
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

STG301

# Amazon S3 security and access control best practices

Meg Rose

Senior Software Development Manager
Amazon Web Services

Raymond Lui

Senior Technical Product Manager
Amazon Web Services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data lakes



Log data







Infrastructure data



Content/websites

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data lakes

Log data



Infrastructure data

Content/websites

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Agenda: Securing your data in Amazon S3

This session is by builders, for builders

You will come away with practical tips and strategies for

- Applying S3 Block Public Access settings
- Encrypting data at rest: options and recommendations
- Using policies to share data and enforce assertions
- Simplified approaches to managing S3 objects
- Taking advantage of S3's monitoring tool to understand and log access

aws

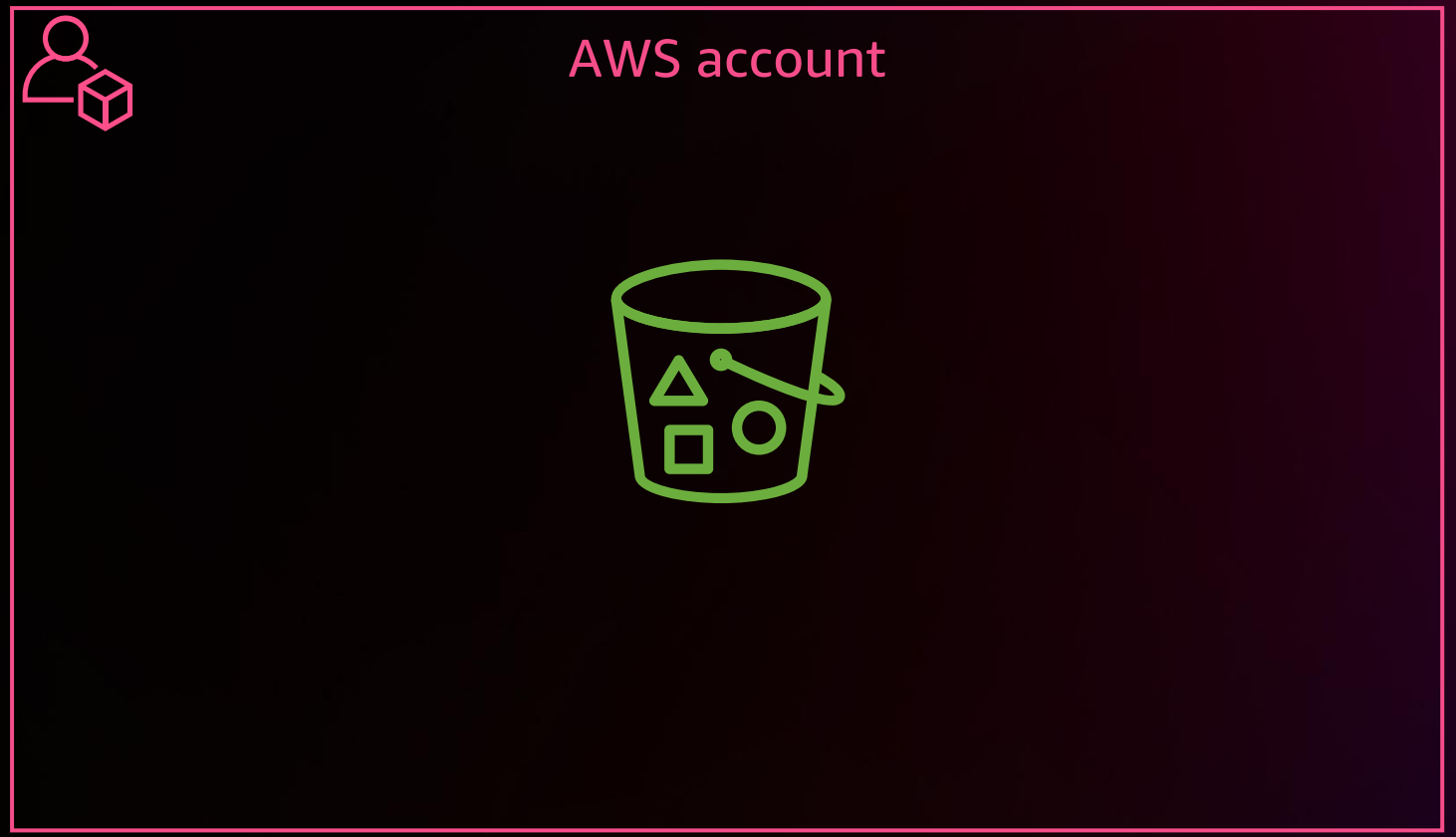
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice #1: Block Public Access

# (Or, if you take away nothing else from this talk)

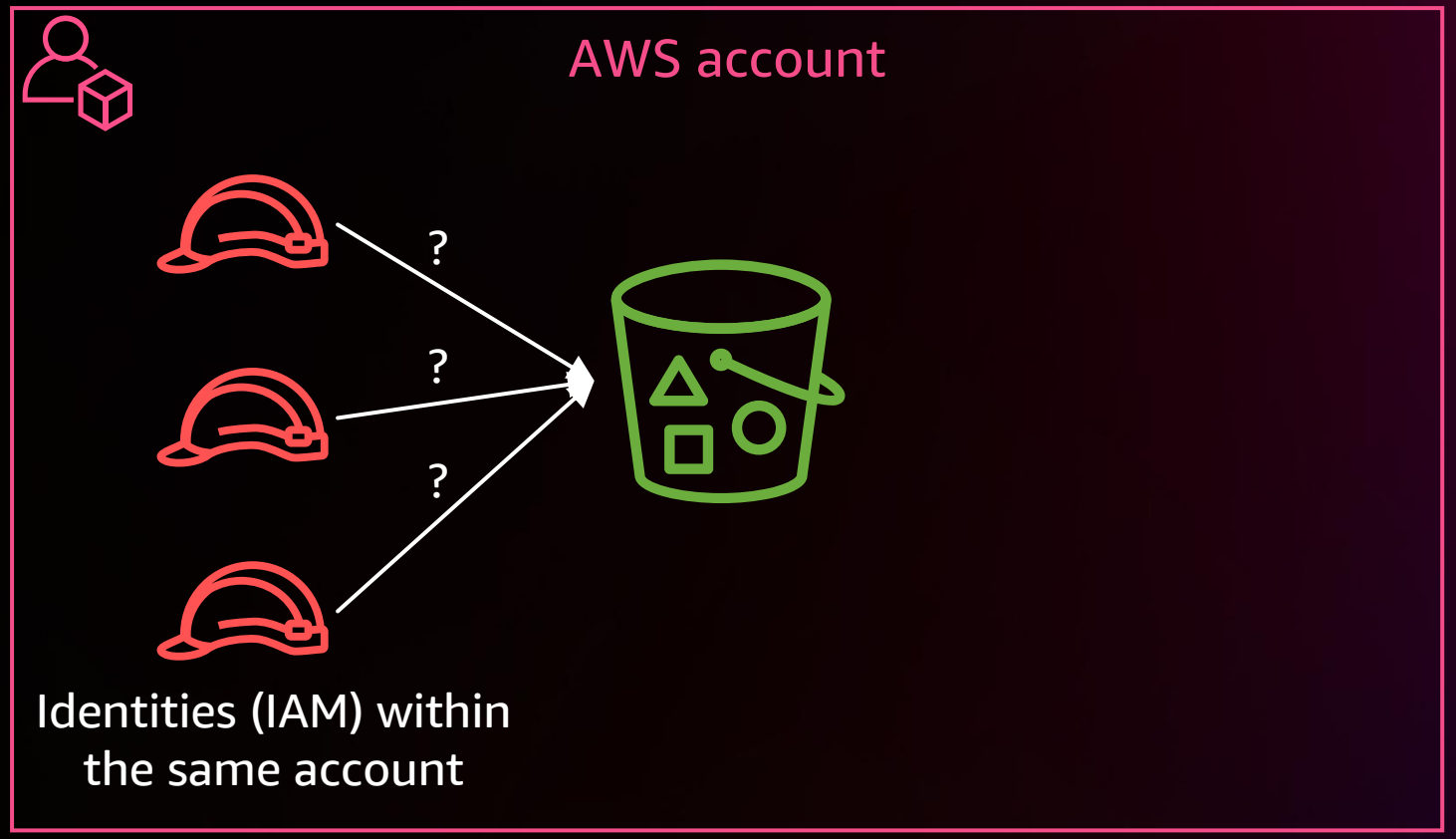
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# S3 buckets are private by default



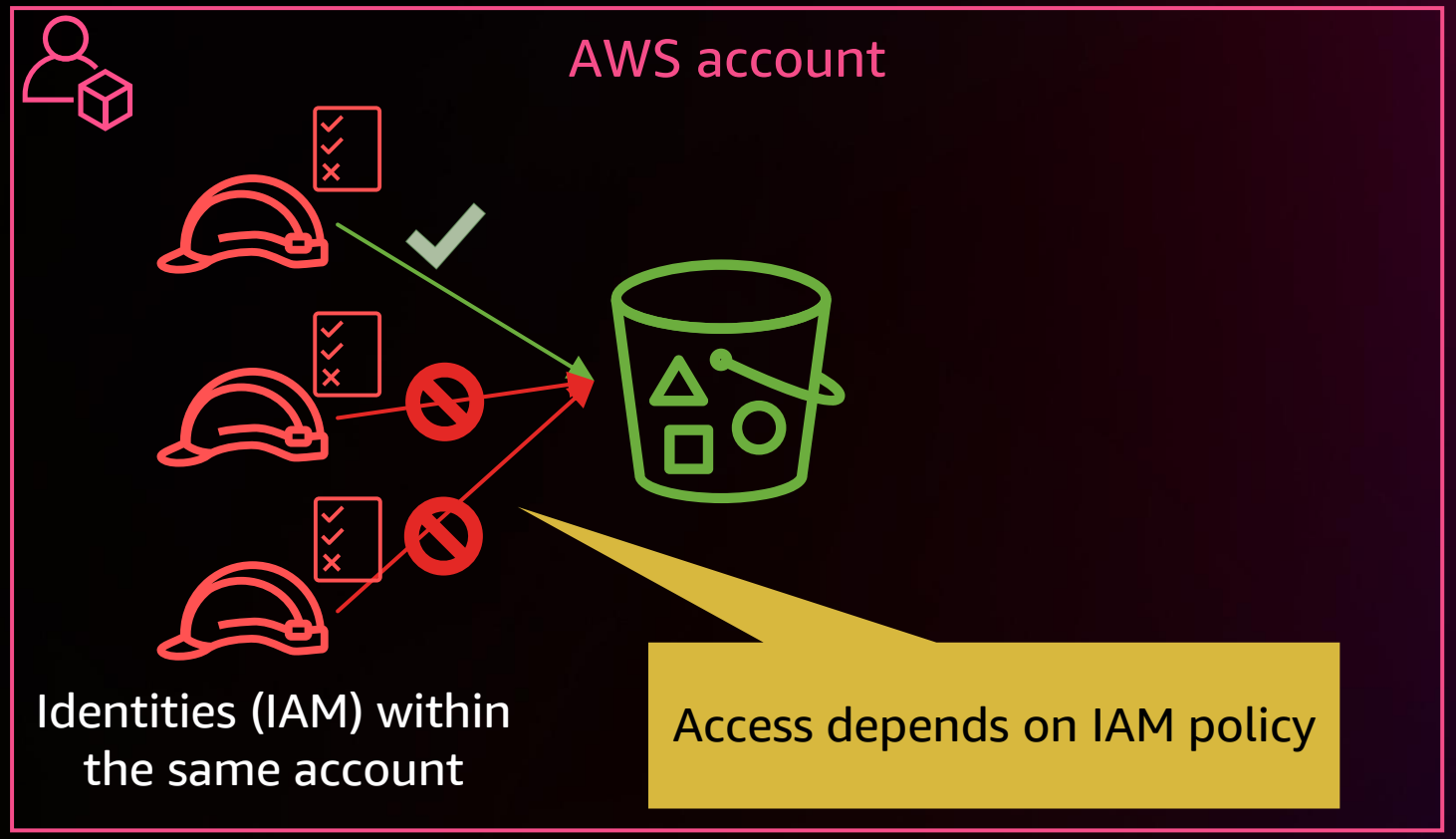

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# S3 buckets are private by default



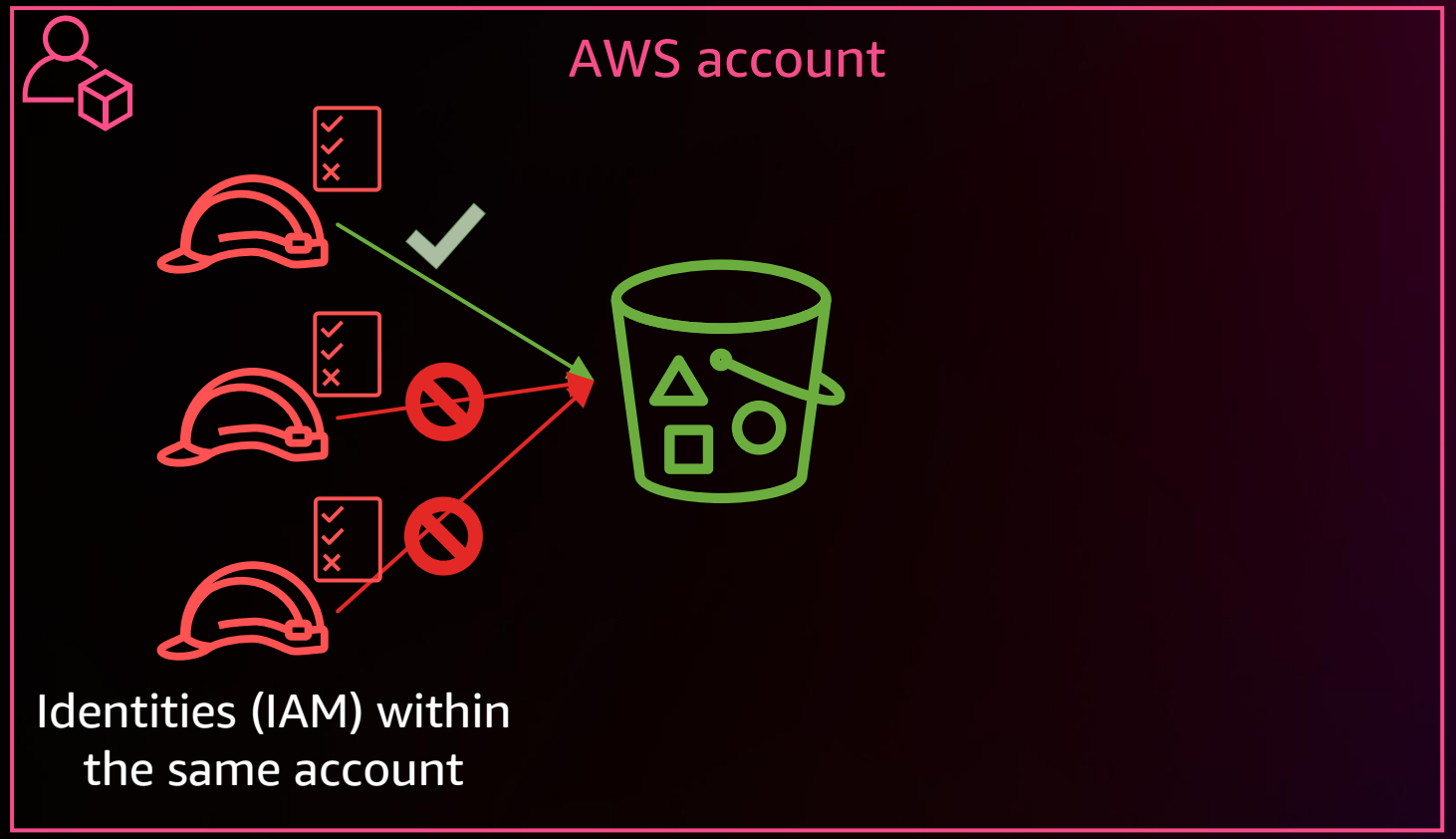

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# S3 buckets are private by default




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# S3 buckets are private by default








Identities outside the account

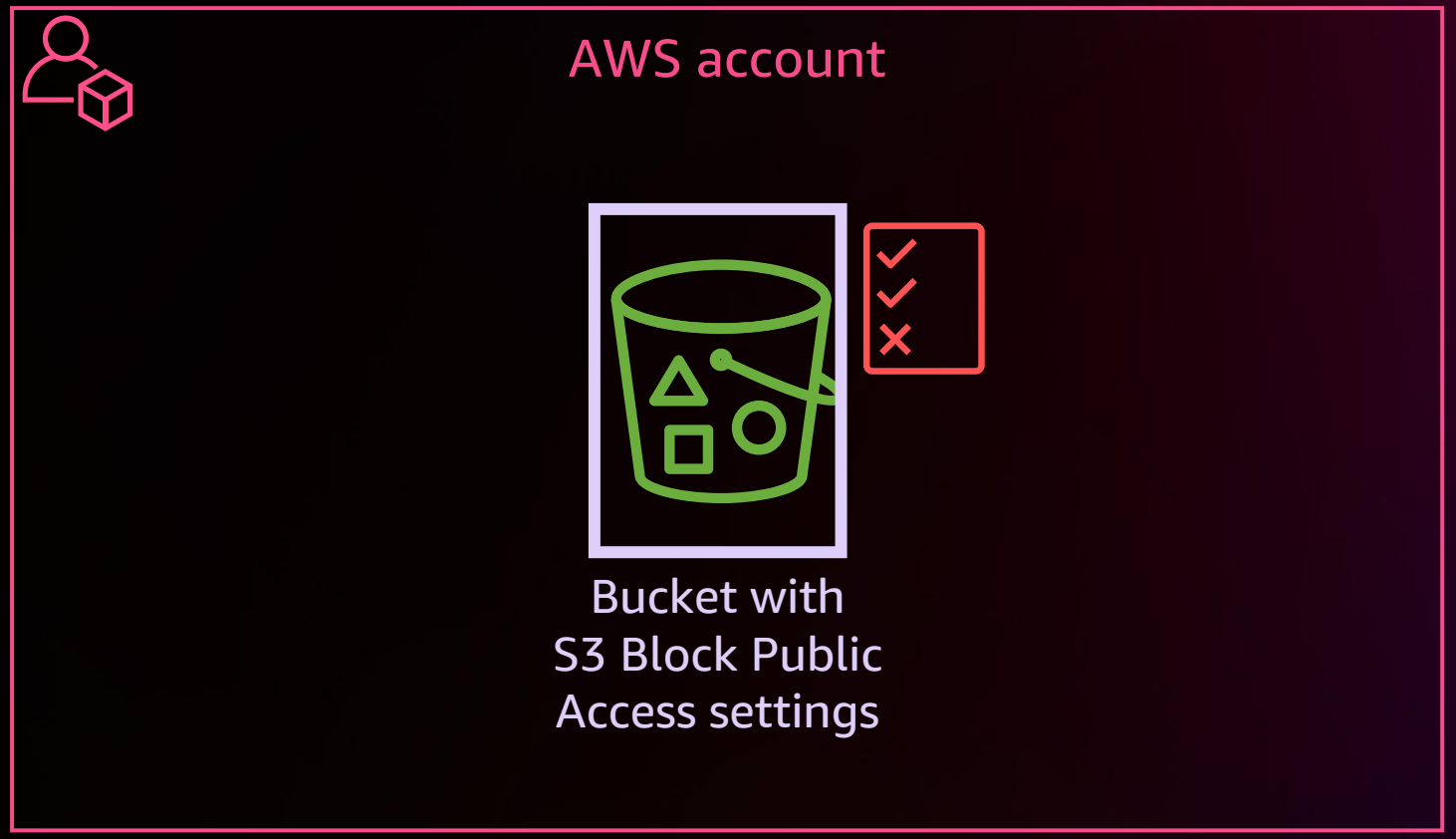
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# S3 buckets are private by default



