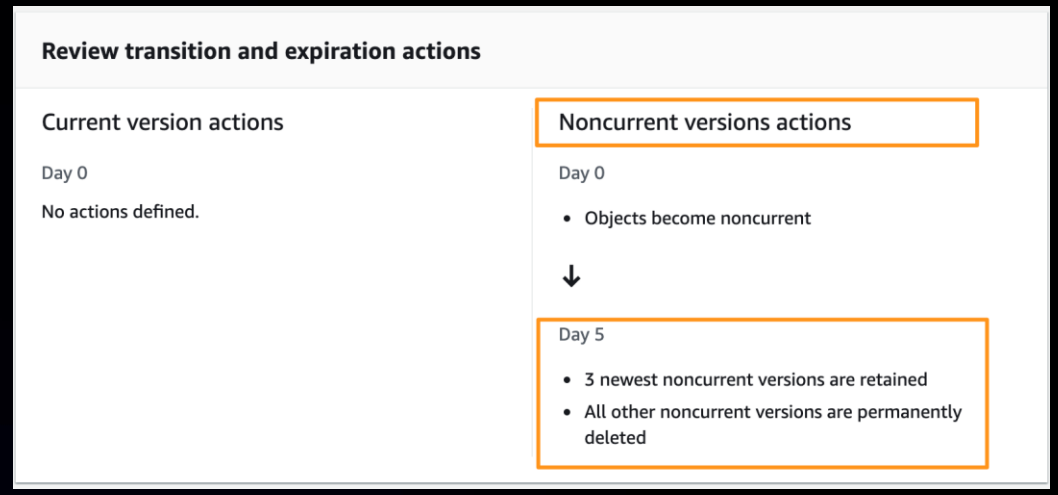



```
$ aws s3api list-object-versions --bucket eab-test-bucket-1
{
    "Versions": [
        {
            "ETag": "\"6cbfb39d127bb55d78e6d63f8c19218b\"",
            "Size": 283654,
            "StorageClass": "STANDARD",
            "Key": "Alkmaar-Netherlands.jpg",
            "VersionId": "n83G6ulXOgtB1jBjZ4IQSJ3JdA_ZDNJ4",
            "IsLatest": true,
            "LastModified": "2021-10-22T17:55:44+00:00",
            "Owner": {
                "ID": "81a51a63f12409b022f0c7cd97d80ec19e78b330acdfc5271f93ca456b1b7620"
            }
        },
        {
            "ETag": "\"6cbfb39d127bb55d78e6d63f8c19218b\"",
            "Size": 283654,
            "StorageClass": "STANDARD",
            "Key": "Alkmaar-Netherlands.jpg",
            "VersionId": "2TiOi25n2SiDLrYxdzFNo23OiyaasEC3",
            "IsLatest": false,
            "LastModified": "2021-04-27T16:15:41+00:00",
            "Owner": {
                "ID": "81a51a63f12409b022f0c7cd97d80ec19e78b330acdfc5271f93ca456b1b7620"
            }
```

rights reserved.

Using Amazon S3 Lifecycle to manage noncurrent versions





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Replication with ownership override

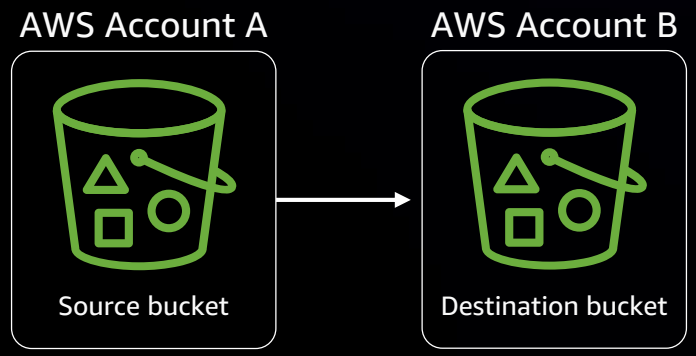
If you want to protect your data from…

- Actions from malicious actors leading to permanent data overwrites or deletes
- Unintended user actions or application failures leading to data overwrites or deletes

…use replication with ownership override to restrict access to object replicas

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How replication works



SELECT

Select data

Replicate the whole bucket
… or based on a Prefix
… or based on Object Tags

PROTECT

Cross Region

- Replicate any second AWS Region
- Continuous replication as your data changes
- **Satisfy geographical distance requirements**

Change ownership

- Object ownership override
- **Protect against bad actors & IAM account compromise**

Cross account

- Replicate into a second account
- Often this is a locked down “Archive” account
- **Protect against AWS root account compromise**

OPTIMIZE

Set storage class

Maintain production access characteristics
… or Land and Lifecycle
… or replicate straight to any S3 Glacier storage class

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Object ownership override

Destination

You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. **Learn more**

or see **Amazon S3 pricing**

- ○ Choose a bucket in this account
- ◉ Specify a bucket in another account

Account ID

123456789999

Bucket name

Choose the bucket that will receive replicated objects.

