black hat
USA 2021

August 4-5, 2021

BRIEFINGS

Breaking the Isolation

Cross-Account AWS Vulnerabilities

Shir Tamari and Ami Luttwak

Wiz.io

Background:

The Wiz Research Team

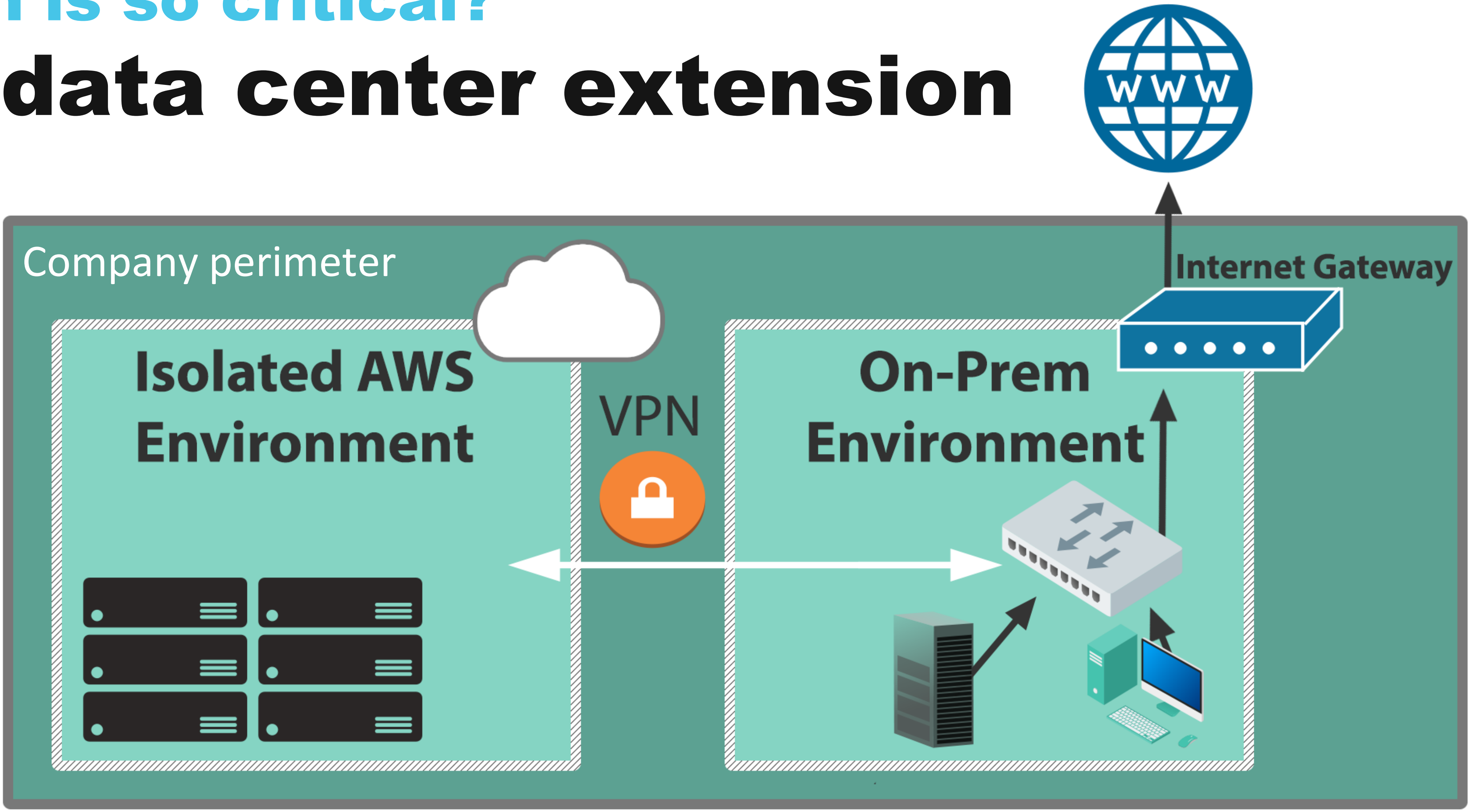
- Experienced security researchers
- Microsoft Cloud Security Group veterans
- Groundbreaking cloud security research to uncover new cloud vulnerabilities

Research question:

Can we break the isolation of AWS Environments?

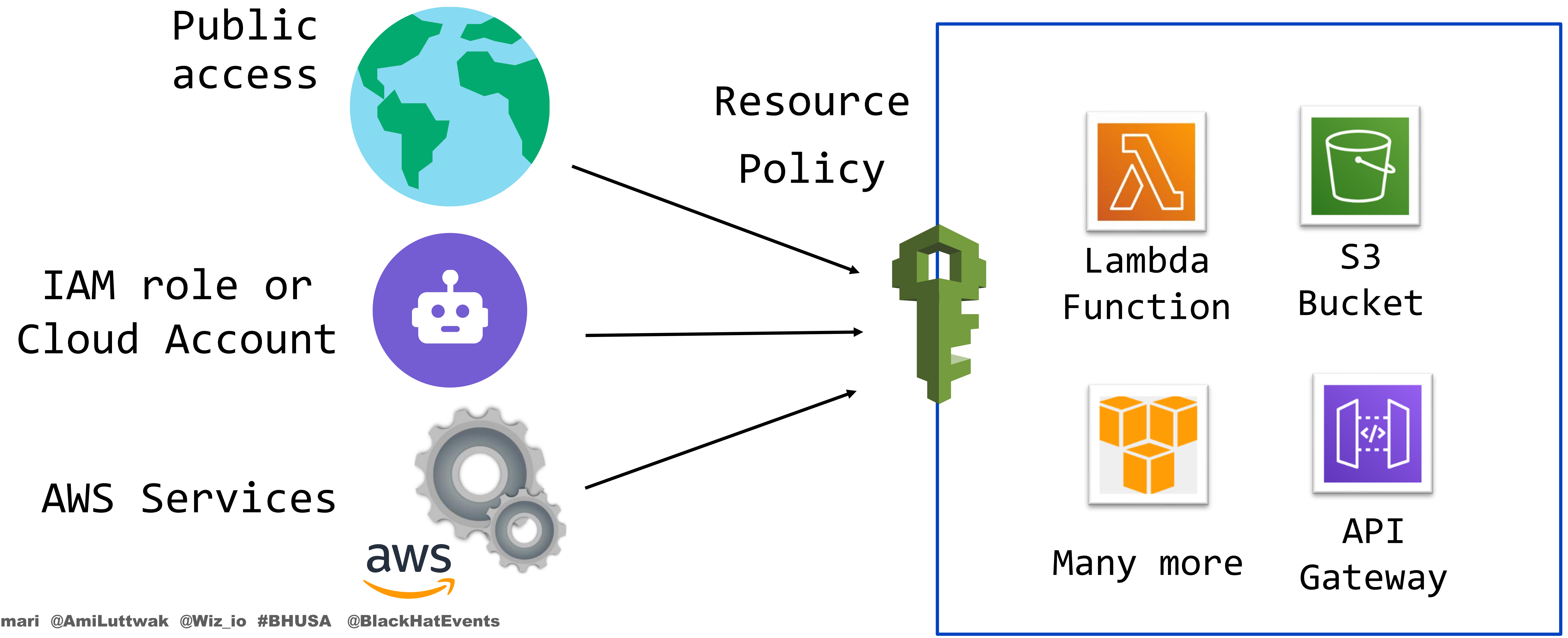
Why isolation is so critical?