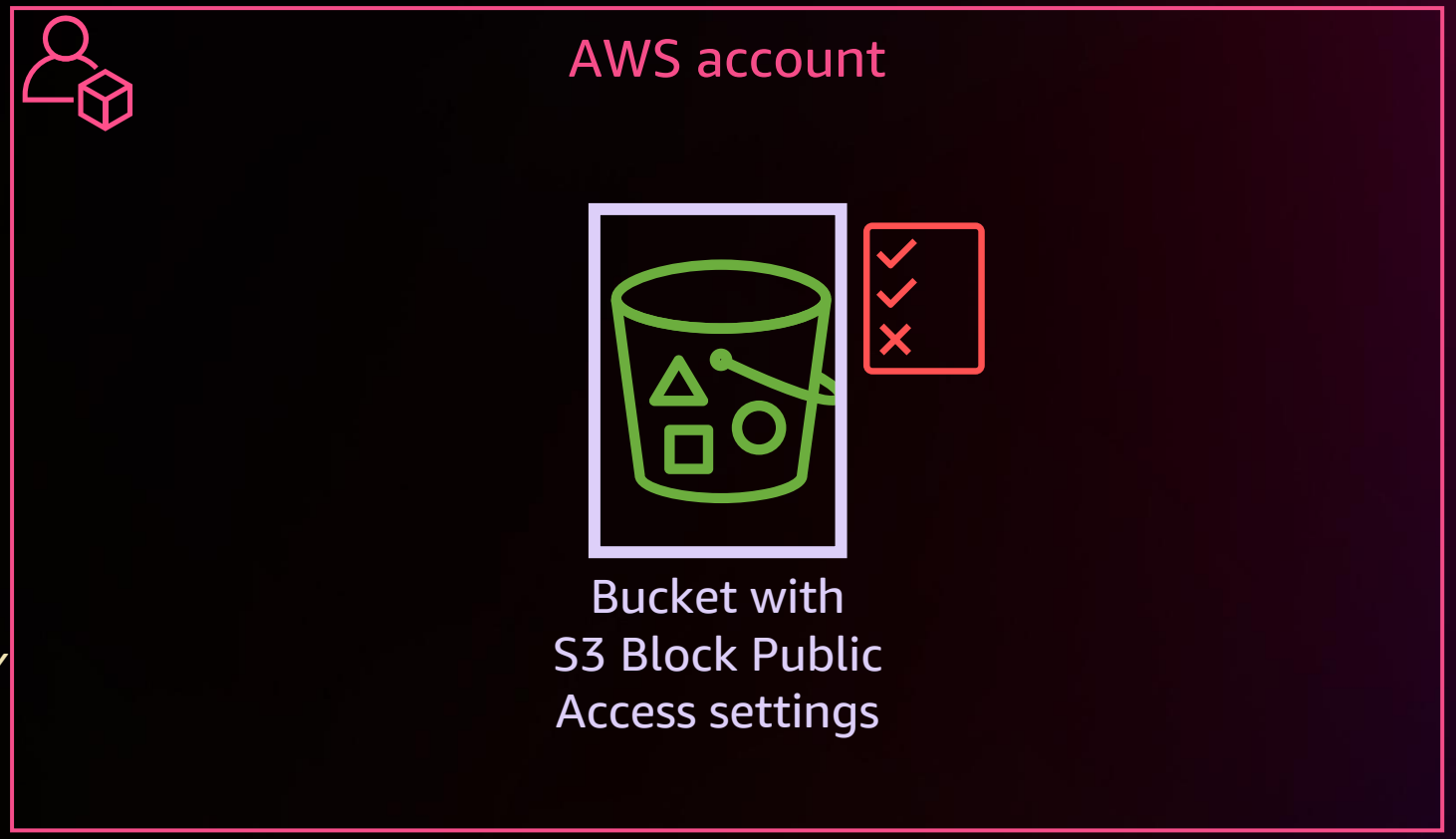

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Block public access in Amazon S3: Do it now




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

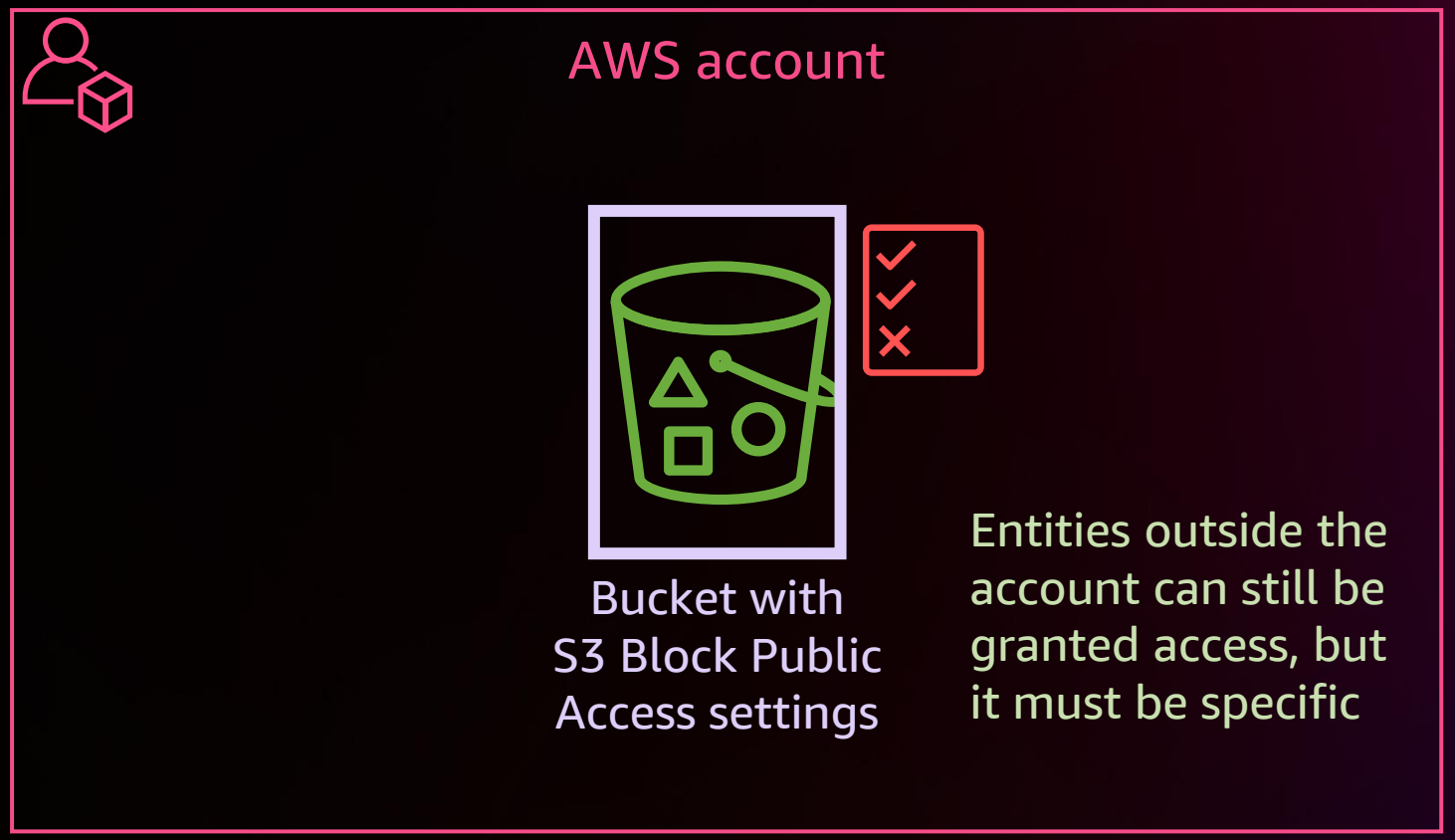
# Block public access in Amazon S3: Do it now




Parties not *explicitly* granted access will not have access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Block public access in Amazon S3: Do it now




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Block public access in Amazon S3: Apply to your entire account

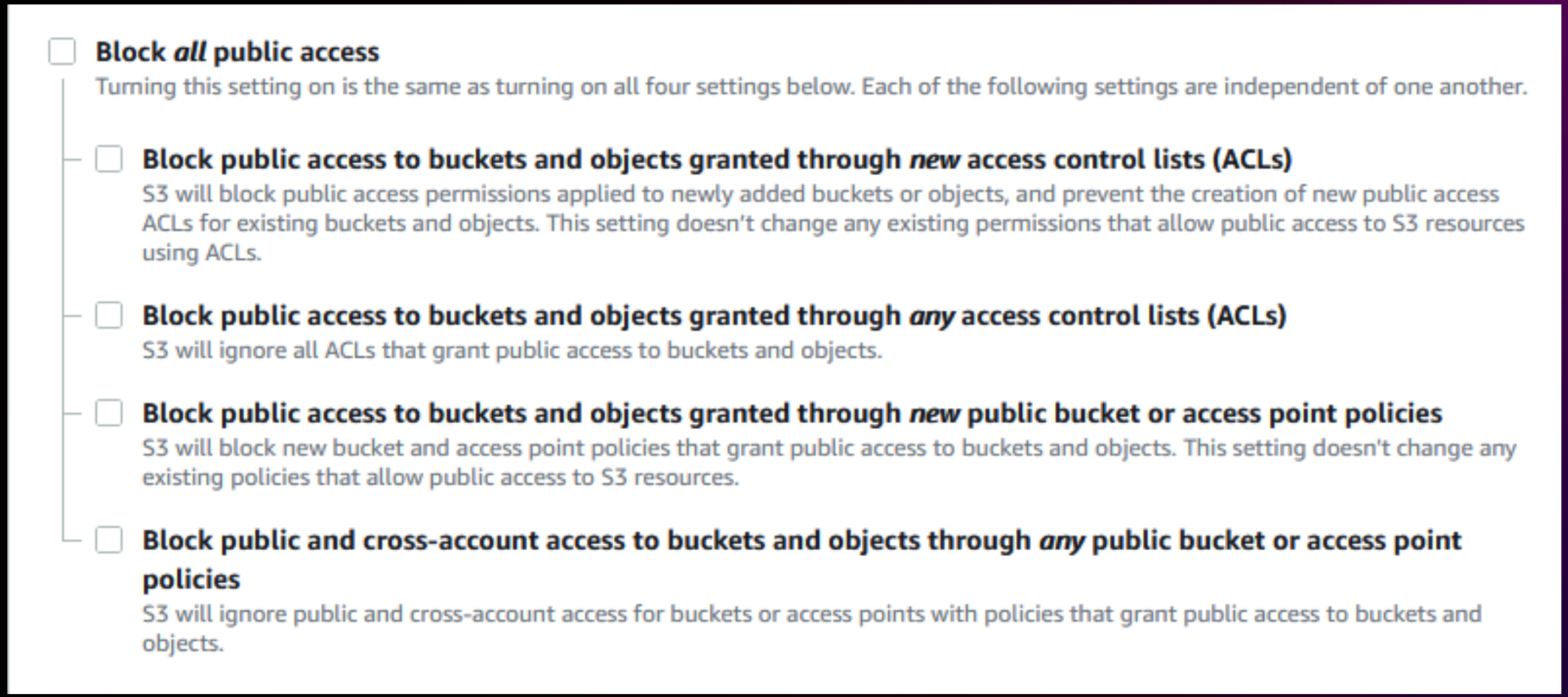



AWS account with S3 Block Public Access settings

aws

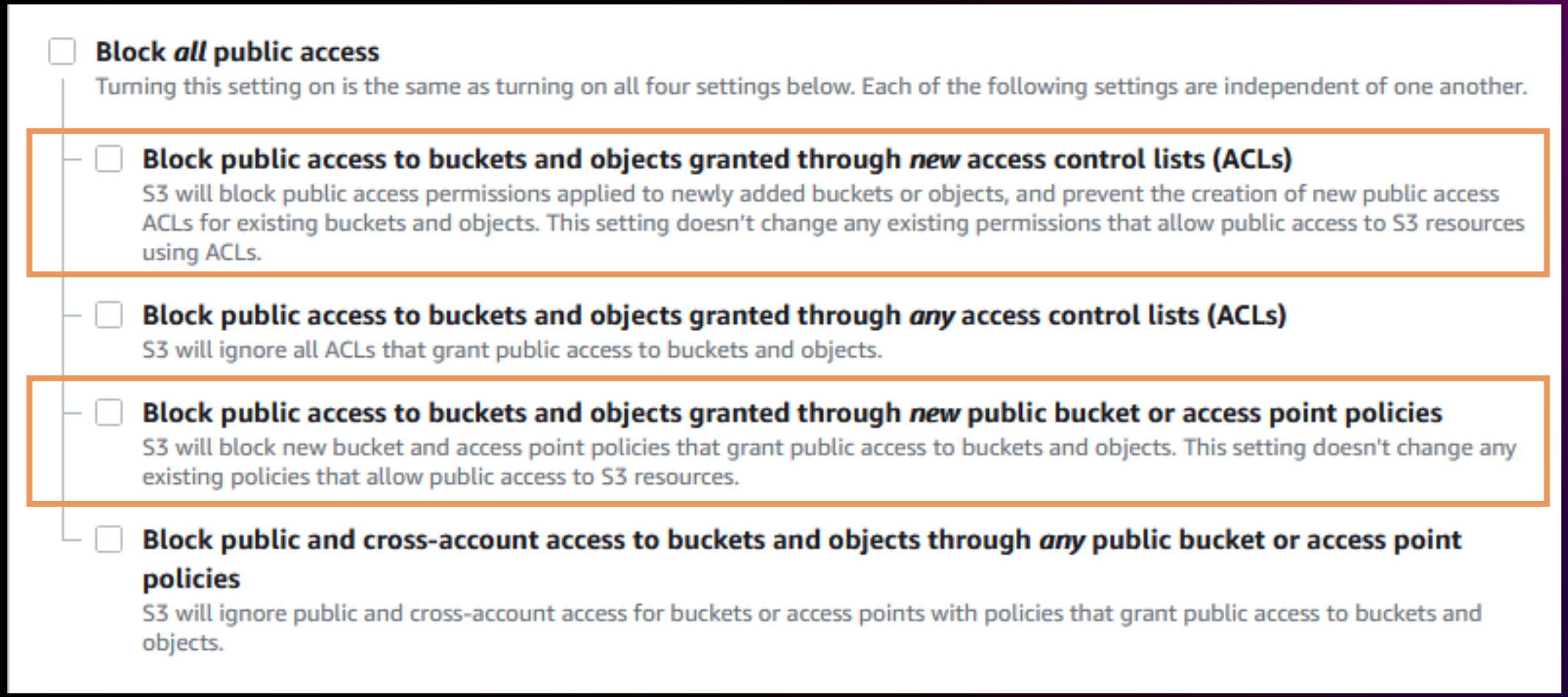
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Block Public Access: The details



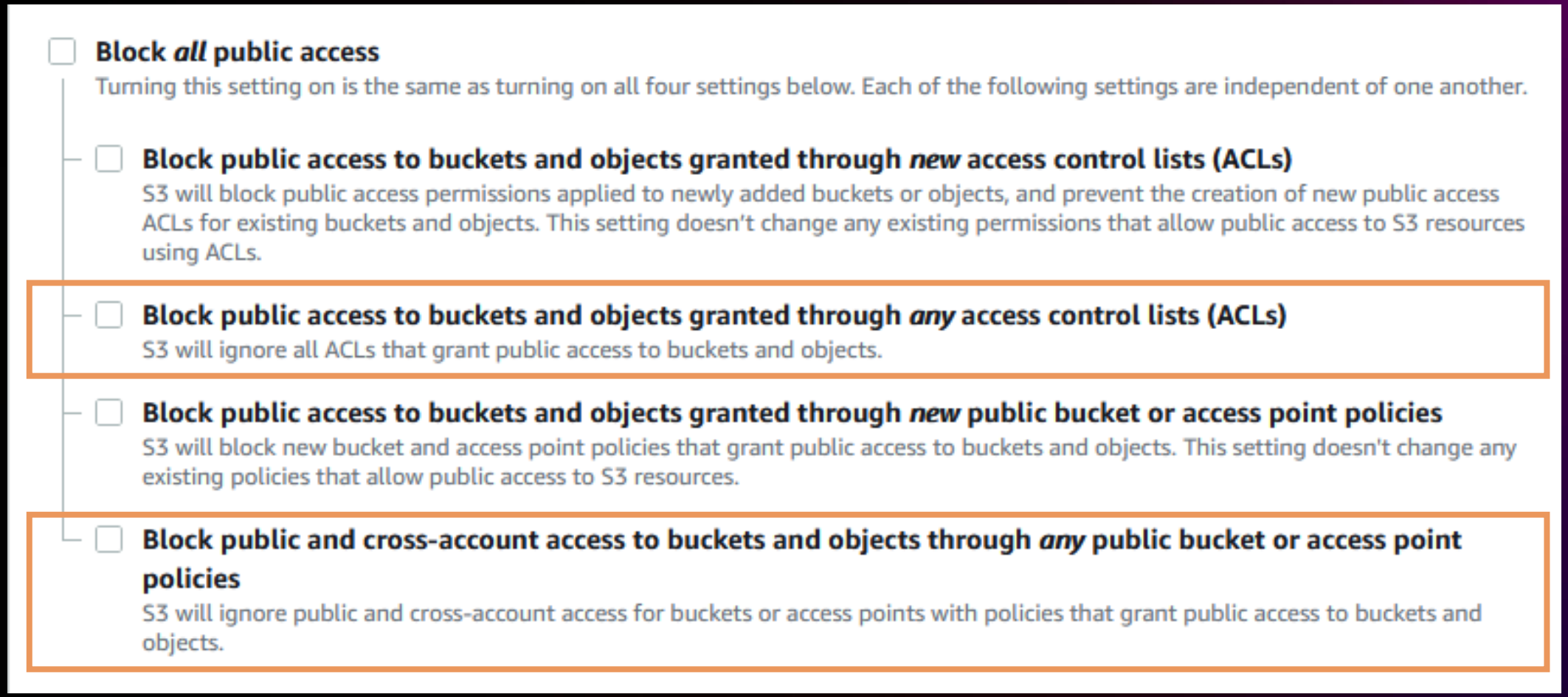

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Block Public Access: The details



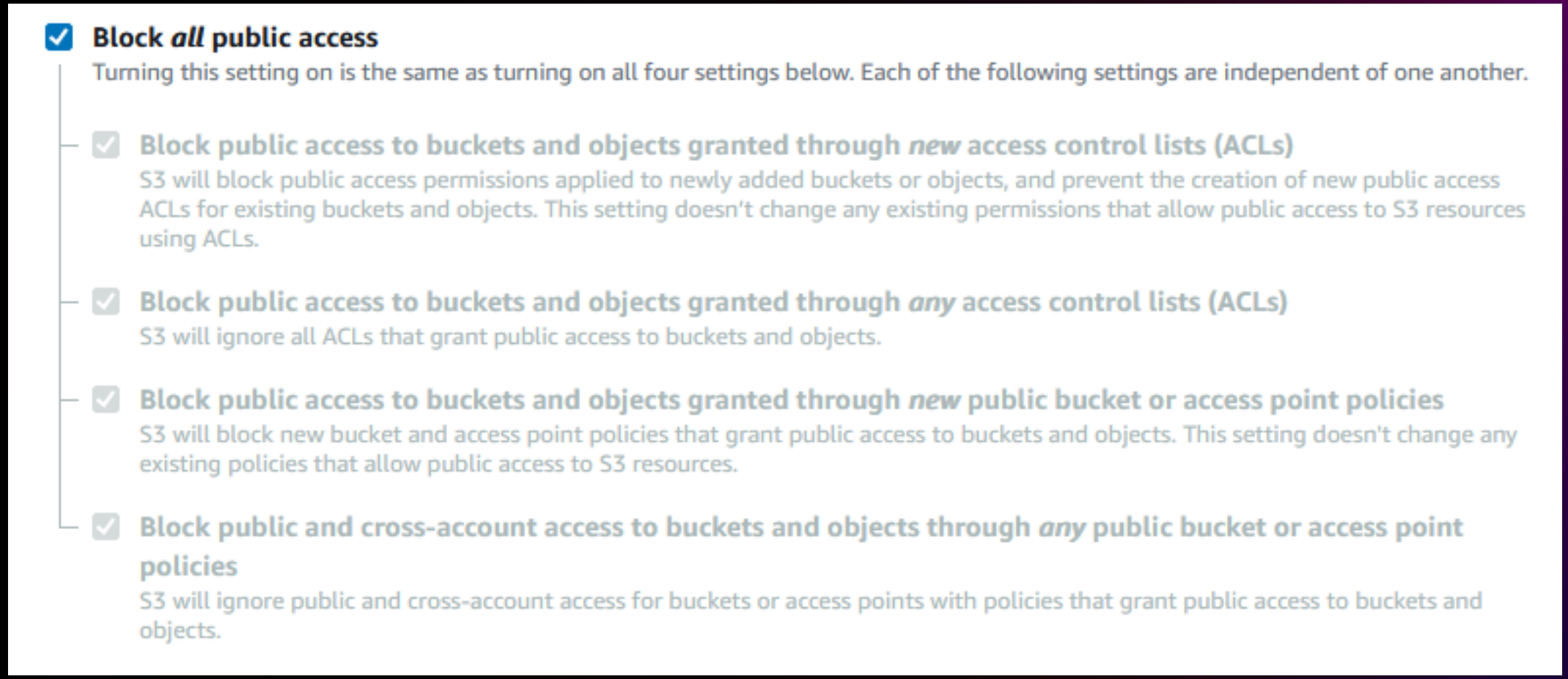

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Block Public Access: The details




aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Block Public Access: The details




aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Scenarios for S3 Block Public Access

Is S3 Block Public Access a good fit for

- ✓ Data lake buckets?
- ✓ Buckets containing application configuration?
- ✓ Log data?
- ✓ Static website content? Yes! As an Amazon CloudFront origin
- ⊘ Public datasets that you wish to make directly available from S3?



