AWS re:Invent

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

STG345

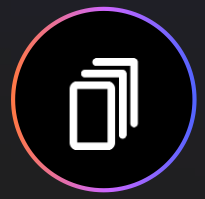
What's new for data protection on Amazon S3

Nitish Pandey
Product Manager, Amazon S3
AWS

John Robe
Software Engineer, Amazon S3
AWS

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

New data protection features for Amazon S3



S3 support for AWS PrivateLink

Direct access to S3 via a private endpoint within your virtual private network

Launched: February 2021



S3 Access Point Aliases

Allow any application that requires an S3 bucket name to easily use an access point

Launched: July 2021



S3 Multi-Region Access Points

Accelerate performance by up to 60% when accessing replicated data sets

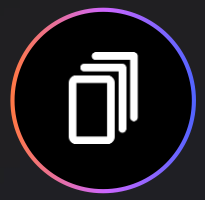
Launched: September 2021



S3 Object Ownership Enhancements

New setting disables access control lists, simplifying access management

Launched: Today!



Policy Validation

Console reports security warnings, errors, and suggestions as you author S3 policies

Launched: Today!



New Checksum Options

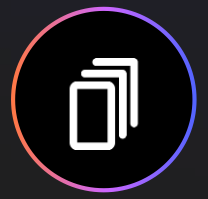
Amazon S3 accelerates integrity checking of requests by up to 92%

Coming Soon!

aws

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

New data protection features for Amazon S3



S3 support for AWS PrivateLink

Direct access to S3 via a private endpoint within your virtual private network

Launched: February 2021



S3 Access Point Aliases

Allow any application that requires an S3 bucket name to easily use an access point

Launched: July 2021



S3 Multi-Region Access Points

Accelerate performance by up to 60% when accessing replicated data sets

Launched: September 2021



S3 Object Ownership Enhancements

New setting disables access control lists, simplifying access management

Launched: Today!



Policy Validation

Console reports security warnings, errors, and suggestions as you author S3 policies

Launched: Today!



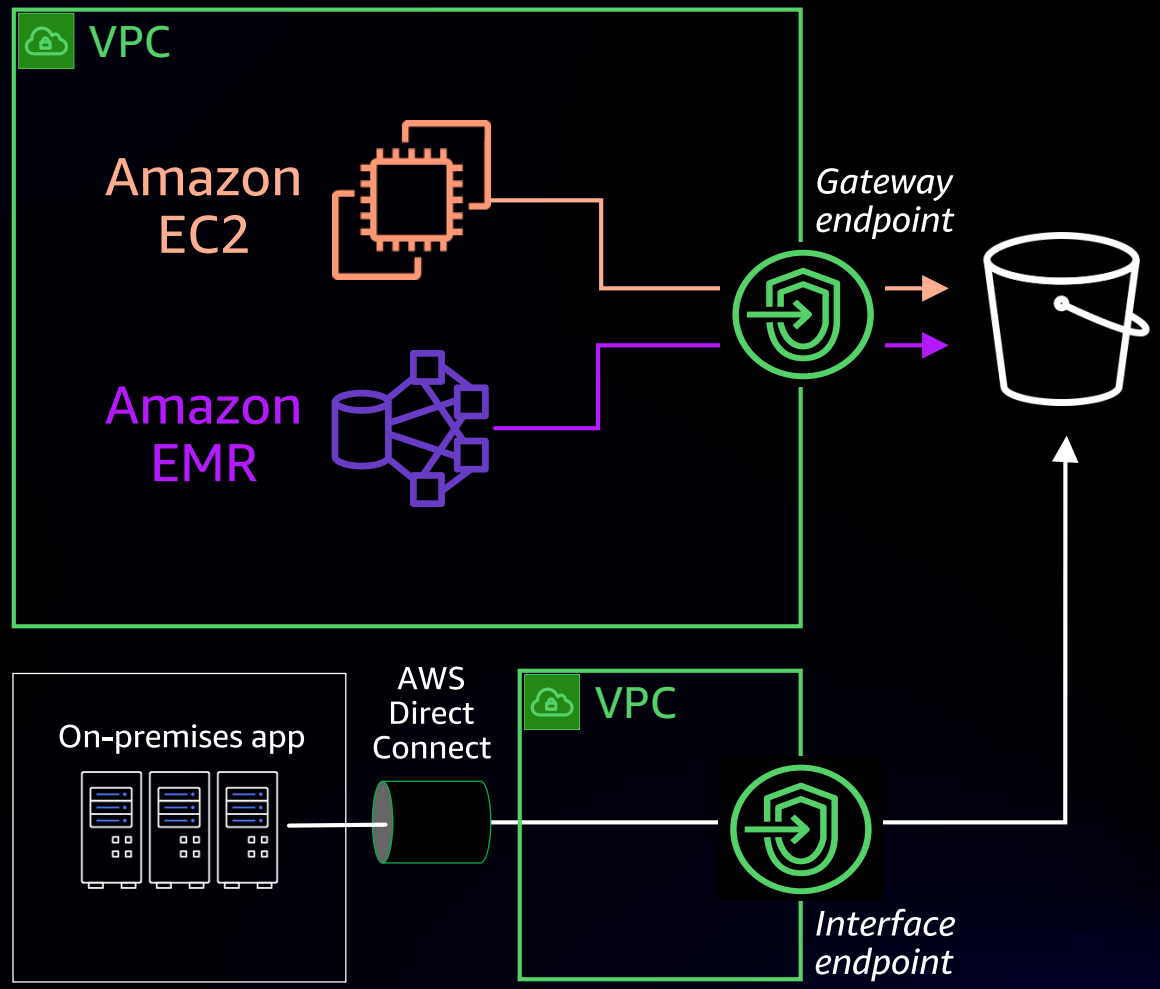
New Checksum Options

Amazon S3 accelerates integrity checking of requests by up to 92%

Coming Soon!

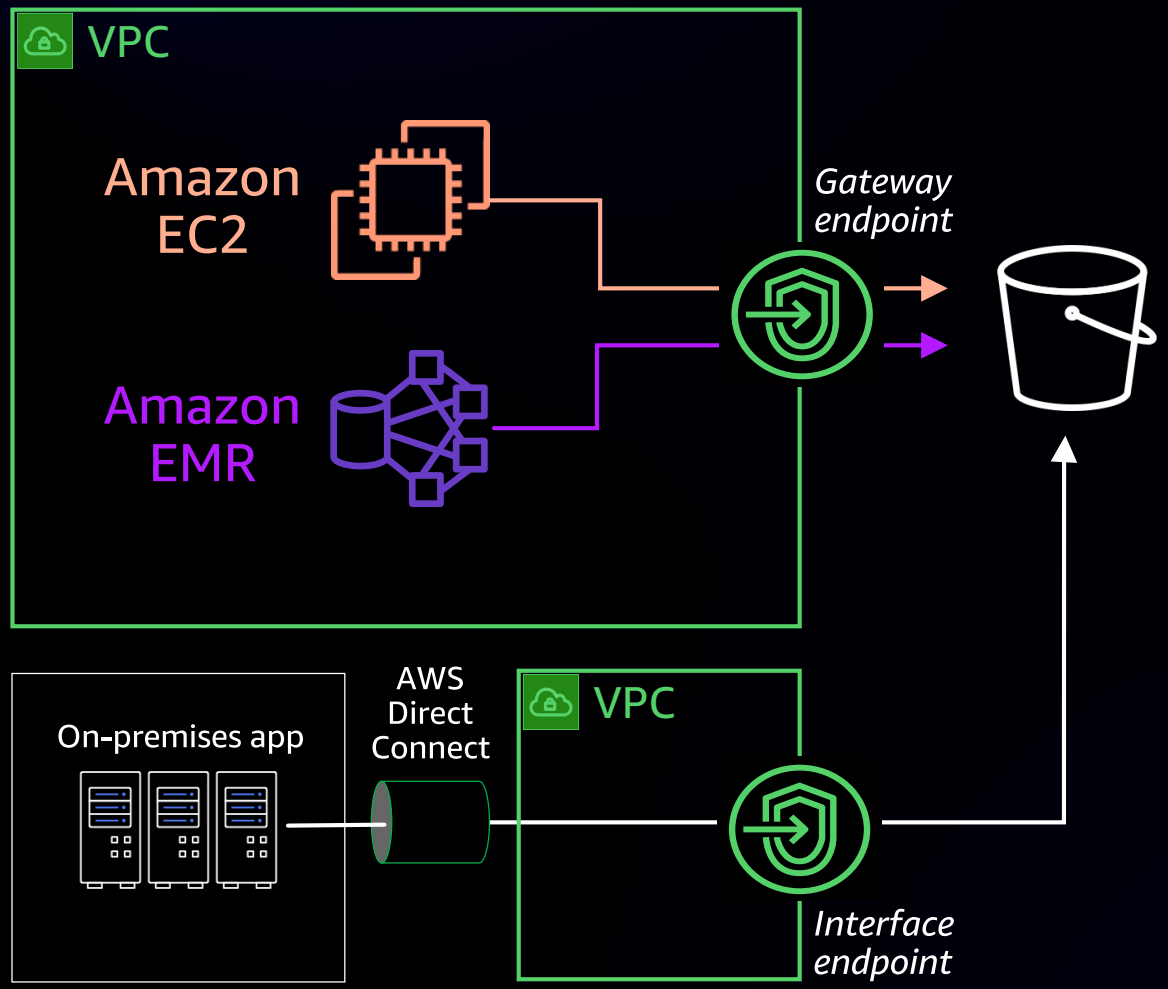
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 support for AWS PrivateLink



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

Amazon S3 support for AWS PrivateLink

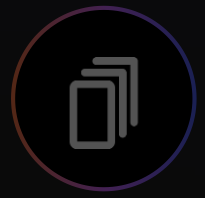


Connect on-premises apps to S3

- Simple network architecture
- Connections avoid the public internet
- Additional visibility and access control

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

New data protection features for Amazon S3



S3 support for AWS PrivateLink

Direct access to S3 via a private endpoint within your virtual private network

Launched: February 2021



S3 Access Point Aliases

Allow any application that requires an S3 bucket name to easily use an access point

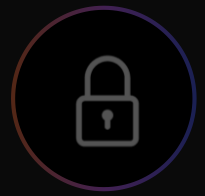
Launched: July 2021



S3 Multi-Region Access Points

Accelerate performance by up to 60% when accessing replicated data sets

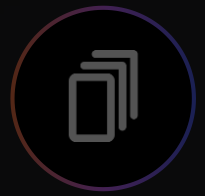
Launched: September 2021



S3 Object Ownership Enhancements

New setting disables access control lists, simplifying access management

Launched: Today!



Policy Validation

Console reports security warnings, errors, and suggestions as you author S3 policies

Launched: Today!