destination-bucket

Destination Region

US East (N. Virginia) us-east-1

☑ Change object ownership to destination bucket owner

Objects in the source bucket not owned by the source bucket owner will be replaced with ac
the destination bucket owner

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Role>arn:aws:iam::account-id:role/role-name</Role>
   <Rule>
      <ID>Rule-1</ID>
      <Priority>1</Priority>
      <Status>Enabled</Status>
      <DeleteMarkerReplication>
         <Status>Disabled</Status>
      </DeleteMarkerReplication>
      <Filter>
         <Prefix>Tax</Prefix>
      </Filter>
      <Destination>
         <Bucket>arn:aws:s3:::destination-bucket</Bucket>
         <Account>destination-bucket-owner-account-id</Account>
         <AccessControlTranslation>
            <Owner>Destination</Owner>
         </AccessControlTranslation>
      </Destination>
   </Rule>
</ReplicationConfiguration>
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 Object Lock



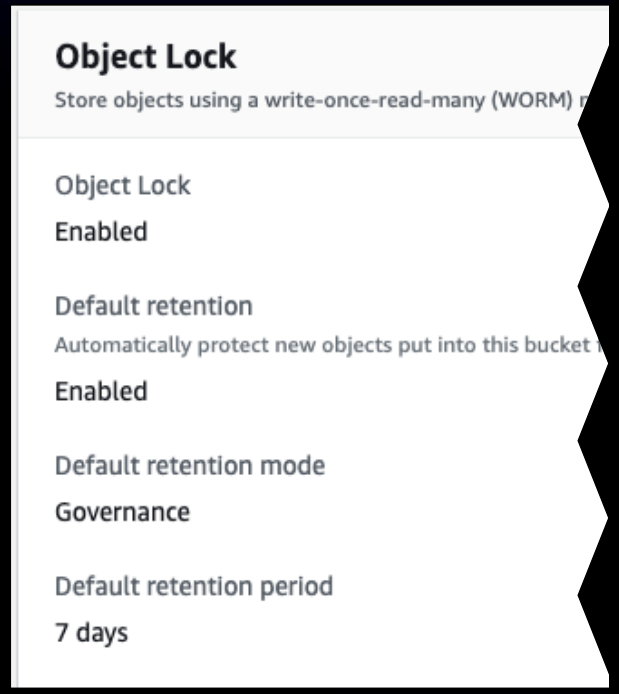
If you want to…

- Meet regulatory requirements that require you to store immutable data
- Add another layer of protection against object changes and deletion

…use Amazon S3 Object Lock to store store objects using a write-once-read-many (WORM) model on Amazon S3

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bucket-level defaults



WORM state

- Boolean – WORM can be on or off for a bucket
- WORM must be on for the bucket in order to lock an object

Default retention period

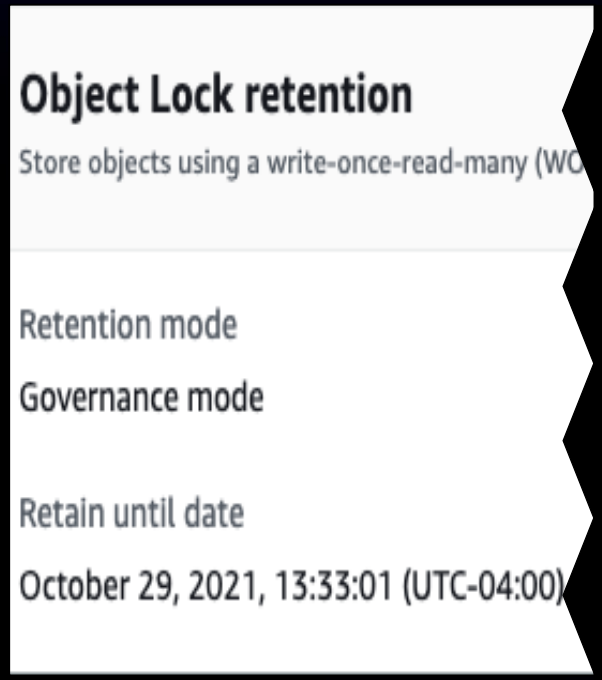
- Defines the default retention for new objects
- Automatically calculates and applies a Retain Until Date
- Can be overridden with a Retain Until Date in the PUT payload
- Does not affect existing objects

Default mode

- Defines the default mode for automatically applied locks

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Object-level metadata



Retain Until Date

- Defines the date until which the object is immutable
- Can be applied on PUT, or added after the fact
- Can be changed, but only moved further into the future

Object Lock mode

- Governance mode – Delete possible with special permissions
- Compliance mode – Delete is not possible, even by root account
- Can escalate from governance to compliance, but not deescalate

Legal Hold flag

- Boolean – Legal Hold can be on or off for an object
- Independent from Retain Until Date
- Applied and removed with a new API that can be restricted by IAM