Bucket with S3 Block Public Access settings

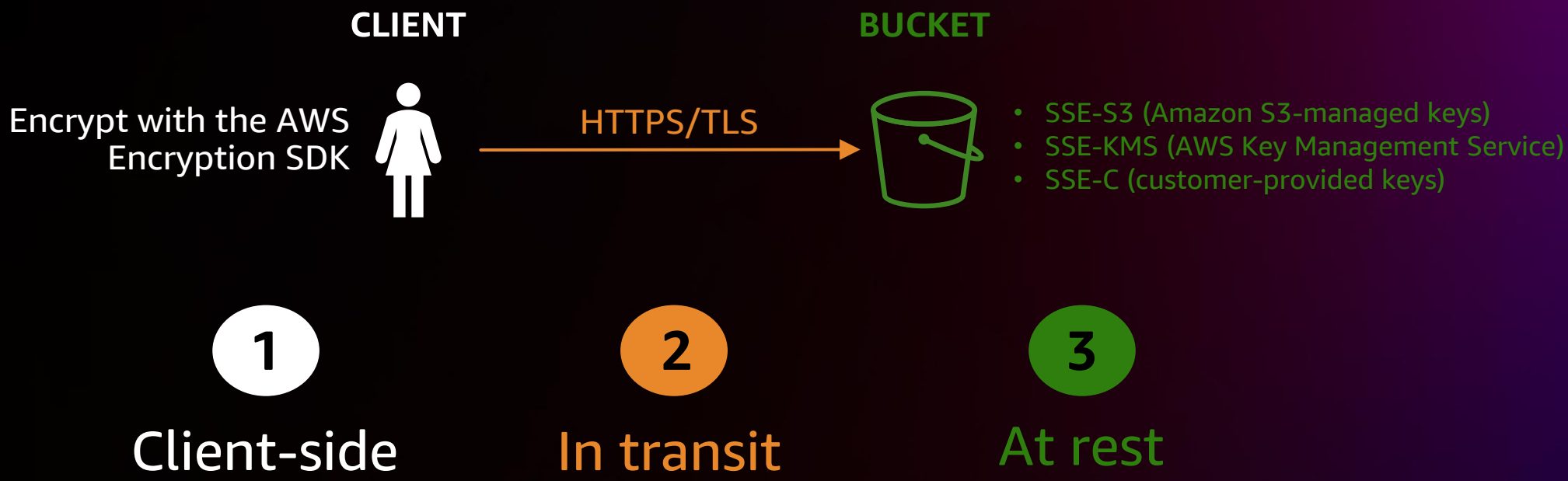
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice #2: Encryption

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon S3 encryption support




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon S3 encryption at rest options

| | Amazon S3- managed keys (SSE-S3) | AWS KMS keys (SSE-KMS) with Customer Managed Key | AWS KMS keys (SSE-KMS) with AWS Managed Key |
|---|---|---|---|
| Manage Key Policies | ✗ | ✓ | ✗ |
| AWS CloudTrail Logging | ✗ | ✓ | ✓ |
| Key Rotation | Rotated Regularly by S3 | ✓ | Rotated Regularly by AWS |
| Data Shareability | ✓ | ✓ | ✗ |

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Specifying encryption at the object level



**SSE-S3**

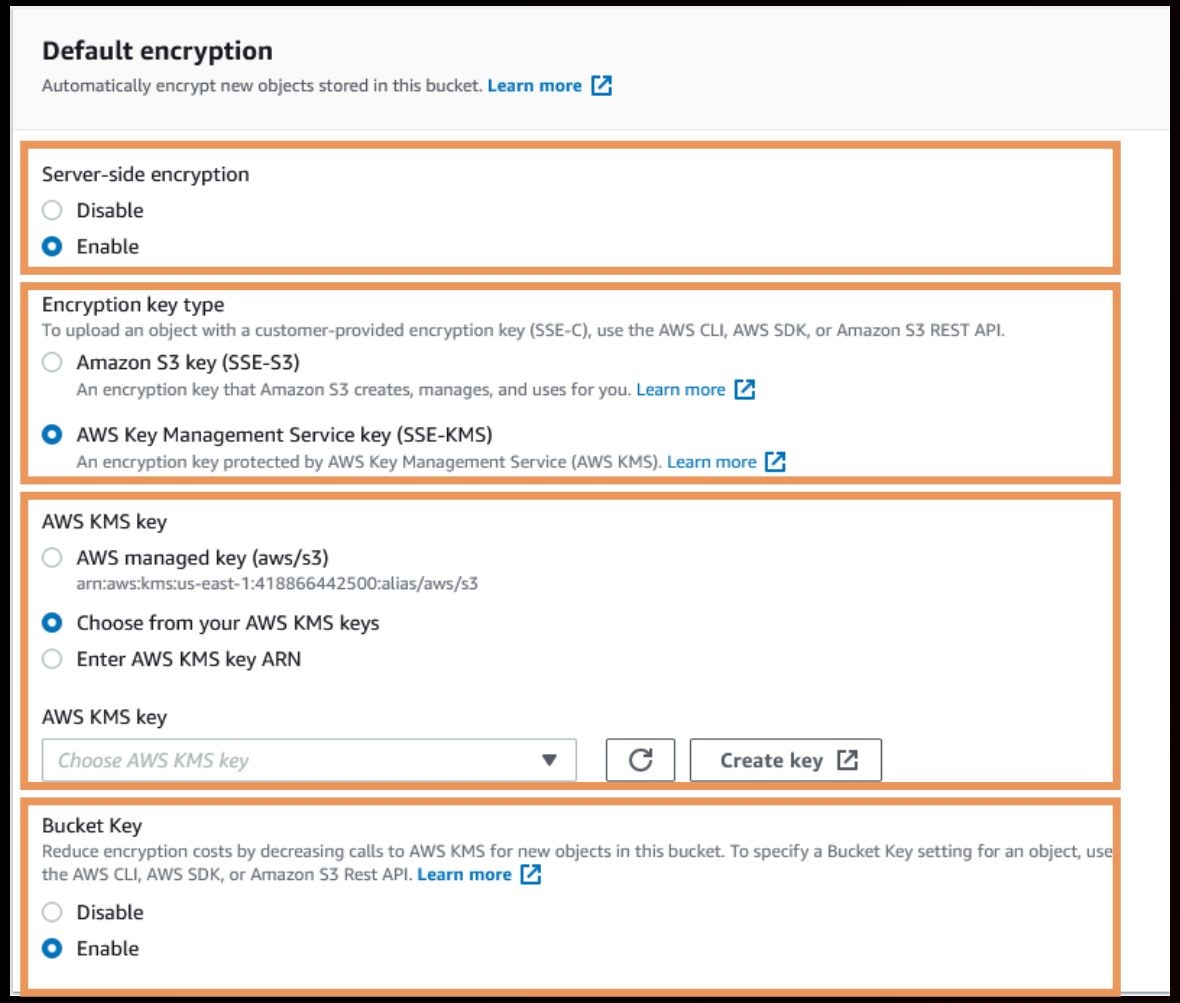
"x-amz-server-side-encryption": "AES:256"

**SSE-KMS**

"x-amz-server-side-encryption": "aws:kms"
"x-amz-server-side-encryption-aws-kms-key-id": *“your KMS key ID”*

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Enabling Amazon S3 default encryption




- One-time bucket-level setup
- Automatically encrypts all new objects

- Specify key management strategy
- You manage keys, or offload to Amazon S3

- If AWS KMS, then specify a key
- Use your own or a service-managed key

- Reduce AWS KMS costs with a bucket key
- Results in up to 99% fewer AWS KMS requests

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Scenarios for encryption settings

Object PUT: No encryption specified
Bucket: SSE-S3 default enabled

**SSE-S3**

Object PUT: SSE-KMS specified
Bucket: No default encryption

**SSE-KMS**

Object PUT: SSE-S3 specified
Bucket: SSE-KMS default enabled

**SSE-S3**

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Use bucket policy to mandate specific encryption



Unless the object will be encrypted at rest with SSE-KMS, reject the attempt to write it