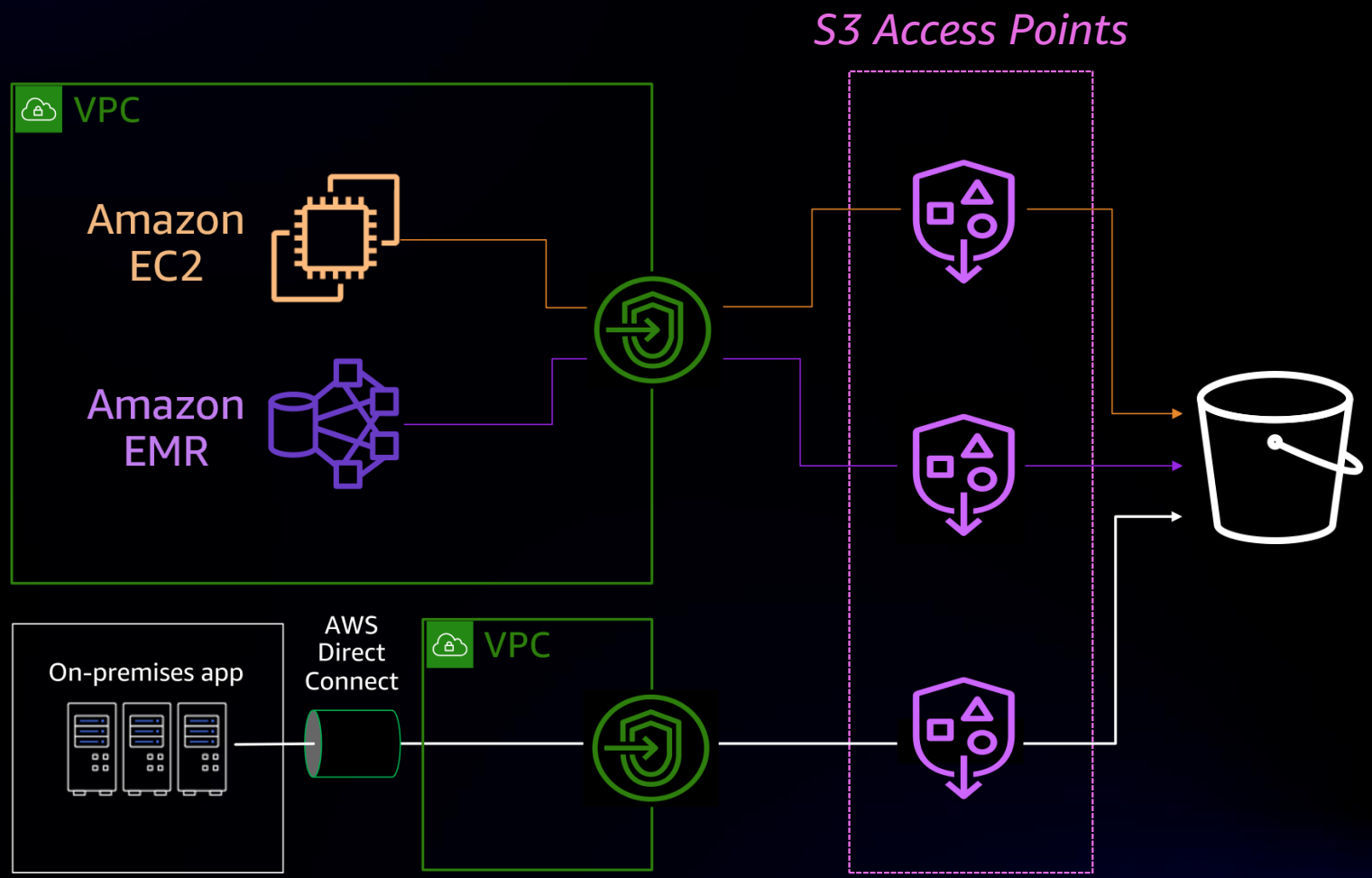
New Checksum Options

Amazon S3 accelerates integrity checking of requests by up to 92%

Coming Soon!

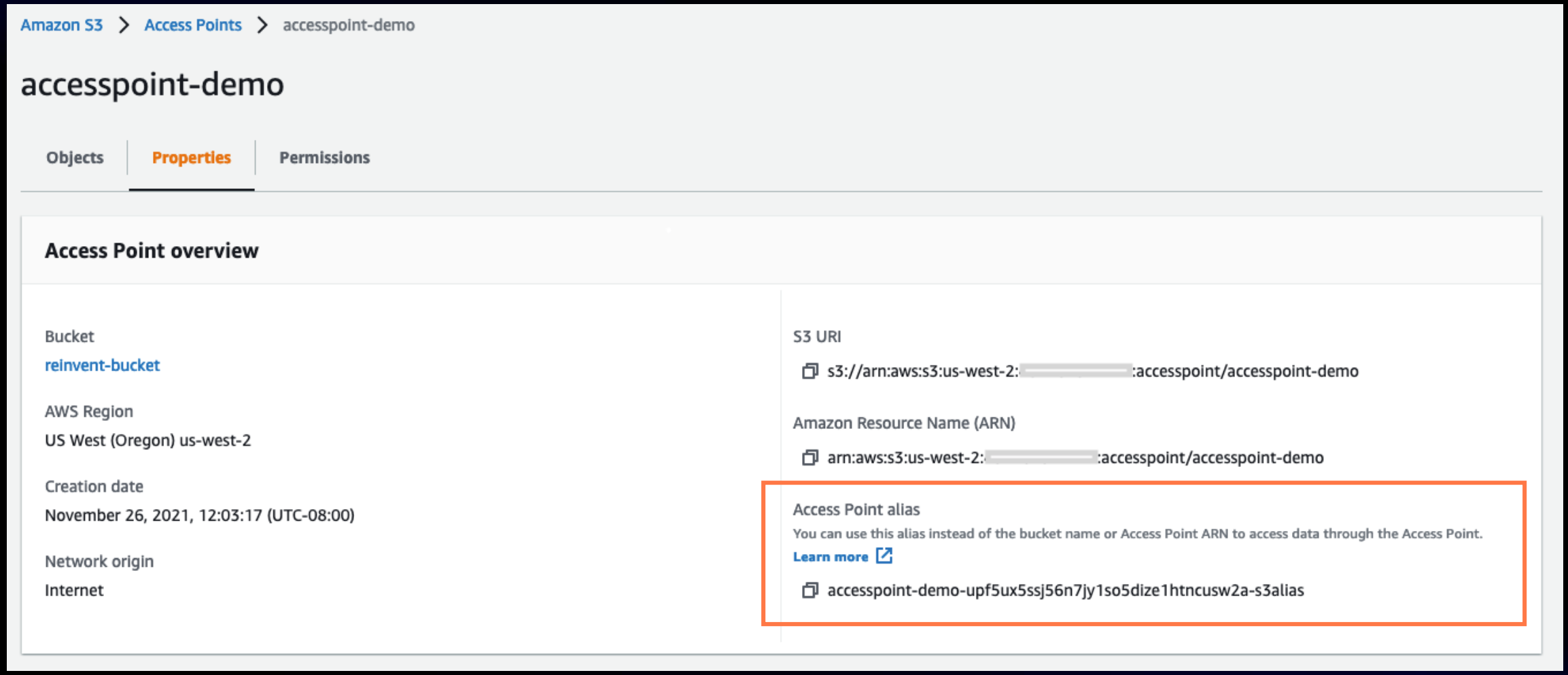
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3 Access Points



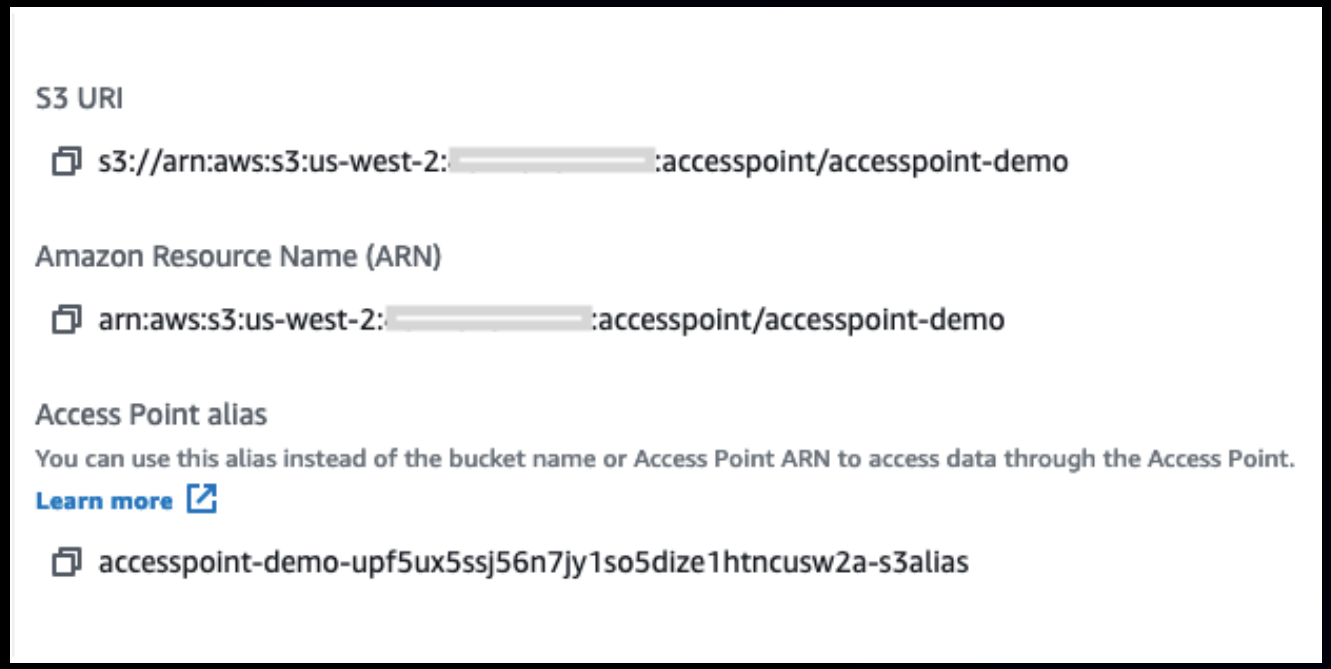
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3 Access Points aliases



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

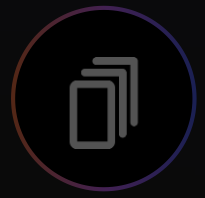
S3 Access Points aliases



- All Access Points receive a unique alias
- Aliases can be used anywhere you use bucket name URI's for data access
- Enables applications to be compatible without code change

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

New data protection features for Amazon S3



S3 support for AWS PrivateLink

Direct access to S3 via a private endpoint within your virtual private network

Launched: February 2021



S3 Access Point Aliases

Allow any application that requires an S3 bucket name to easily use an access point

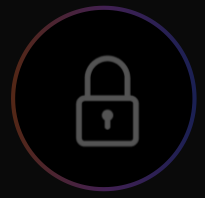
Launched: July 2021



S3 Multi-Region Access Points

Accelerate performance by up to 60% when accessing replicated data sets

Launched: September 2021



S3 Object Ownership Enhancements

New setting disables access control lists, simplifying access management

Launched: Today!



Policy Validation

Console reports security warnings, errors, and suggestions as you author S3 policies

Launched: Today!



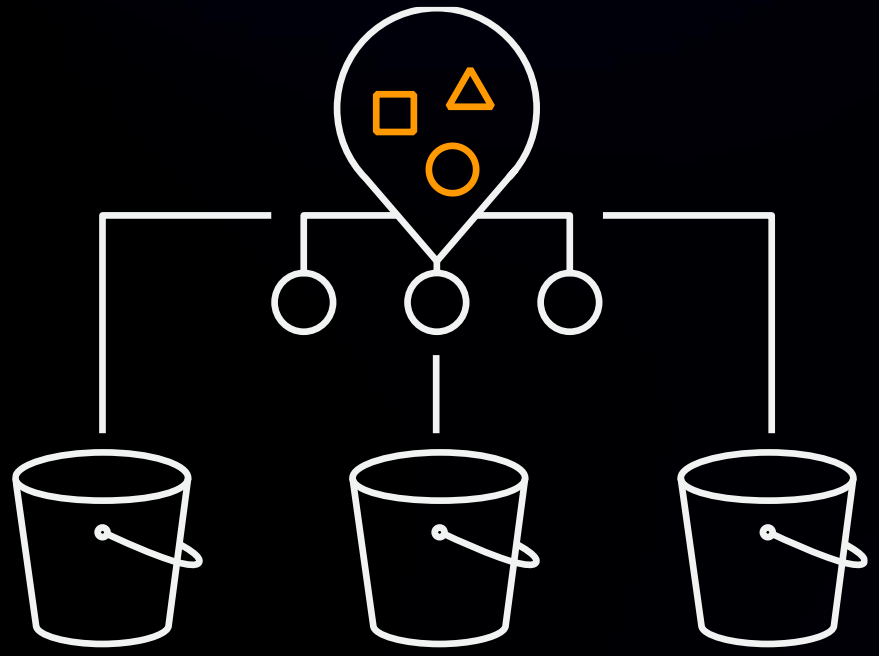
New Checksum Options

Amazon S3 accelerates integrity checking of requests by up to 92%

Coming Soon!