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 encryption support



Encryption in transit

HTTPS/TLS

Encryption at rest

Server side

- SSE-S3 (Amazon S3 managed keys)
- SSE-KMS (AWS Key Management Service)

Client side

- SSE-C (customer-provided keys)
- Encrypt with the AWS Encryption SDK

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 default encryption



One-time bucket level setup



Automatically encrypts all new objects



Simplified compliance



Supports SSE-S3 and SSE-KMS

Provides S3 encryption-at-rest support for applications that **do not otherwise support encrypting data in Amazon S3**

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Restrict encryption types – Bucket policy

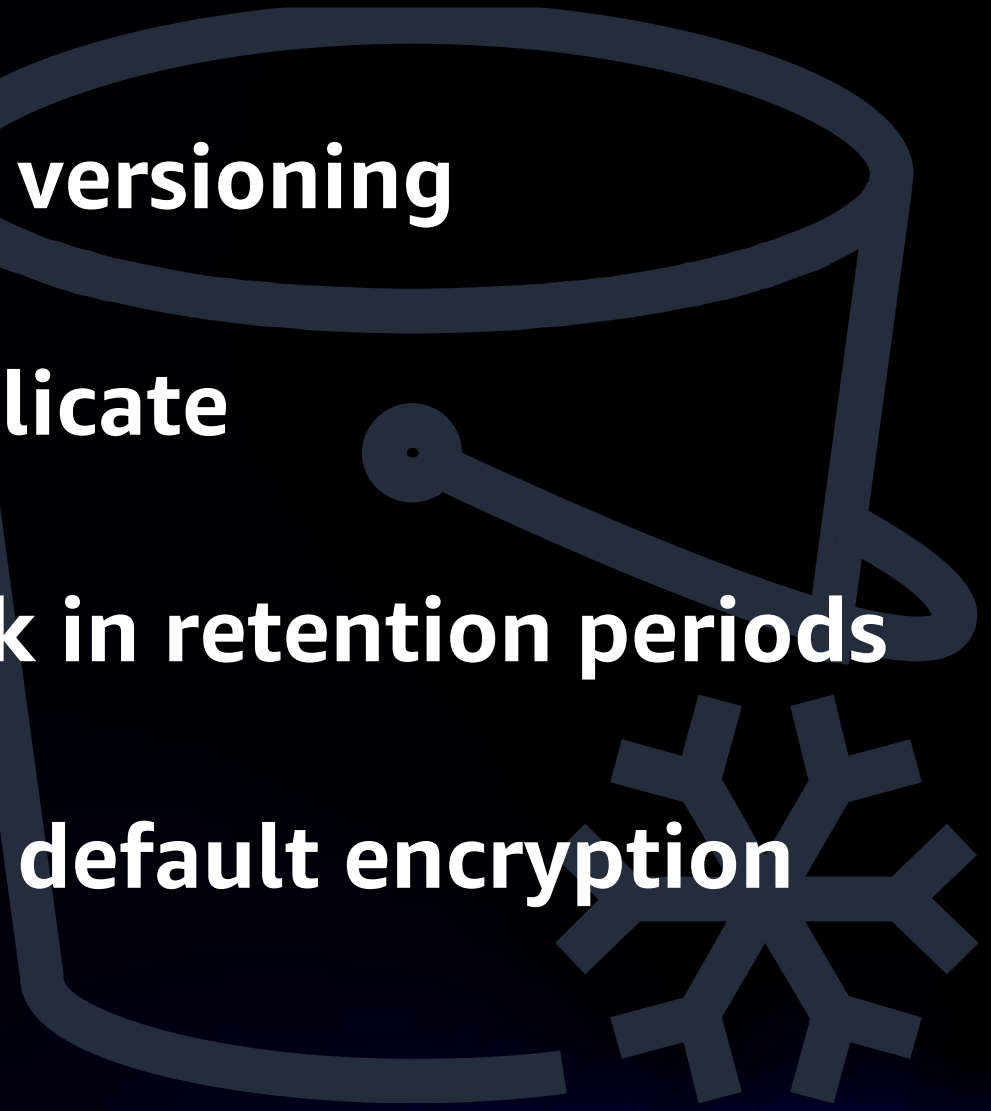
```
"Version": "2012-10-17",
"Id": "PutObjPolicy",
"Statement": [
    {
        "Sid": "DenyIncorrectEncryptionHeader",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::<bucket_name>/*",
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices

4 steps for maximum peace of mind

- Use versioning
- Replicate
- Lock in retention periods
- Use default encryption



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario storage requirements

- AnyCompany's financial records must be kept for seven (7) years to satisfy New York State requirements
- AnyCompany generates 3 GB of financial data daily
- This data is rarely/never accessed once archived but must be rapidly accessible if needed for financial investigations
- AnyCompany must take reasonable steps to ensure the integrity of the data
- AnyCompany must encrypt the data – external regulators do not specify an encryption method, but Acme's risk management team requires that encryption keys are rotated every six (6) months

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.