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::EXAMPLE-BUCKET/*",
  "Condition": {
    "StringNotEquals": {
      "s3:x-amz-server-side-encryption":"aws:kms"
    }
  }
}
```

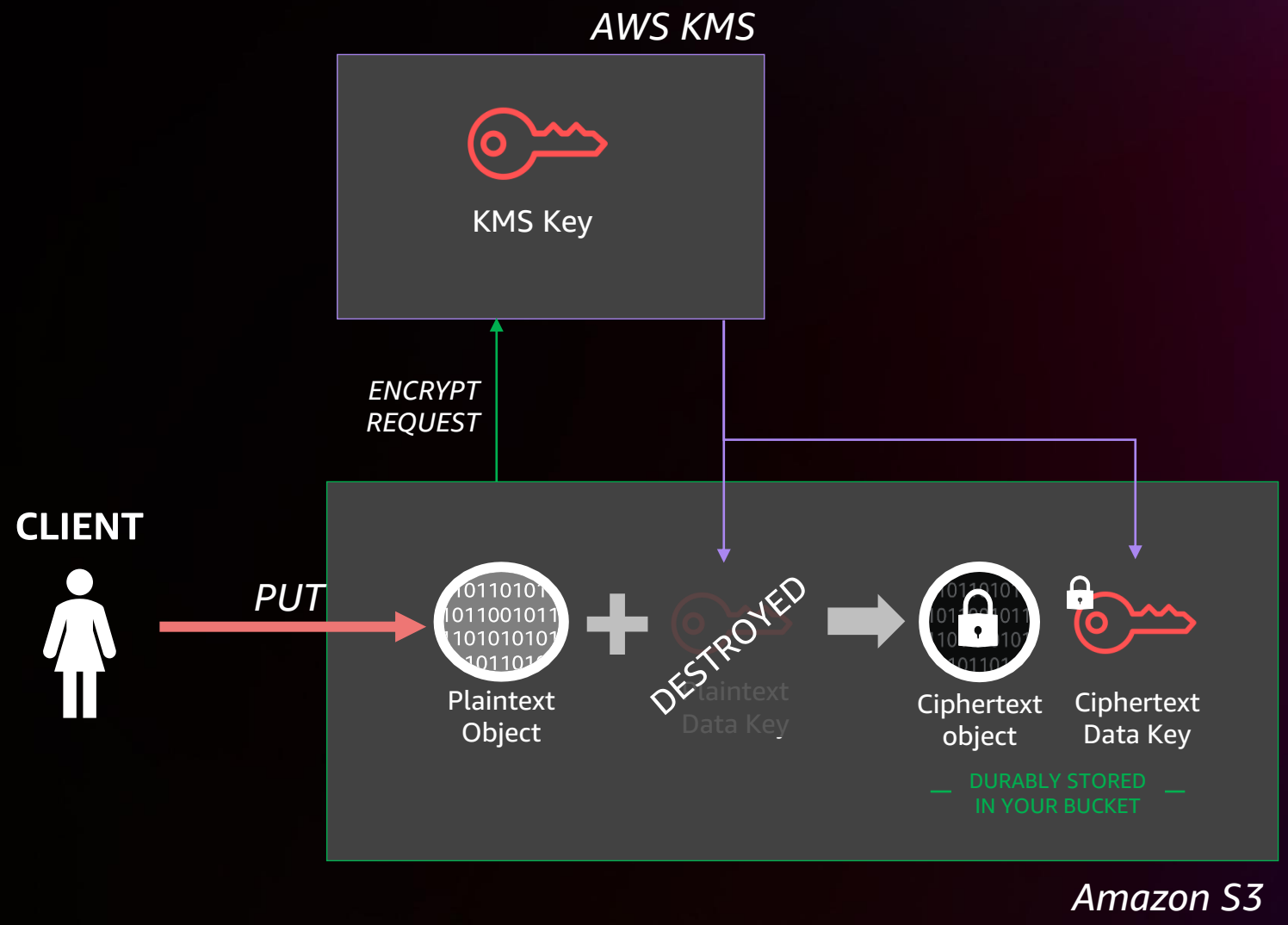
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How encryption works in S3

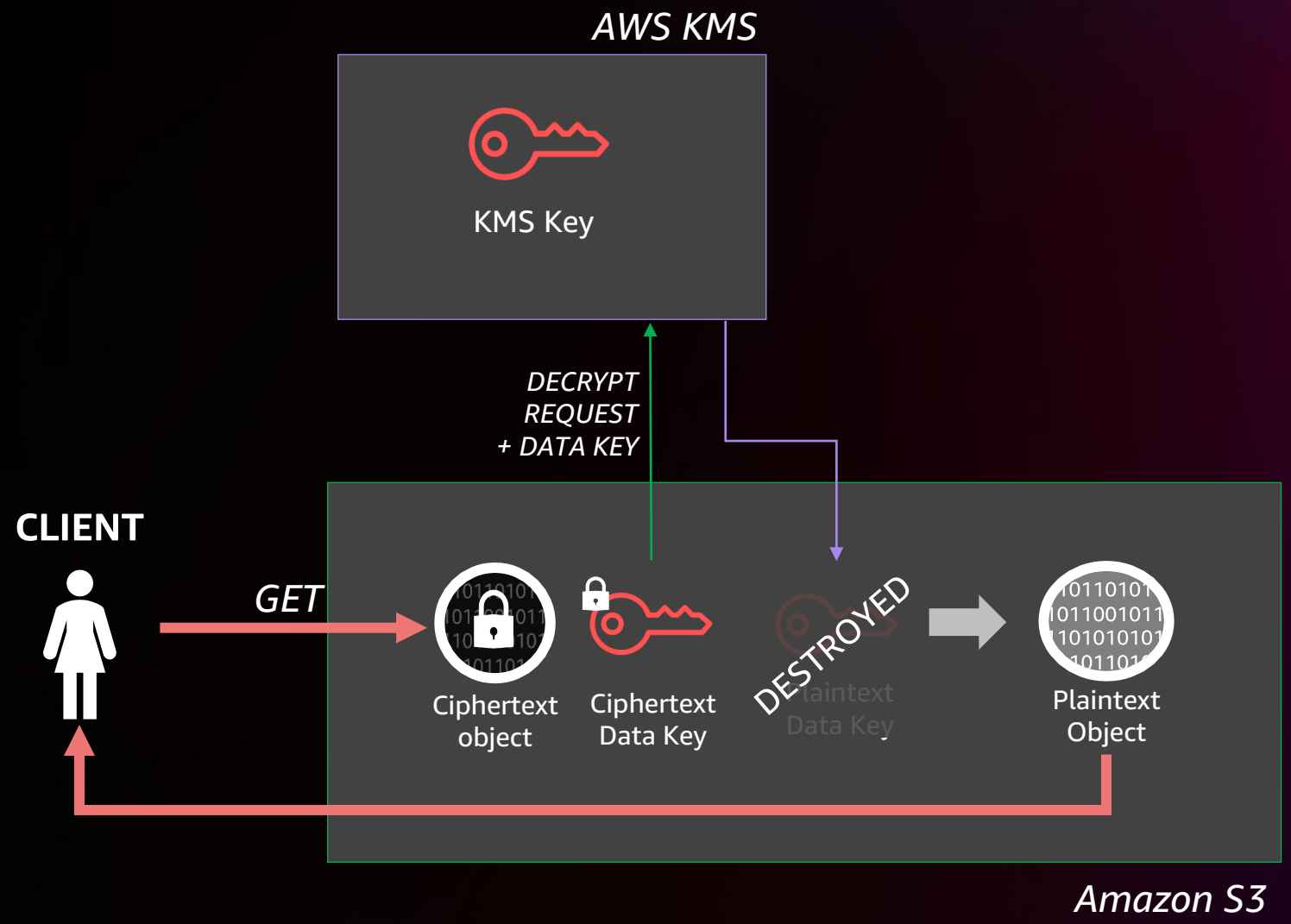
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How an encrypt request works with AWS KMS




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How a decrypt request works with AWS KMS




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon S3 bucket keys

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon S3 bucket keys



Increase performance for encryption



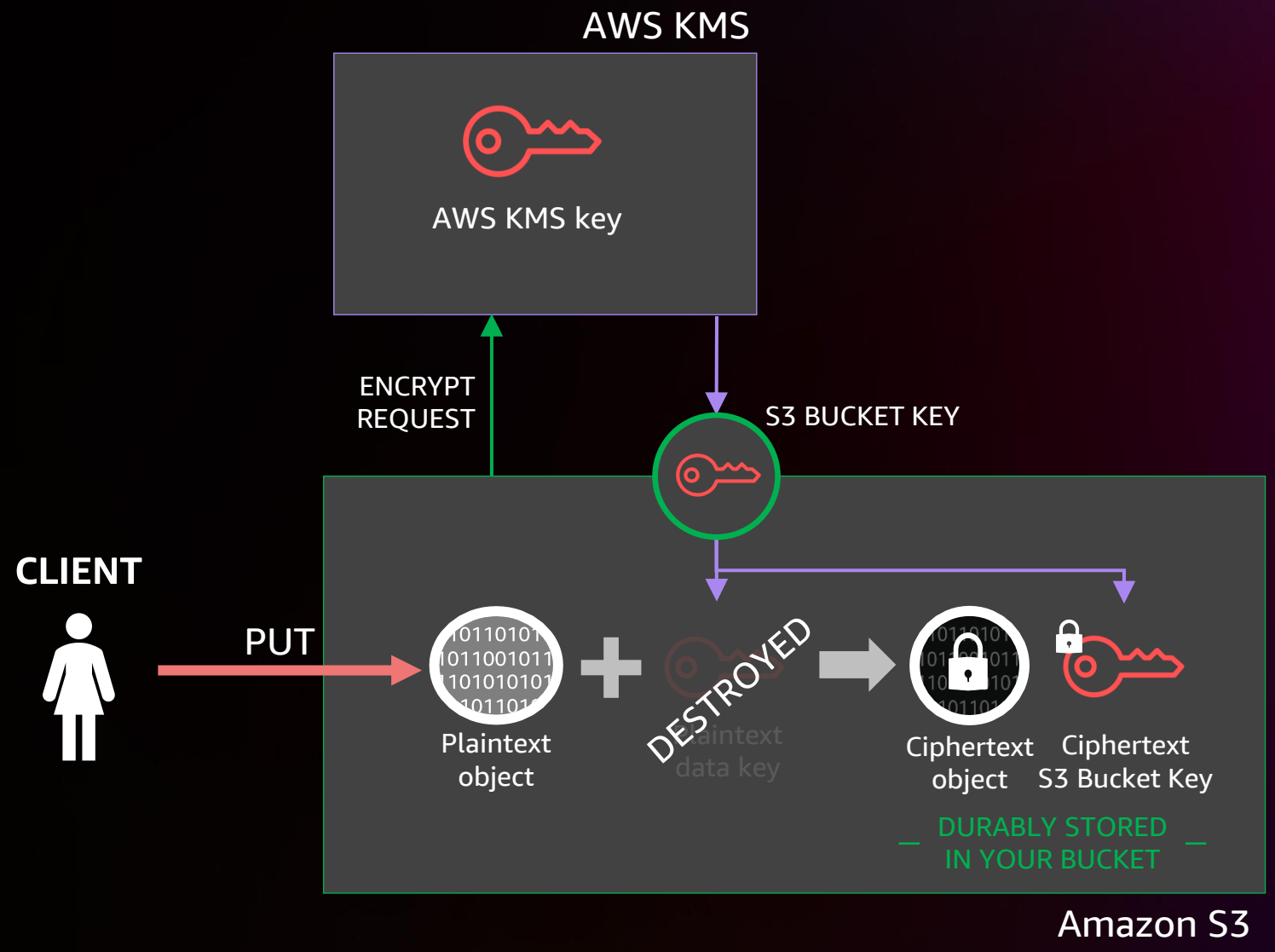
Reduce request costs for KMS-backed server-side encryption by

**UP TO 99%**

aws

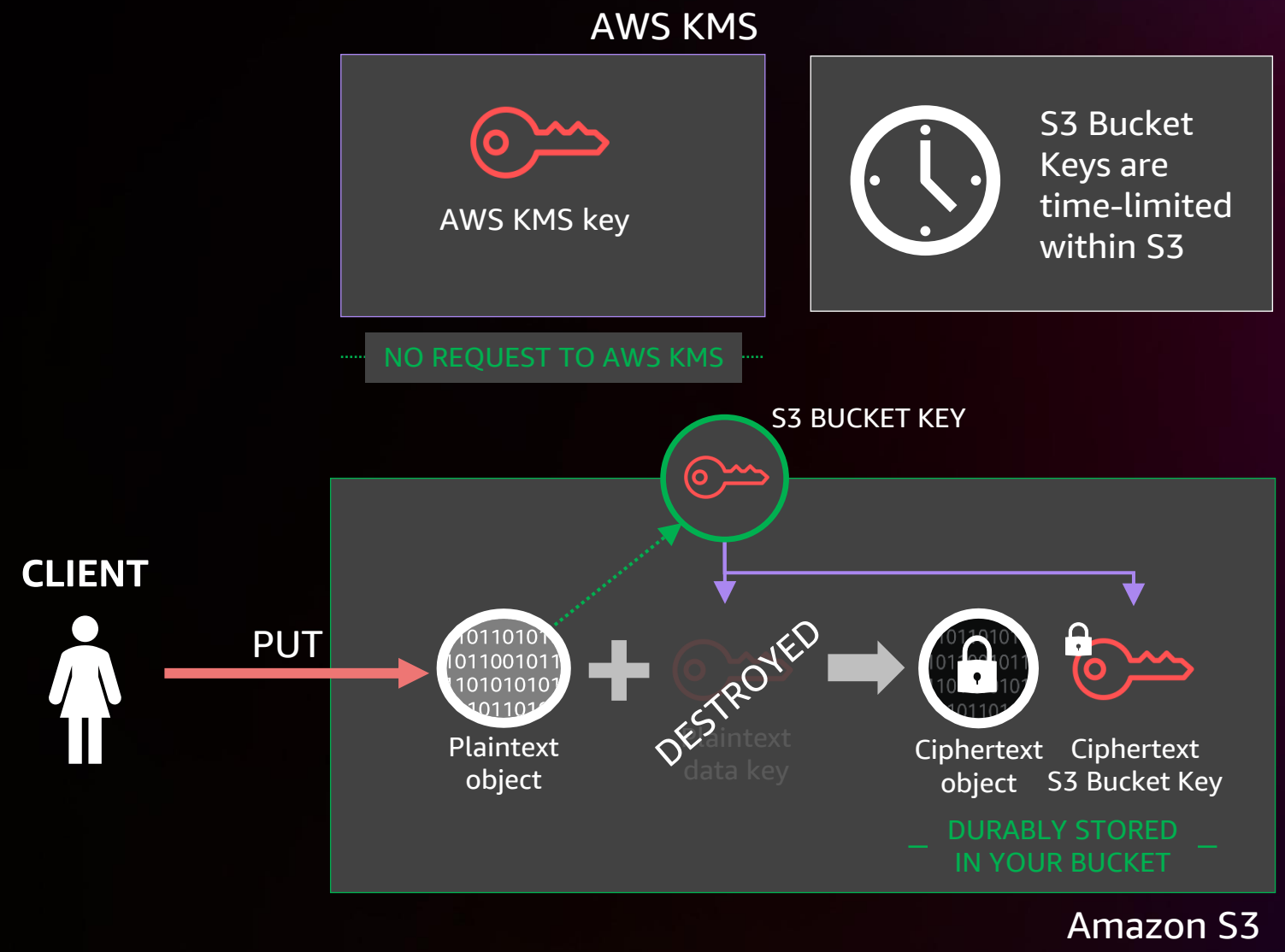
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How do Amazon S3 bucket keys work? (1st request)



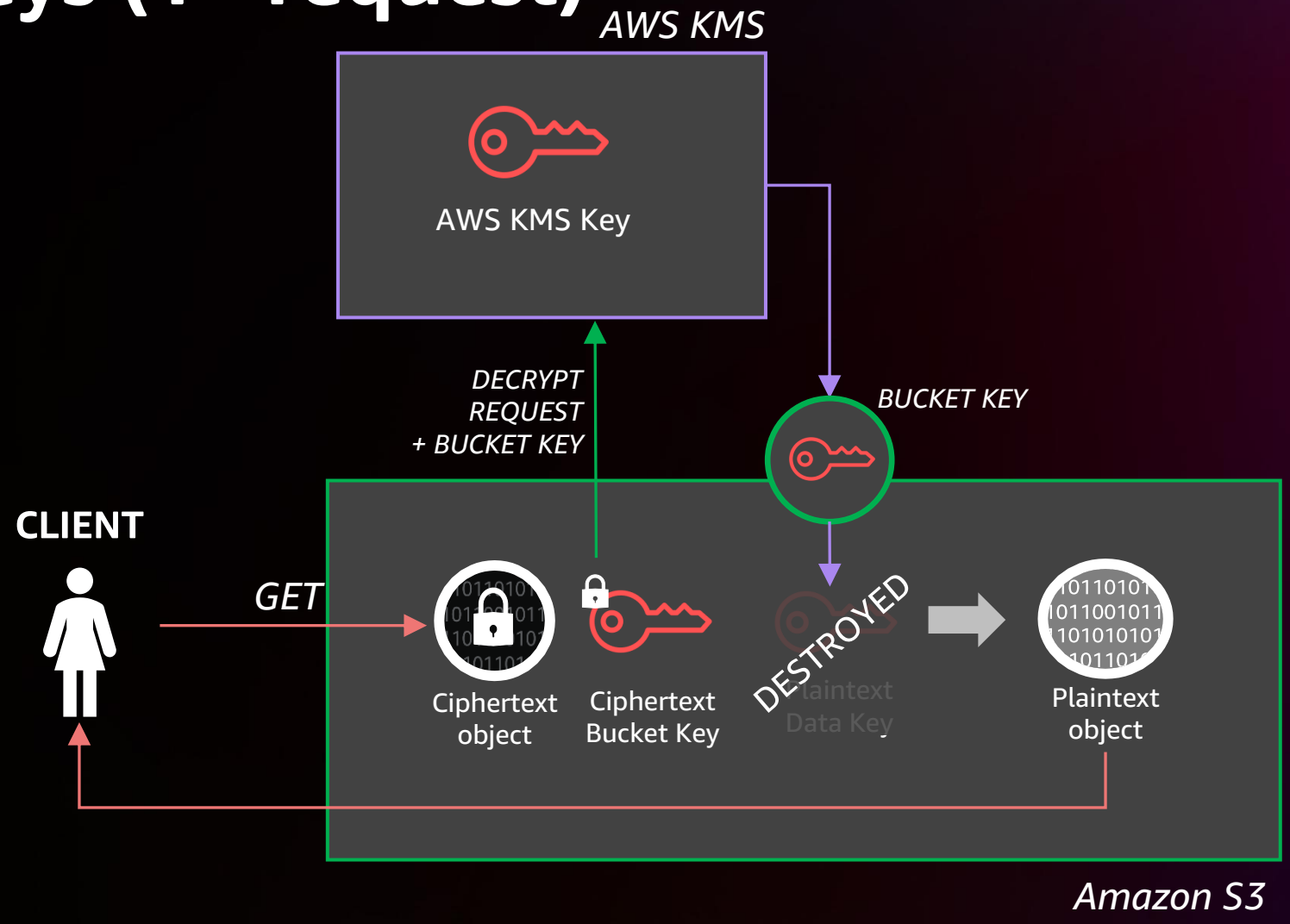

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How do Amazon S3 bucket keys work? (Nth request)



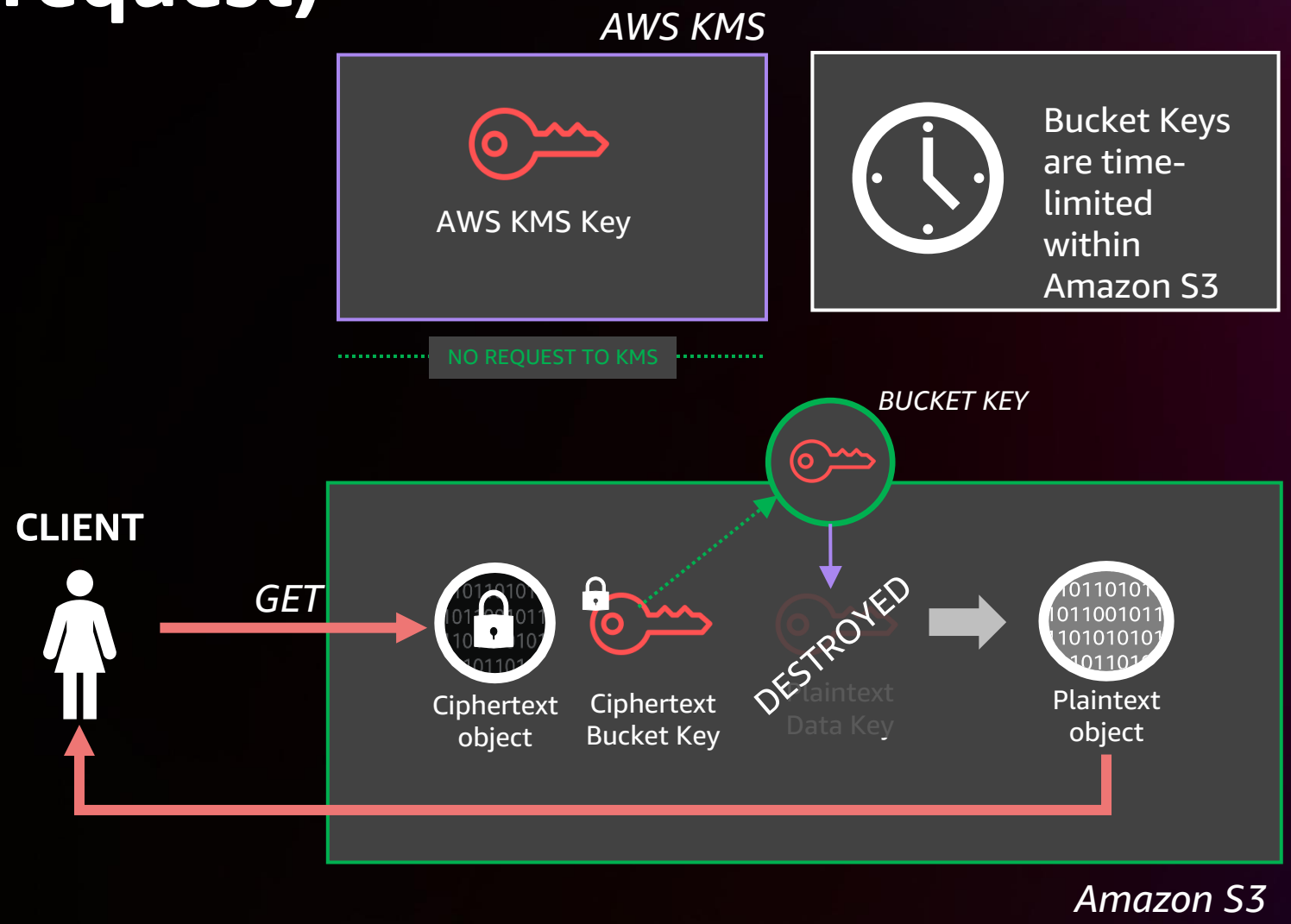

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How a decrypt request works with Amazon S3 bucket keys (1st request)




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How a decrypt request works with Amazon S3 bucket keys (N$^{th}$ request)




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Auditing encryption status

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon S3 Storage Lens

A storage analytics service that provides organization-wide visibility into storage usage and activity to improve cost efficiency and data protection



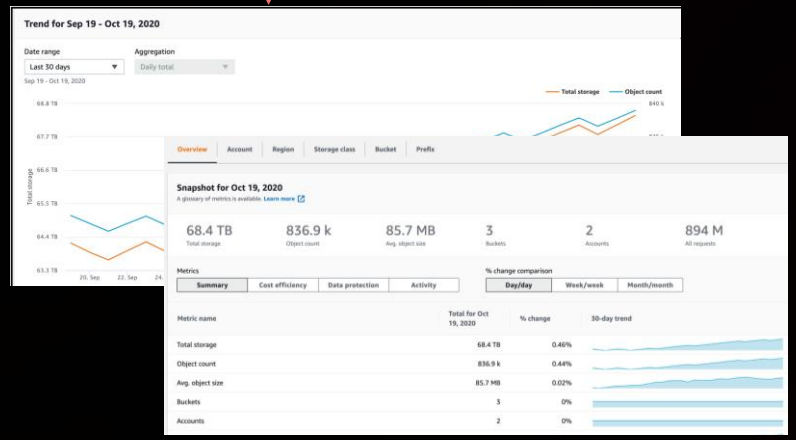
1. Interactive dashboard experience in the Amazon S3 console – free to all customers
2. Organization-wide visibility
3. Drill-down by Region, storage class, bucket, and prefix
4. Multiple ways to access Storage Lens data
5. Granular usage and activity metrics

aws

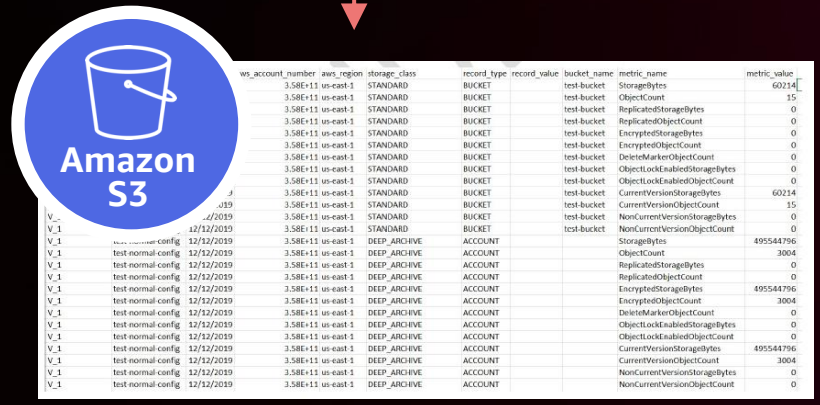
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Multiple ways to access Storage Lens data

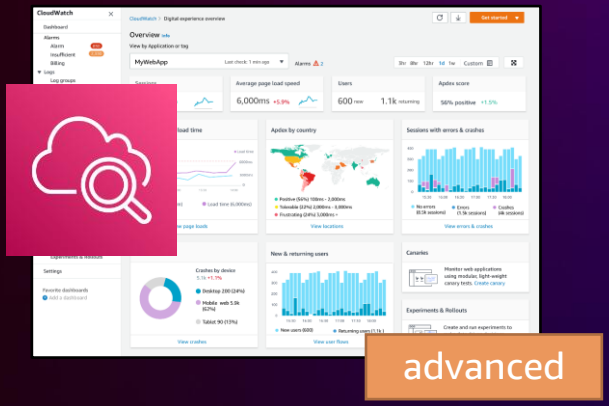
Amazon S3 Storage Lens




Integrated dashboard
(Amazon S3 Console)




Metrics export
(Daily to Amazon S3 bucket)




Amazon CloudWatch
(Dashboards, API)

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# “Which buckets have the highest number of unencrypted objects?”

**Buckets** (6)

You can view an export of data in this dashboard at your metrics export destination. A glossary of metrics is available. Learn more

Metrics categories

*Choose metrics categories*

Data protection ×

*Search buckets*

1

| Bucket name | Encrypted bytes | % encrypted bytes | Unencrypted bytes | % unencrypted bytes | ıcrypted bytes |
|---|---|---|---|---|---|
| development-us-w 610229646266 | - | - | 1.5 TB | 100.00% | 100.00% |
| data-lake-us-west-2-610229646266 | 139.7 GB | 100.00% | - | - | - |
| secondary-us-west-2-610229646266 | 46.6 GB | 100.00% | - | - | - |
| production-us-west-2-610229646266 | 931.3 GB | 100.00% | - | - | - |
| archive-us-west-2-610229646266 | 465.7 GB | 100.00% | - | - | - |
| ingest-us-west-2-610229646266 | 46.6 GB | 100.00% | - | - | - |

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# “How can I identify discrepancies in encryption configuration?”

**Buckets** (30)

You can view an export of data in this dashboard by configuring a metrics export. A glossary of metrics is available. Learn more

Metrics categories

*Choose metrics categories*

Data protection

*Search buckets*

1 2 3

| Bucket name | Encrypted bytes | Encrypted object count | Unencrypted bytes | Unencrypted object count | SSE-KMS enabled bucket count | All SSE-KMS requests |
|---|---|---|---|---|---|---|
| demo-2022-5 | 16.0 GB | 9 | - | - | - | - |
| demo-2022-6 | 45.7 GB | 119 | - | - | - | - |
| demo-2022-7 | 183.2 GB | 102 | - | - | - | - |
| gameday-test-delegateadmin | 2.5 GB | 4.4 k | - | - | - | 2 |
| gameday-test-orgowner | 935.4 MB | 4.4 k | 91.9 MB | 1.4 k | - | 2 |
| lenz-prod-verification-af-south-1 | - | - | 9.0 MB | 34 | - | - |
| lenz-prod-verification-ap-northeast-1 | - | - | 9.0 MB | 34 | - | - |
| lenz-prod-verification-ap-northeast-2 | - | - | 9.0 MB | 34 | - | - |
| lenz-prod-verification-ap-south-1 | - | - | 9.0 MB | 34 | - | - |
| lenz-prod-verification-ap-southeast-1 | - | - | 9.0 MB | 34 | - | - |

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice 3:
# Writing good IAM policies for S3

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Access control fundamentals: IAM, bucket policy, and access control list

**AWS Identity and Access Management (IAM)**

**Amazon S3**

**Identity**



✓ **IAM policy**

**Bucket**



`mybucket.s3.amazonaws.com`

✓ **Bucket policy**

**Object**



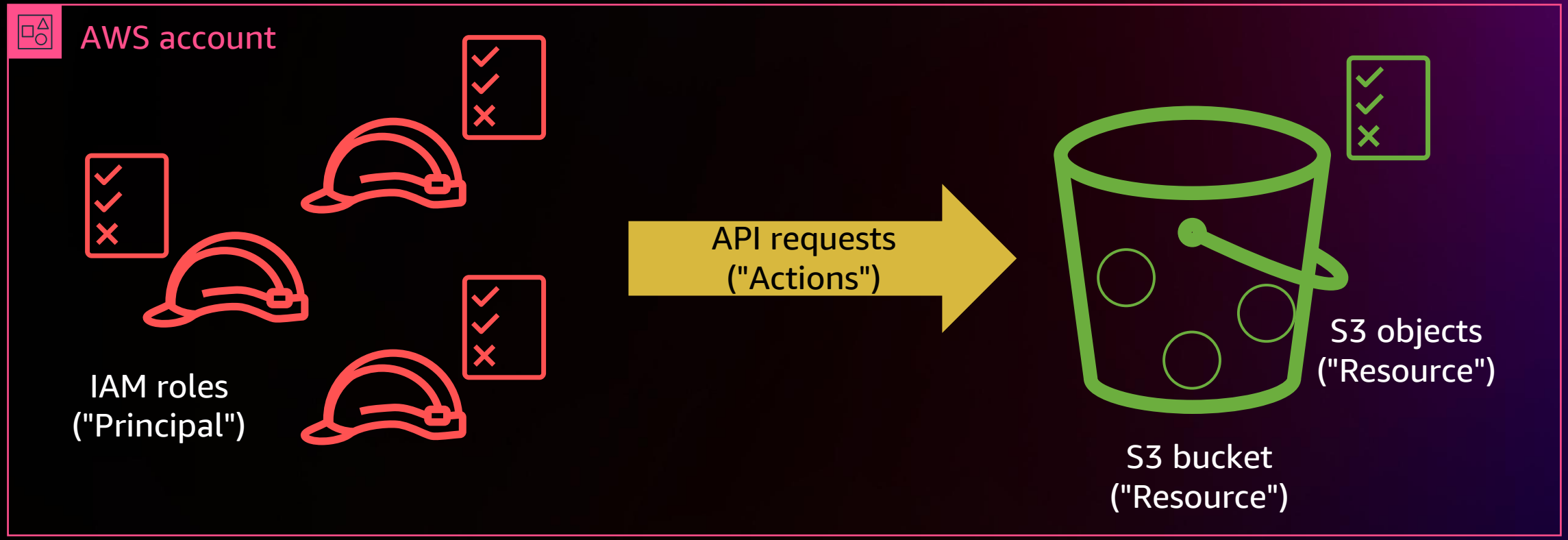
```
folder1/
| subfolder1/
| | file1.txt
| | file2.txt
```

**Access control list (bucket & object)**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Identity and Access Management (IAM): Modern permissions management for S3 (and all other AWS services)




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# IAM policy

**What actions** can this IAM user perform?

**An IAM policy that allows an IAM user to read and write to the bucket “reinvent-sample-bucket”**

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource": "arn:aws:s3:::/reinvent-sample-bucket/*"
      }
   ]
}
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# IAM policy example

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource": "arn:aws:s3:::/reinvent-sample-bucket/*"
      }
   ]
}
```