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

Introducing S3 Multi-Region Access Points

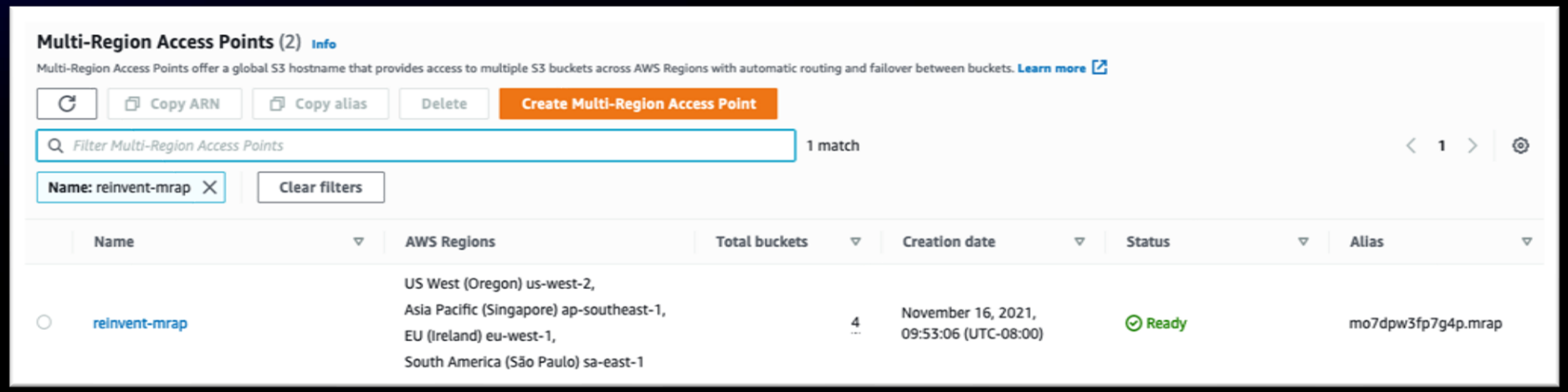


- Add **multiple S3 buckets** to a new global **Multi-Region Access Point**
- Create a **new, unique global hostname** to access data in buckets in multiple AWS Regions
- Allows applications to operate across **multiple AWS Regions** without code changes
- Requests made to a MRAP global hostname are routed and accelerated across **AWS Global Accelerator** network

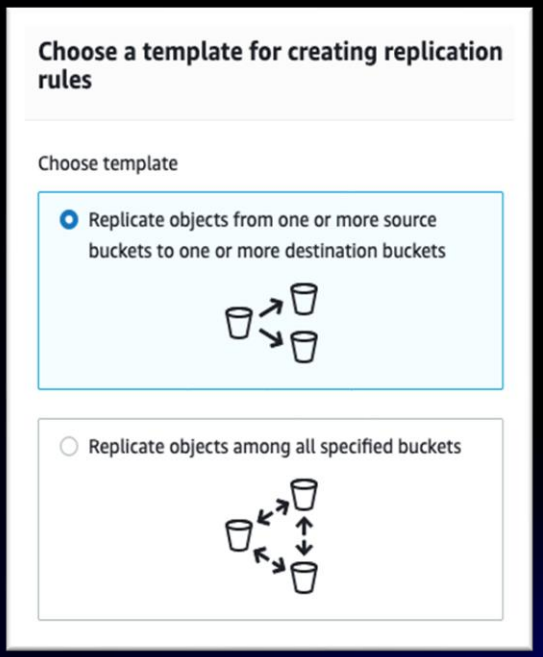
aws

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

Introducing S3 Multi-Region Access Points

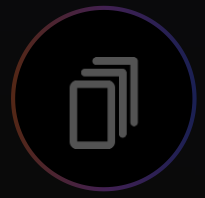






© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New data protection features for Amazon S3



S3 support for AWS PrivateLink
Direct access to S3 via a private endpoint within your virtual private network

Launched: February 2021



S3 Access Point Aliases
Allow any application that requires an S3 bucket name to easily use an access point

Launched: July 2021



S3 Multi-Region Access Points
Accelerate performance by up to 60% when accessing replicated data sets

Launched: September 2021



S3 Object Ownership Enhancements
New setting disables access control lists, simplifying access management

Launched: Today!



Policy Validation
Console reports security warnings, errors, and suggestions as you author S3 policies

Launched: Today!



New Checksum Options
Amazon S3 accelerates integrity checking of requests by up to 92%

Coming Soon!

aws

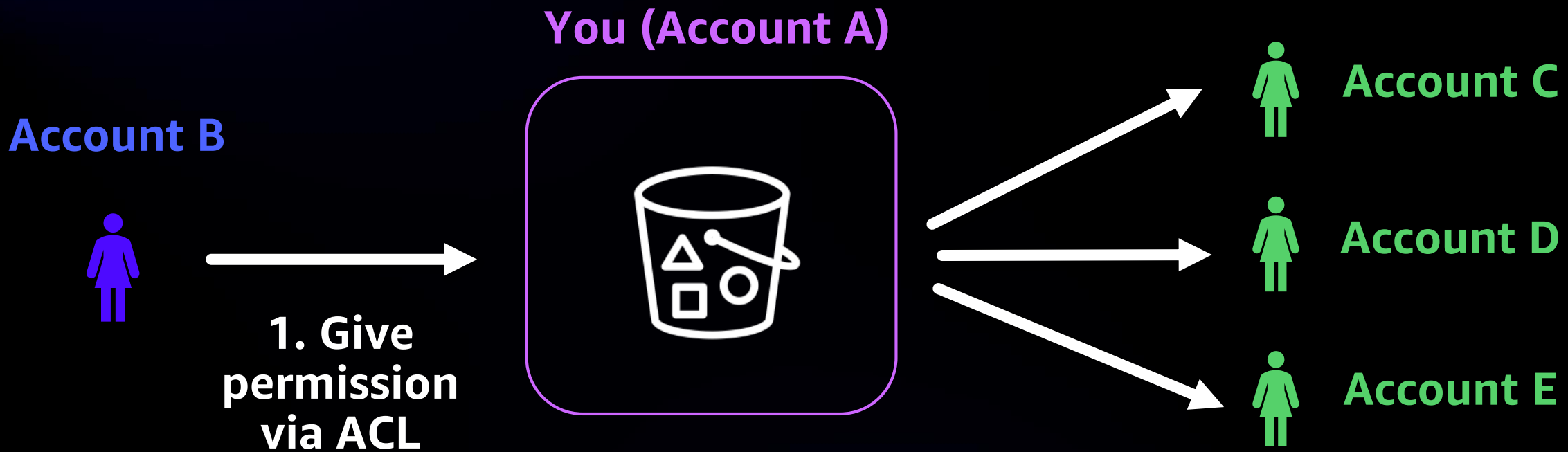
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multiple mechanisms for access management

AWS Identity and Access Management (IAM)	Amazon S3	Amazon S3
		
IAM policy	Bucket policy	Access control list (ACL)
Applies to	IAM Identity	S3 Bucket	S3 Bucket S3 Object

