

AWS Academy Cloud Security Foundations

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

Ketaj Youssef

3ACI Info

1. Lab Overview and Objectives

The objective of this lab was to understand the difference between IAM identity -based policies and resource -based policies (specifically S3 bucket policies). We explored how these policies interact to define fine -grained access control.

Key Goals:

- Distinguish between identity -based and resource -based policies.
- Demonstrate how an IAM user can assume an IAM role to change permissions.
- Analyze how policies affect console visibility and actions.

Architecture

Starting Architecture:

The lab began with a devuser (IAM user) who is a member of the `DeveloperGroup`.

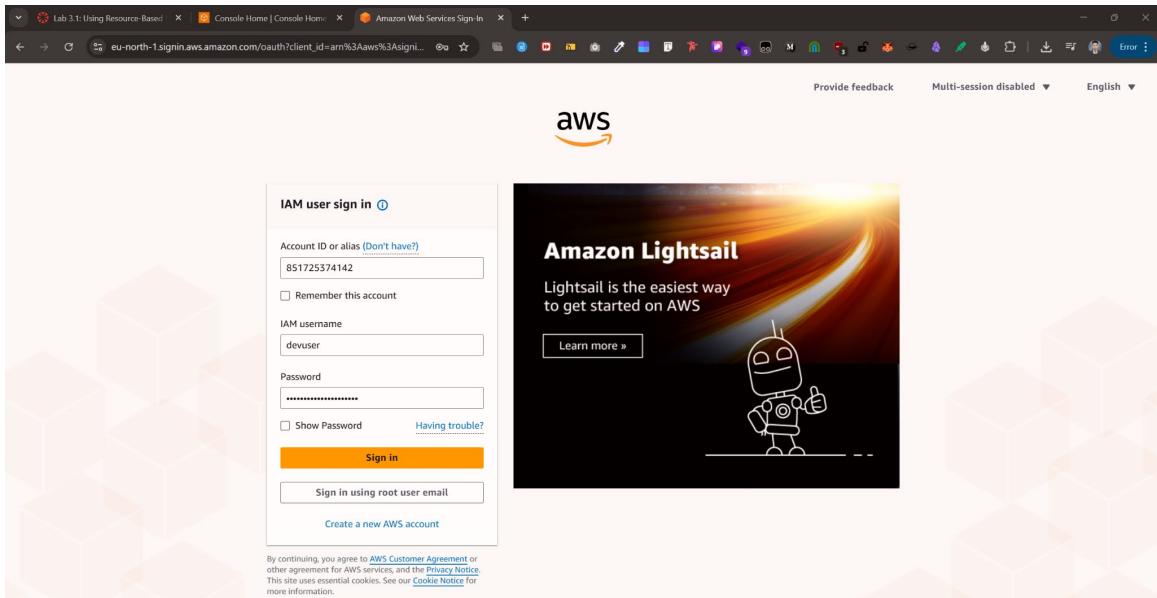
Target Architecture:

By the end, we utilized specific IAM roles (`BucketAccessRole` and `OtherBucketAccessRole`) to interact with restricted S3 buckets.

2. Detailed Task Walkthrough

Task 1: Accessing the Console

- **Action:** Logged into the AWS Management Console using the provided devuser credentials.



- Observation:** The login was successful, placing us in the AWS Console Home.

The screenshot shows the AWS Console Home interface. On the left, a 'Service menu' box is open, showing options like 'Next'. Below it, there's a section for 'No recently visited services' with links to EC2, S3, Aurora and RDS, and Lambda. The main area contains several widgets: one for 'Applications' (0) which shows a message about access denied for 'servicatalog>ListApplications'; another for 'AWS Health' which says 'No health data' and 'You don't have permissions to access'; and a third for 'Cost and usage' which also shows 'Access denied' messages for current and forecasted months. At the bottom, there are links for CloudShell, Feedback, and Console Mobile App.

Task 2: Attempting Read -Level Access to AWS Services

Action 1: Accessing Amazon EC2

- Step:** Navigated to the EC2 Dashboard to view instances.
- Observation:** The console displayed multiple "API Error" messages. We were unable to list instances, view instance types, or see any EC2 resources.

- **Reason:** The devuser does not have the necessary permissions (e.g., `ec2:DescribeInstances`) attached to their identity policy.

The screenshot shows the AWS EC2 console interface. The top navigation bar includes the AWS logo, search bar, and account information: Account ID: 8517-2537-4142, Europe (Stockholm), and devuser. The left sidebar menu is open, showing categories like Dashboard, Instances, Images, Elastic Block Store, Network & Security, and more. The main content area is titled "Resources" and displays a message: "You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:". Below this, there is a grid of resource status cards, each with an "API Error" icon. The resources listed are: Instances (running) 0, Auto Scaling Groups, Capacity Reservations, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, and Volumes. In the bottom right corner of the main content area, there is a red-bordered callout box with the text: "An error occurred An error occurred retrieving service health information" and a "Diagnose with Amazon Q" button.