Cloud as data center extension



AWS Identity Recap

Cross-account access in AWS



Public access

IAM role or Cloud Account

AWS Services

Resource Policy

Lambda Function

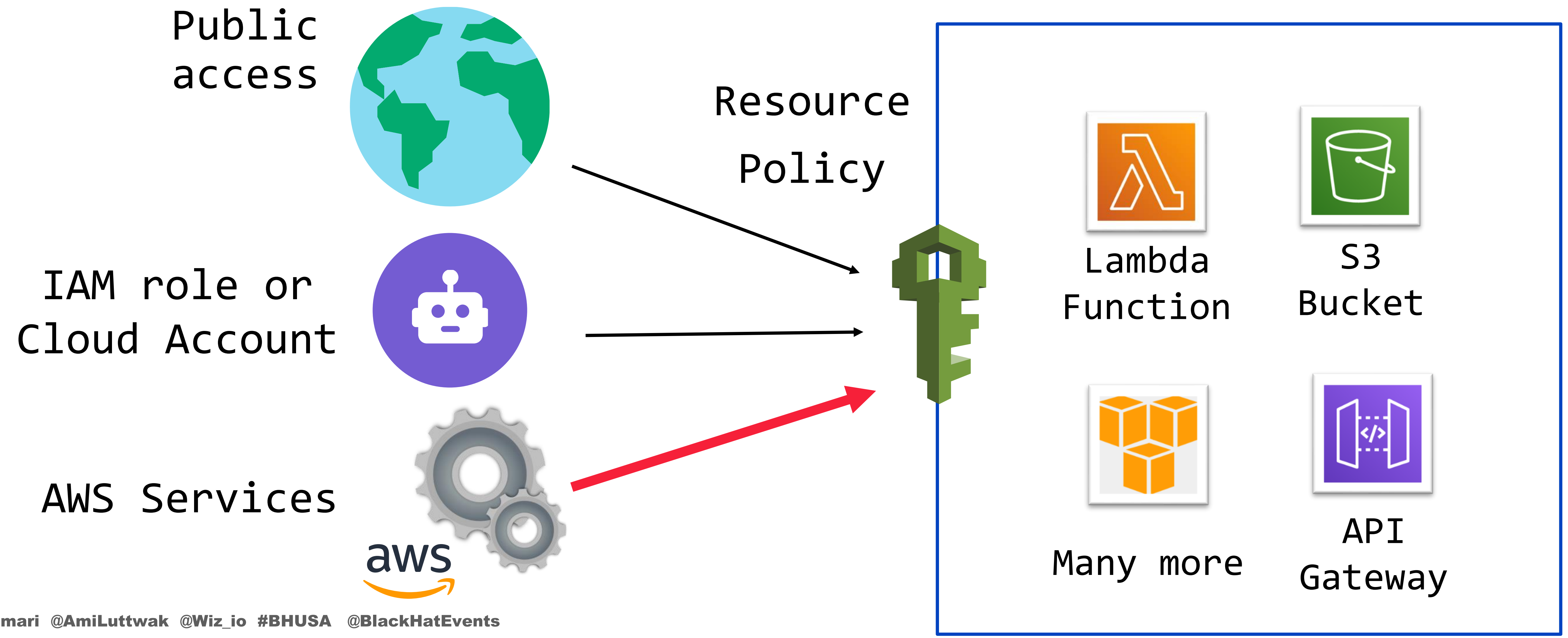
S3 Bucket

Many more

API Gateway