**Effect** – Specifies whether the policy results in a deny or allow

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# IAM policy example

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource": "arn:aws:s3:::/reinvent-sample-bucket/*"
      }
   ]
}
```



**Action** – Specifies the action that is denied or allowed

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# IAM policy example

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource": "arn:aws:s3:::/reinvent-sample-bucket/*"
      }
   ]
}
```

**Resource** – Specifies which AWS resource the action applies to



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Mapping action to resource

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:ListBucket"
         ],
         "Resource": "arn:aws:s3:::/reinvent-sample-bucket/*"
         "Resource": "arn:aws:s3:::/reinvent-sample-bucket"
      }
   ]
}
```

Action for listing bucket contents

Bucket resource

An action on a bucket requires a bucket resource

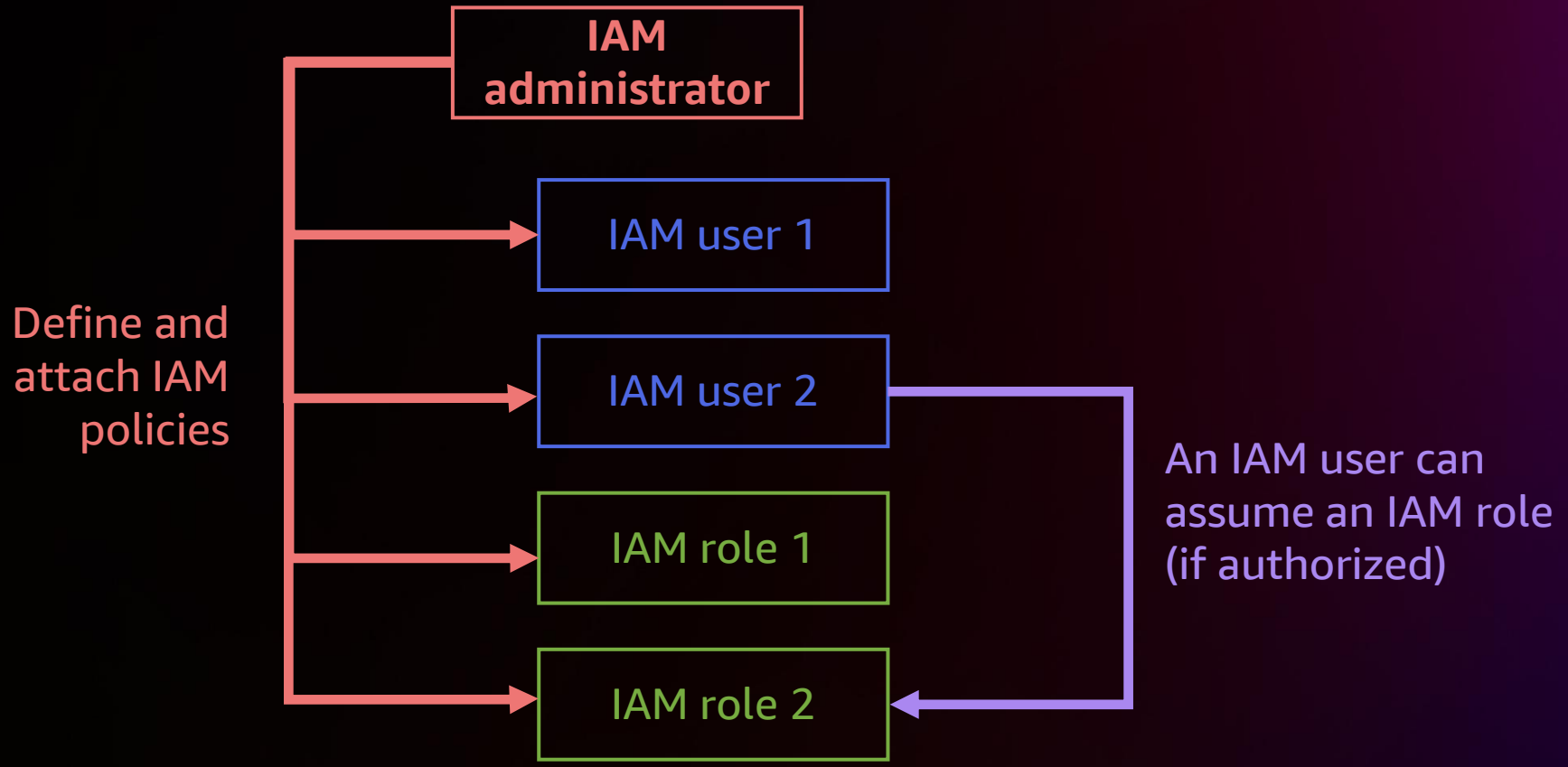


**Bookmark the IAM documentation for S3**
https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazons3.html

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Who can apply IAM policies?

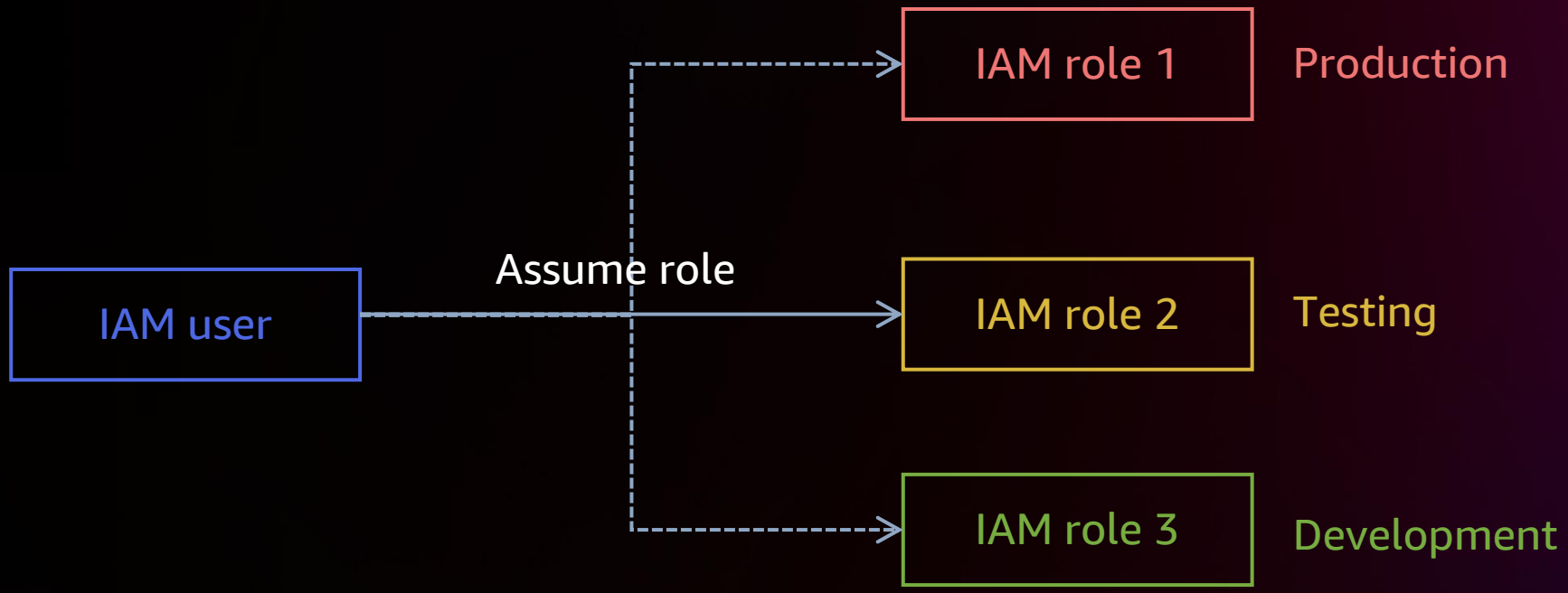
An IAM administrator attaches an IAM policy to each IAM user or role




aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# IAM role assumption

Use role assumption when handling multiple environments with different permissions




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# What's needed for role assumption?

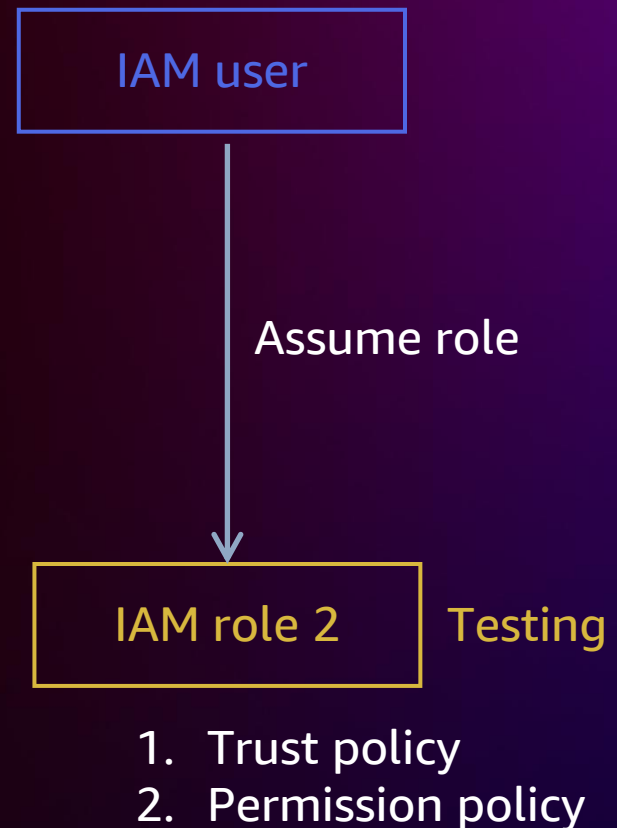
1. Trust policy (attached to the IAM role)

```
{ "Version": "2012-10-17",
  "Statement": {
        "Effect": "Allow",
        "Principal": { "AWS": "arn:aws:iam::
111122223333:user/user1" },
        "Action": "sts:AssumeRole"  } }
```

2. Permission policy (attached to the IAM role)

```
{ "Version": "2012-10-17",
  "Statement": {
        "Effect": "Allow",
        "Action": [ "s3:PutObject", "s3:GetObject" ],
        "Resource": "arn:aws:s3:::/reinvent-sample-bucket/*"  } }
```

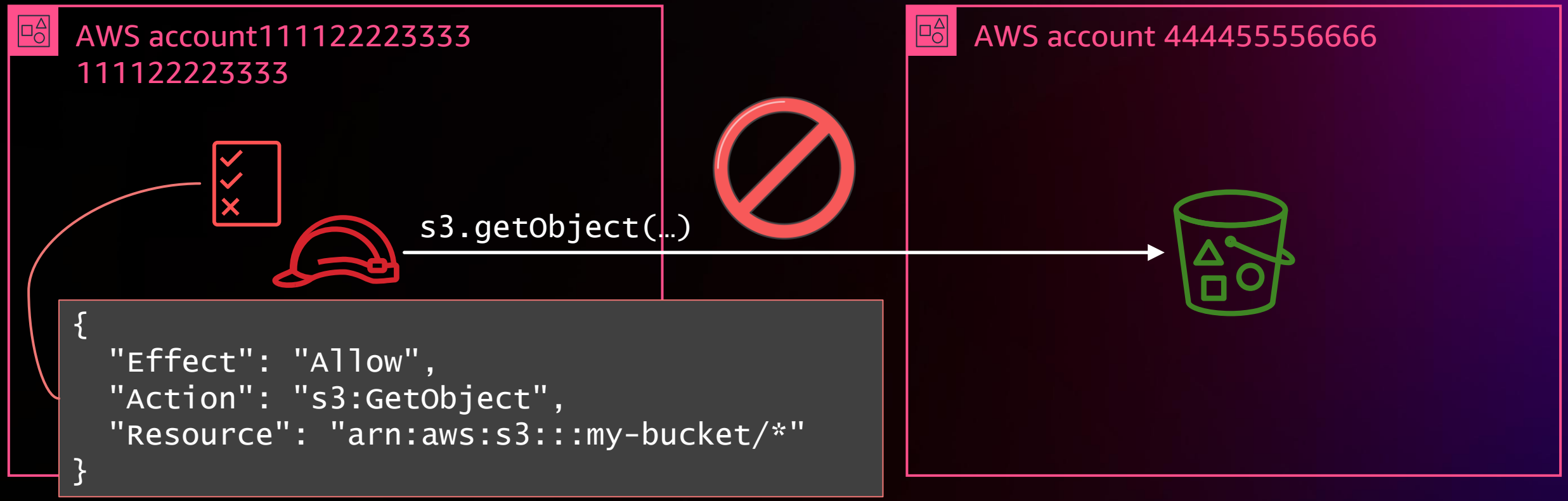
Diagram




1. Trust policy
2. Permission policy

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Sharing data in S3 across AWS accounts




Question: What happens here?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Access control fundamentals: IAM and bucket policies

AWS Identity and Access Management (IAM)

Identity



IAM policy

Amazon S3

Bucket



Bucket policy

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Bucket policy

## Who can access the contents of my S3 bucket?

**A bucket policy that allows a principal (AWS account ID 1111111111) to read and write to the bucket “reinvent-sample-bucket”**

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource": "arn:aws:s3:::/reinvent-sample-bucket/*“,
         ”Principal”: {"AWS":"111122223333"}
      }
   ]
}
```

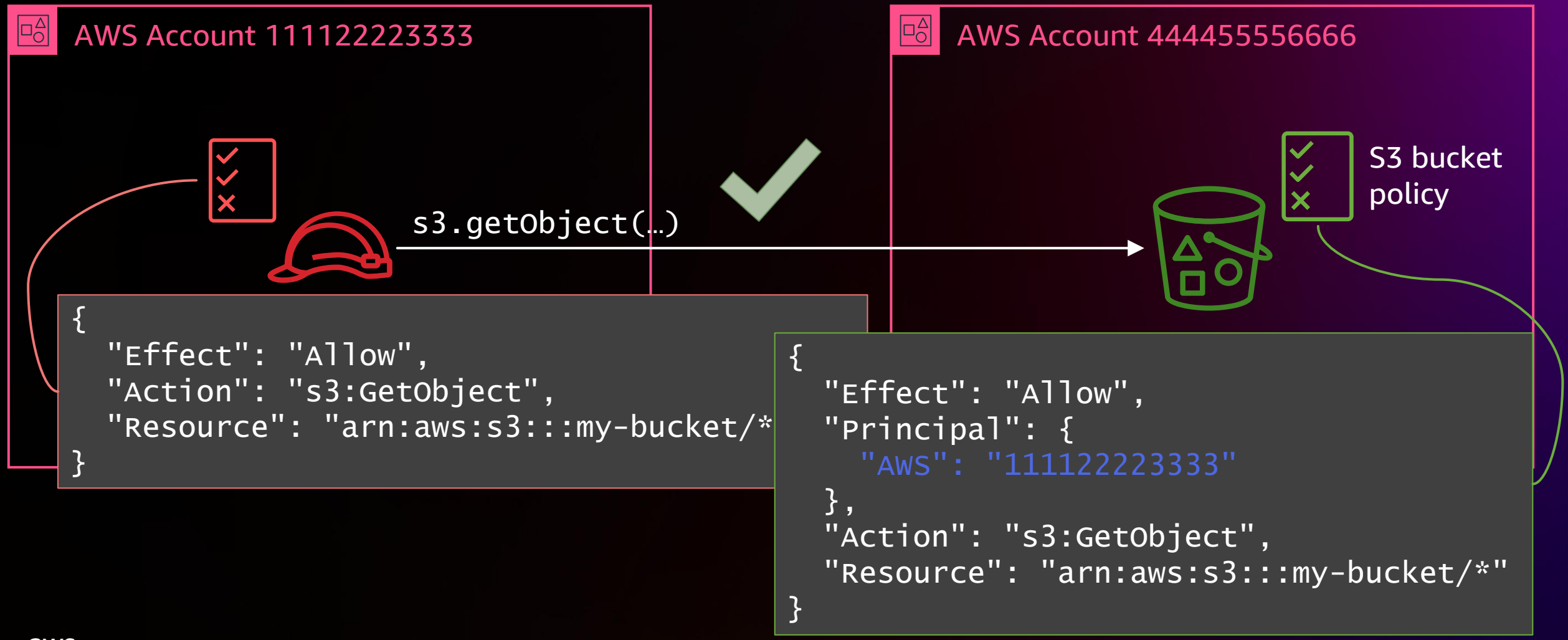
**Same syntax as an IAM policy but adds a principal statement**