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

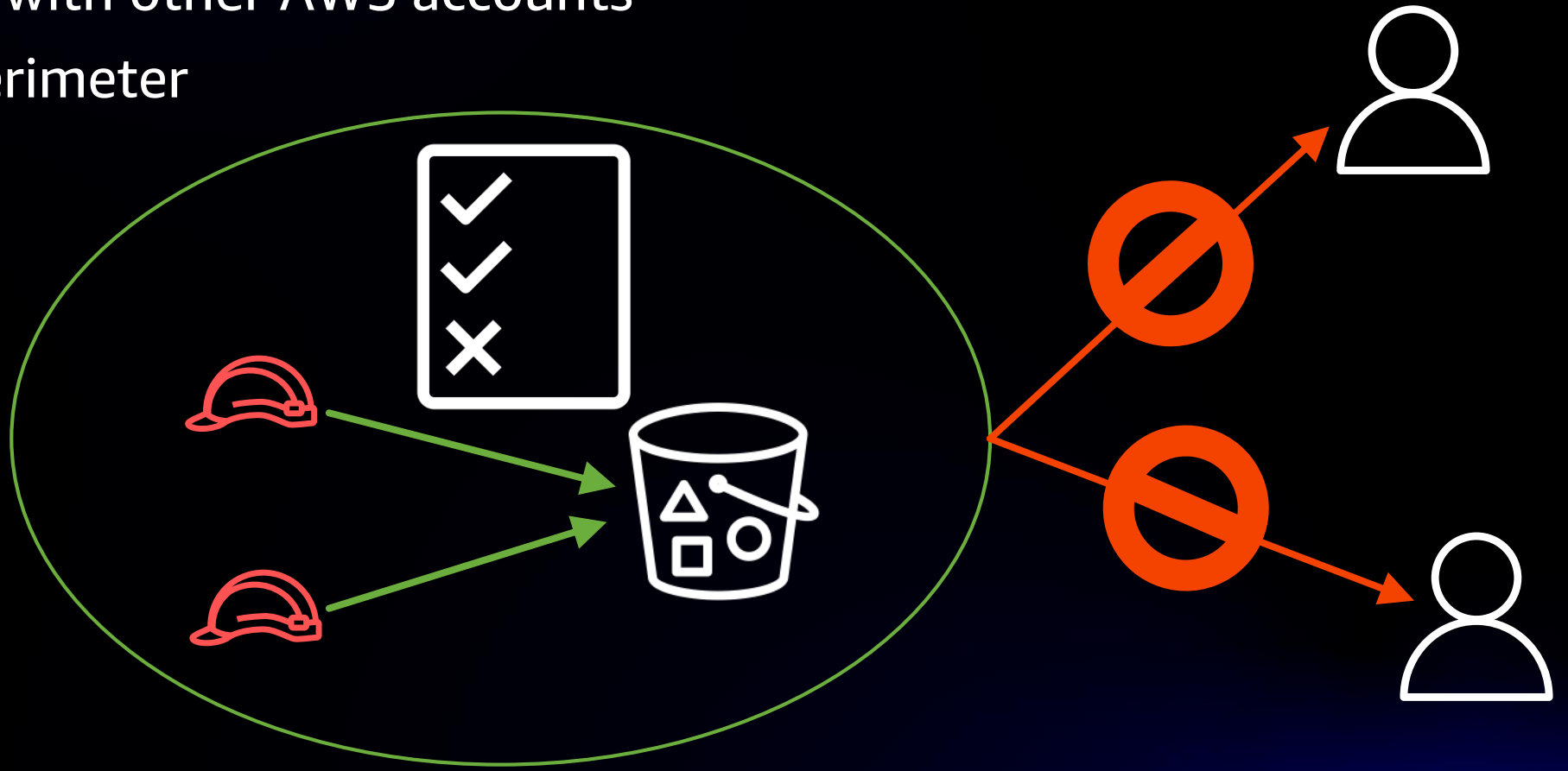
How cross-account write is done today



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

Best practice for building a data lake: Use bucket policies

- Sharing data with other AWS accounts
- Creating a perimeter



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

ACL affects bucket policy applicability



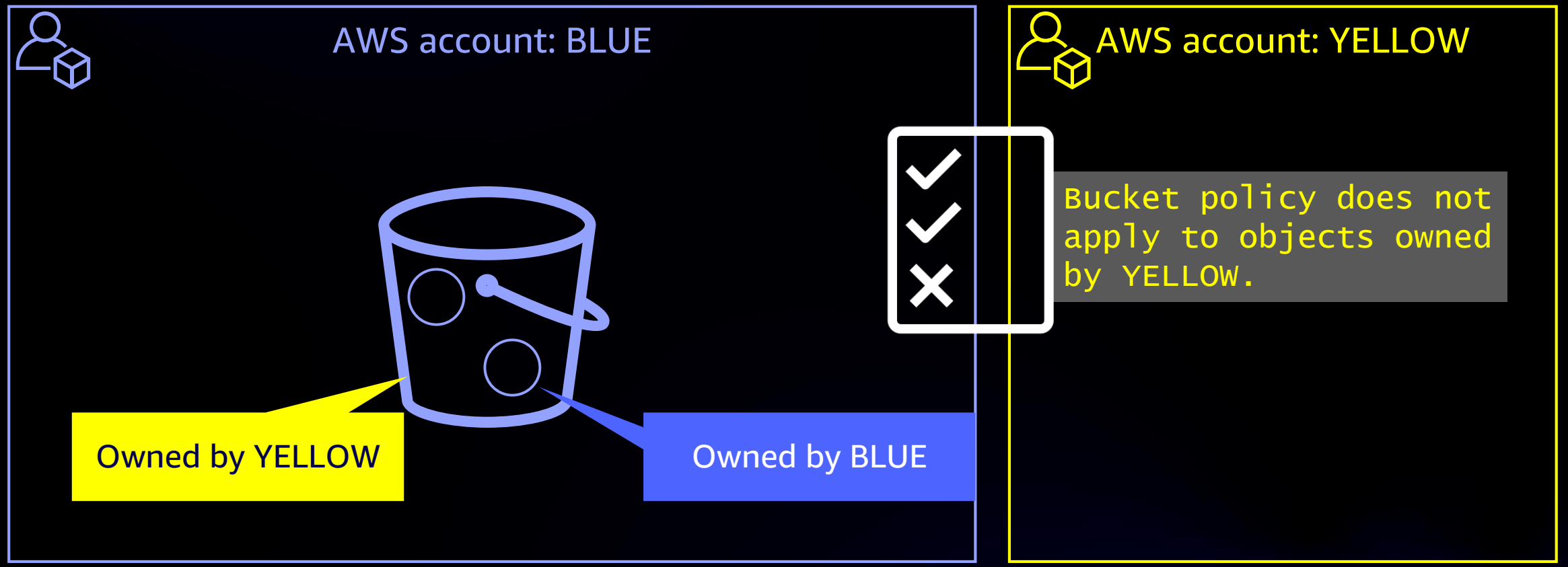
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ACL affects bucket policy applicability



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

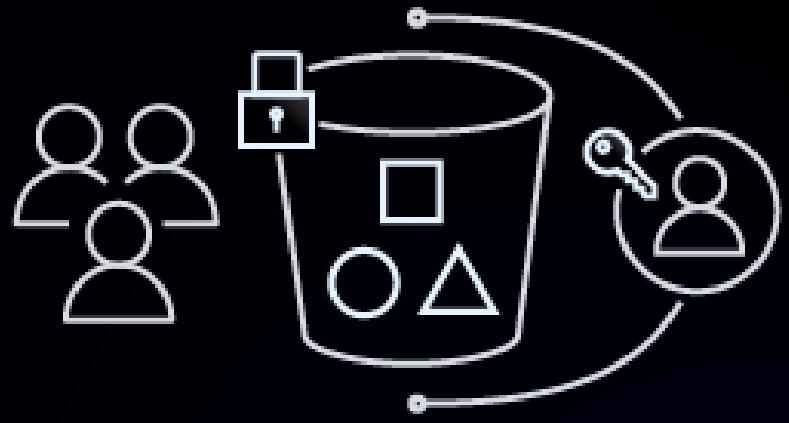
ACL assigns ownership that affects bucket policy applicability



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

New at re:Invent

S3 Object Ownership
New Setting



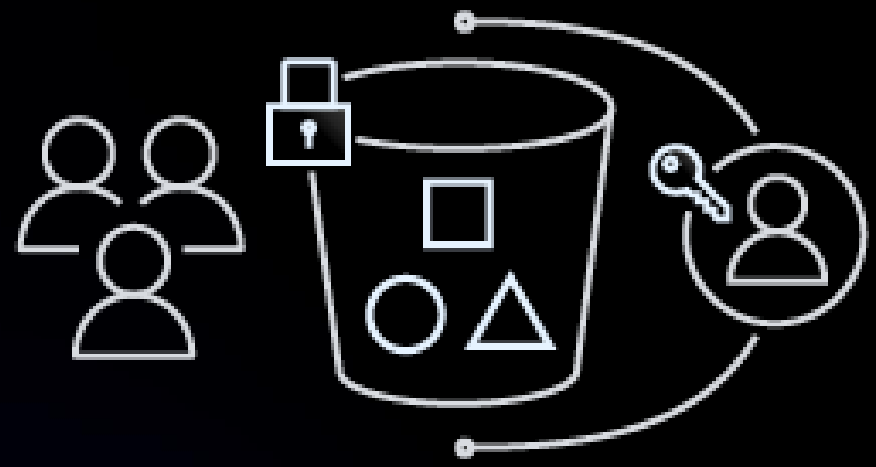
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3 Object Ownership new setting: Bucket owner enforced

Simplifying access management

- Access control lists (ACLs) are disabled and no longer used to grant permission
- ACLs cannot be edited
- Every object in your bucket is owned by you

S3 Object Ownership



A bucket-level setting

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

Simplifying access control

AWS Identity and Access Management (IAM)	Amazon S3	Amazon S3
		
IAM policy	Bucket policy	Access control list (ACL)
Applies to	IAM Identity	S3 Bucket S3 ARN	S3 Bucket S3 Object

aws

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

Simplifying access control

AWS Identity and Access Management (IAM)	Amazon S3
	
IAM policy	Bucket policy
Applies to	IAM Identity	S3 Bucket S3 ARN

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

Simplifying access control

AWS Identity and Access Management (IAM)	Amazon S3
	
IAM policy	Bucket policy
Applies to	IAM Identity	S3 Bucket S3 ARN

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

Simplifying access control

AWS Identity and Access Management (IAM)



IAM policy

All access controls defined using policies



Amazon S3



Bucket policy

Applies to

IAM Identity

S3 Bucket
S3 ARN

aws

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

You own every object in your bucket

AWS account: BLUE

Bucket ownership setting:
`BucketOwnerEnforced`



AWS account: YELLOW

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

You own every object in your bucket

AWS account: BLUE

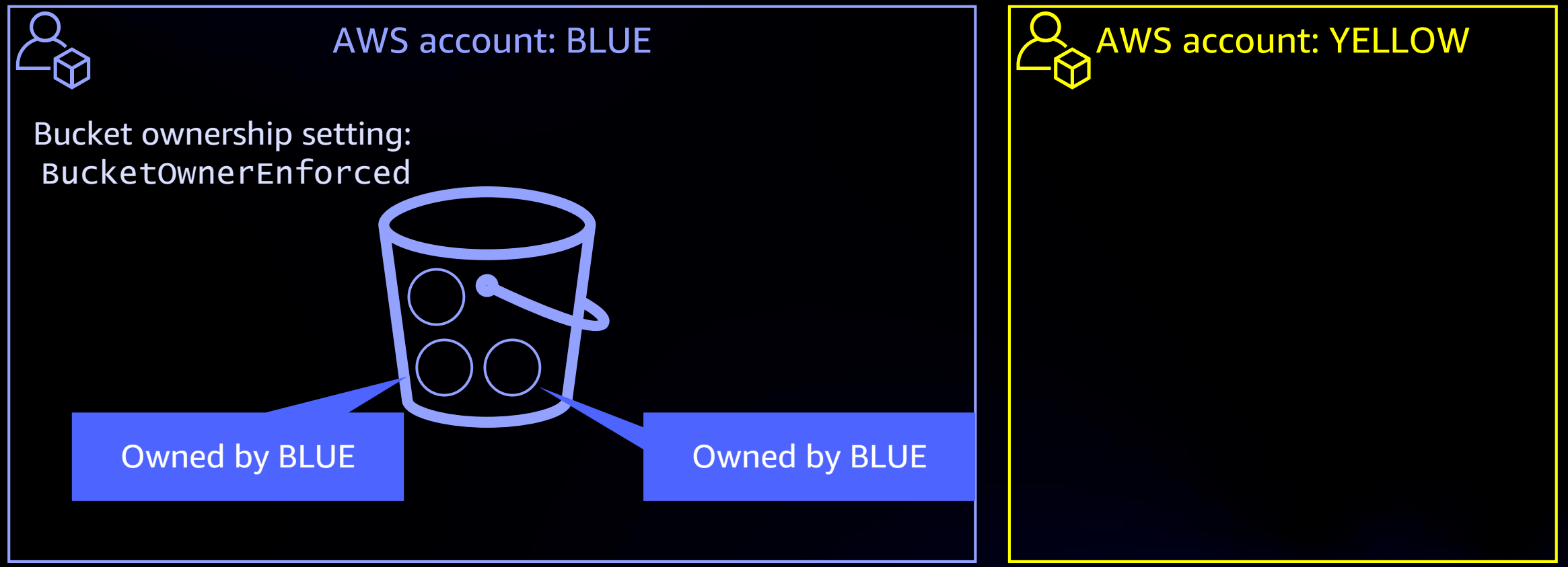
Bucket ownership setting:
`BucketOwnerEnforced`



AWS account: YELLOW

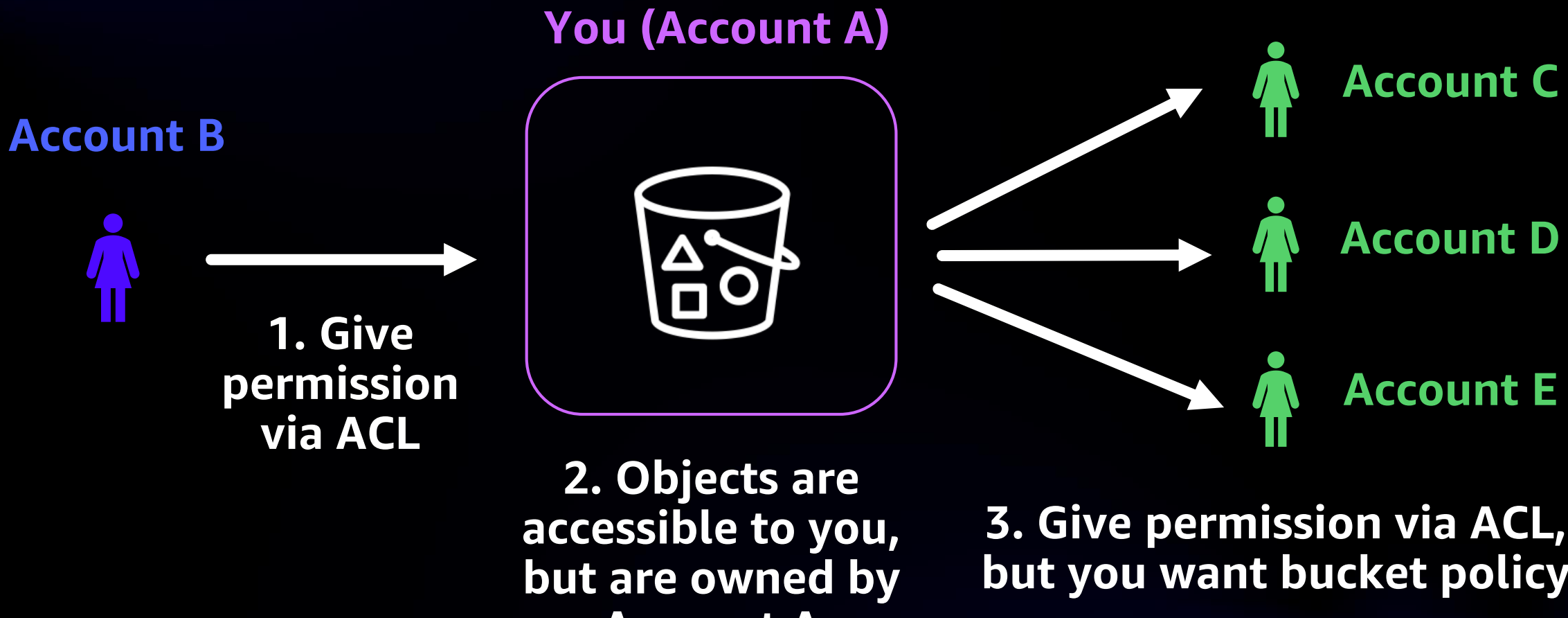
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