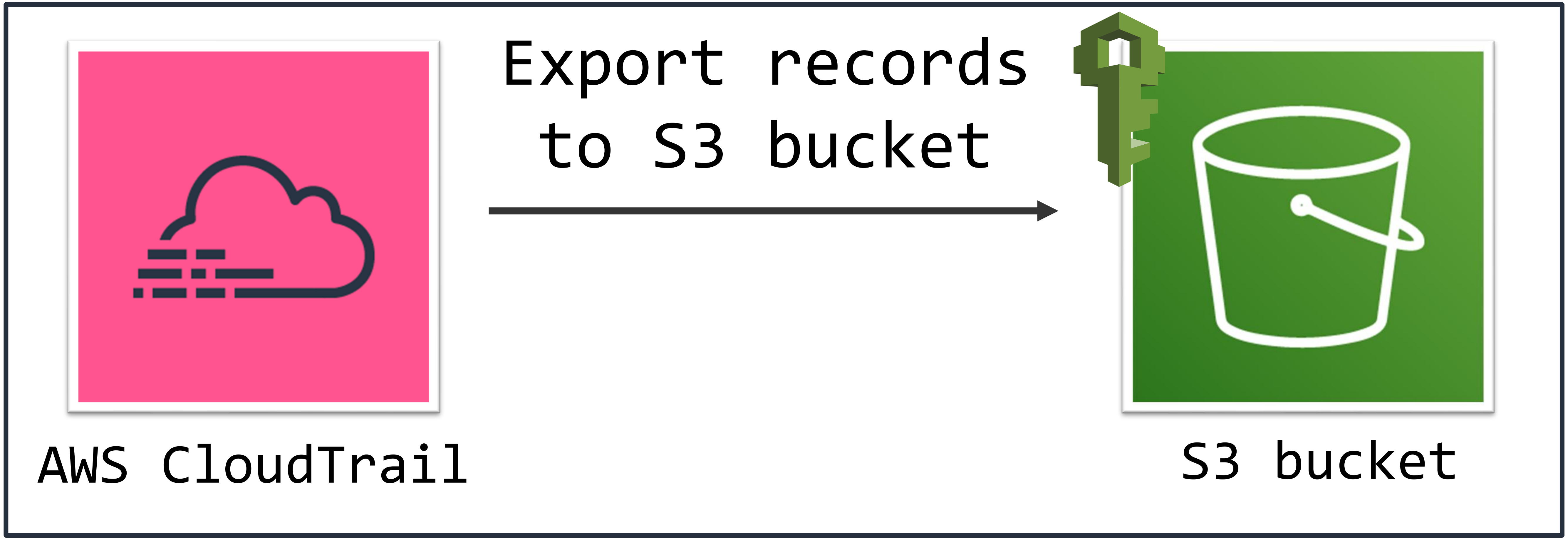
AWS Identity Recap

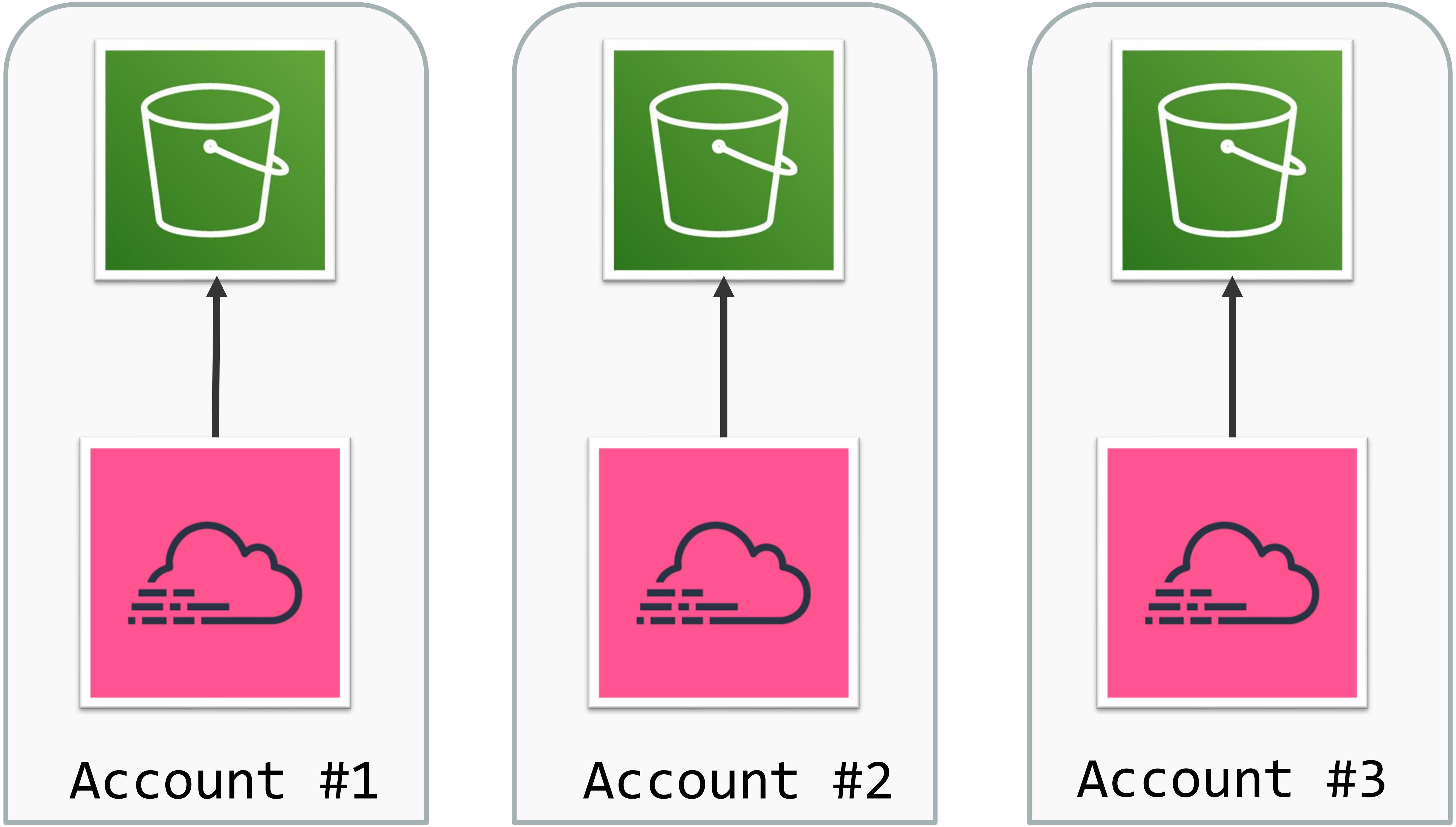
Let's focus on AWS services access



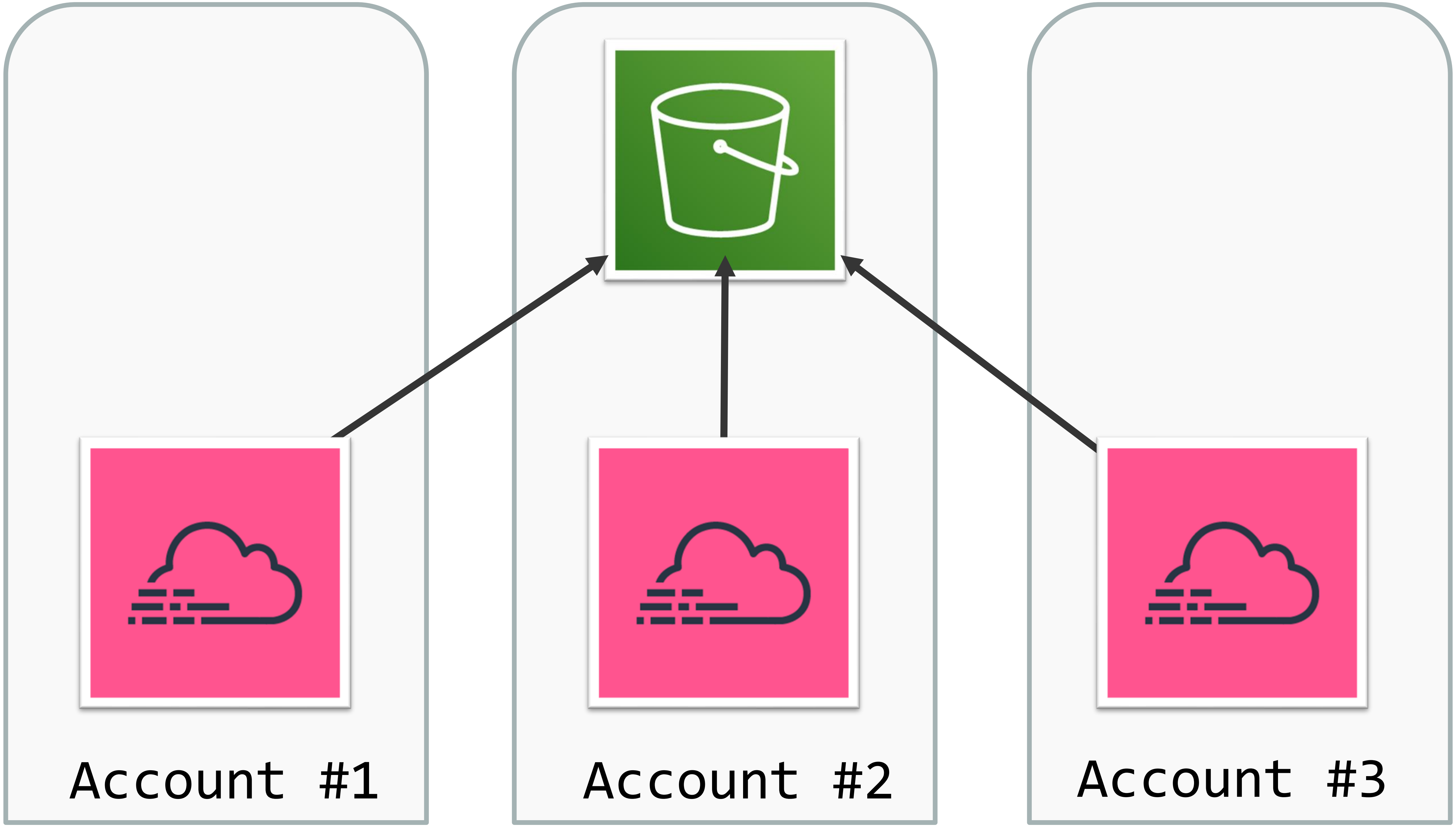
Resource Policy Deep Dive:

Why do services require cross-account access?