**Principal** – Specifies who the statement covers

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Sharing data in S3 across AWS accounts




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice 3 (continued): Using a policy to create a perimeter

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Adding granularity with condition keys

You can add a condition statement to an IAM or bucket policy

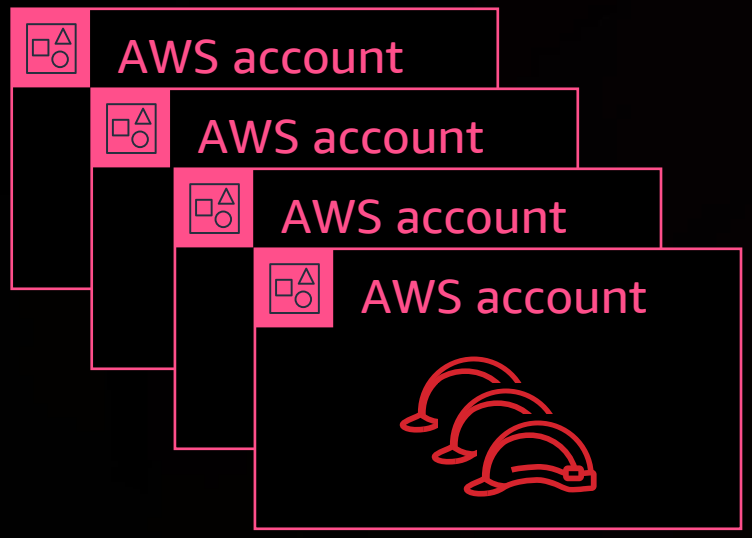
**A bucket policy that limits access to objects that have the “ReInvent” tag**

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
        "Effect":”Allow",
        "Action":[
           "s3:PutObject",
           "s3:GetObject"
       ],
       "Resource":"arn:aws:s3:::/reinvent-sample-bucket/*”,
        ”Principal”:{"AWS":"111111111111"},
        "Condition": {
                "StringEquals":{"s3:ExistingObjectTag/Project":”ReInvent"}
        }
       }
  ]
}
```



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Who needs access to your data?




Your own accounts in your organization





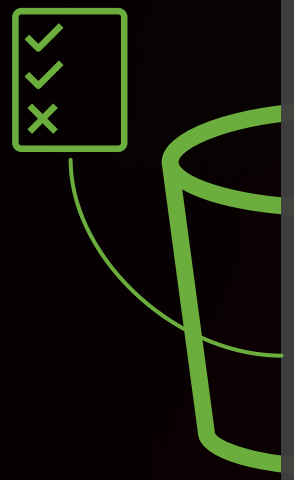
AWS services that read and write your data

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Using a policy to assert expected callers



```
{
  "Sid": "AssertExpectedCallers",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": [
    "arn:aws:s3:::example-bucket",
    "arn:aws:s3:::example-bucket/*"
  ],
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:PrincipalOrgId": "o-a1b2"
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false"
    }
  }
}
// Plus other statements to grant access…
```

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Using a policy to assert expected callers



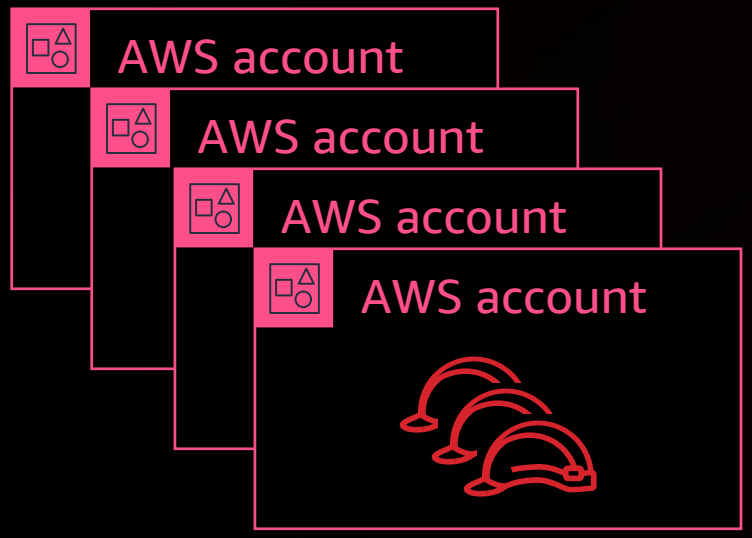


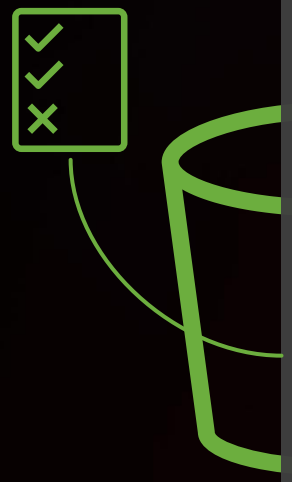

Caller is not from my organization, AND…

```
{
  "Sid": "AssertExpectedCallers",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": [
    "arn:aws:s3:::example-bucket",
    "arn:aws:s3:::example-bucket/*"
  ],
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:PrincipalOrgId": "o-a1b2"
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false"
    }
  }
}
// Plus other statements to grant access…
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Using a policy to assert expected callers



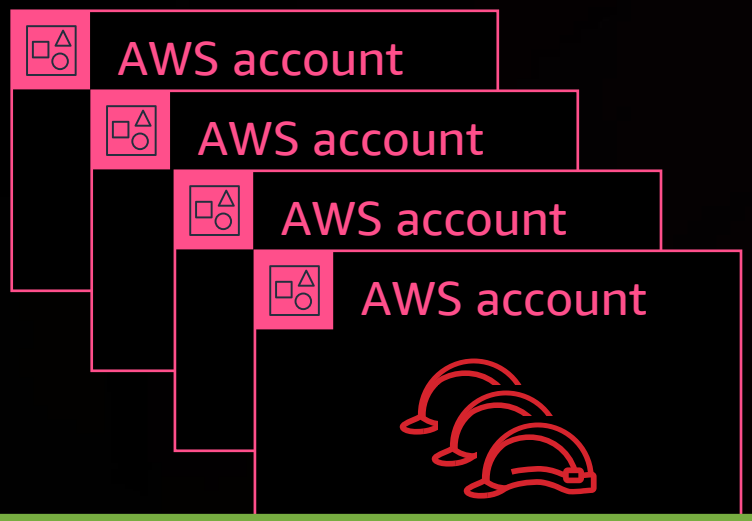



…Caller is not an AWS service

```
{
  "Sid": "AssertExpectedCallers",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": [
    "arn:aws:s3:::example-bucket",
    "arn:aws:s3:::example-bucket/*"
  ],
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:PrincipalOrgId": "o-a1b2"
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false"
    }
  }
}
// Plus other statements to grant access…
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Using a policy to assert expected callers






Caller is not from my organization, AND…

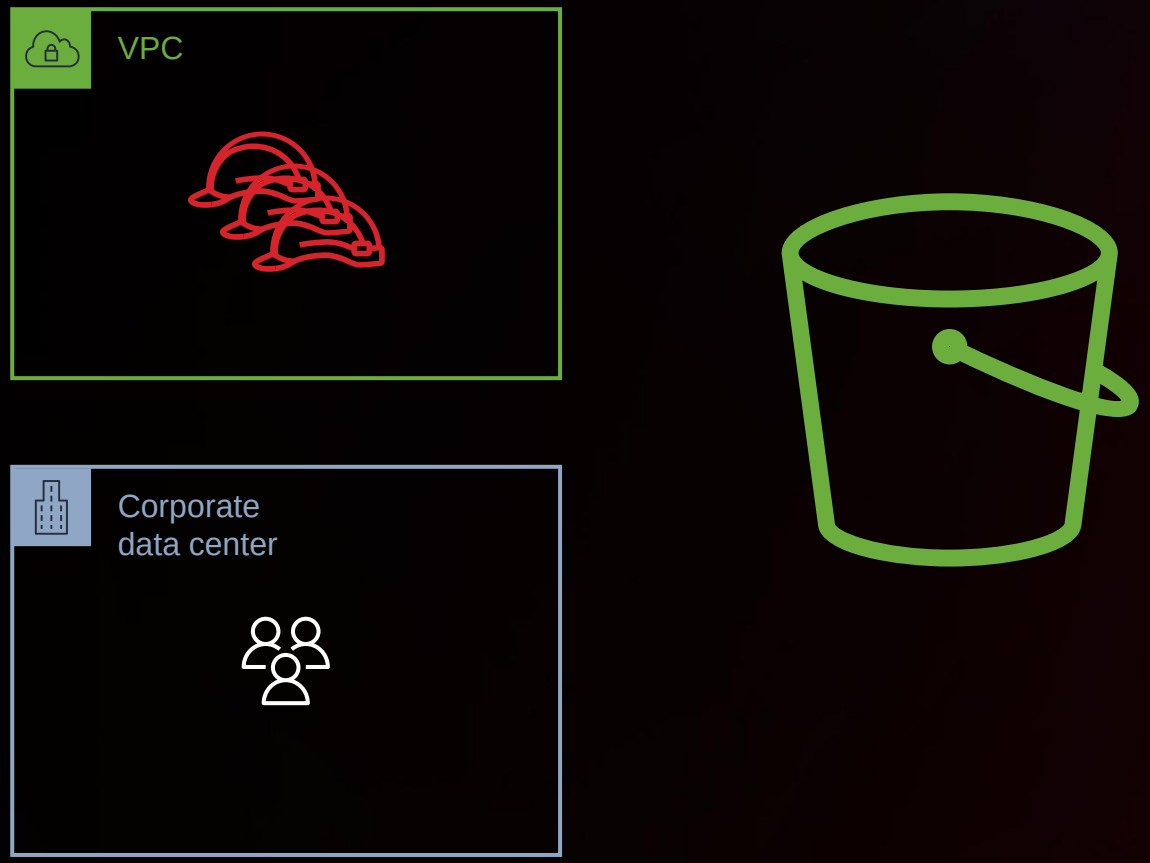
…Caller is not an AWS service

➔ Always block the access ("Deny")

```
{
  "Sid": "AssertExpectedCallers",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": [
    "arn:aws:s3:::example-bucket",
    "arn:aws:s3:::example-bucket/*"
  ],
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:PrincipalOrgId": "o-a1b2"
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false"
    }
  }
}
```

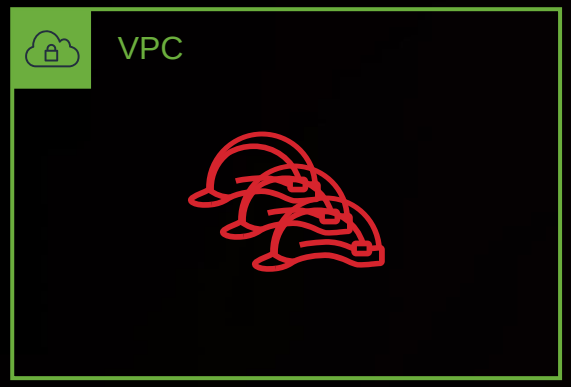
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

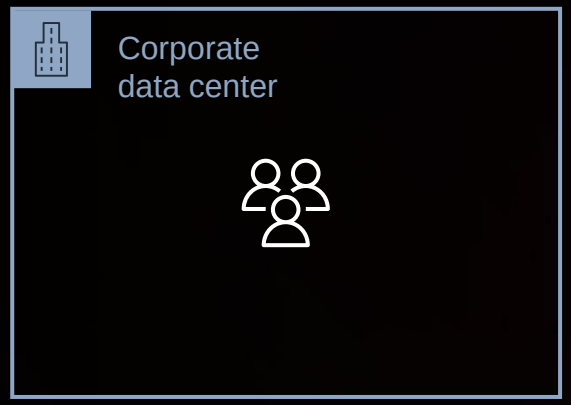
# Using policy to exclude unexpected networks




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Using policy to exclude unexpected networks



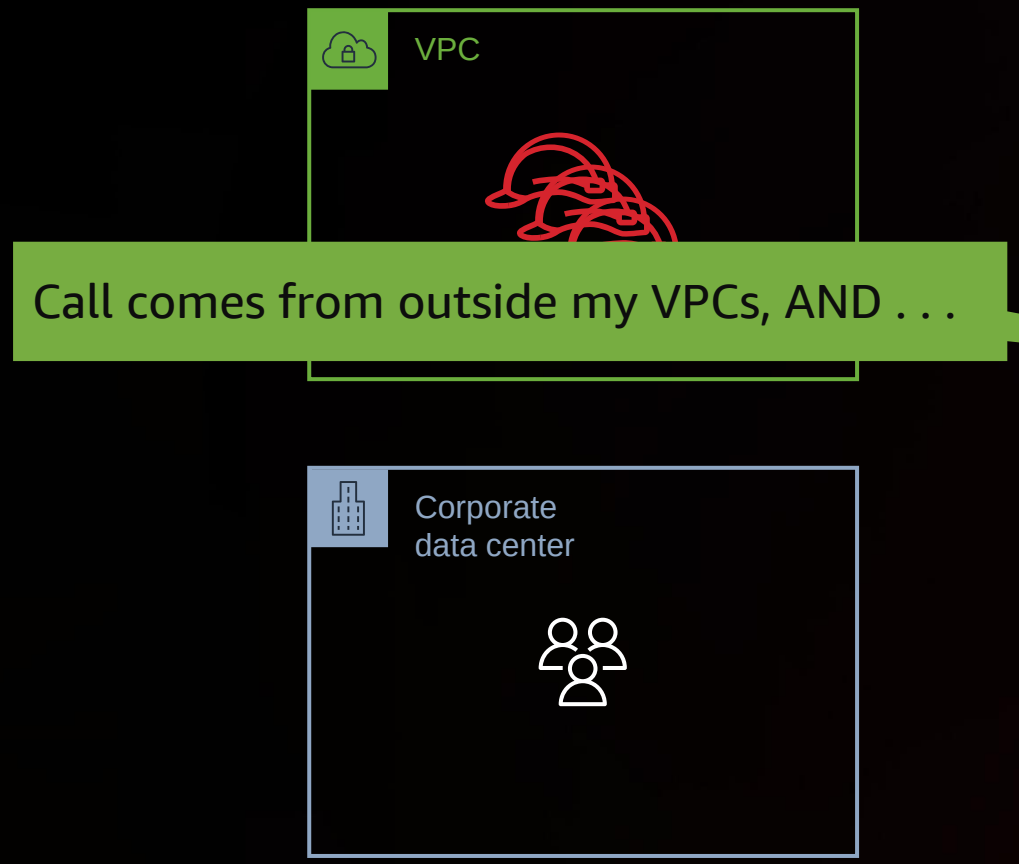



```
{
  "Sid": "AssertExpectedNetworks",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "arn:aws:s3:::example-bucket/*",
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:SourceVpc": "vpc-11112222"
    },
    "NotIpAddress": {
      "aws:SourceIp": $CORP_IP_RANGE
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false",
      "aws:ViaAwsService": "false"
    }
  }
}
// Plus other statements to grant access…
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

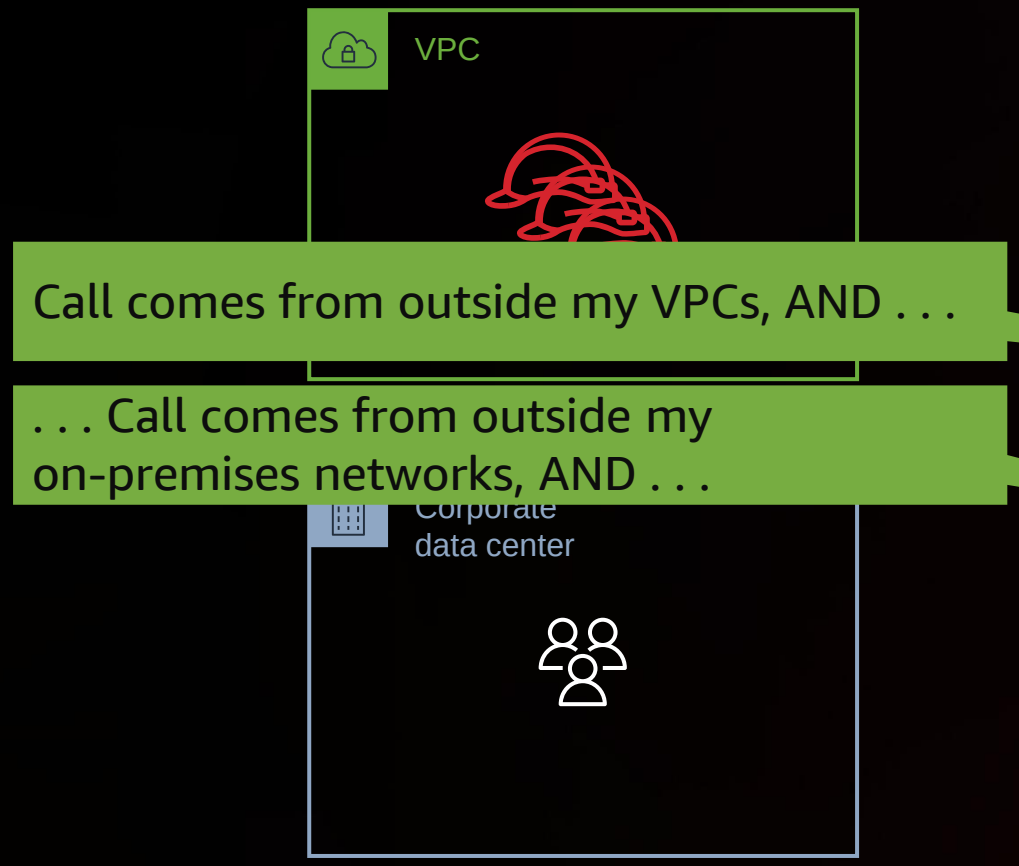
# Using policy to exclude unexpected networks




```
{
  "Sid": "AssertExpectedNetworks",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "arn:aws:s3:::example-bucket/*",
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:SourceVpc": "vpc-11112222"
    },
    "NotIpAddress": {
      "aws:SourceIp": $CORP_IP_RANGE
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false",
      "aws:ViaAwsService": "false"
    }
  }
}
// Plus other statements to grant access…
```

