

AWS Academy Cloud Security

Foundations

Lab 3.1 Report: Using Resource -Based Policies to Secure an S3 Bucket

TAKI Oussama

3ACI Info

1. Présentation du laboratoire et objectifs

L'objectif principal de ce laboratoire était de comprendre la différence entre les politiques basées sur l'identité (IAM identity-based policies) et les politiques basées sur les ressources, notamment celles appliquées aux buckets S3. Nous avons également examiné la manière dont ces politiques interagissent pour fournir un contrôle d'accès granulaire.

Objectifs clés :

- Comprendre la distinction entre politiques basées sur l'identité et basées sur les ressources.
- Démontrer comment un utilisateur IAM peut assumer un rôle (assume role) afin de modifier ou d'étendre ses permissions.
- Analyser l'impact des différentes politiques sur la visibilité et l'exécution des actions dans la console AWS.

Architecture :

- **Architecture initiale :**

Le laboratoire débute avec un utilisateur IAM nommé *devuser*, appartenant au groupe *DeveloperGroup*.

- **Architecture cible :**

À la fin de l'exercice, nous utilisons des rôles IAM spécifiques (*BucketAccessRole* et *OtherBucketAccessRole*) permettant d'interagir avec des buckets S3 soumis à des restrictions d'accès.

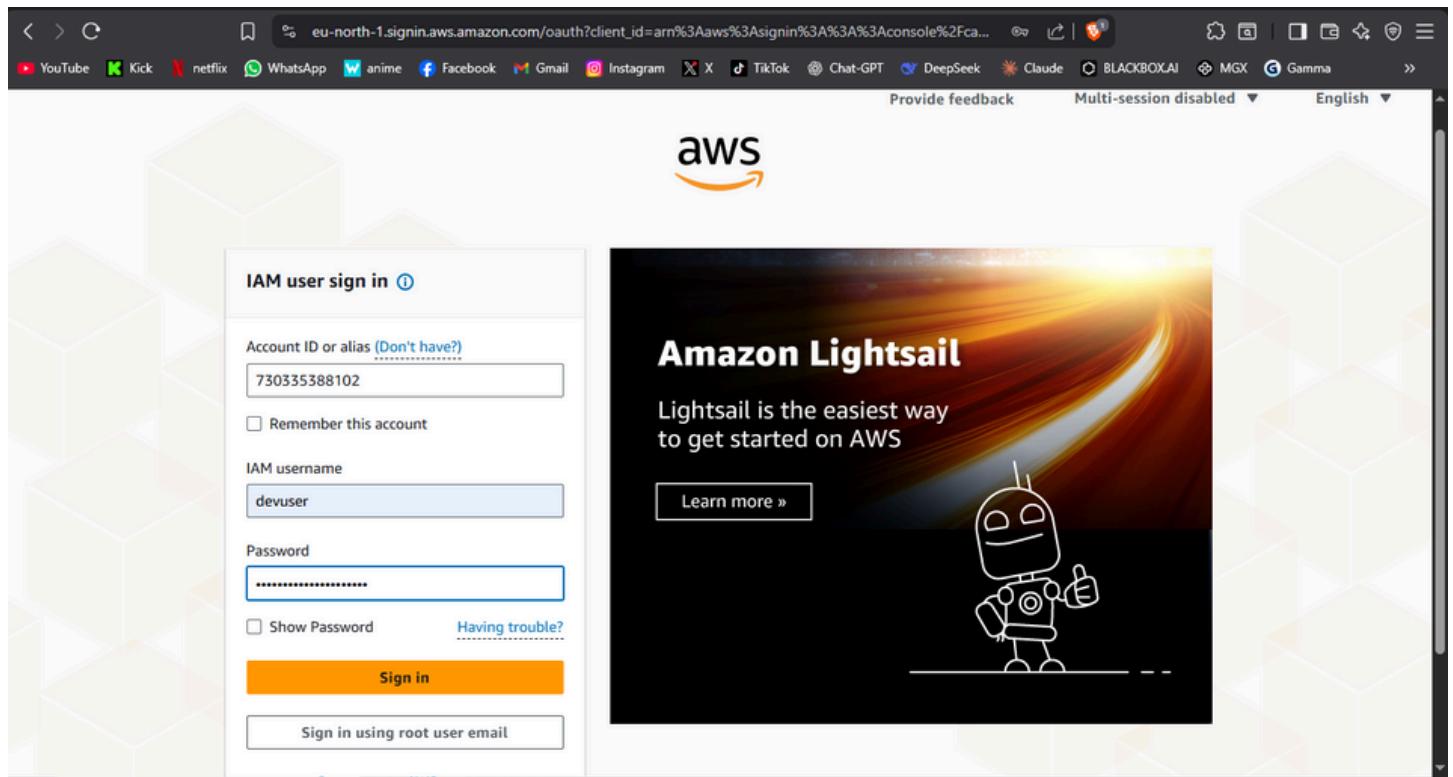
2. Description détaillée des tâches

Tâche 1 : Accès à la console

- **Action :** Connexion à la console de gestion AWS en utilisant les identifiants fournis pour *devuser*.

The screenshot shows the AWS Academy interface. On the left, there's a sidebar with various navigation links: Account, Dashboard, Courses, Calendar, Inbox, History, and Help. The main content area displays the title "Lab 3.1: Using Resource-Based Policies to Secure an S3 Bucket". Below the title, it says "Due No Due Date Points 100 Submitting an external tool". A progress bar indicates "02:58". To the right, there's a "AWS Details" section with buttons for "Start Lab", "End Lab", "AWS Details", "Details", "Submit", "Submission Report", and "Grades". It also shows "Accumulated lab time: 02:04:00 (124 minutes)" and "No running instance". Under "AWS Details", there are buttons for "SSH key Show", "Download PEM", "Download PPK", "AWS SSO Download URL", and a table with the following data:

| | |
|-----------------|---|
| IAMUserPassword | igw-09480c139c0ff28e7 |
| AccountID | 730335388102 |
| IAMUserLoginURL | https://730335388102.signin.aws |
| Region | us-east-1 |



Observation :

La connexion s'est effectuée avec succès, nous amenant directement sur la page d'accueil de la console AWS.