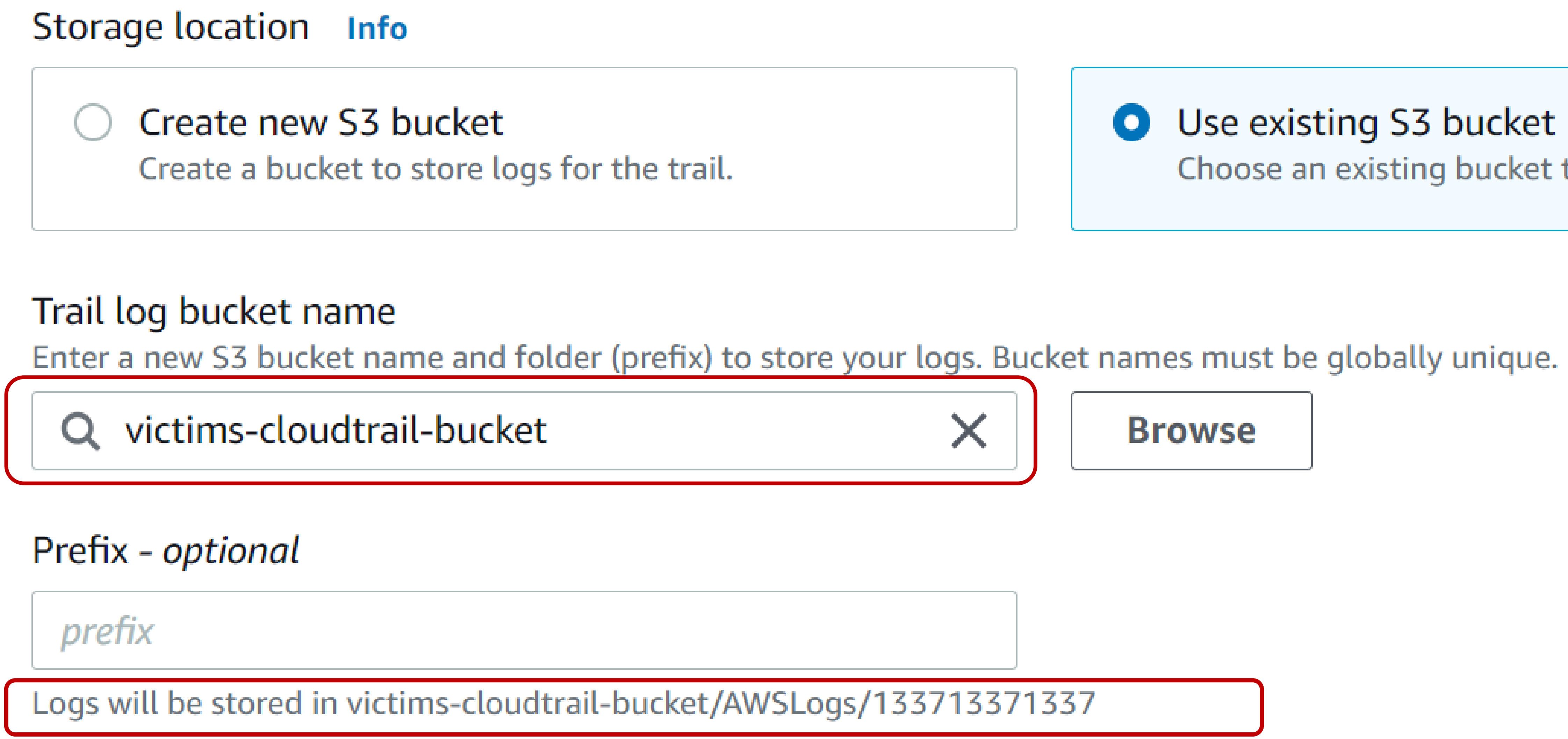
Account #1
Account #2
Account #3


Account #1
Account #2
Account #3

CloudTrail Resource Policy:

What is missing here?

```
{
  "Sid": "AWSCloudTrailWrite20150319",
  "Effect": "Allow",
  "Principal": {"Service": "cloudtrail.amazonaws.com"},
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::victims-cloudtrail-bucket/AWSLogs/123456789012/*",
  "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-control"}}
}
```



Storage location Info

○ Create new S3 bucket
Create a bucket to store logs for the trail.

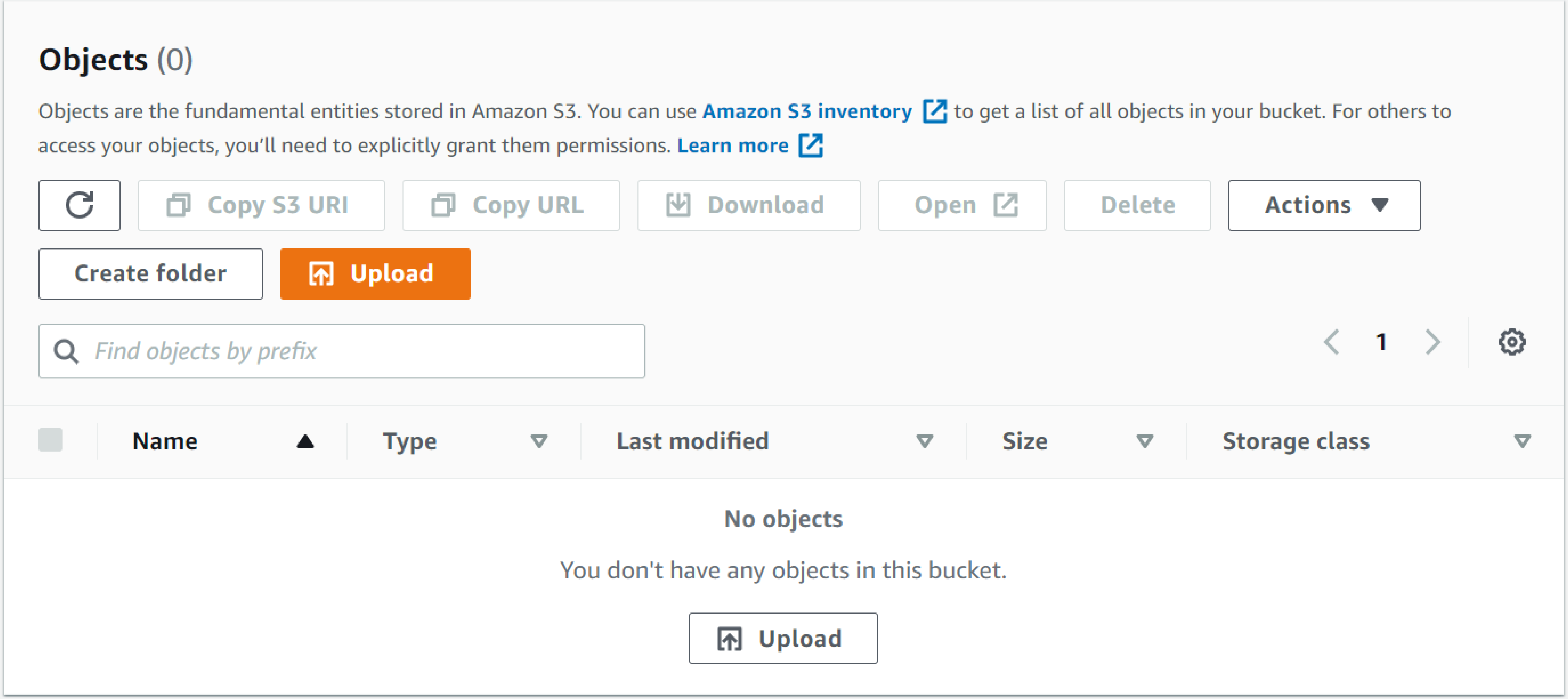
● Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket name
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

victims-cloudtrail-bucket

Prefix - *optional*

Logs will be stored in victims-cloudtrail-bucket/AWSLogs/133713371337



Objects (0)