You own every object in your bucket



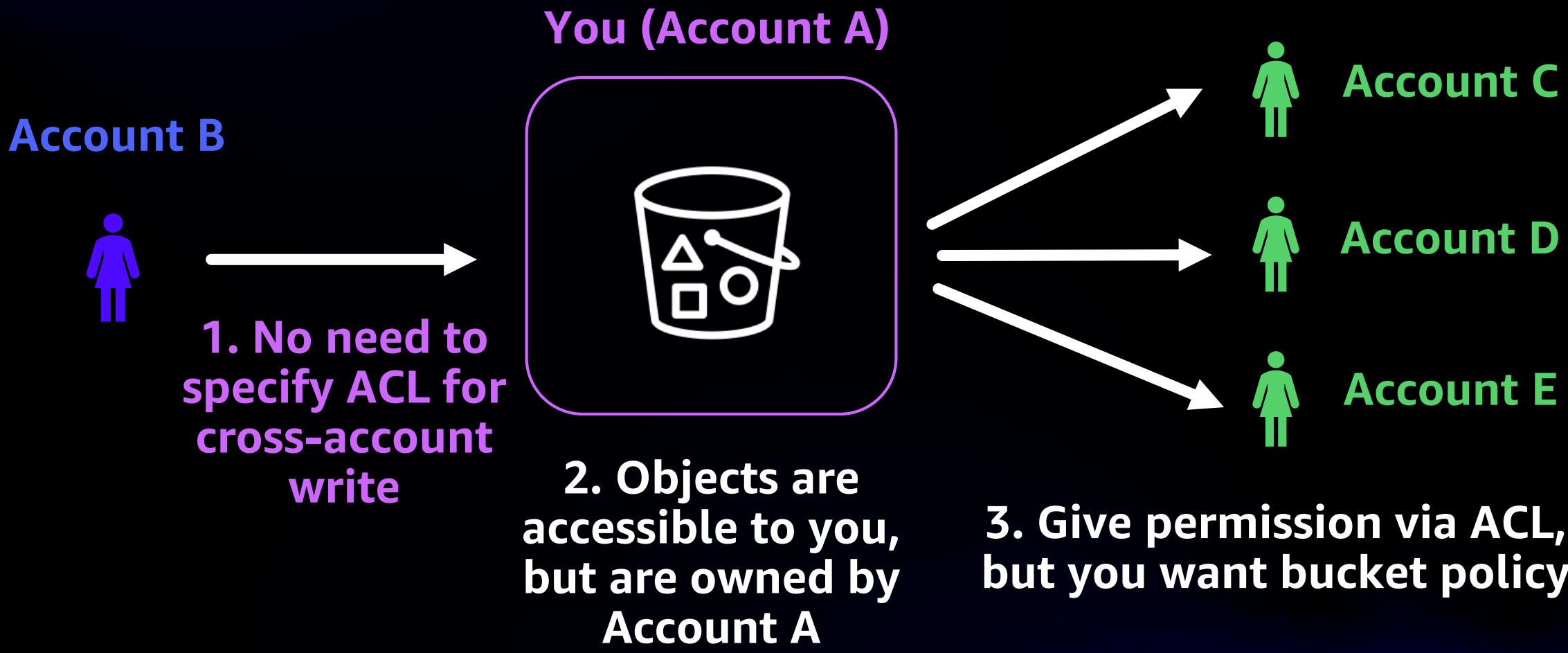
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sharing data with Object Ownership



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

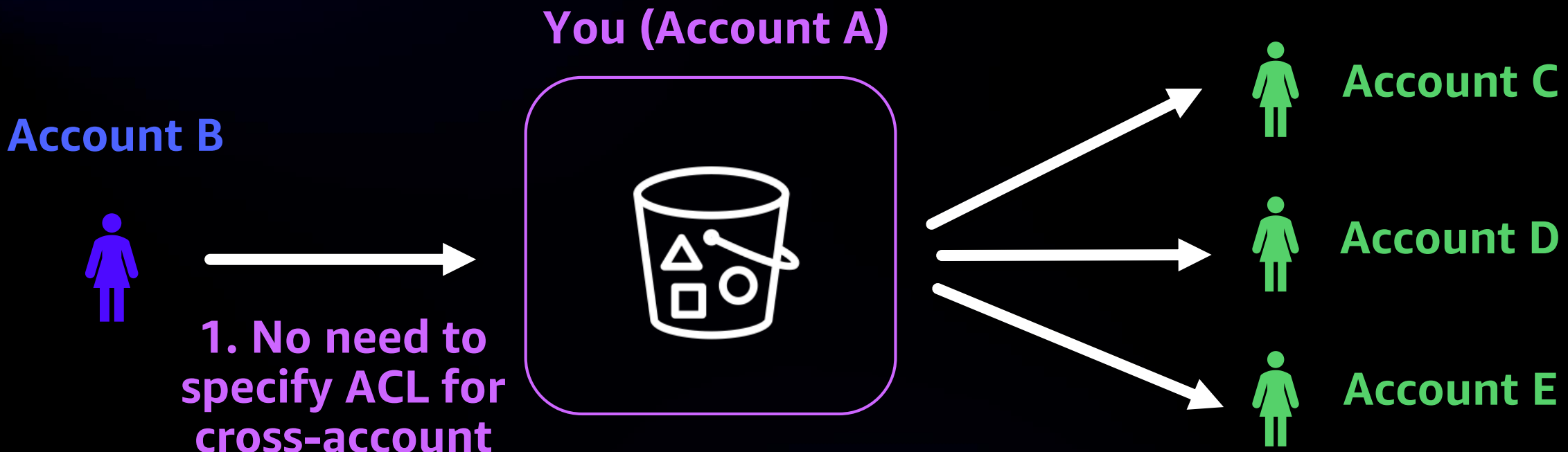
Sharing data with Object Ownership



aws

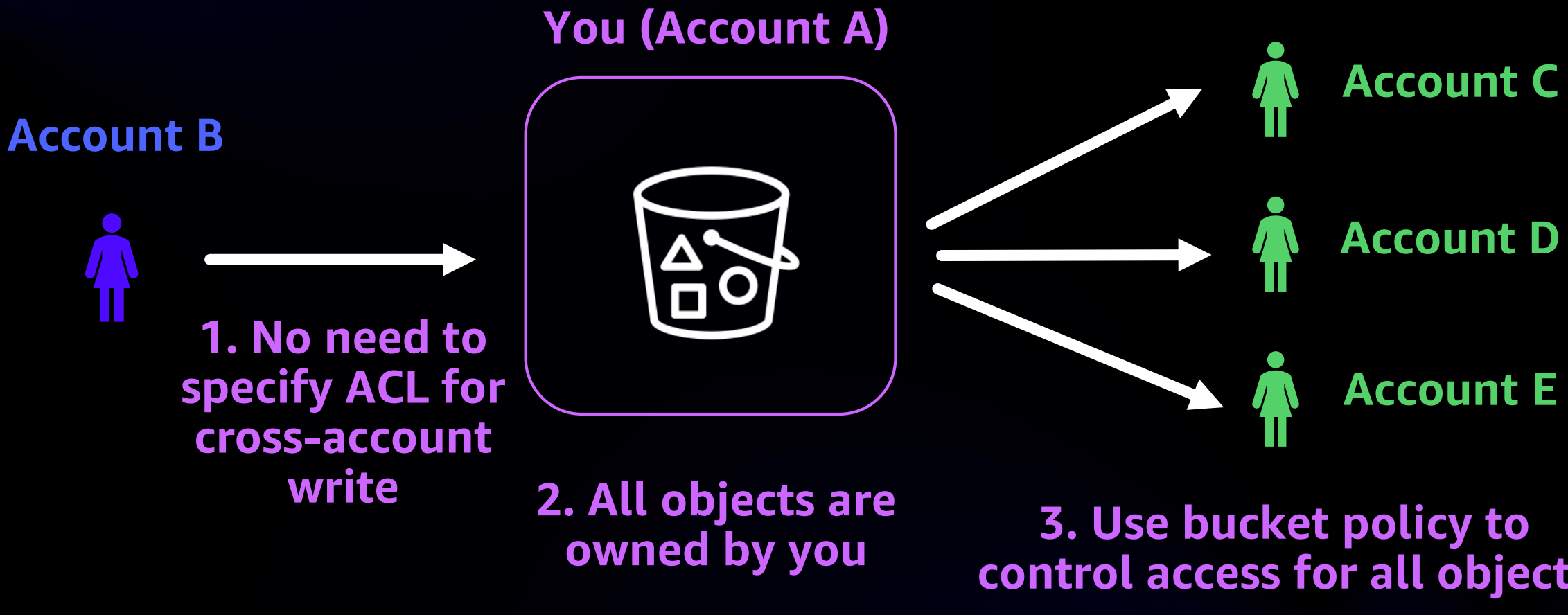
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sharing data with Object Ownership



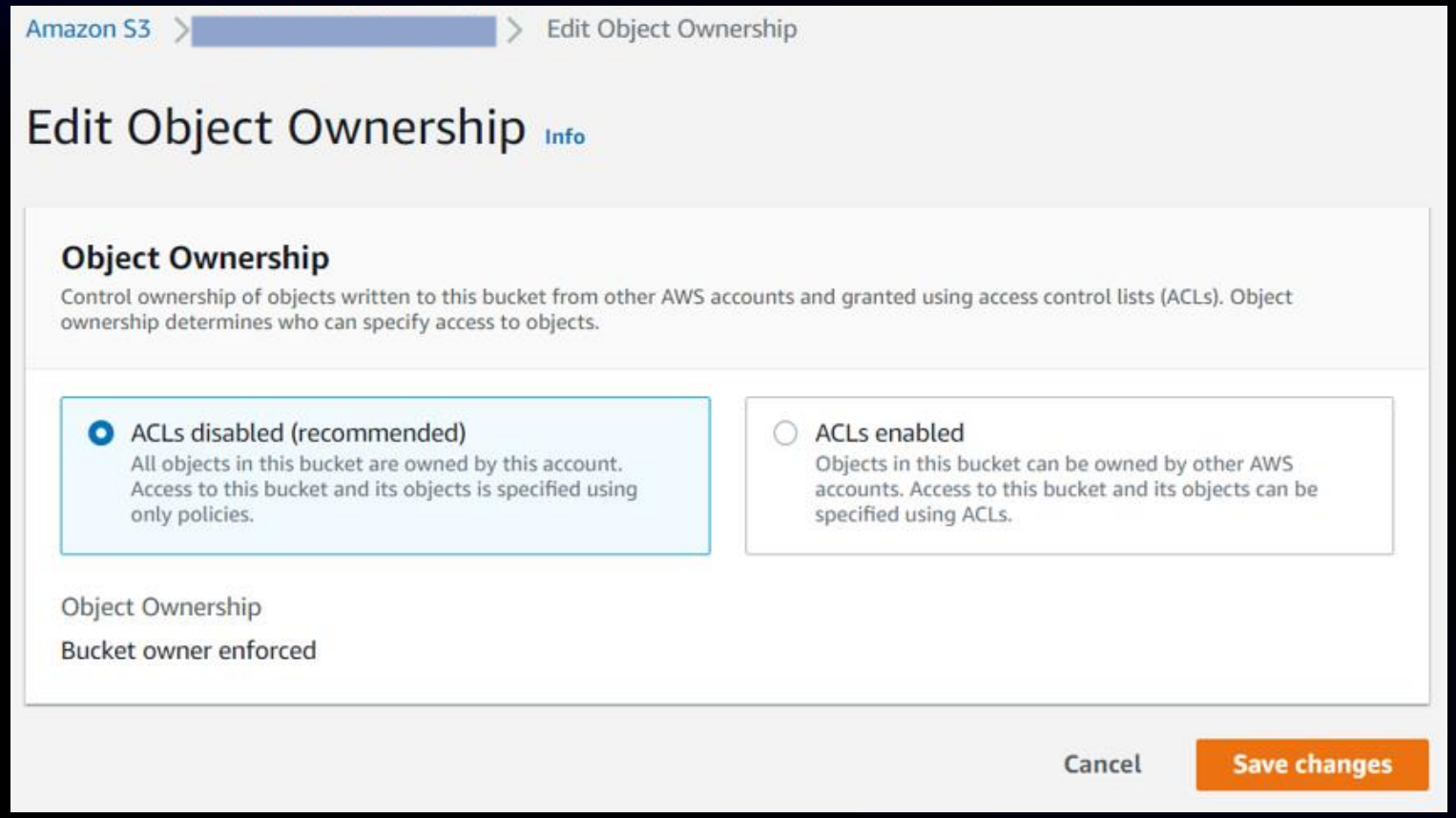
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sharing data with Object Ownership