A screenshot of the AWS Console Home page. The URL in the address bar is "eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1#". The page has a white header with the AWS logo and a search bar. Below the header, there are two main sections. The first section, "Recently visited", shows icons for EC2, S3, Aurora and RDS, and Lambda, with a message "No recently visited services". The second section, "Applications", shows a table with one row, indicating "(0)" applications. The table includes columns for Name, Description, Region, and Originati... (partially cut off). A message at the bottom of this section says "The data couldn't be retrieved. Try again later." At the bottom of the page, there are links for "View all services", "Go to myApplications", and "CloudShell", "Feedback", "Console Mobile App". The footer contains copyright information: "© 2025, Amazon Web Services, Inc. or its affiliates." and links for "Privacy", "Terms", and "Cookie preferences".

Tâche 2 : Tentative d'accès en lecture aux services AWS

Action 1 : Accéder à Amazon EC2

- **Étape :** Navigation vers le tableau de bord EC2 pour consulter les instances.

- **Observation :** Plusieurs messages d'« API Error » sont apparus. Il était impossible d'afficher la liste des instances, de consulter les types d'instances ou d'accéder à toute ressource EC2
- **Raison :**
L'utilisateur *devuser* ne possède pas les permissions nécessaires — comme *ec2:DescribeInstances* — dans sa politique IAM, ce qui empêche l'accès aux ressources EC2.

The screenshot shows the AWS EC2 console interface. On the left, there's a sidebar with navigation links like 'Instances', 'Images', and 'Elastic Block Store'. The main area has a blue header bar with a message: 'You can change your default landing page for EC2.' Below it, there are two buttons: 'Permanently dismiss' and 'Change landing page'. The central part of the screen is titled 'Resources' and displays a grid of EC2 resources. Most of the resource cards show an 'API Error' icon. A red box highlights an error message in the 'Account attributes' section: 'An error occurred: An error occurred checking for a default VPC'. Another red box highlights an error message in the 'Service health' section: 'An error occurred: An error occurred retrieving service health information'. At the bottom right, there's a note about saving up to 90% on EC2 with Spot Instances.

Action 2 : Accès à Amazon S3

- **Étape :** Navigation vers la console Amazon S3.