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

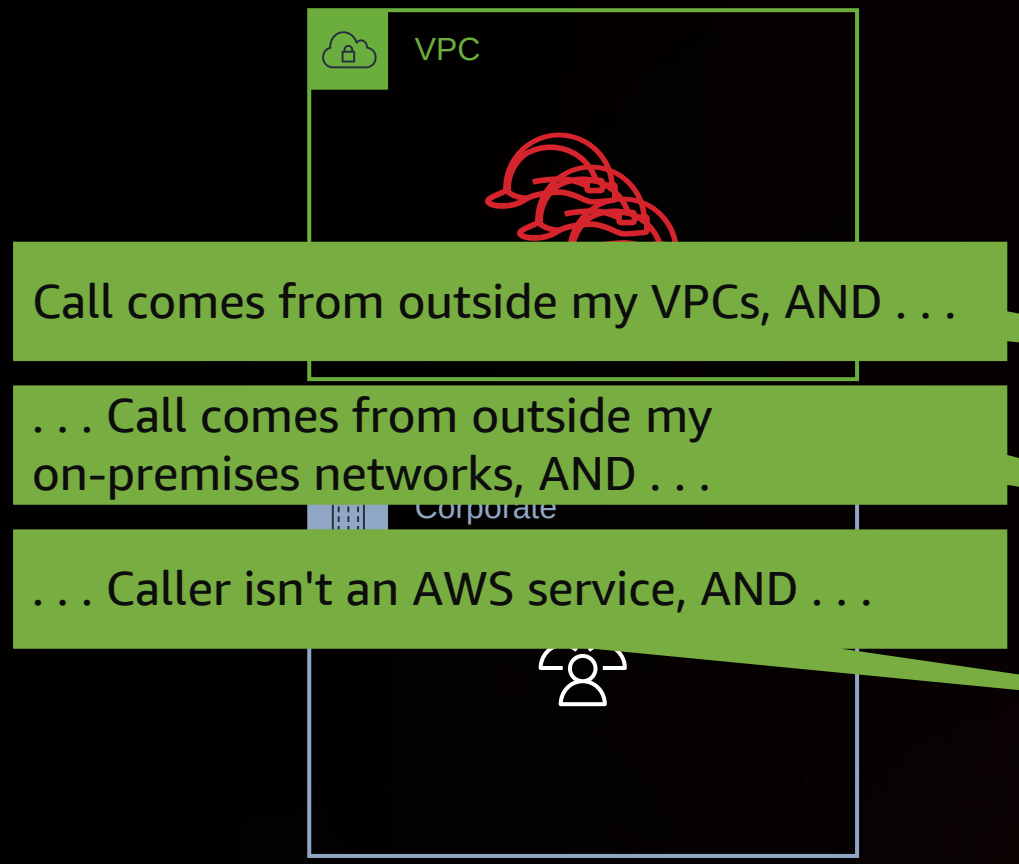
# Using policy to exclude unexpected networks




```
{
  "Sid": "AssertExpectedNetworks",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "arn:aws:s3:::example-bucket/*",
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:SourceVpc": "vpc-11112222"
    },
    "NotIpAddress": {
      "aws:SourceIp": $CORP_IP_RANGE
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false",
      "aws:ViaAwsService": "false"
    }
  }
}
// Plus other statements to grant access…
```

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

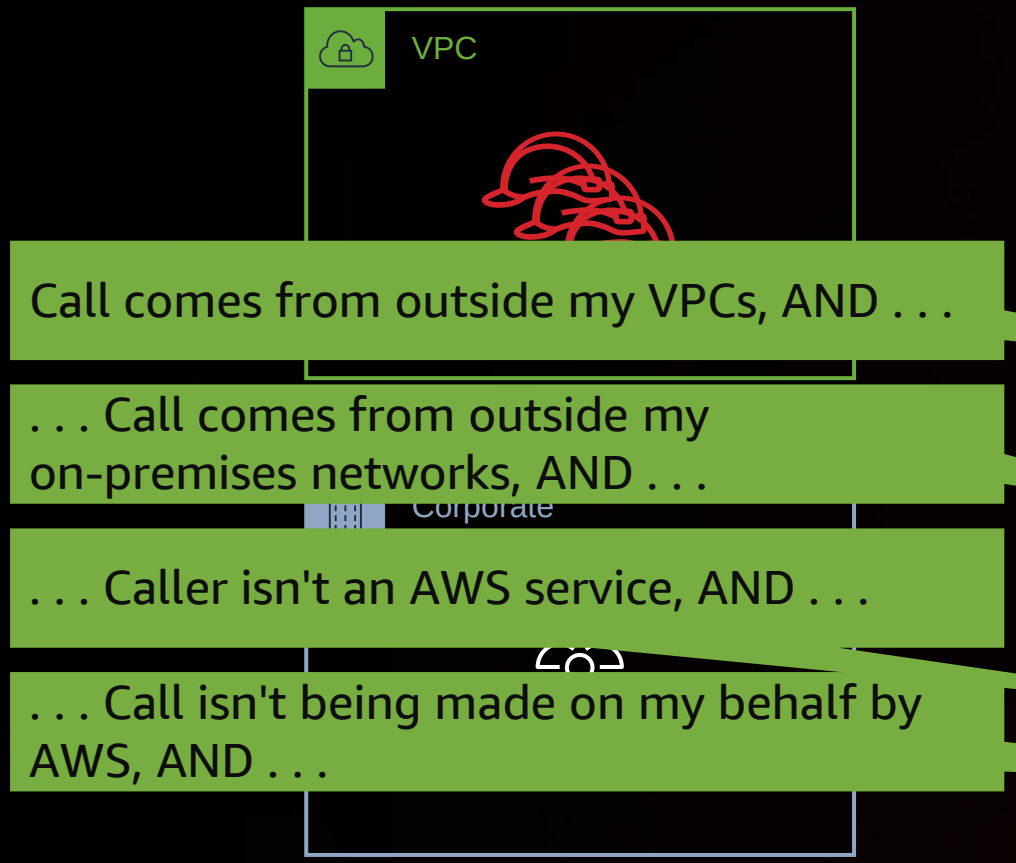
# Using policy to exclude unexpected networks




```
{
  "Sid": "AssertExpectedNetworks",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "arn:aws:s3:::example-bucket/*",
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:SourceVpc": "vpc-11112222"
    },
    "NotIpAddress": {
      "aws:SourceIp": $CORP_IP_RANGE
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false",
      "aws:ViaAwsService": "false"
    }
  }
}
// Plus other statements to grant access…
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

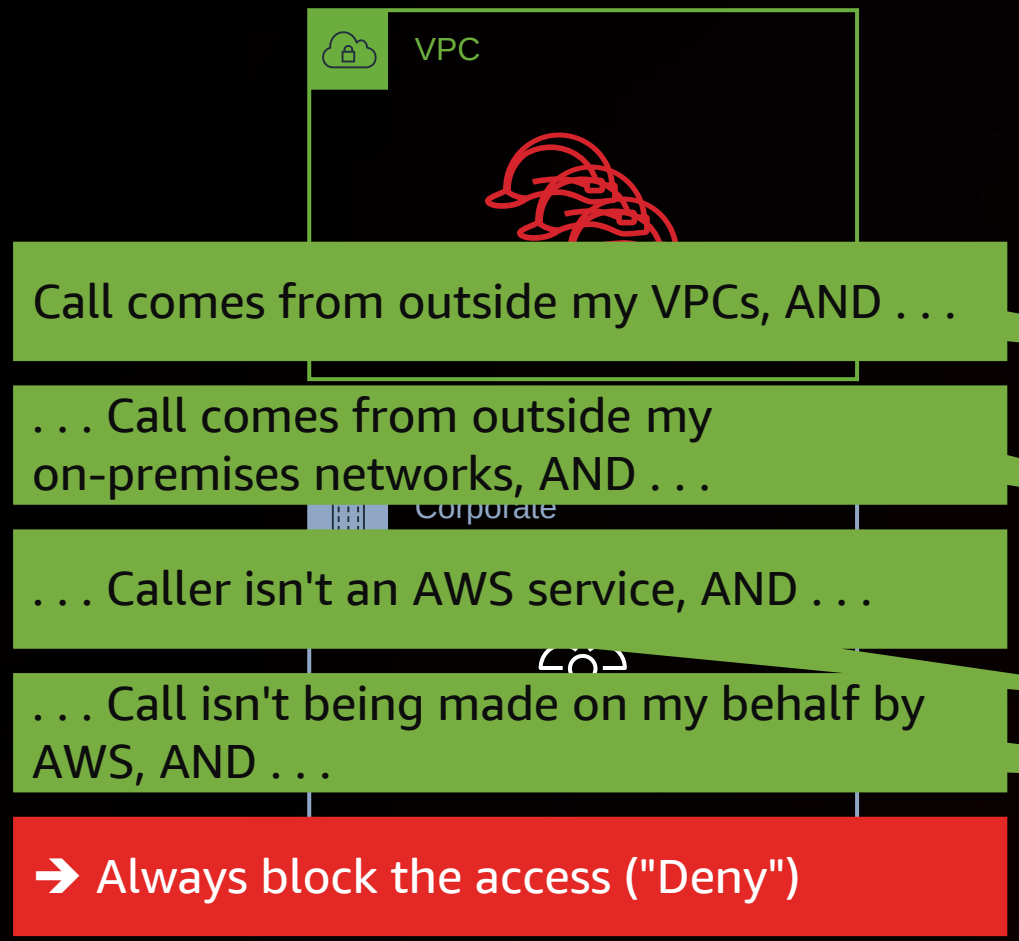
# Using policy to exclude unexpected networks




```
{
  "Sid": "AssertExpectedNetworks",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "arn:aws:s3:::example-bucket/*",
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:SourceVpc": "vpc-11112222"
    },
    "NotIpAddress": {
      "aws:SourceIp": $CORP_IP_RANGE
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false",
      "aws:ViaAwsService": "false"
    }
  }
}
// Plus other statements to grant access…
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Using policy to exclude unexpected networks




```
{
  "Sid": "AssertExpectedNetworks",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "arn:aws:s3:::example-bucket/*",
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:SourceVpc": "vpc-11112222"
    },
    "NotIpAddress": {
      "aws:SourceIp": $CORP_IP_RANGE
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false",
      "aws:ViaAwsService": "false"
    }
  }
}
// Plus other statements to grant access…
```

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# You have many condition keys to work with

## A condition key for virtually every occasion:

s3:object-lock-legal-hold
s3:object-lock-mode
s3:object-lock-remaining-retention-days
s3:AccessPointNetworkOrigin
s3:object-lock-retain-until-date
s3:DataAccessPointAccount
s3:prefix
s3:DataAccessPointArn
s3:signatureAge
s3:ExistingJobOperation
s3:signatureversion
s3:ExistingJobPriority
s3:versionid
s3:locationconstraint
s3:max-keys
s3:x-amz-website-redirect-location
s3:ExistingObjectTag/<key>
s3:x-amz-acl
s3:JobSuspendedCause
s3:x-amz-content-sha256

s3:LocationConstraint
s3:x-amz-copy-source
s3:RequestJobOperation
s3:x-amz-grant-full-control
s3:RequestJobPriority
s3:x-amz-grant-read
s3:RequestObjectTag/<key>
s3:x-amz-grant-read-acp
s3:RequestObjectTagKeys
s3:x-amz-grant-write
s3:VersionId
s3:x-amz-grant-write-acp
s3:authType
s3:x-amz-metadata-directive
s3:x-amz-server-side-encryption-aws-kms-key-id
s3:x-amz-storage-class

aws:CalledVia
aws:CurrentTime
aws:FederatedProvider
aws:PrincipalAccount
aws:PrincipalArn
aws:PrincipalIsAWSService
aws:PrincipalOrgID
aws:PrincipalOrgPaths
aws:PrincipalServiceName
aws:PrincipalServiceNamesList
aws:PrincipalTag/*tag-key*
aws:PrincipalType
aws:ResourceOrgID
aws:ResourceTag/*tag-key*
aws:SourceIdentity
aws:UserAgent
aws:userid
aws:ViaAWSService
aws:VpcSourceIp

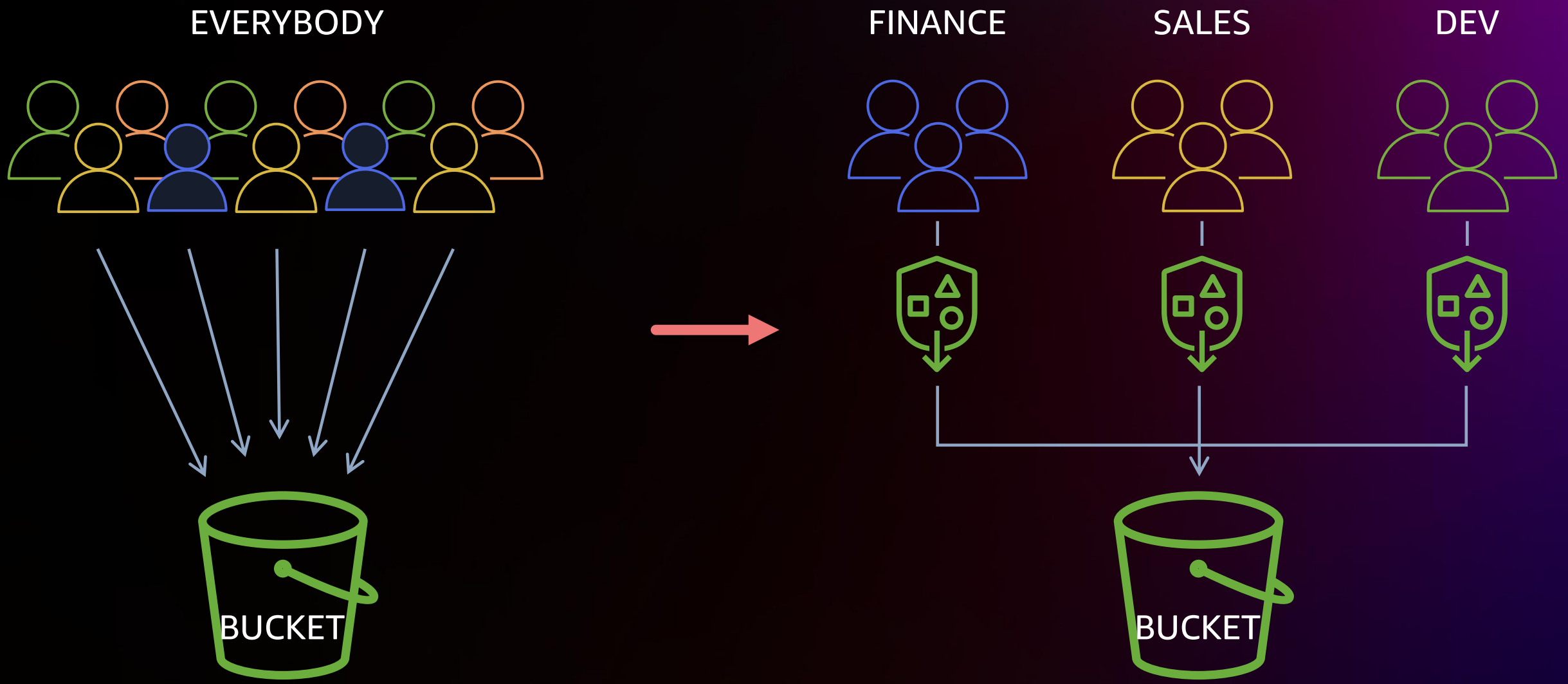
**For detailed descriptions and non-tiny text:**

https://docs.aws.amazon.com/IAM/latest/UserGuide/list_amazons3.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

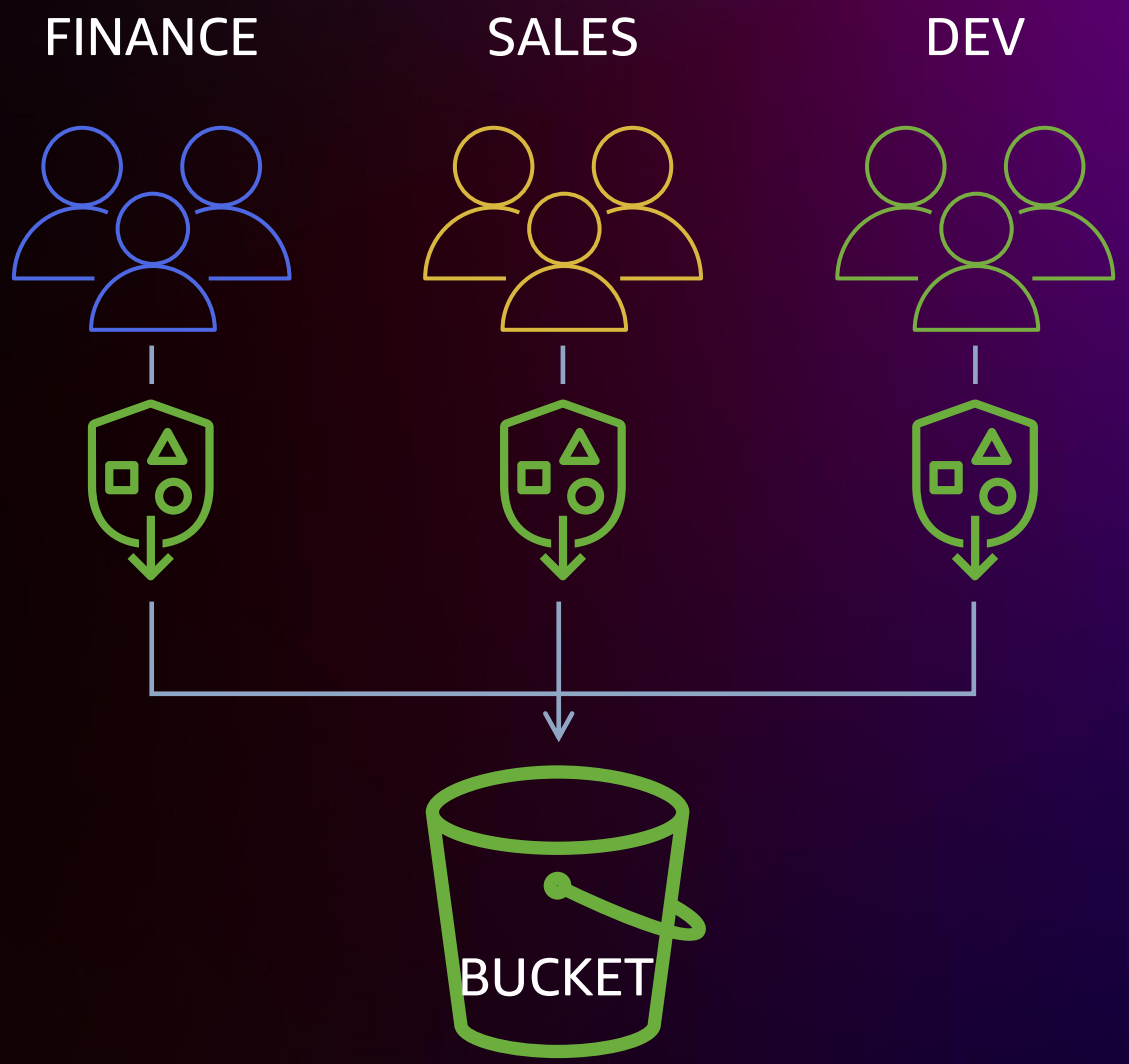
# Amazon S3 access points




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon S3 access points

1. Simplify access management for **shared buckets**
2. One permission policy per access point – break down your large bucket policy
3. Restrict end users to specific prefixes
4. Restrict traffic to **specific VPCs**

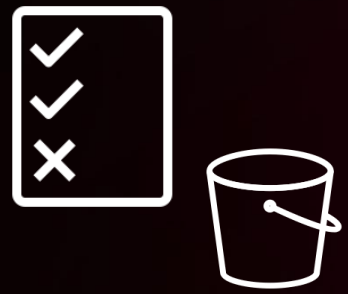



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice 4: Disable ACLs

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Multiple mechanisms for access management