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

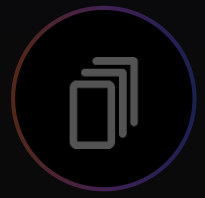
Simple bucket-level setting



- Can be applied to a new or existing bucket
- Can be turned off at any time – previous ACLs will be restored

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

New data protection features for Amazon S3



S3 support for AWS PrivateLink

Direct access to S3 via a private endpoint within your virtual private network

Launched: February 2021



S3 Access Point Aliases

Allow any application that requires an S3 bucket name to easily use an access point

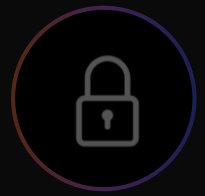
Launched: July 2021



S3 Multi-Region Access Points

Accelerate performance by up to 60% when accessing replicated data sets

Launched: September 2021



S3 Object Ownership Enhancements

New setting disables access control lists, simplifying access management

Launched: Today!



Policy Validation

Console reports security warnings, errors, and suggestions as you author S3 policies

Launched: Today!



New Checksum Options

Amazon S3 accelerates integrity checking of requests by up to 92%

Coming Soon!

aws

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

AWS IAM Access Analyzer: Policy validation



Easy to use



Validates automatically



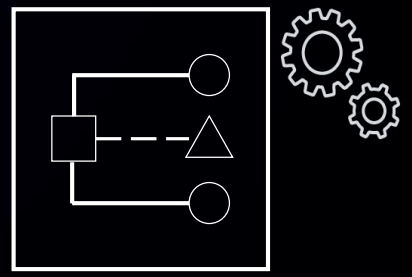
Improves security



Saves time

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

Dynamically generate findings



Warning: Broad access with NotPrincipal

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
       "Effect": "Allow",
       ”NotPrincipal": {
                "AWS": ”abc"},
          "Action": [
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObject”
     ],
  "Resource": [
                "arn:aws:s3:::my-bucket/*"
  ]
 }]
```

Error: Invalid actions

s3:ListBuckets → s3:ListAllMyBuckets

S3:HeadBucket → s3:ListBucket

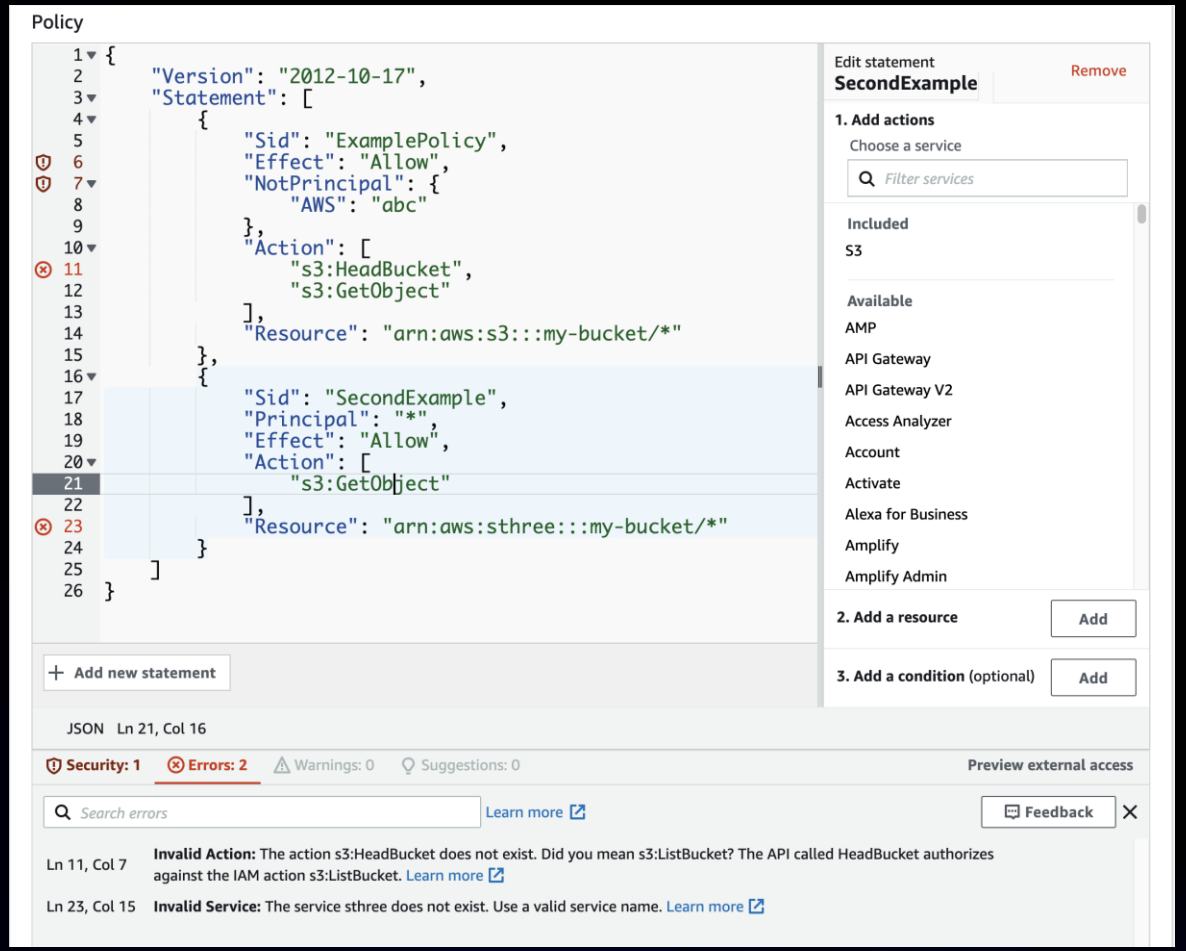
Suggestion: Redundant actions

S3:Get* and S3:GetObject
(included within S3:Get*)

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

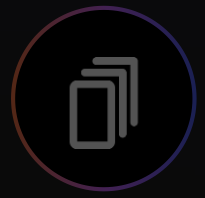
Policy validation in the S3 console

- IAM Access Analyzer policy validation is now available in the S3 console policy editor for bucket policies
- Runs more than 100 policy checks as you're authoring your bucket policy
- Highlights security warnings, errors, and suggestions as you're authoring your bucket policies
- Helps you attach secure and functional policies to your S3 buckets



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

New data protection features for Amazon S3



S3 support for AWS PrivateLink