The screenshot shows the AWS S3 console. The left sidebar includes sections for 'Buckets', 'Access management and security', and 'Storage management and insights'. The main area is titled 'General purpose buckets' and shows a list of three buckets. Each bucket entry includes the name, AWS Region (US East (N. Virginia)), and Creation date (December 9, 2025). To the right of the bucket list, there are two callout boxes: 'Account snapshot' (updated daily) and 'External access summary - new' (info). Both boxes provide links to their respective dashboards. At the bottom right, there's a note about Storage Lens providing visibility into storage usage and activity trends.

- **Observation** : La liste des buckets (*bucket1*, *bucket2*, *bucket3*) était visible, mais la colonne « Access » affichait « Insufficient permissions » ou « Error ».
- **Raison** : L'utilisateur *devuser* dispose de la permission *ListAllMyBuckets*, ce qui lui permet de voir les noms des buckets. Cependant, il ne possède pas les autorisations nécessaires pour consulter la configuration ou les paramètres d'accès public de chaque bucket.

Tâche 3 : Analyse de la politique basée sur l'identité

Action :

- Accès à la console IAM → *Users* → *devuser* → *Groups* → *DeveloperGroup* → *Permissions*.

The screenshot shows the AWS IAM Groups page for the 'DeveloperGroup'. The 'Permissions' tab is active, showing one attached policy named 'DeveloperGroupPolicy'. This policy is a Customer inline policy. The policy details are as follows:

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "s3:ListAllMyBuckets",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "s3:CreateBucket",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "s3>ListBucket",
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
  
```

- Ouverture de la politique *DeveloperGroupPolicy* afin d'examiner le fichier JSON.

Analyse de la politique :

La politique associée au groupe est une **Identity-Based Policy** (politique basée sur l'identité).

- **Actions autorisées** : *s3>ListAllMyBuckets*, *s3>CreateBucket*, *s3>ListBucket*.
- **Actions manquantes ou non autorisées** : Absence d'autorisations *ec2*: (ce qui explique les erreurs lors de l'accès à EC2) et absence de permission *s3:PutObject* au niveau global.

Cela explique pourquoi nous pouvions voir les noms des buckets (permission de liste), mais pas exécuter d'autres actions administratives.

Step 1 **Modify permissions in DeveloperGroupPolicy** Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Step 2 **Review and save**

Policy editor