Action 2: Accessing Amazon S3

- **Step:** Navigated to the S3 Console.

General purpose buckets (3)

Name	AWS Region	Creation date
c185581a4806215l1 3009332t1w851725	US East (N. Virginia) us-east-1	December 6, 2025, 10:36:38 (UTC+01:00)
c185581a4806215l1 3009332t1w851725 374142-bucket2- kzeplvymu8ht	US East (N. Virginia) us-east-1	December 6, 2025, 10:36:38 (UTC+01:00)
c185581a4806215l1 3009332t1w851725 374142-bucket3- nq4cmfzgodfh	US East (N. Virginia) us-east-1	December 6, 2025, 10:36:38 (UTC+01:00)

Account snapshot

Updated daily

Storage Lens provides visibility into storage usage and activity trends.

External access summary - new

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

- Observation:** We could see the list of buckets (bucket1, bucket2, bucket3), but the "Access" column showed "Insufficient permissions" or "Error".
- Reason:** The devuser has permission to `ListAllMyBuckets`, allowing them to see the bucket names, but lacks permissions to query the specific configuration or public access settings of those buckets.

Task 3: Analyzing the Identity -Based Policy

Action:

- Navigated to the IAM Console -> Users -> devuser -> Groups -> DeveloperGroup ->

Permissions.

- Opened the **DeveloperGroupPolicy** to inspect the JSON.

Policy Analysis:

The policy attached to our group was an Identity-Based Policy.

- **Allowed Actions:** `s3>ListAllMyBuckets`, `s3>CreateBucket`, and `s3>ListBucket`.
- **Denied/Missing Actions:** It did *not* explicitly allow `ec2:*` actions (explaining the EC2 errors) and did not allow `s3:PutObject` globally.

This explains why we could see the bucket names (List) but failed to perform other administrative tasks.

The screenshot shows the AWS IAM Policy Editor interface. The main area displays the JSON code for the policy:

```
1 {  
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:Get*",  
21                "logs:List*",  
22                "s3:CreateBucket",  
23                "s3:ListAllMyBuckets",  
24                "s3:ListBucket",  
25                "s3:PutBucketPublicAccessBlock",  
26                "s3:PutBucketOwnershipControls",  
27                "s3:PutBucketPublicAccessBlock",  
28                "sts:AssumeRole"  
29            ],  
30            "Resource": "",  
31            "Effect": "Allow"  
32        },  
33    ]  
34}
```

The right side of the interface shows the "Edit statement" panel with a "Select a statement" dropdown and a "+ Add new statement" button. The bottom status bar indicates "4572 of 5120 characters remaining".

Task 4: Attempting Write -Level Access to AWS Services

Action 1: Creating a Bucket

- Step: Clicked "Create bucket" and named it `yk2120`.

The screenshot shows the AWS S3 buckets page. At the top, there are two notifications: one green box stating 'Successfully created bucket "yk2120"' and a red box stating 'Insufficient permissions to apply Default Encryption'. Below these, the 'General purpose buckets' section lists four buckets, all created on December 6, 2025. The buckets are: c185581a4806215l13009332t1w851725374142-bucket1-z04qm4kqb6ml, c185581a4806215l13009332t1w851725374142-bucket2-kzep4yvmu8ht, c185581a4806215l13009332t1w851725374142-bucket3-nq4cmfzgodfh, and yk2120. The yk2120 bucket is selected. At the bottom, there are sections for 'Account snapshot' and 'External access summary'.

Name	AWS Region	Creation date
c185581a4806215l13009332t1w851725374142-bucket1-z04qm4kqb6ml	US East (N. Virginia) us-east-1	December 6, 2025, 10:36:38 (UTC+01:00)
c185581a4806215l13009332t1w851725374142-bucket2-kzep4yvmu8ht	US East (N. Virginia) us-east-1	December 6, 2025, 10:36:38 (UTC+01:00)
c185581a4806215l13009332t1w851725374142-bucket3-nq4cmfzgodfh	US East (N. Virginia) us-east-1	December 6, 2025, 10:36:38 (UTC+01:00)
yk2120	US East (N. Virginia) us-east-1	December 6, 2025, 11:10:13 (UTC+01:00)

- **Result:** Success .
- **Reason:** The [DeveloperGroupPolicy](#) explicitly allowed `s3:CreateBucket`.

Action 2: Uploading an Object

- **Step:** Opened the newly created bucket and attempted to upload Image1.jpg.
- **Result:** Failed (Upload failed message).
- **Reason:** While we can create the bucket (owner), the IAM policy attached to devuser does not grant `s3:PutObject` permission. In AWS, permission to create a resource does not automatically imply permission to modify its contents if the policy is 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 the banner, the title "Upload: status" is displayed, along with a "Close" button. A note says "After you navigate away from this page, the following information is no longer available." In the "Summary" section, it shows the destination "s3://yk2120" and two rows: "Succeeded" (0 files, 0 B (0%)) and "Failed" (1 file, 1.0 KB (100.00%)). Below the summary, there are two tabs: "Files and folders" (selected) and "Configuration". The "Files and folders" tab displays a table with one item: "DeveloperGroupPol..." (Type: application/json, Size: 1.0 KB). To the right of the table, a tooltip box appears with the title "Access denied" and the message "You don't have permissions to upload files and folders." At the bottom of the page, there are links for CloudShell, Feedback, and Console Mobile App, along with copyright information: "© 2025, Amazon Web Services, Inc. or its affiliates." and links for Privacy, Terms, and Cookie preferences.