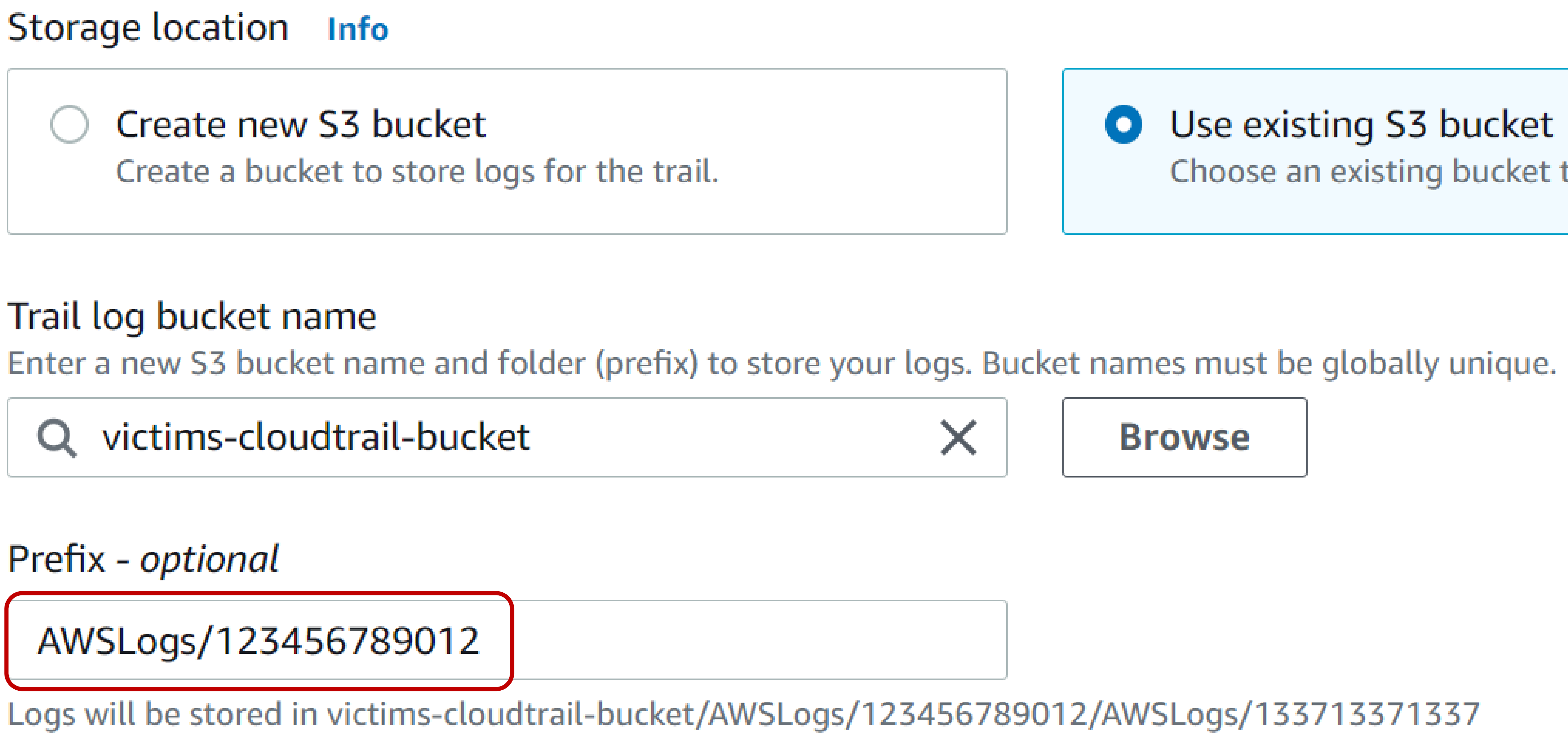
Objects are the fundamental entities stored in Amazon S3. You can use **Amazon S3 inventory** to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. **Learn more**

No objects

You don't have any objects in this bucket.

Breaking Identities:
CloudTrail Resource Policy

```
{
   "Sid": " AWSCloudTrailWrite20150319",
   "Effect": "Allow",
   "Principal": {"Service": "cloudtrail.amazonaws.com"},
   "Action": "s3:PutObject",
   "Resource": "arn:aws:s3:::victims-cloudtrail-bucket/AWSLogs/123456789012/*",
   "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-control"}}
}
```



Storage location Info

○ Create new S3 bucket
Create a bucket to store logs for the trail.

● Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

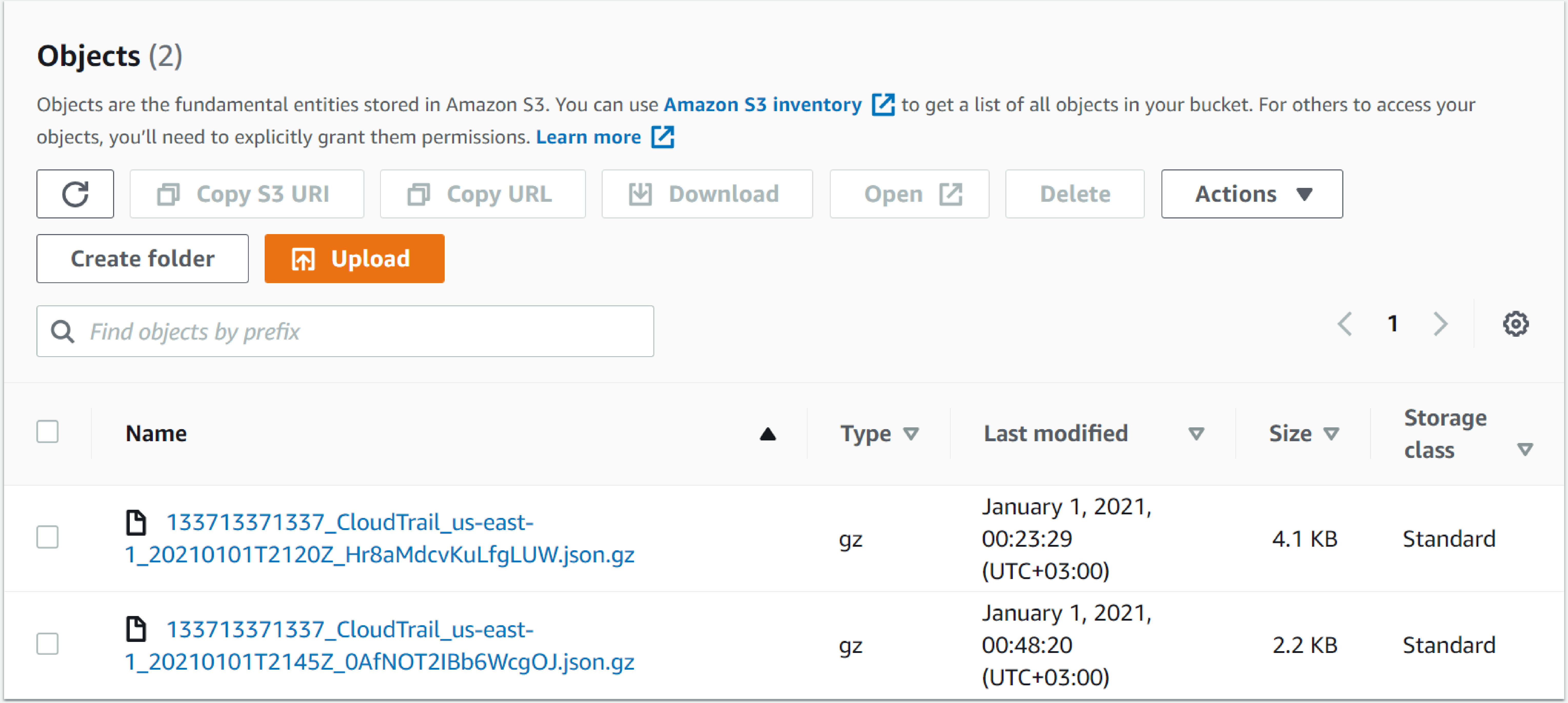
Trail log bucket name
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