```

1 v {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "cloudformation:Describe",
7         "cloudformation:Get",
8         "cloudformation>List",
9         "iam:Describe",
10        "iam:GetAccountAuthorizationDetails",
11        "iam:GetGroup",
12        "iam:GetGroupPolicy",
13        "iam:GetPolicy",
14        "iam:GetRole",
15        "iam:GetRolePolicy",
16        "iam:GetUser",
17        "iam GetUserPolicy",
18        "iam:List",
19        "logs:Describe",
20        "logs:DescribeLogStreams",
21        "logs:FilterLogEvents",
22        "s3:CreateBucket",
23        "s3:ListAllMyBuckets",
24        "s3:ListBucket",
25        "s3:PutAccountPublicAccessBlock",
26        "s3:PutBucketOwnershipControls",
27        "s3:PutBucketPublicAccessBlock",
28        "sts:AssumeRole"
29      ],
30      "Effect": "Allow",
31      "Resource": "*"
32    }
33  ]
34}
  
```

+ Add new statement

JSON - Line 7, Col 14

Visual JSON Actions ▾

Edit statement Remove

Add actions

Choose a service

Included

- Cloud Control API
- CloudFormation
- CloudWatch Logs
- IAM
- S3
- STS

Available

- AI Operations
- AMP

Add a resource

Add a condition (optional)

4572 of 5120 characters remaining

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Tâche 4 : Tentative d'accès en écriture aux services AWS

Action 1 : Crédation d'un bucket

- Étape : Clic sur « Create bucket » puis création d'un bucket nommé **to4973**.

Successfully created bucket "to4973". To upload files and folders, or to configure additional bucket settings, choose View details.

Insufficient permissions to apply Default Encryption You need the s3:PutEncryptionConfiguration permission to apply Default Encryption on this bucket. After you or your AWS admin has updated your Identity and Access Management (IAM) permissions to allow s3:PutEncryptionConfiguration, go to edit Default Encryption.

General purpose buckets All AWS Regions Directory buckets

| Name | AWS Region | Creation date |
|---|---------------------------------|--|
| c185581a4806215113043277t1w8913769574 61-bucket1-kruxc8ctralm2 | US East (N. Virginia) us-east-1 | December 9, 2025, 15:58:41 (UTC+02:00) |
| c185581a4806215113043277t1w8913769574 61-bucket2-ovz8gc2fpgj | US East (N. Virginia) us-east-1 | December 9, 2025, 15:58:42 (UTC+02:00) |
| c185581a4806215113043277t1w8913769574 61-bucket3-qkcfwlipbqg9 | US East (N. Virginia) us-east-1 | December 9, 2025, 15:58:42 (UTC+02:00) |
| to4973 | US East (N. Virginia) us-east-1 | December 9, 2025, 16:03:26 (UTC+02:00) |

Account snapshot Info Updated daily Storage Lens provides visibility into storage usage and activity trends.

External access summary - new Info Updated daily External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Résultat : Succès.
- Raison : La politique *DeveloperGroupPolicy* autorise explicitement l'action *s3:CreateBucket*.

Action 2 : Téléversement d'un objet

- **Étape** : Ouverture du bucket nouvellement créé, puis tentative de téléverser *Image1.jpg*.
- **Résultat** : Échec (message *Upload failed*).
- **Raison** : Bien que nous soyons propriétaires du bucket que nous venons de créer, la politique IAM associée à *devuser* ne contient pas l'autorisation *s3:PutObject*. Dans AWS, la permission de créer une ressource n'implique pas automatiquement la permission de modifier son contenu si la politique reste restrictive.