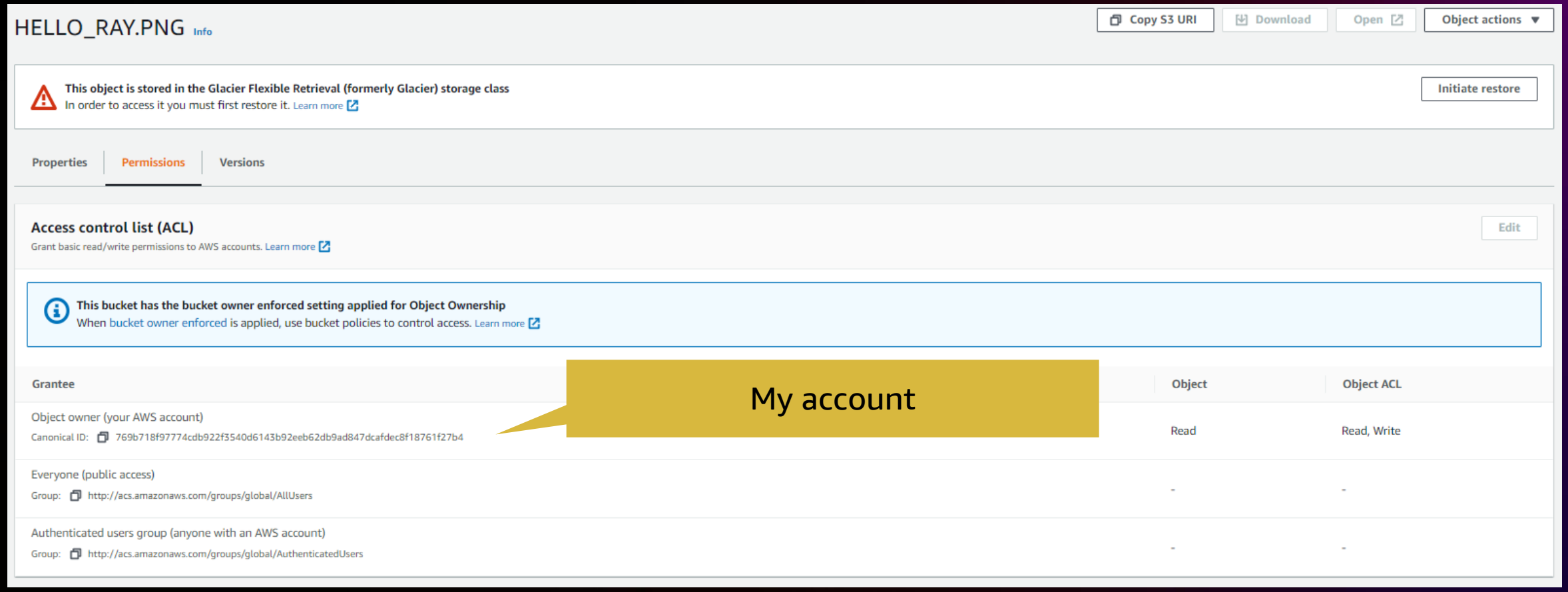
| | AWS Identity and Access Management (IAM) | Amazon S3 | Amazon S3 |
|---|---|---|---|
| |  |  |  |
| | IAM policy | Bucket policy | Access control list |
| Applies to | IAM identity | S3 bucket | S3 bucket<br>S3 object |

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Access control list (ACL)

An ACL is a list of permissions that specify which users or groups of users are granted access to your S3 object or bucket; it predates IAM

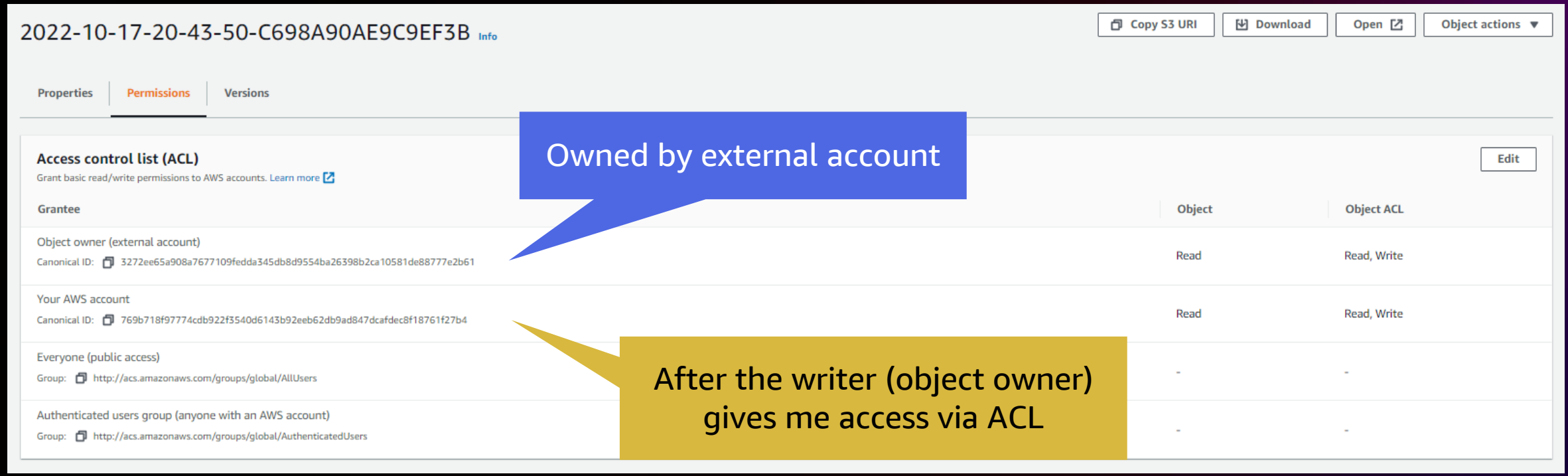



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Access control lists for cross-account write

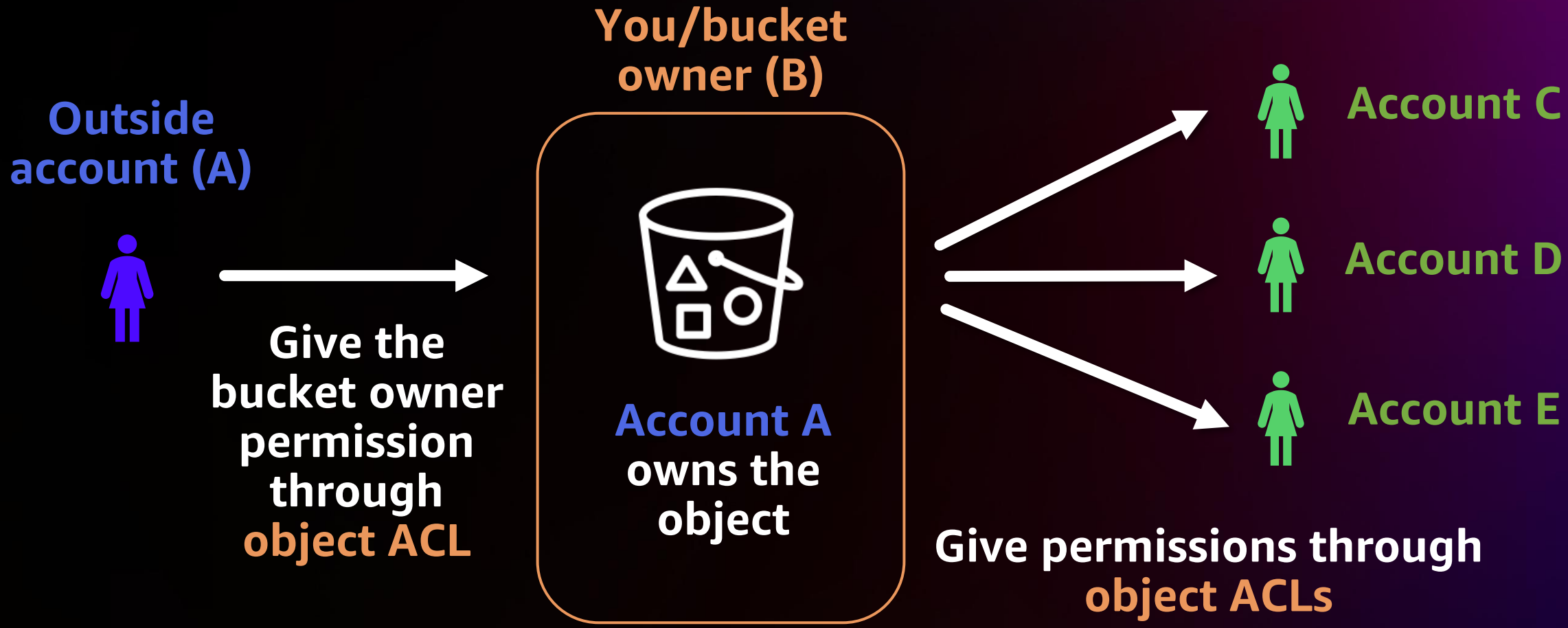
When an external account writes an object to your bucket

- That account owns the object
- That account gives you access to the object via ACL




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How cross-account write is done today (when ACLs are enabled)



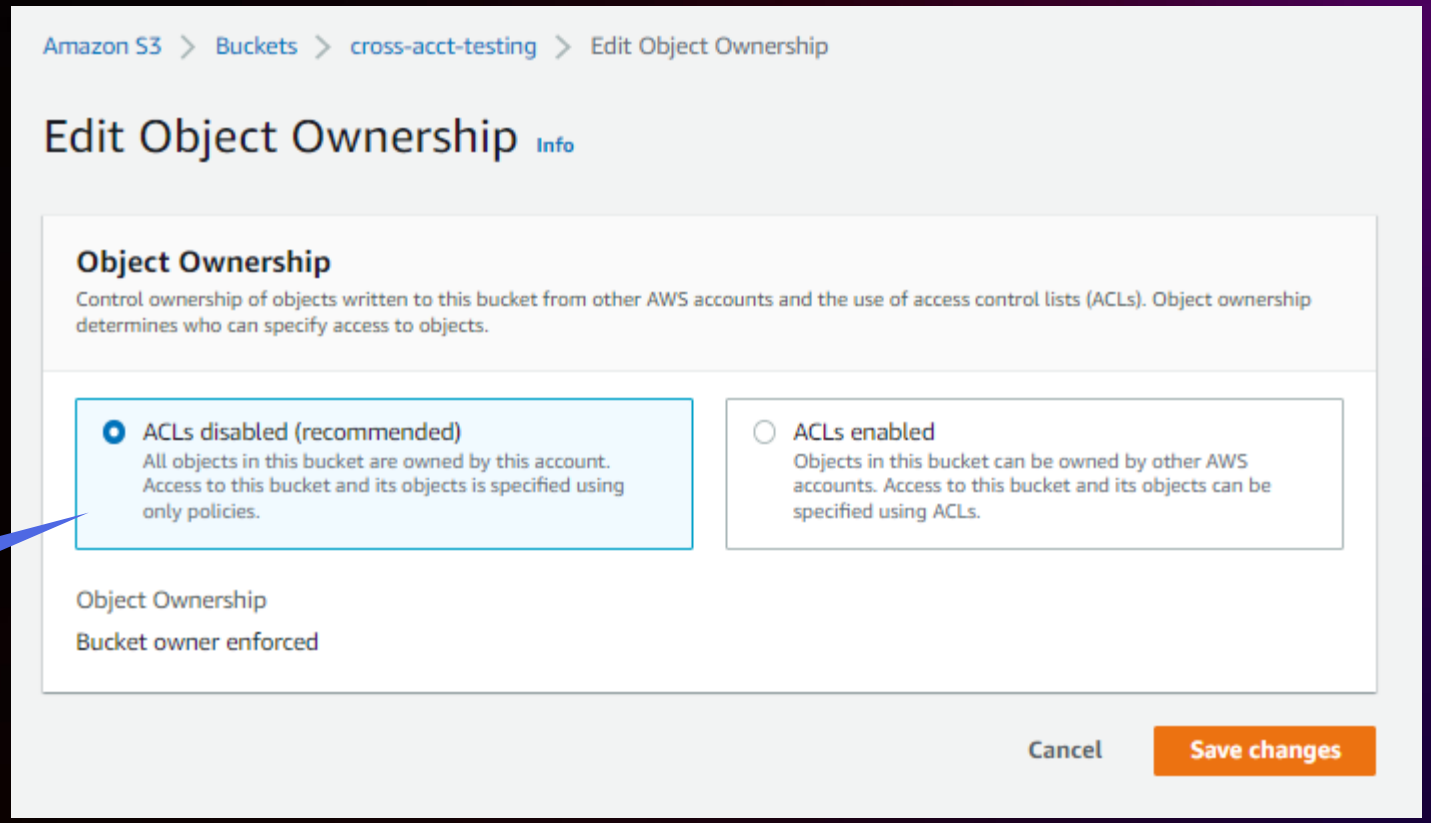

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# You can now disable ACLs

You can now use S3 Object Ownership to disable ACLs for your bucket and all the objects in the bucket (recommended)

- ACLs are disabled
- All objects are now owned by you (the bucket owner)
- Bucket policy applies to all objects in your bucket

**Recommended best practice**




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon S3 server access log and AWS CloudTrail adds ACL usage information

`aclRequired` NEW

- A new field in Amazon S3 server access log and AWS CloudTrail event log
- Returns “Yes” if an Amazon S3 request requires an ACL for authorization
- Otherwise, returns “-” in Amazon S3 server access log or is not emitted in AWS CloudTrail

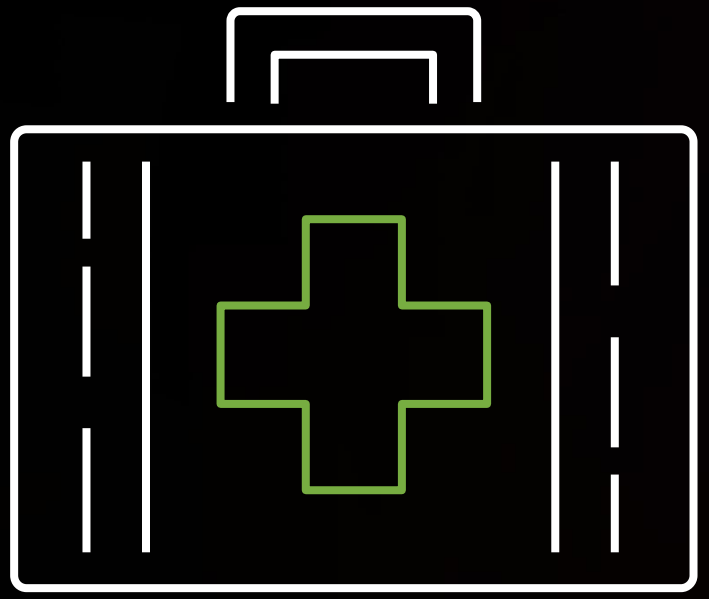
→ Gives usage-based data to migration ACL permissions to bucket policy

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice 5: Review permissions with IAM Access Analyzer and log requests with Amazon S3 server access log or AWS CloudTrail

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Review permissions to your bucket with IAM Access Analyzer



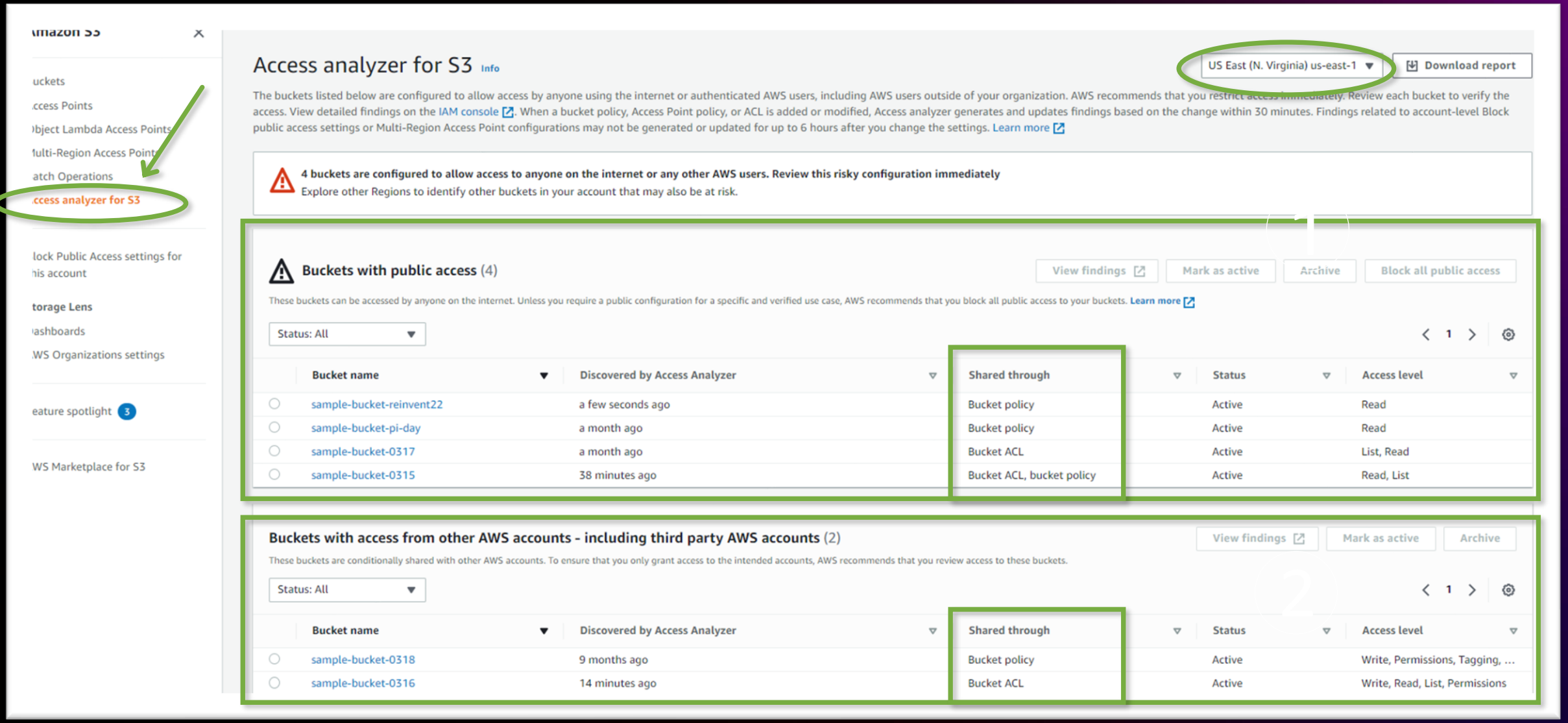
## Access Analyzer for S3

- Analyzes permissions for all buckets in an AWS Region
- A simple dashboard to show public buckets and buckets shared with external entities

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# IAM Access Analyzer for S3 example




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Starts with Amazon S3 server access log and AWS CloudTrail



## Amazon S3 server access log and AWS CloudTrail

- Detailed records for the requests made to your bucket
- Useful in security and access audits
- Ability to query and analyze requests

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Details in Amazon S3 server access log



| | | |
|---|---|---|
| Bucket Owner | Object Size | aclRequired NEW |
| Bucket | Total Time | |
| Time | Turn-Around Time | |
| Remote IP | Referer | |
| Requester | User-Agent | |
| Request ID | Version ID | |
| Operation | Signature Version | |
| Key | Cipher Suite | |
| Request-URI | Authentication Type | |
| HTTP status | Host Header | |
| Error Code | TLS version | |
| Bytes Sent | Access Point ARN | |

Documentation: https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerLogs.html

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practices recap

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice 1: Block public access



**Block public access**

Enable **Amazon S3 Block Public Access** at the account level

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice 2: Encryption



## Encryption

- Enable **default encryption** at the bucket level
- Turn on **Amazon S3 Bucket Keys** to reduce costs for your AWS KMS–encrypted objects

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice 3: Bucket policies



**Bucket policies**

Use deny statements to **define perimeters**, such as expected caller organization

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice 4: Disable ACLs



**Bucket owner enforced to disable ACLs**

Configure **bucket owner enforced** on your bucket's S3 Object Ownership setting to disable ACLs

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Best practice 5: IAM Access Analyzer and logging your requests



**IAM Access Analyzer**

Review findings in IAM Access Analyzer to confirm your intended permission settings



**Amazon S3 server access log and AWS CloudTrail**

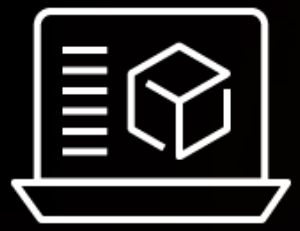
Retain detailed records for the requests made to your bucket

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Continue your AWS storage learning

## Build a learning plan



Set your AWS storage learning plans via **AWS Skill Builder**

## Increase your knowledge



Use **AWS Ramp-Up Guides** to build your storage knowledge

## Earn AWS storage badges




Demonstrate your knowledge by achieving **digital badges**

# aws.training/storage

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.