victims-cloudtrail-bucket

Prefix - *optional*

AWSLogs/123456789012

Logs will be stored in victims-cloudtrail-bucket/AWSLogs/123456789012/AWSLogs/133713371337



Objects (2)

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

□	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class ▽
□	133713371337_CloudTrail_us-east-1_20210101T2120Z_Hr8aMdcvKuLfgLUW.json.gz	gz	January 1, 2021, 00:23:29 (UTC+03:00)	4.1 KB	Standard
□	133713371337_CloudTrail_us-east-1_20210101T2145Z_0AfNOT2IBb6WcgOJ.json.gz	gz	January 1, 2021, 00:48:20 (UTC+03:00)	2.2 KB	Standard

X-Account vulnerability #1:

CloudTrail

- Exporting records to other accounts
- A single mistake or a pattern?
- Does it represent something bigger?

X-Account:

Further Research

- **AWS Config** is also vulnerable
- What other services could be vulnerable?
- Can we read data?

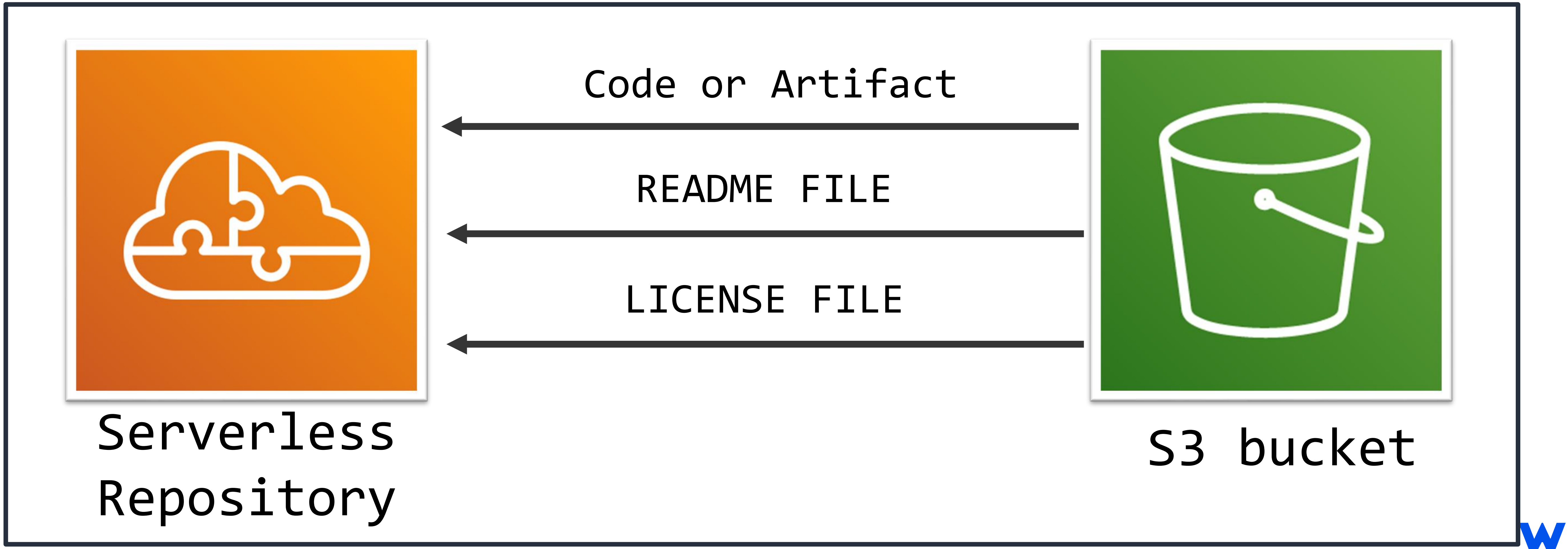
X-Account:

AWS Serverless Repository

- Managed repository for serverless applications
- Pulls app image and resources from S3 Bucket
- Does this service perform cross account actions?

X-Account:

AWS Serverless Repository



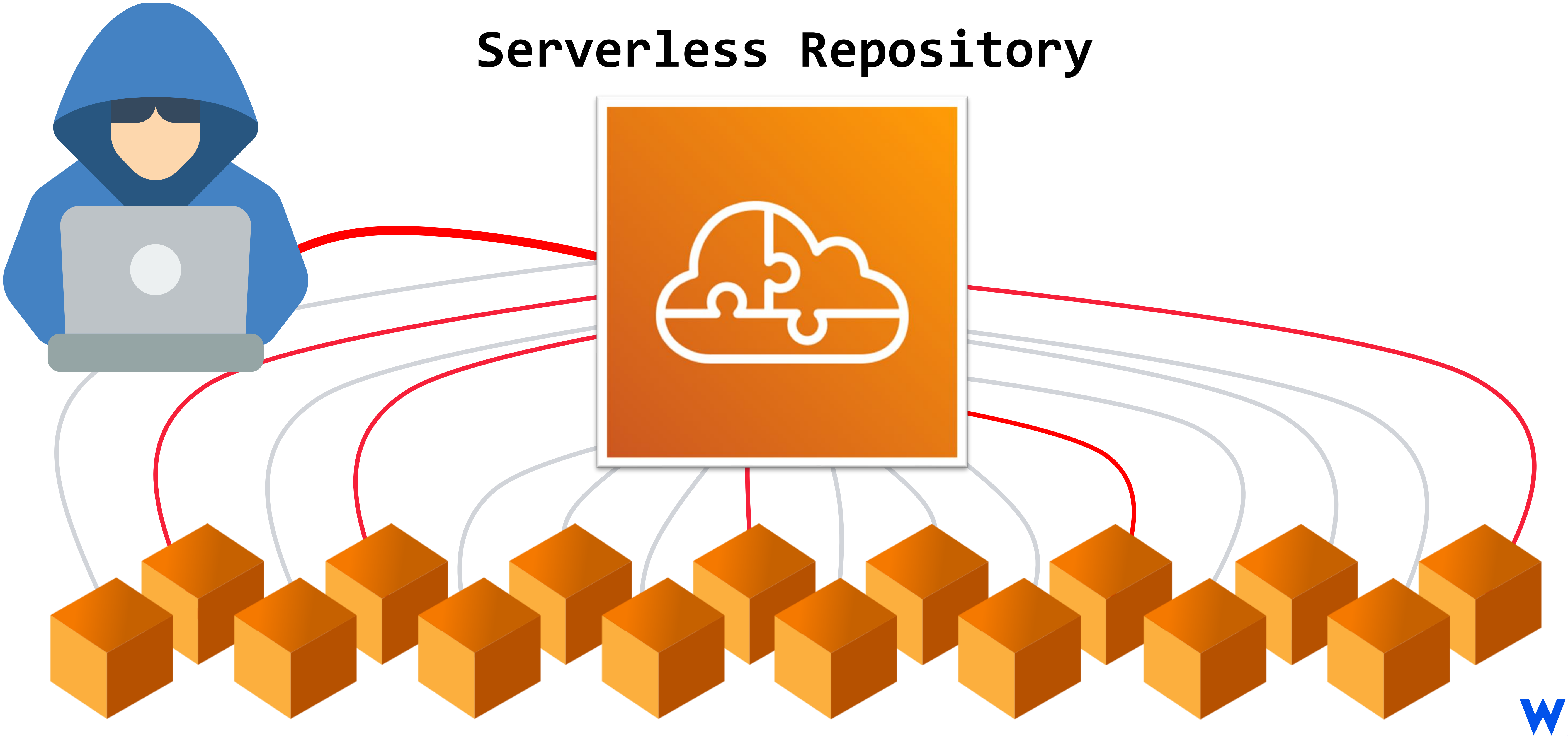
X-Account:

AWS Serverless Repository

```
{
   "Effect": "Allow",
   "Principal": {"Service": "serverlessrepo.amazonaws.com"},
   "Action": "s3:GetObject",
   "Resource": "arn:aws:s3:::bucketname/*"
}
```

Serverless Repository

Serverless Repository



AWS Serverless Repository:

An Exploit

```
shir@lp:~$ aws serverlessrepo update-application \
 --application-id arn:aws:serverlessrepo:*:*:applications/test \
 --readme-url https://serverless-repo-app10.s3.amazonaws.com/config.yaml
```

Demo

Breaking the Isolation:

Serverless Repository

- Reading object from private S3 buckets

  Source code, Artifacts, Secrets

- Data exfiltration
- It is a pattern!

Summary:

We Broke the Isolation

- 3 vulnerabilities disclosed
- Several more are in disclosure process
- This is just the tip of the iceberg

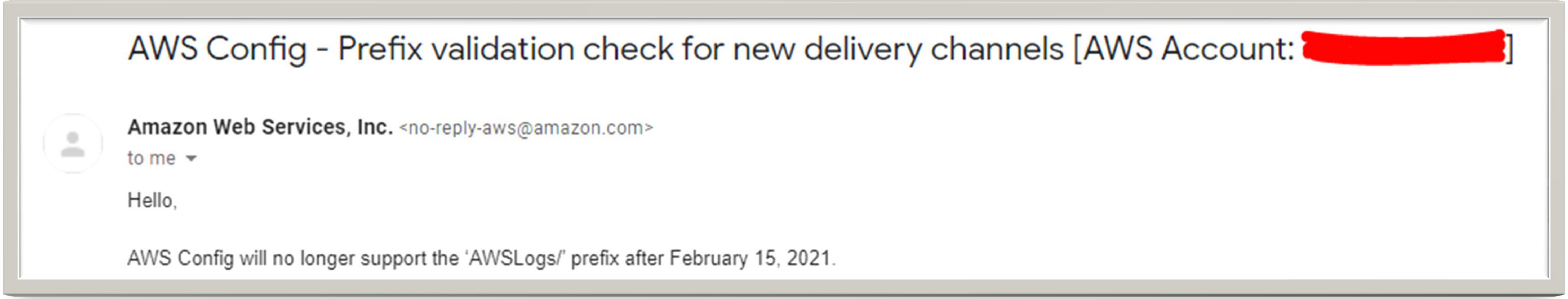
Breaking the Isolation:

Disclosure Timeline

- November 30th, 2020 – Report sent
- December 19th, 2020 – Acknowledged
- January 26th, 2021 – Resolved

The Fix:
AWS Config and CloudTrail

- Added prefix input validation:



AWS Config - Prefix validation check for new delivery channels [AWS Account: [redacted]]

Amazon Web Services, Inc. <no-reply-aws@amazon.com>
to me

Hello,

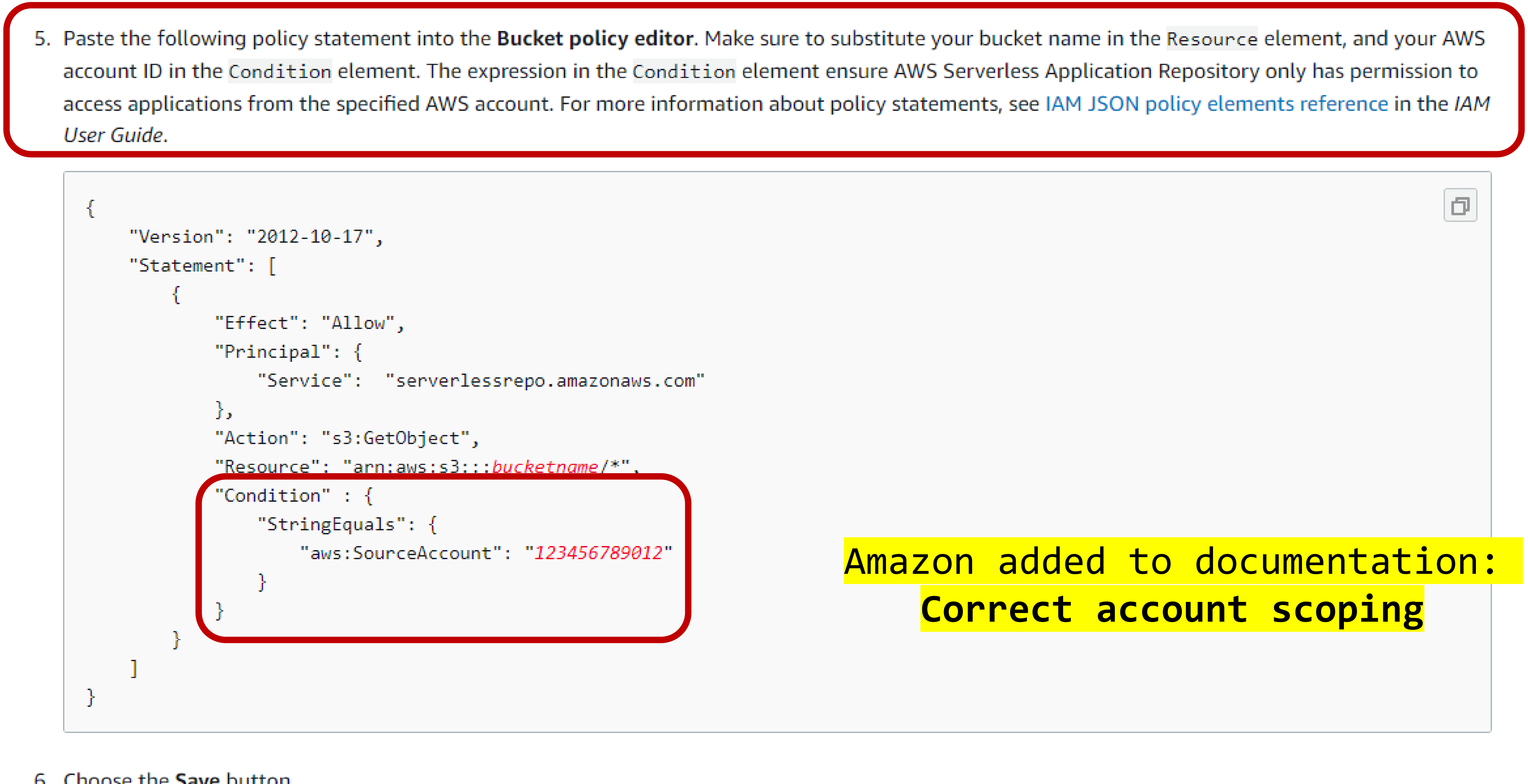
AWS Config will no longer support the 'AWSLogs/' prefix after February 15, 2021.