The screenshot shows the AWS S3 console interface. At the top, there's a red banner with the message "Upload failed" and a link to "Diagnose with Amazon Q". Below this, a header bar includes "Search" and "Account ID: 8913-7695-7461". The main area is titled "Upload: status". A message says "After you navigate away from this page, the following information is no longer available." Under "Summary", it shows "Destination s3://to4973" with "Succeeded" (0 files, 0 B (0%)) and "Failed" (1 file, 1.0 KB (100.00%)). The "Files and folders" tab is selected, showing a table with one item: "CloudShell" (1 total, 1.0 KB). The table has columns for Name, Folder, Type, Size, Status, and Error. The status for the file is "Failed". The bottom of the screen includes links for "CloudShell", "Feedback", "Console Mobile App", and copyright information: "© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

Tâche 5 : Assumer un rôle IAM

Test préalable : tentative de téléchargement avant d'assumer le rôle

- **Action** : Navigation vers *bucket1* puis tentative de téléchargement d'un fichier existant.
- **Résultat** : Échec (erreur *Access Denied*).

Screenshot of the AWS S3 console showing the bucket `c185581a4806215l13043277t1w891376957461-bucket1-krux8c1raim2`. The left sidebar shows navigation links for Buckets, Access management and security, and Storage management and insights. The main content area displays two objects: `Image1.jpg` and `Image2.jpg`, both of which are jpg files. The table lists their details: Name, Type, Last modified, Size, and Storage class.

| Name | Type | Last modified | Size | Storage class |
|-------------------------|------|--|----------|---------------|
| <code>Image1.jpg</code> | jpg | December 9, 2025, 15:59:13 (UTC+02:00) | 1.1 MB | Standard |
| <code>Image2.jpg</code> | jpg | December 9, 2025, 15:59:15 (UTC+02:00) | 375.4 KB | Standard |

Screenshot of the AWS S3 console showing the object `Image2.jpg` within the bucket `c185581a4806215l13043277t1w891376957461-bucket1-krux8c1raim2`. The left sidebar shows the same navigation links as the previous screenshot. The main content area displays the properties of `Image2.jpg`, including its owner, AWS Region, last modified date, size, type, and various URLs.

Object overview

- Owner:** 63af3c4c9fca9d8e4dadf100cbc51518983187f0e1e00e808c85d2036831aee7
- AWS Region:** US East (N. Virginia) us-east-1
- Last modified:** December 9, 2025, 15:59:15 (UTC+02:00)
- Size:** 375.4 KB
- Type:** jpg

S3 URI: <https://c185581a4806215l13043277t1w891376957461-bucket1-krux8c1raim2/Image2.jpg>

Amazon Resource Name (ARN): <arn:aws:s3:::c185581a4806215l13043277t1w891376957461-bucket1-krux8c1raim2/Image2.jpg>

Entity tag (Etag): [a3ae359c8a2fe046e2297c458c8a5](#)

Object URL: <https://c185581a4806215l13043277t1w891376957461-bucket1-krux8c1raim2.s3.us-east-1.amazonaws.com/Image2.jpg>

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

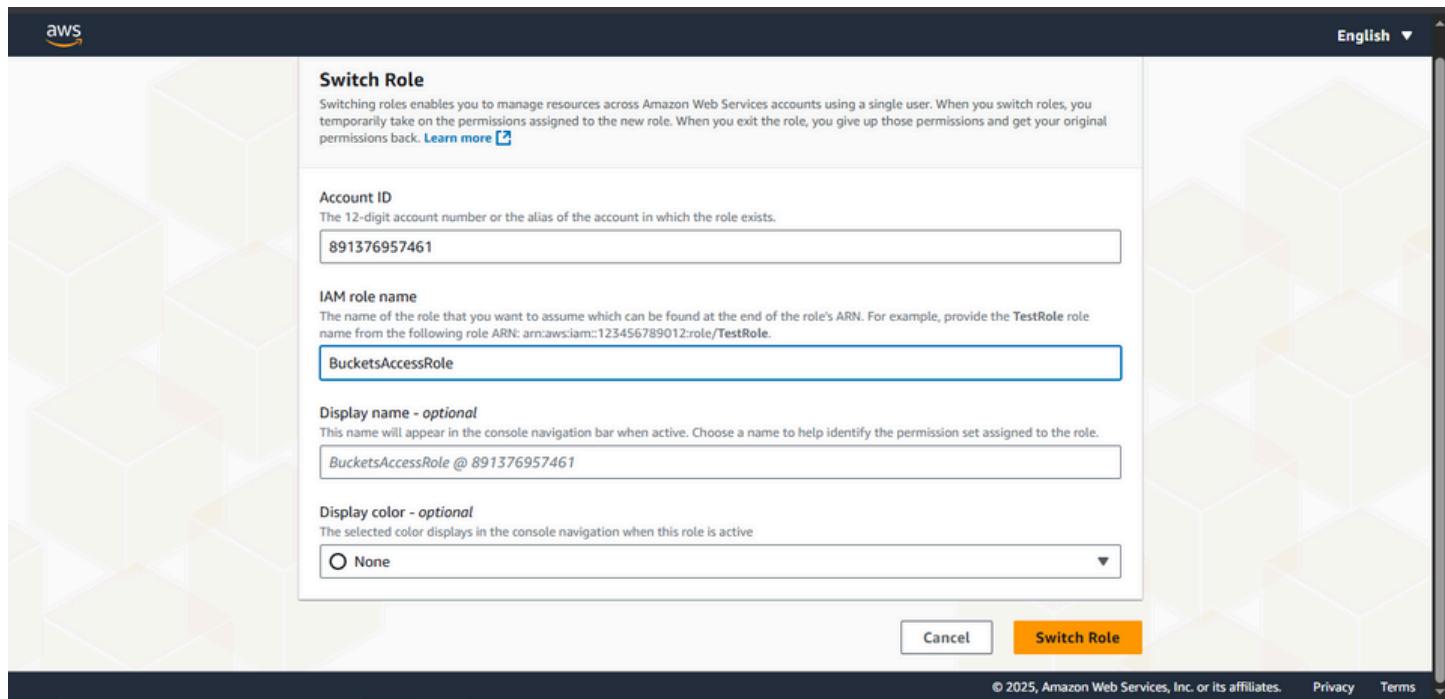
```
<Error>
  <Code>AccessDenied</Code>
  <Message>Request has expired</Message>
  <X-Amz-Expires>300</X-Amz-Expires>
  <Expires>2025-12-09T13:30:11Z</Expires>
  <ServerTime>2025-12-09T14:24:34Z</ServerTime>
  <RequestId>G9RCX7C44REST0FY</RequestId>
  <HostId>aePwISe4yrqinMcJEAzwhwYMxG6JazAS/vFUM2Vy7BnWv1t0BRbVKnL2165k+4NSX+6Y0uM45nQ=</HostId>
</Error>
```

Raison :