Direct access to S3 via a private endpoint within your virtual private network

Launched: February 2021



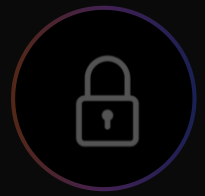
S3 Access Point Aliases
Allow any application that requires an S3 bucket name to easily use an access point.

Launched: July 2021



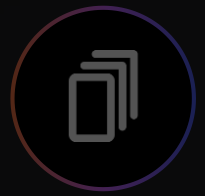
S3 Multi-Region Access Points
Accelerate performance by up to 60% when accessing replicated data sets

Launched: September 2021



S3 Object Ownership Enhancements
New setting disables access control lists, simplifying access management

Launched: Today!



Policy Validation
Console reports security warnings, errors, and suggestions as you author S3 policies

Launched: Today!



New Checksum Options
Amazon S3 accelerates integrity checking of requests by up to 92%

Coming Soon!

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

Checksum

Coming Soon

It’s the fingerprint of an object

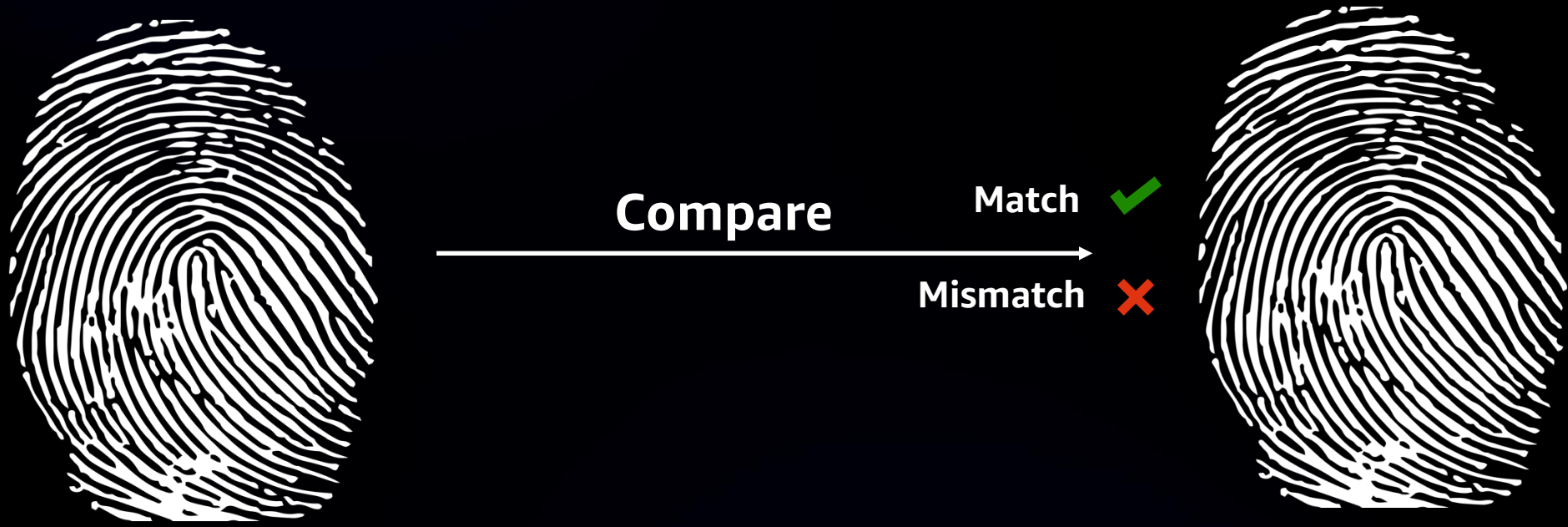


[Note: This is not a checksum. This is a FINGERPRINT. ☺]

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

Checksum

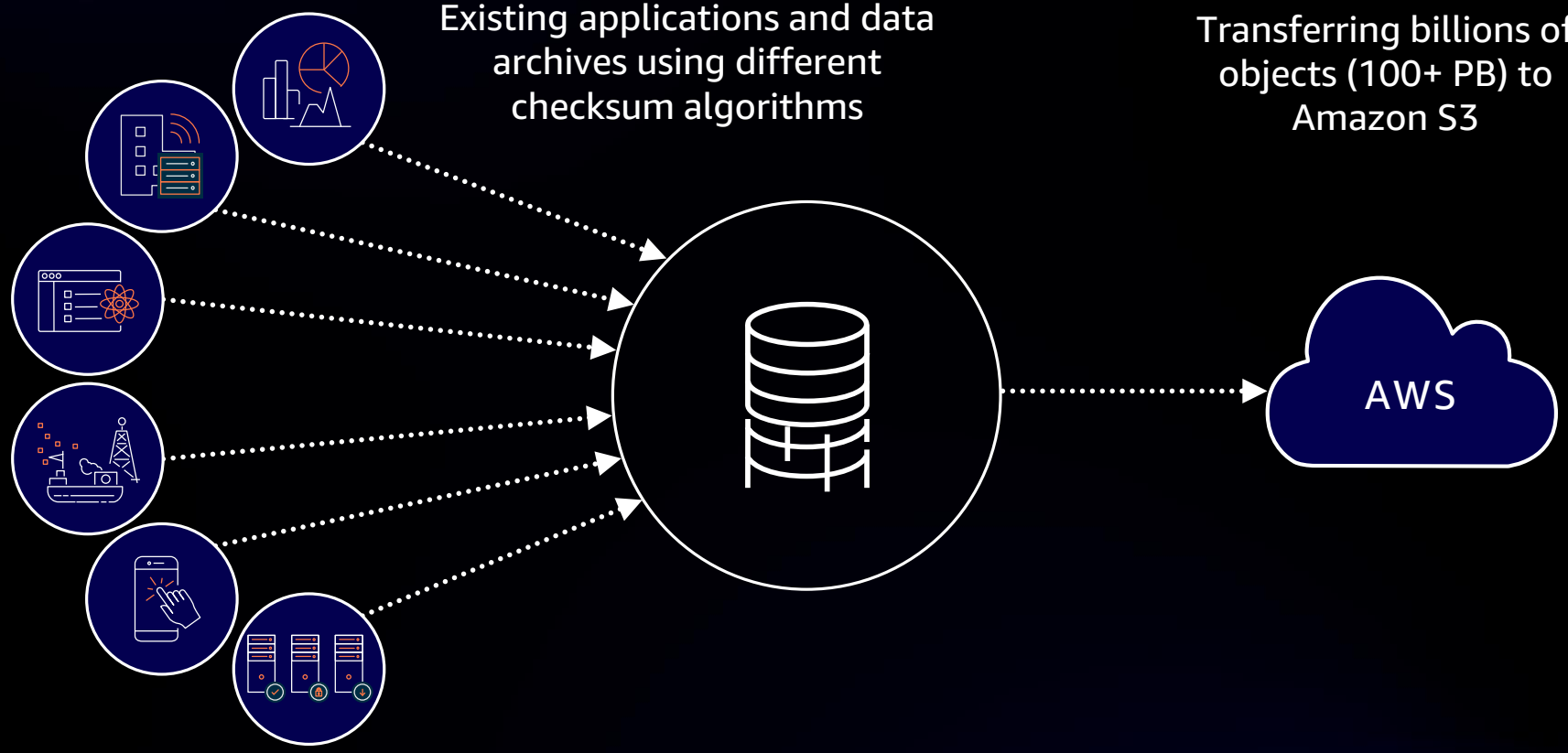
Coming Soon



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

Coming Soon

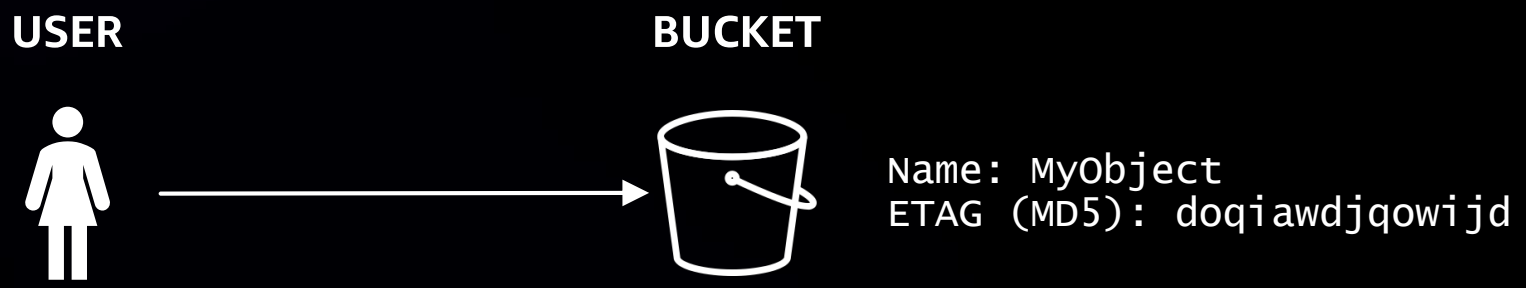
Migrating data to AWS



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

Checksums in S3 today

Coming Soon



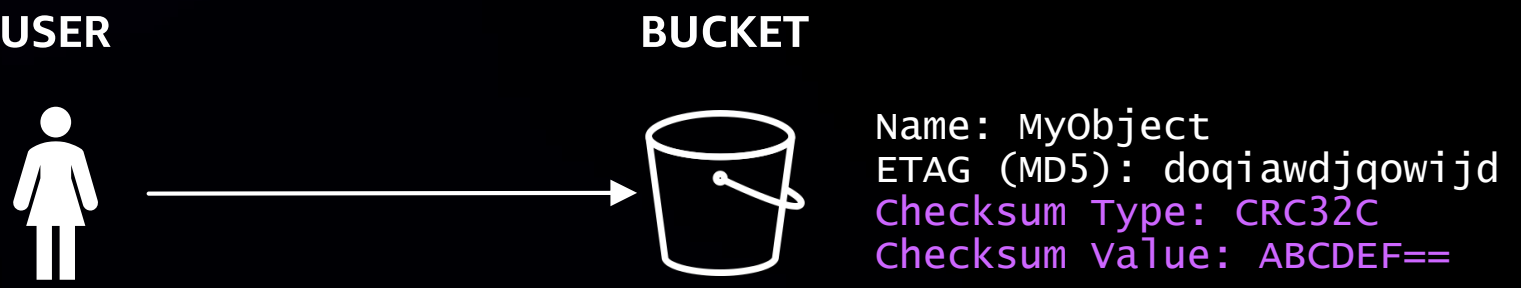
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New checksum options

Coming Soon

New checksum

`x-amz-checksum = CRC32C`



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

New checksum options

Coming Soon

New checksum

`x-amz-checksum = CRC32C`

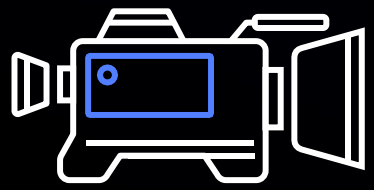


SHA-256 | **SHA-1** | **CRC32** | **CRC32C**

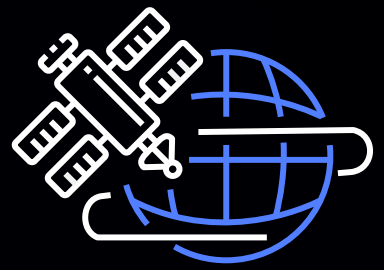
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Objects are getting bigger

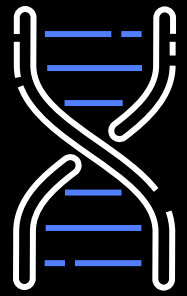
Coming Soon



Media files



Geospatial images



Genome data

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

Coming Soon

Accelerate integrity checks by up to 92%

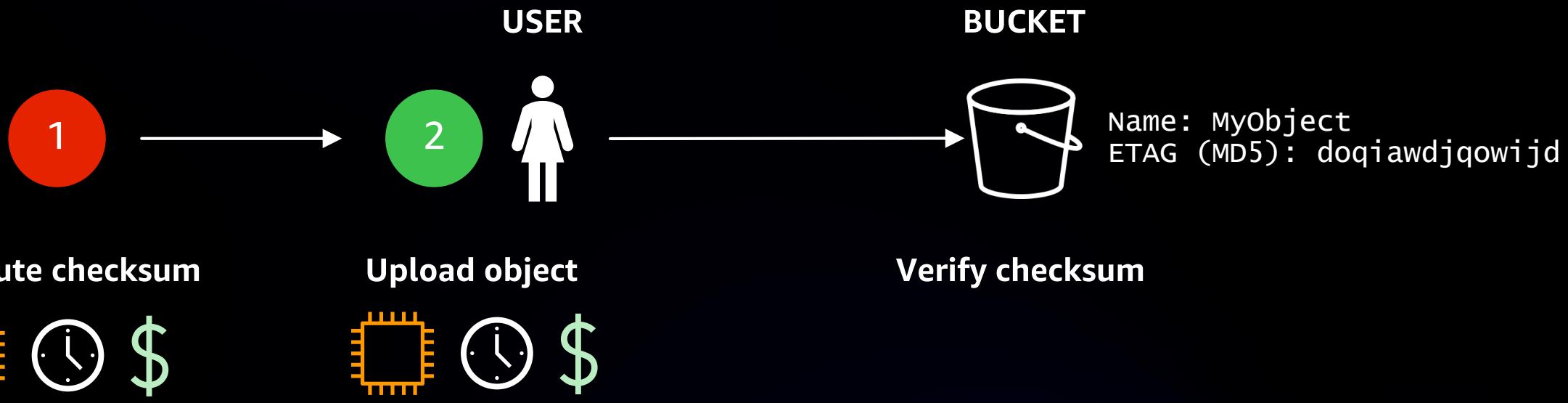
1. Trailing checksums allow you to check data while you stream it in

2. Parallel checksums allow you to break up large objects and leverage many cores

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

Checksums in S3 today

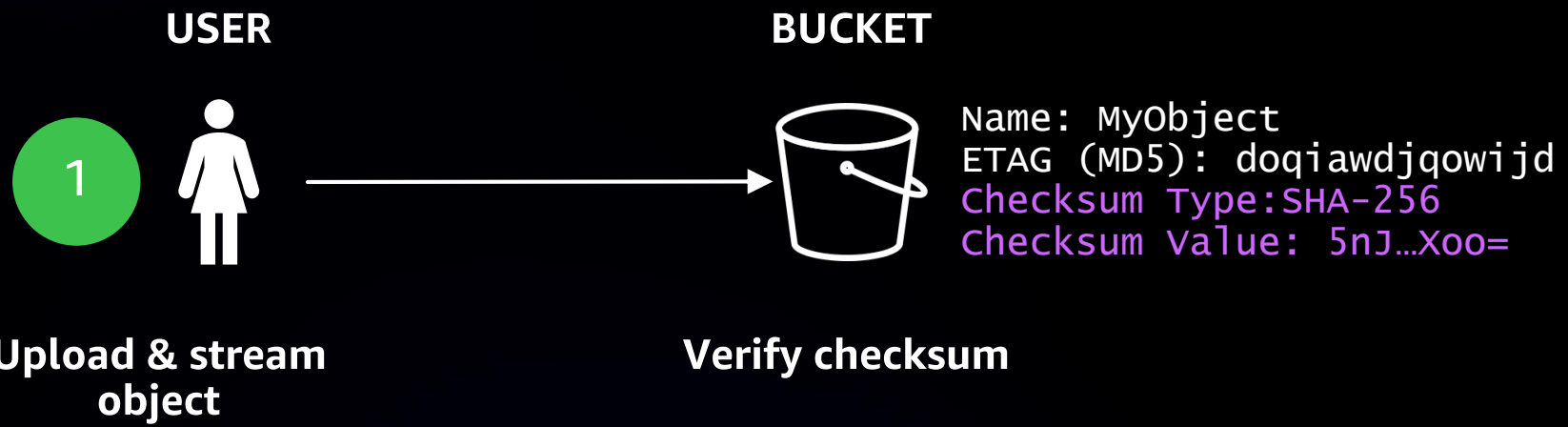
Coming Soon



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

Trailing checksums

Coming Soon



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

Trailing checksums

Coming Soon