AWS Personal Health Dashboard

The Fix:

Serverless Repository

- AWS added new scoping condition
- Email was sent to customers
- Alert was issued on the AWS Personal Health Dashboard



5. Paste the following policy statement into the **Bucket policy editor**. Make sure to substitute your bucket name in the `Resource` element, and your AWS account ID in the `Condition` element. The expression in the `Condition` element ensure AWS Serverless Application Repository only has permission to access applications from the specified AWS account. For more information about policy statements, see IAM JSON policy elements reference in the *IAM User Guide*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service":  "serverlessrepo.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::bucketname/*",
            "Condition" : {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                }
            }
        }
    ]
}
```

Amazon added to documentation:
Correct account scoping

6. Choose the **Save** button

The aftermath - 5 months later

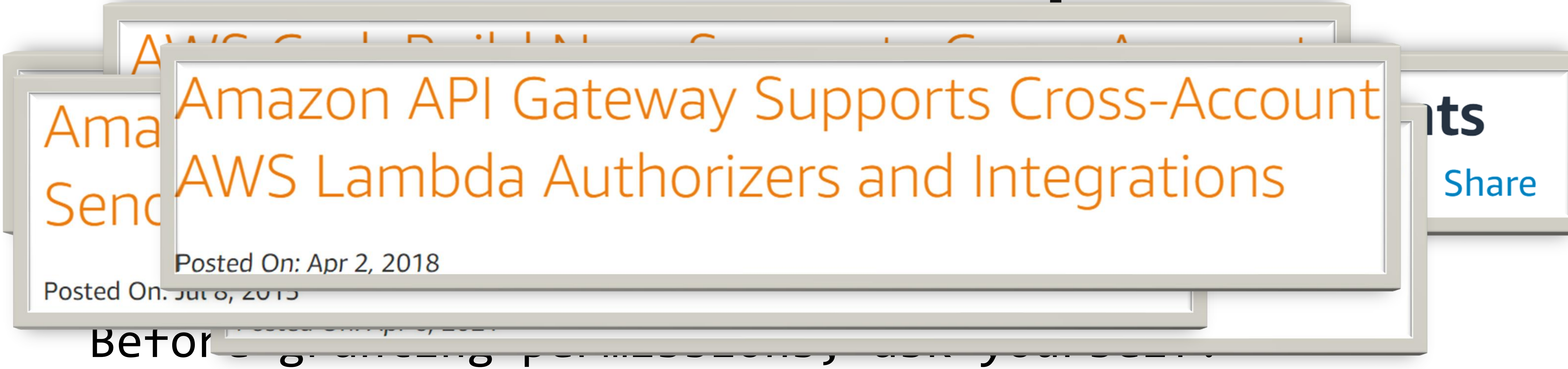
Most environments are still vulnerable

- **Our survey results:** 90% of the Serverless Repository buckets are still improperly configured
- **Why? The process is broken**

Users are responsible to update their resource policies but security teams are not aware of the risks

Takeaways #1:

Service access is a new cloud exposure risk



Amazon API Gateway Supports Cross-Account AWS Lambda Authorizers and Integrations

Posted On: Apr 2, 2018

Befor

- Could this service expose my environment?
- Can I scope the service access to specific accounts?

Takeaways #2:

Cloud Vulnerabilities - an industry problem

Email notifications are not enough.

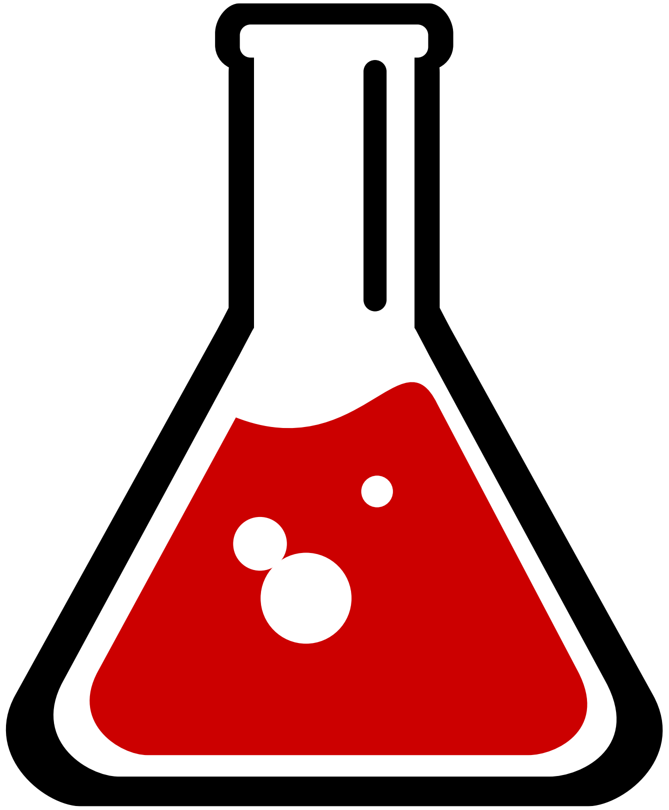
Is it time for a central cloud CVE DB?

- Formal identification
- ▪ Severity mechanism
- ▪ Tracking system

Breaking the Isolation:

Further research

- Map services with cross-account functionality
- More cloud providers



@AmiLuttwak ami@wiz.io
@ShirTamari shir@wiz.io

Breaking the Isolation:

Q&A

?

@AmiLuttwak, ami@wiz.io

@ShirTamari, shir@wiz.io