La politique basée sur l'identité de `devuser` (`DeveloperGroupPolicy`) autorise `s3>ListAllMyBuckets` et `s3>ListBucket`, mais ne contient pas la permission `s3:GetObject`, indispensable pour télécharger un objet depuis un bucket. Cela confirme que les

permissions par défaut de l'utilisateur limitent l'accès en lecture au contenu des objets, même s'il peut voir la liste des buckets.

Action : (tu peux m'envoyer la suite pour la reformuler)



Action :

- Ouverture du menu utilisateur en haut à droite puis clic sur Switch Role.
- Saisie de l'ID du compte ainsi que du nom du rôle : BucketsAccessRole.
- Changement visible : L'identité affichée en haut à droite a été remplacée par *BucketsAccessRole*, confirmant que le rôle a bien été assumé.

Test d'accès : (envoie-moi la suite et je te la reformule)

aws Search [Alt+S] United States (N. Virginia) Account ID: 8913-7695-7461 BucketsAccessRole @ 891376957461

Amazon S3 > Buckets > c185581a4806215l13043277t1w891376957461-bucket1-krux8c1raim2

Amazon S3 Buckets General purpose buckets Directory buckets Table buckets Vector buckets New Access management and security Access Points Access Points for FSx Access Grants IAM Access Analyzer Storage management and insights Storage Lens Batch Operations

c185581a4806215l13043277t1w891376957461-bucket1-krux8c1raim2 Info

Objects (1/2)

Copy S3 URI Copy URL Download Open Delete Actions Create folder

Upload

Objects are 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](#)

Find objects by prefix Show versions

| Name | Type | Last modified | Size | Storage class |
|------------|------|--|----------|---------------|
| Image1.jpg | jpg | December 9, 2025, 15:59:13 (UTC+02:00) | 1.1 MB | Standard |
| Image2.jpg | jpg | December 9, 2025, 15:59:15 (UTC+02:00) | 375.4 KB | Standard |

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Search [Alt+S] Global Account ID: 8913-7695-7461 BucketsAccessRole @ 891376957461

IAM Roles

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management User groups Users Roles Policies Identity providers Account settings Root access management Temporary delegation requests New

Access reports Access Analytics

Roles (0) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short duration you trust.

Search

| Role name | Trusted entities |
|--------------------------------|---|
| Access denied to iam>ListRoles | You don't have permission to <code>iam>ListRoles</code> . To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors. |

User: arn:aws:sts::891376957461:assumed-role/BucketsAccessRole/devuser
Action: iam>ListRoles
On resource(s): arn:aws:iam::891376957461:role/
Context: no identity-based policy allows the action

Switch back

Role history BucketsAccessRole @ 891376957461

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS IAM Roles page. The left sidebar is titled "Identity and Access Management (IAM)" and includes sections for "Access management" (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests) and "Access reports". The main content area displays a table of managed policies:

| Policy name | Type | Attached entities |
|--------------------------------------|-----------------|-------------------|
| GetBucketPolicy | Customer inline | 0 |
| GrantBucket1Access | Customer inline | 0 |
| ListAllBucketsPolicy | Customer inline | 0 |

Below the table, the "ListAllBucketsPolicy" is expanded to show its JSON content:

```

1 [{}]
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "s3>ListAllMyBuckets"
7       ],
8       "Resource": "*",
9       "Effect": "Allow"
10    }
11 ]
12 ]

```

Buttons for "Copy JSON" and "Edit" are visible next to the policy name.

1. **Bucket 1 :** Le téléchargement des objets a fonctionné sans problème.
2. **Bucket 2 :** L'upload d'objets était autorisé, car le rôle disposait de la permission *s3:PutObject* spécifiquement sur *bucket2*.

The screenshot shows the AWS S3 "Upload: status" page. A green banner at the top indicates "Upload succeeded". The summary table shows:

| Destination | Succeeded | Failed |
|--|----------------------------|-------------------|
| s3://c185581a480621513043277t1w449039445877-bucket2-ylsfa5cpevhb | 1 file, 375.4 KB (100.00%) | 0 files, 0 B (0%) |

The "Files and folders" tab is selected, showing a table of uploaded files:

| Name | Folder | Type | Size | Status | Error |
|------------|--------|------------|----------|-----------|-------|
| Image2.jpg | - | image/jpeg | 375.4 KB | Succeeded | - |

Analyse :

En assumant le rôle, nous avons temporairement abandonné les permissions de *devuser* pour adopter celles de *BucketsAccessRole*. Ce rôle possédait une politique dédiée autorisant la lecture et/ou l'écriture sur certains buckets, des permissions que *devuser* ne détenait pas initialement.

Voici la reformulation :

Tâche 6 : Comprendre les politiques basées sur les ressources

Action :

- En étant connecté avec le rôle *bucket-access-role*, nous avons navigué vers *Bucket 2* puis ouvert l'onglet **Permissions**.
- Nous avons consulté la **Bucket Policy**.

Analyse de la politique :

Il s'agit d'une **Resource-Based Policy**, c'est-à-dire une politique attachée directement à la ressource (le bucket S3), contrairement aux politiques basées sur l'identité qui sont liées à un utilisateur ou à un rôle IAM.

- La politique mentionnait explicitement *BucketsAccessRole* comme **Principal** autorisé.
- Cela confirme que l'accès à une ressource peut être accordé soit par la politique de l'utilisateur (Identity-Based Policy), soit par la politique de la ressource (Resource-Based Policy) lorsqu'il s'agit du même compte.
- Dans un contexte inter-comptes (cross-account), les deux types de politiques sont souvent nécessaires, mais dans ce laboratoire l'objectif principal était d'observer comment le rôle obtenait l'autorisation via la bucket policy.

Si tu veux, envoie-moi la dernière partie (conclusion, résumé, etc.) et je la reformule aussi.

The screenshot shows the AWS S3 console with the 'Bucket policy' tab selected for a specific bucket. The policy JSON is displayed:

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "S3Write",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::449039445877:role/BucketsAccessRole"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::c185581a4806215l13043277t1w449039445877-bucket2-ylsfa5cpervhb/*"
    },
    {
      "Sid": "ListBucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::449039445877:role/BucketsAccessRole"
      }
    }
  ]
}
```

3. Challenge Task: : Téléversement dans Bucket 3

Objectif : Envoyer *Image2.jpg* dans *bucket3*.

Tentative 1 : En tant que *devuser*

Upload failed
For more information, see the Error column in the Files and folders table.

Diagnose with Amazon Q

Upload: status

After you navigate away from this page, the following information is no longer available.

| Summary | |
|---|-------------------|
| Destination | Succeeded |
| s3://c185581a4806215113043277t1w449039445877-bucket3-cay0am8i935d | 0 files, 0 B (0%) |

| Files and folders (1 total, 375.4 KB) | | | | | | |
|---------------------------------------|--------|------------|----------|--------|---------------|--|
| Find by name | | | | | | |
| Name | Folder | Type | Size | Status | Error | |
| Image2 (1).jpg | - | image/jpeg | 375.4 KB | Failed | Access denied | |

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Amazon S3 > Buckets > c185581a4806215113043277t1w449039445877-bucket3-cay0am8i935d

Access denied

API response

User: arn:aws:iam::449039445877:user/devuser is not authorized to perform: s3:GetBucketPublicAccessBlock on resource: "arn:aws:s3:::c185581a4806215113043277t1w449039445877-bucket3-cay0am8i935d" because no identity-based policy allows the s3:GetBucketPublicAccessBlock action

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](#)

You don't have permission to get bucket policy

You or your AWS administrator must update your IAM permissions to allow s3:GetBucketPolicy. After you obtain the necessary permission, refresh the page. Learn more about [Identity and access management in Amazon S3](#)

API response

Object Ownership

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

You don't have permission to view Object ownership (bucket settings) configuration

You need s3:GetBucketOwnershipControls to view Object ownership (bucket settings) configuration. Learn more about [Object ownership in Amazon S3](#)

API response

https://us-east-1.console.aws.amazon.com/s3/get-started?region=us-east-1

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Tentative 2 : En utilisant le rôle *BucketAccessRole*

The screenshot shows the AWS S3 console with the path [Amazon S3 > Buckets > c185581a4806215l13043277t1w449039445877-bucket3-cay0am8i935d](#). The left sidebar includes sections for Buckets, Access management and security, Storage management and insights, and Account and organization settings. The main content area is titled "Objects" and displays a message: "Insufficient permissions to list objects. After you or your AWS administrator has updated your permissions to allow the s3>ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3". A "Diagnose with Amazon Q" button is also present.