```
PUT /key HTTP/1.1
Host: bucket.s3.amazonaws.com
x-amz-date: Mon, 22 Mar 2021 23:00:00 GMT
Authorization: <authorization string>
```

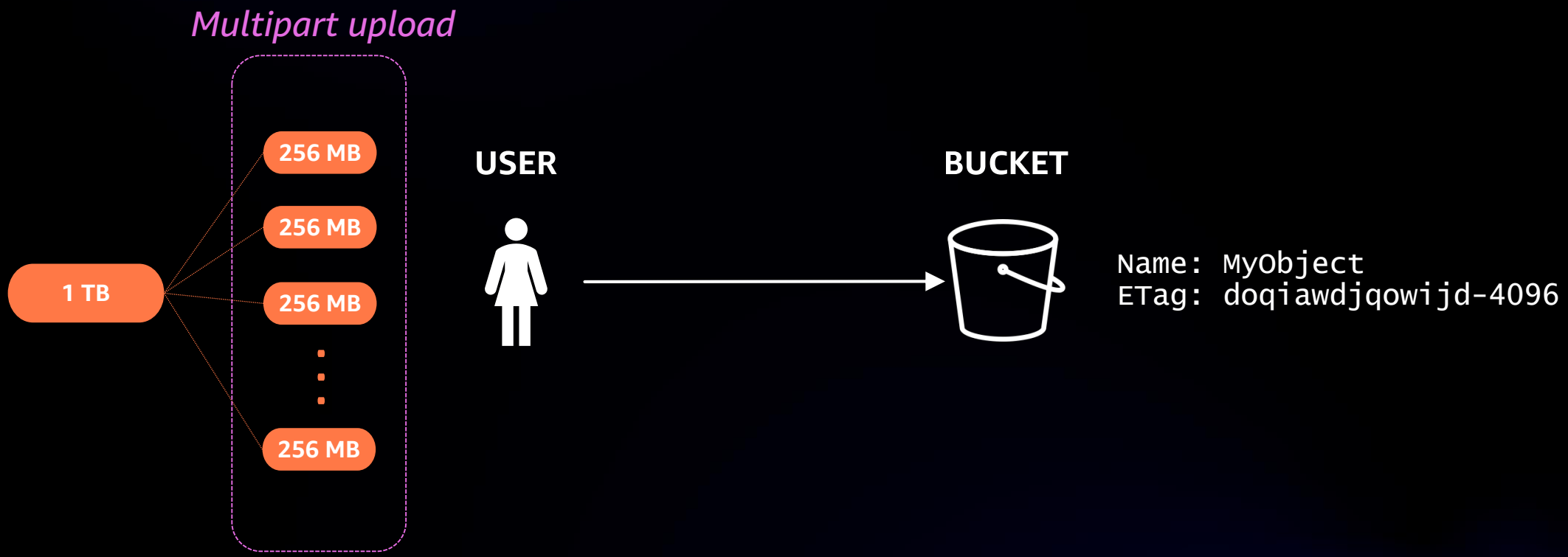
```
x-amz-decoded-content-Length: 268435456
Content-Encoding: aws-chunked
x-amz-trailer: x-amz-checksum-sha256
…
Hex(268435456);
[268435456 byte chunk]
0;
x-amz-checksum-sha256: 9D0K0M1 … F0493d3f=
```

aws

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

Checksums in S3 today

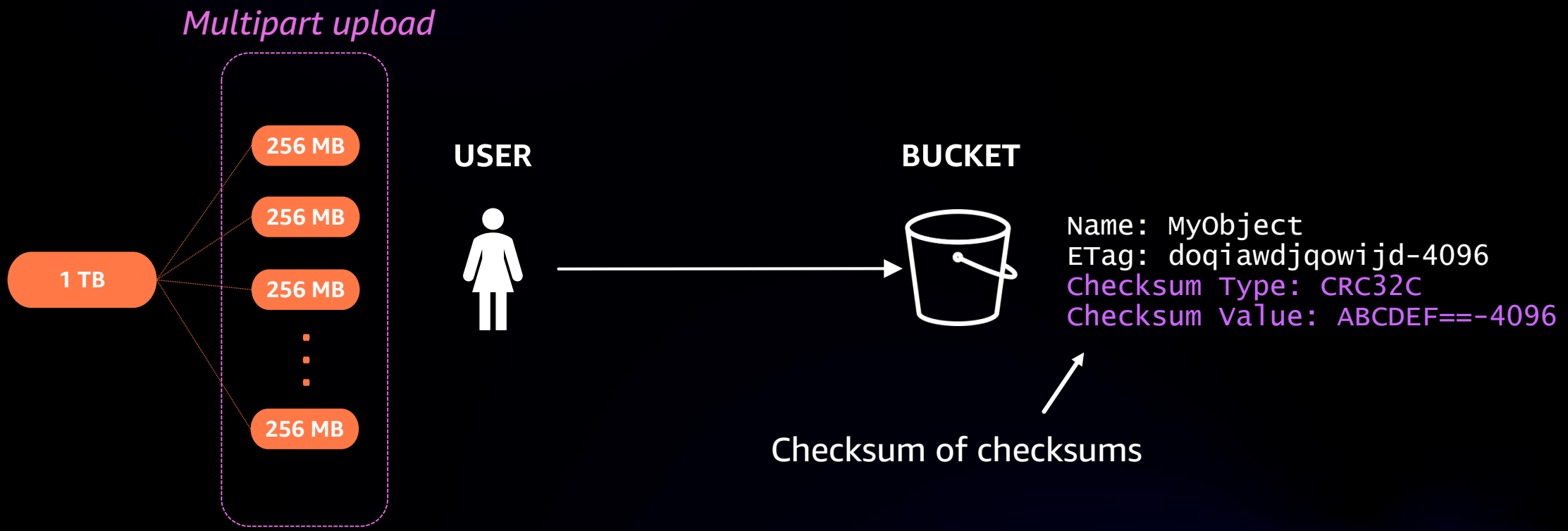
Coming Soon



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

Coming Soon

With new checksums

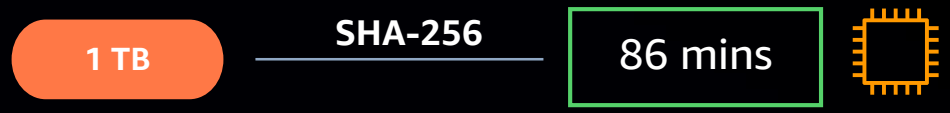


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Checksums in S3 today

Coming Soon

Calculating full object checksum



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

The GetObjectAttributes API

Coming Soon



A new S3 API that gives you:

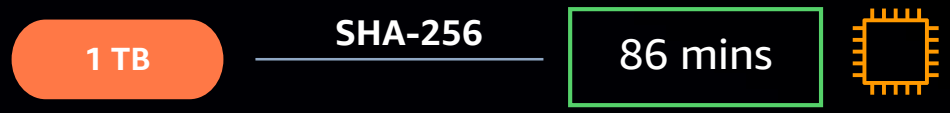
- Checksum algorithm
- Checksum value
- Number of parts
- Part boundaries
- Part-level checksum values

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

Checksums in S3 today

Coming Soon

Calculating full object checksum



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

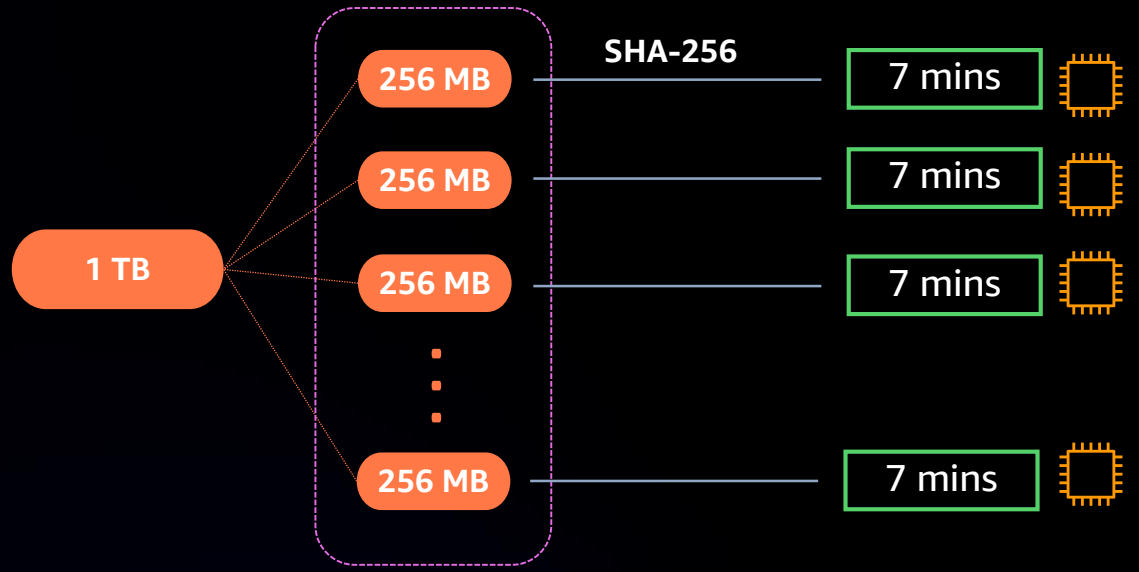
Parallelized checksums

Coming Soon

Calculating full object checksum



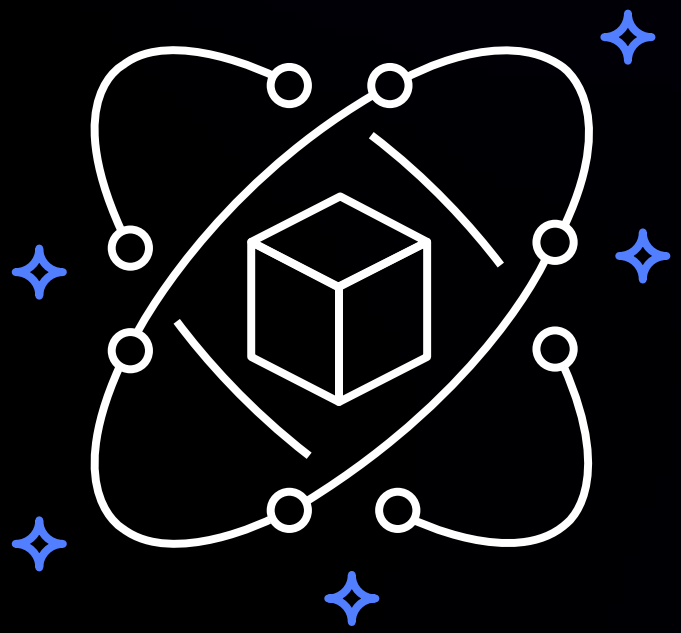
Performing parallel checksum operations



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

Coming Soon

S3 Checksums – Summary

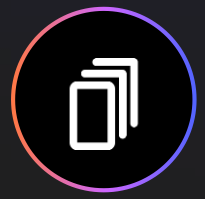


- Accelerate integrity checking of requests by up to 92%
- Choose from four supported checksum algorithms
- Supports data integrity checking on uploads and downloads
- Enhancements to the AWS SDK and S3 API significantly improve checksum efficiency

aws

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

New data protection features for Amazon S3



S3 support for AWS PrivateLink

Direct access to S3 via a private endpoint within your virtual private network

Launched: February 2021



S3 Access Point Aliases

Allow any application that requires an S3 bucket name to easily use an access point

Launched: July 2021



S3 Multi-Region Access Points

Accelerate performance by up to 60% when accessing replicated data sets

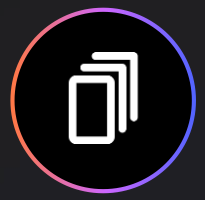
Launched: September 2021



S3 Object Ownership Enhancements

New setting disables access control lists, simplifying access management

Launched: Today!



Policy Validation

Console reports security warnings, errors, and suggestions as you author S3 policies

Launched: Today!



New Checksum Options

Amazon S3 accelerates integrity checking of requests by up to 92%

Coming Soon!

aws

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

Thank you!

Nitish Pandey
npandey@amazon.com

John Robe
jrobej@amazon.com

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