Résultat : Échec. La politique associée au rôle ne contenait aucune permission permettant d'interagir avec *bucket3*. Toutefois, nous pouvions consulter la bucket policy.

The screenshot shows the AWS S3 console with the path [Amazon S3 > Buckets > c185581a4806215l13043277t1w449039445877-bucket3-cay0am8i935d](#). The left sidebar includes sections for Buckets, Access management and security, Storage management and insights, and Account and organization settings. The main content area is titled "Bucket policy" and displays a JSON policy document:

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "S3Write",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::449039445877:role/OtherBucketAccessRole"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::c185581a4806215l13043277t1w449039445877-bucket3-cay0am8i935d/*"
    },
    {
      "Sid": "ListBucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::449039445877:role/OtherBucketAccessRole"
      }
    }
  ]
}
```

Solution :

1. Nous avons identifié un second rôle disponible dans le compte : **OtherBucketAccessRole**.
2. Nous avons de nouveau utilisé la fonctionnalité **Switch Role** pour passer du rôle *BucketsAccessRole* au rôle *OtherBucketAccessRole*.

Switch Role

Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. [Learn more](#)

Account ID
The 12-digit account number or the alias of the account in which the role exists.
449039445877

IAM role name
The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the TestRole role name from the following role ARN: arn:aws:iam::123456789012:role/TestRole.

Display name - optional
This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.
OtherBucketsAccessRole @ 449039445877

Display color - optional
The selected color displays in the console navigation when this role is active.
None

Cancel **Switch Role**

1. Nous avons navigué vers *bucket3*.
2. Nous avons cliqué sur **Upload**, sélectionné *Image2.jpg*, puis validé l'envoi.
3. **Résultat :** Succès.

Explication :

Le rôle **OtherBucketAccessRole** possédait une politique autorisant explicitement l'action *s3:PutObject* sur la ressource *bucket3*. En assumant ce rôle spécifique, nous avons obtenu les permissions nécessaires pour réaliser la tâche.

Upload succeeded
For more information, see the [Files and folders](#) table.

Upload: status

After you navigate away from this page, the following information is no longer available.

| Summary | | Failed | |
|---|----------------------------|-------------------|-------|
| Destination | Succeeded | Failed | Error |
| s3://c185581a4806215113043277t1w449039445877-bucket3-cay0am8i935d | 1 file, 375.4 KB (100.00%) | 0 files, 0 B (0%) | |

Files and folders (1 total, 375.4 KB)

| Name | Folder | Type | Size | Status | Error |
|----------------------------|--------|------------|----------|-----------|-------|
| Image2.jpg | - | image/jpeg | 375.4 KB | Succeeded | |

Total score **15/15**

TASK 4 - Create bucket **5/5**

TASK 5 - Uploaded object **5/5**

CHALLENGE TASK - Uploaded object **5/5**

4. Conclusion

Ce laboratoire a clairement démontré la flexibilité et la granularité du contrôle d'accès dans AWS :

1. **Les politiques d'identité** associées à *devuser* offraient un accès de base, mais limitaient les actions sensibles, comme la création d'instances EC2 ou l'écriture dans des buckets non autorisés.
2. **Les rôles IAM** nous ont permis d'élever temporairement nos permissions afin d'accomplir des tâches spécifiques (gestion ciblée de certains buckets) sans avoir à attribuer ces priviléges de manière permanente à l'utilisateur.
3. **Les politiques basées sur les ressources**, appliquées directement aux buckets S3, ont ajouté une couche supplémentaire de contrôle, en définissant précisément quels *principals* (utilisateurs ou rôles) étaient autorisés à interagir avec les données du bucket.