Task 5: Assuming an IAM Role

Testing Download Before Assuming Role

Action:

- Navigated to bucket1 and attempted to download an existing file.

Result: Failed (Access Denied error).

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>User: arn:aws:iam::851725374142:user/devuser is not authorized to perform: s3:GetObject on resource: "arn:aws:s3:::c185581a4806215113009332t1w851725374142-bucket1-z04qm4kqb6m1/image2.jpg" because no identity-based policy allows the s3:GetObject action</Message>
  <RequestId>H9XJZVP70SDJV8Y</RequestId>
  <HostId>b20ZjIHuiee6Uzp0yVAU13JAPJ9L/0TJzzCdmme22Q1/v2+NfL5GbN8yxxCL6z9QU+8A2BDxAQ=</HostId>
</Error>
```

:root { --wh-slate-50: #f8fafc;--wh-slate-100: #f1f5f9;--wh-slate-200: #e2e8f0;--wh-slate-300: #cbd5e1;--wh-slate-400: #94a3b8;--wh-slate-500: #64748b;--wh-slate-600: #475569;--wh-slate-700: #334155;--wh-slate-800: #e293b;--wh-slate-900: #0f172a;--wh-slate-950: #020617;--wh-primary-50: rgb(188, 220, 205);--wh-primary-100: rgb(154, 208, 185);--wh-primary-200: rgb(120, 197, 164);--wh-primary-300: rgb(86, 186, 144);--wh-primary-400: rgb(53, 176, 125);--wh-primary-500: rgb(0, 179, 122);--wh-primary-600: hsl(161, 100%, 33%);--wh-primary-700: hsl(161, 100%, 31%);--wh-primary-800: hsl(161, 100%, 29%);--wh-primary-900: hsl(161, 100%, 25%);--wh-primary-950: hsl(161, 100%, 20%);--wh-secondary-50: hsl(218, 22%, 27%);--wh-secondary-100: hsl(218, 22%, 23%);--wh-secondary-200: hsl(218, 22%, 22%);--wh-secondary-300: hsl(218, 22%, 19%);--wh-secondary-400: hsl(218, 22%, 17%);--wh-secondary-500: hsl(218, 22%, 15%);--wh-secondary-600: hsl(218, 22%, 13%);--wh-secondary-700: hsl(218, 22%, 11%);--wh-secondary-800: hsl(218, 22%, 9%);--wh-secondary-900: hsl(218, 22%, 5%);--wh-secondary-950: hsl(218, 22%, 3%);--wh-gray-50: #f9fafb;--wh-gray-100: #f3f4f6;--wh-gray-200: #e5e7eb;--wh-gray-300: #d1d5db;--wh-gray-400: #9ca3af;--wh-gray-500: #6b7280;--wh-gray-600: #4b5563;--wh-gray-700: #374151;--wh-gray-800: #f2937;--wh-gray-900: #111827;--wh-gray-950: #030712;--wh-zinc-50: #fafafa;--wh-zinc-100: #f4f4f5;--wh-zinc-200: #e4e4e7;--wh-zinc-300: #d4d4d8;--wh-zinc-400: #a1aa;--wh-zinc-500: #71717a;--wh-zinc-600: #52525b;--wh-zinc-700: #3f3f46;--wh-zinc-800: #27272a;--wh-zinc-900: #18181b;--wh-zinc-950: #09090b;--wh-neutral-50: #fafafa;--wh-neutral-100: #f5f5f5;--wh-neutral-200: #e5e5e5;--wh-neutral-300: #d4d4d4;--wh-neutral-400: #a3a3a3;--wh-neutral-500: #737373;--wh-neutral-600: #525252;--wh-neutral-700: #404040;--wh-neutral-800: #262626;--wh-neutral-900: #171717;--wh-neutral-950: #0a0a0a;--wh-stone-50: #fafaf9;--wh-stone-100: #f5f5f4;--wh-stone-200: #e7e5e4;--wh-stone-300: #d6d3d1;--wh-stone-400: #a8a29e;--wh-stone-500: #78716c;--wh-stone-600: #57534e;--wh-stone-700: #44403c;--wh-stone-800: #292524;--wh-stone-900: #1c1917;--wh-stone-950: #0c0a09;--wh-red-50: #fef2f2;--wh-red-100: #fee2e2;--wh-red-200: #fecaca;--wh-red-300: #fca5a5;--wh-red-400: #f87171;--wh-red-500: #fe4444;--wh-red-600: #dc2626;--wh-red-700: #b91c1c;--wh-red-800: #991b1b;--wh-red-900: #7f1d1d;--wh-red-950: #450a0a;--wh-orange-50: #fff7ed;--wh-orange-100: #ffedd5;--wh-orange-200: #fed7aa;--wh-orange-300: #fdb74;--wh-orange-400: #fb923c;--wh-orange-500: #f97316;--wh-orange-600: #ea580c;--wh-orange-700: #c2410c;--wh-orange-800: #9a3412;--wh-orange-900: #7c2d12;--wh-orange-950: #431407;--wh-amber-50: #ffbeb;--wh-amber-100: #fef3c7;--wh-amber-200: #fde68a;--wh-amber-300: #fcfd3d;--wh-amber-400: #fbfb24;--wh-amber-500: #f59e0b;--wh-amber-600: #d97706;--wh-amber-700: #b45309;--wh-amber-800: #92400e;--wh-amber-900: #78350f;--wh-amber-950: #451a03;--wh-yellow-50: #fce8e8;--wh-yellow-100: #fe9c3c;--wh-yellow-200: #fef08a;--wh-yellow-300: #fde047;--wh-yellow-400: #facc15;--wh-yellow-500: #eab308;--wh-yellow-600: #ca8a04;--wh-yellow-700: #a16207;--wh-yellow-800: #854d0e;--wh-yellow-900: #713f12;--wh-yellow-950: #422006;--wh-lime-50: #f7fee7;--wh-lime-100: #ecfcbb;--wh-lime-200: #d9f99d;--wh-lime-300: #bef264;--wh-lime-400: #a3e635;--wh-lime-500: #84cc16;--wh-lime-600: #65a30d;--wh-lime-700: #4d7c0f;--wh-lime-800: #3f6212;--wh-lime-900: #365314;--wh-lime-950: #1a2e05;--wh-green-50: #f0fdfd;--wh-green-100: #dcfce7;--wh-green-200: #bbf7d0;--wh-green-300: #86efac;--wh-green-400: #4ade80;--wh-green-500: #22c55e;--wh-green-600: #16a34a;--wh-green-700: #15803d;--wh-green-800: #166534;--wh-green-900: #14532d;--wh-green-950: #052e16;--wh-emerald-50: #ecfd5;--wh-emerald-100: #d1fae5;--wh-emerald-200: #a7f3d0;--wh-emerald-300: #6ee7b7;--wh-emerald-400: #34d399;--wh-emerald-500: #10b981;--wh-emerald-600: #059669;--wh-emerald-700: #047857;--wh-emerald-800: #065f46;--wh-emerald-900: #064e3b;--wh-emerald-950: #022c22;--wh-teal-50: #f0fdff;--wh-teal-100: #ccfbff;--wh-teal-200: #99f6e4;--wh-teal-300: #5e4ead;--wh-teal-400: #2dd4bf;--wh-teal-500: #14b8a6;--wh-teal-600: #0d9488;--wh-teal-700: #0f766e;--wh-teal-800: #115e59;--wh-teal-900: #134e4a;--wh-teal-950: #042f2e;--wh-cyan-50: #ecfeff;--wh-cyan-100: #cffafe;--wh-cyan-200: #a5f3fc;--wh-cyan-300: #67e8f9;--wh-cyan-400: #22d3ee;--wh-cyan-500: #06b6d4;--wh-cyan-600: #0891b2;--wh-cyan-700: #0e7490;--wh-cyan-800: #155e75;--wh-cyan-900: #164e63;--wh-cyan-950: #083344;--wh-sky-50: #f0f9ff;--wh-sky-100: #e0f2fe;--wh-sky-200: #bae6fd;--wh-sky-300: #7dd3fc;--wh-sky-400: #38bfd8;--wh-sky-500: #0e5a5e;--wh-sky-600: #0284c7;--wh-sky-700: #0369a1;--wh-sky-800: #075985;--wh-sky-900: #0c4a6e;--wh-sky-950: #082f49;--wh-blue-50: #eff6ff;--wh-blue-100: #dbeafe;--wh-blue-200: #bfbdbf;--wh-blue-300: #93c5fd;--wh-blue-400: #60a5fa;--wh-blue-500: #3b82f6;--wh-blue-600: #2563eb;--wh-blue-700: #1d4ed8;--wh-blue-800: #1e40af;--wh-blue-900: #1e3a8a;--wh-blue-950: #172554;--wh-indigo-50: #eef2ff;--wh-indigo-100: #e0e7ff;--wh-indigo-200: #c7d2fe;--wh-indigo-300: #a5b4fc;--wh-indigo-400: #818cf8;--wh-indigo-500: #6366f1;--wh-indigo-600: #4f46e5;--wh-indigo-700: #4338ca;--wh-indigo-800: #3730a3;--wh-indigo-900: #312e81;--wh-indigo-950: #1e1b4b;--wh-violet-50: #f5f3ff;--wh-violet-100: #ede9fe;--wh-violet-200: #ddd6fe;--wh-violet-300: #c4b5fd;--wh-violet-400: #a78bfa;--wh-violet-500: #8b5cf6;--wh-violet-600: #7c3aed;--wh-violet-700: #6d28d9;--wh-violet-800: #5b21b6;--wh-violet-900: #4c1d95;--wh-violet-950: #2e1065;--wh-purple-50: #faf5ff;--wh-purple-100: #f3e8ff;--wh-purple-200: #e9d5ff;--wh-purple-300: #a884fe;--wh-purple-400: #c084fc;--wh-purple-500: #a855f7;--wh-purple-600: #9333ea;--wh-purple-700: #7e22ce;--wh-purple-800: #6b21a8;--wh-purple-900: #581c87;--wh-purple-950: #3b0764;--wh-fuchsia-50: #fdf4ff;--wh-fuchsia-100: #fae8ff;--wh-fuchsia-200: #f5d0fe;--wh-fuchsia-300: #f0abfc;--wh-fuchsia-400: #e879f9;--wh-fuchsia-500: #d946ef;--wh-fuchsia-600: #c026d3;--wh-fuchsia-700: #a21caf;--wh-fuchsia-800: #86198f;--wh-fuchsia-900: #000000;--wh-fuchsia-950: #000000;--wh-fuchsia-100: #000000;--wh-fuchsia-110: #000000;--wh-fuchsia-120: #000000;--wh-fuchsia-130: #000000;--wh-fuchsia-140: #000000;--wh-fuchsia-150: #000000;--wh-fuchsia-160: #000000;--wh-fuchsia-170: #000000;--wh-fuchsia-180: #000000;--wh-fuchsia-190: #000000;--wh-fuchsia-200: #000000;--wh-fuchsia-210: #000000;--wh-fuchsia-220: #000000;--wh-fuchsia-230: #000000;--wh-fuchsia-240: #000000;--wh-fuchsia-250: #000000;--wh-fuchsia-260: #000000;--wh-fuchsia-270: #000000;--wh-fuchsia-280: #000000;--wh-fuchsia-290: #000000;--wh-fuchsia-300: #000000;--wh-fuchsia-310: #000000;--wh-fuchsia-320: #000000;--wh-fuchsia-330: #000000;--wh-fuchsia-340: #000000;--wh-fuchsia-350: #000000;--wh-fuchsia-360: #000000;--wh-fuchsia-370: #000000;--wh-fuchsia-380: #000000;--wh-fuchsia-390: #000000;--wh-fuchsia-400: #000000;--wh-fuchsia-410: #000000;--wh-fuchsia-420: #000000;--wh-fuchsia-430: #000000;--wh-fuchsia-440: #000000;--wh-fuchsia-450: #000000;--wh-fuchsia-460: #000000;--wh-fuchsia-470: #000000;--wh-fuchsia-480: #000000;--wh-fuchsia-490: #000000;--wh-fuchsia-500: #000000;--wh-fuchsia-510: #000000;--wh-fuchsia-520: #000000;--wh-fuchsia-530: #000000;--wh-fuchsia-540: #000000;--wh-fuchsia-550: #000000;--wh-fuchsia-560: #000000;--wh-fuchsia-570: #000000;--wh-fuchsia-580: #000000;--wh-fuchsia-590: #000000;--wh-fuchsia-600: #000000;--wh-fuchsia-610: #000000;--wh-fuchsia-620: #000000;--wh-fuchsia-630: #000000;--wh-fuchsia-640: #000000;--wh-fuchsia-650: #000000;--wh-fuchsia-660: #000000;--wh-fuchsia-670: #000000;--wh-fuchsia-680: #000000;--wh-fuchsia-690: #000000;--wh-fuchsia-700: #000000;--wh-fuchsia-710: #000000;--wh-fuchsia-720: #000000;--wh-fuchsia-730: #000000;--wh-fuchsia-740: #000000;--wh-fuchsia-750: #000000;--wh-fuchsia-760: #000000;--wh-fuchsia-770: #000000;--wh-fuchsia-780: #000000;--wh-fuchsia-790: #000000;--wh-fuchsia-800: #000000;--wh-fuchsia-810: #000000;--wh-fuchsia-820: #000000;--wh-fuchsia-830: #000000;--wh-fuchsia-840: #000000;--wh-fuchsia-850: #000000;--wh-fuchsia-860: #000000;--wh-fuchsia-870: #000000;--wh-fuchsia-880: #000000;--wh-fuchsia-890: #000000;--wh-fuchsia-900: #000000;--wh-fuchsia-910: #000000;--wh-fuchsia-920: #000000;--wh-fuchsia-930: #000000;--wh-fuchsia-940: #000000;--wh-fuchsia-950: #000000;--wh-fuchsia-960: #000000;--wh-fuchsia-970: #000000;--wh-fuchsia-980: #000000;--wh-fuchsia-990: #000000;--wh-fuchsia-1000: #000000;--wh-fuchsia-1010: #000000;--wh-fuchsia-1020: #000000;--wh-fuchsia-1030: #000000;--wh-fuchsia-1040: #000000;--wh-fuchsia-1050: #000000;--wh-fuchsia-1060: #000000;--wh-fuchsia-1070: #000000;--wh-fuchsia-1080: #000000;--wh-fuchsia-1090: #000000;--wh-fuchsia-1100: #000000;--wh-fuchsia-1110: #000000;--wh-fuchsia-1120: #000000;--wh-fuchsia-1130: #000000;--wh-fuchsia-1140: #000000;--wh-fuchsia-1150: #000000;--wh-fuchsia-1160: #000000;--wh-fuchsia-1170: #000000;--wh-fuchsia-1180: #000000;--wh-fuchsia-1190: #000000;--wh-fuchsia-1200: #000000;--wh-fuchsia-1210: #000000;--wh-fuchsia-1220: #000000;--wh-fuchsia-1230: #000000;--wh-fuchsia-1240: #000000;--wh-fuchsia-1250: #000000;--wh-fuchsia-1260: #000000;--wh-fuchsia-1270: #000000;--wh-fuchsia-1280: #000000;--wh-fuchsia-1290: #000000;--wh-fuchsia-1300: #000000;--wh-fuchsia-1310: #000000;--wh-fuchsia-1320: #000000;--wh-fuchsia-1330: #000000;--wh-fuchsia-1340: #000000;--wh-fuchsia-1350: #000000;--wh-fuchsia-1360: #000000;--wh-fuchsia-1370: #000000;--wh-fuchsia-1380: #000000;--wh-fuchsia-1390: #000000;--wh-fuchsia-1400: #000000;--wh-fuchsia-1410: #000000;--wh-fuchsia-1420: #000000;--wh-fuchsia-1430: #000000;--wh-fuchsia-1440: #000000;--wh-fuchsia-1450: #000000;--wh-fuchsia-1460: #000000;--wh-fuchsia-1470: #000000;--wh-fuchsia-1480: #000000;--wh-fuchsia-1490: #000000;--wh-fuchsia-1500: #000000;--wh-fuchsia-1510: #000000;--wh-fuchsia-1520: #000000;--wh-fuchsia-1530: #000000;--wh-fuchsia-1540: #000000;--wh-fuchsia-1550: #000000;--wh-fuchsia-1560: #000000;--wh-fuchsia-1570: #000000;--wh-fuchsia-1580: #000000;--wh-fuchsia-1590: #000000;--wh-fuchsia-1600: #000000;--wh-fuchsia-1610: #000000;--wh-fuchsia-1620: #000000;--wh-fuchsia-1630: #000000;--wh-fuchsia-1640: #000000;--wh-fuchsia-1650: #000000;--wh-fuchsia-1660: #000000;--wh-fuchsia-1670: #000000;--wh-fuchsia-1680: #000000;--wh-fuchsia-1690: #000000;--wh-fuchsia-1700: #000000;--wh-fuchsia-1710: #000000;--wh-fuchsia-1720: #000000;--wh-fuchsia-1730: #000000;--wh-fuchsia-1740: #000000;--wh-fuchsia-1750: #000000;--wh-fuchsia-1760: #000000;--wh-fuchsia-1770: #000000;--wh-fuchsia-1780: #000000;--wh-fuchsia-1790: #000000;--wh-fuchsia-1800: #000000;--wh-fuchsia-1810: #000000;--wh-fuchsia-1820: #000000;--wh-fuchsia-1830: #000000;--wh-fuchsia-1840: #000000;--wh-fuchsia-1850: #000000;--wh-fuchsia-1860: #000000;--wh-fuchsia-1870: #000000;--wh-fuchsia-1880: #000000;--wh-fuchsia-1890: #000000;--wh-fuchsia-1900: #000000;--wh-fuchsia-1910: #000000;--wh-fuchsia-1920: #000000;--wh-fuchsia-1930: #000000;--wh-fuchsia-1940: #000000;--wh-fuchsia-1950: #000000;--wh-fuchsia-1960: #000000;--wh-fuchsia-1970: #000000;--wh-fuchsia-1980: #000000;--wh-fuchsia-1990: #000000;--wh-fuchsia-2000: #000000;--wh-fuchsia-2010: #000000;--wh-fuchsia-2020: #000000;--wh-fuchsia-2030: #000000;--wh-fuchsia-2040: #000000;--wh-fuchsia-2050: #000000;--wh-fuchsia-2060: #000000;--wh-fuchsia-2070: #000000;--wh-fuchsia-2080: #000000;--wh-fuchsia-2090: #000000;--wh-fuchsia-2100: #000000;--wh-fuchsia-2110: #000000;--wh-fuchsia-2120: #000000;--wh-fuchsia-2130: #000000;--wh-fuchsia-2140: #000000;--wh-fuchsia-2150: #000000;--wh-fuchsia-2160: #000000;--wh-fuchsia-2170: #000000;--wh-fuchsia-2180: #000000;--wh-fuchsia-2190: #000000;--wh-fuchsia-2200: #000000;--wh-fuchsia-2210: #000000;--wh-fuchsia-2220: #000000;--wh-fuchsia-2230: #000000;--wh-fuchsia-2240: #000000;--wh-fuchsia-2250: #000000;--wh-fuchsia-2260: #000000;--wh-fuchsia-2270: #000000;--wh-fuchsia-2280: #000000;--wh-fuchsia-2290: #000000;--wh-fuchsia-2300: #000000;--wh-fuchsia-2310: #000000;--wh-fuchsia-2320: #000000;--wh-fuchsia-2330: #000000;--wh-fuchsia-2340: #000000;--wh-fuchsia-2350: #000000;--wh-fuchsia-2360: #000000;--wh-fuchsia-2370: #000000;--wh-fuchsia-2380: #000000;--wh-fuchsia-2390: #000000;--wh-fuchsia-2400: #000000;--wh-fuchsia-2410: #000000;--wh-fuchsia-2420: #000000;--wh-fuchsia-2430: #000000;--wh-fuchsia-2440: #000000;--wh-fuchsia-2450: #000000;--wh-fuchsia-2460: #000000;--wh-fuchsia-2470: #000000;--wh-fuchsia-2480: #000000;--wh-fuchsia-2490: #000000;--wh-fuchsia-2500: #000000;--wh-fuchsia-2510: #000000;--wh-fuchsia-2520: #000000;--wh-fuchsia-2530: #000000;--wh-fuchsia-2540: #000000;--wh-fuchsia-2550: #000000;--wh-fuchsia-2560: #000000;--wh-fuchsia-2570: #000000;--wh-fuchsia-2580: #000000;--wh-fuchsia-2590: #000000;--wh-fuchsia-2600: #000000;--wh-fuchsia-2610: #000000;--wh-fuchsia-2620: #000000;--wh-fuchsia-2630: #000000;--wh-fuchsia-2640: #000000;--wh-fuchsia-2650: #000000;--wh-fuchsia-2660: #000000;--wh-fuchsia-2670: #000000;--wh-fuchsia-2680: #000000;--wh-fuchsia-2690: #000000;--wh-fuchsia-2700: #000000;--wh-fuchsia-2710: #000000;--wh-fuchsia-2720: #000000;--wh-fuchsia-2730: #000000;--wh-fuchsia-2740: #000000;--wh-fuchsia-2750: #000000;--wh-fuchsia-2760: #000000;--wh-fuchsia-2770: #000000;--wh-fuchsia-2780: #000000;--wh-fuchsia-2790: #000000;--wh-fuchsia-2800: #000000;--wh-fuchsia-2810: #000000;--wh-fuchsia-2820: #000000;--wh-fuchsia-2830: #000000;--wh-fuchsia-2840: #000000;--wh-fuchsia-2850: #000000;--wh-fuchsia-2860: #000000;--wh-fuchsia-2870: #000000;--wh-fuchsia-2880: #000000;--wh-fuchsia-2890: #000000;--wh-fuchsia-2900: #000000;--wh-fuchsia-2910: #000000;--wh-fuchsia-2920: #000000;--wh-fuchsia-2930: #000000;--wh-fuchsia-2940: #000000;--wh-fuchsia-2950: #000000;--wh-fuchsia-2960: #000000;--wh-fuchsia-2970: #000000;--wh-fuchsia-2980: #000000;--wh-fuchsia-2990: #000000;--wh-fuchsia-3000: #000000;--wh-fuchsia-3010: #000000;--wh-fuchsia-3020: #000000;--wh-fuchsia-3030: #000000;--wh-fuchsia-3040: #000000;--wh-fuchsia-3050: #000000;--wh-fuchsia-3060: #000000;--wh-fuchsia-3070: #000000;--wh-fuchsia-3080: #000000;--wh-fuchsia-3090: #000000;--wh-fuchsia-3100: #000000;--wh-fuchsia-3110: #000000;--wh-fuchsia-3120: #000000;--wh-fuchsia-3130: #000000;--wh-fuchsia-3140: #000000;--wh-fuchsia-3150: #000000;--wh-fuchsia-3160: #000000;--wh-fuchsia-3170: #000000;--wh-fuchsia-3180: #000000;--wh-fuchsia-3190: #000000;--wh-fuchsia-3200: #000000;--wh-fuchsia-3210: #000000;--wh-fuchsia-3220: #000000;--wh-fuchsia-3230: #000000;--wh-fuchsia-3240: #000000;--wh-fuchsia-3250: #000000;--wh-fuchsia-3260: #000000;--wh-fuchsia-3270: #000000;--wh-fuchsia-3280: #000000;--wh-fuchsia-3290: #000000;--wh-fuchsia-3300: #000000;--wh-fuchsia-3310: #000000;--wh-fuchsia-3320: #000000;--wh-fuchsia-3330: #000000;--wh-fuchsia-3340: #000000;--wh-fuchsia-3350: #000000;--wh-fuchsia-3360: #000000;--wh-fuchsia-3370: #000000;--wh-fuchsia-3380: #000000;--wh-fuchsia-3390: #000000;--wh-fuchsia-3400: #000000;--wh-fuchsia-3410: #000000;--wh-fuchsia-3420: #000000;--wh-fuchsia-3430: #000000;--wh-fuchsia-3440: #000000;--wh-fuchsia-3450: #000000;--wh-fuchsia-3460: #000000;--wh-fuchsia-3470: #000000;--wh-fuchsia-3480: #000000;--wh-fuchsia-3490: #000000;--wh-fuchsia-3500: #000000;--wh-fuchsia-3510: #000000;--wh-fuchsia-3520: #000000;--wh-fuchsia-3530: #000000;--wh-fuchsia-3540: #000000;--wh-fuchsia-3550: #000000;--wh-fuchsia-3560: #000000;--wh-fuchsia-3570: #000000;--wh-fuchsia-3580: #000000;--wh-fuchsia-3590: #000000;--wh-fuchsia-3600: #000000;--wh-fuchsia-3610: #000000;--wh-fuchsia-3620: #000000;--wh-fuchsia-3630: #000000;--wh-fuchsia-3640: #000000;--wh-fuchsia-3650: #000000;--wh-fuchsia-3660: #000000;--wh-fuchsia-3670: #000000;--wh-fuchsia-3680: #000000;--wh-fuchsia-3690: #000000;--wh-fuchsia-3700: #000000;--wh-fuchsia-3710: #000000;--wh-fuchsia-3720: #000000;--wh-fuchsia-3730: #000000;--wh-fuchsia-3740: #000000;--wh-fuchsia-3750: #000000;--wh-fuchsia-3760: #000000;--wh-fuchsia-3770: #000000;--wh-fuchsia-3780: #000000;--wh-fuchsia-3790: #000000;--wh-fuchsia-3800: #000000;--wh-fuchsia-3810: #000000;--wh-fuchsia-3820: #000000;--wh-fuchsia-3830: #000000;--wh-fuchsia-3840: #000000;--wh-fuchsia-3850: #000000;--wh-fuchsia-3860: #000000;--wh-fuchsia-3870: #000000;--wh-fuchsia-3880: #000000;--wh-fuchsia-3890: #000000;--wh-fuchsia-3900: #000000;--wh-fuchsia-3910: #000000;--wh-fuchsia-3920: #000000;--wh-fuchsia-3930: #000000;--wh-fuchsia-3940: #000000;--wh-fuchsia-3950: #000000;--wh-fuchsia-3960: #000000;--wh-fuchsia-3970: #000000;--wh-fuchsia-3980: #000000;--wh-fuchsia-3990: #000000;--wh-fuchsia-4000: #000000;--wh-fuchsia-4010: #000000;--wh-fuchsia-4020: #000000;--wh-fuchsia-4030: #000000;--wh-fuchsia-4040: #000000;--wh-fuchsia-4050: #000000;--wh-fuchsia-4060: #000000;--wh-fuchsia-4070: #000000;--wh-fuchsia-

aws English ▾

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.
851725374142

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`.
BucketsAccessRole

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.
BucketsAccessRole @ 851725374142

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

Cancel **Switch Role**

- Selected the user dropdown in the top right corner and clicked **Switch Role**.
- Entered the account ID and the role name:**BucketsAccessRole**.
- Display Change:** The user identity in the top right changed to **BucketsAccessRole**.

Testing Access:

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with navigation links: 'Amazon S3', 'Buckets', 'General purpose buckets', 'Access management and security', 'Storage management and insights', 'Account and organization settings', and 'AWS Marketplace for S3'. The main area is titled 'c185581a4806215l13009332t1w851725374142-bucket'. It has tabs for 'Objects', 'Metadata', 'Properties', 'Permissions', 'Metrics', and 'Management'. Below the tabs, there's a toolbar with buttons for 'Actions', 'Create folder', and 'Upload'. A search bar says 'Find objects by prefix'. A table lists objects: 'Image1.jpg' (selected, checked) and 'Image2.jpg' (unchecked). The table columns are Name, Type, Last modified, Size, and Storage class.

Name	Type	Last modified	Size	Storage class
Image1.jpg	jpg	December 6, 2025, 10:37:10 (UTC+01:00)	1.1 MB	Standard
Image2.jpg	jpg	December 6, 2025, 10:37:12 (UTC+01:00)	375.4 KB	Standard

1. Bucket 1: We could **download** objects.
2. Bucket 2: We could **upload** objects (Permissions allowed **s3:PutObject** on bucket2).

The screenshot shows the AWS S3 console interface. At the top, there's a green success message: "Upload succeeded" with a link to "Files and folders table". Below it, a modal window titled "Upload: status" contains a note: "After you navigate away from this page, the following information is no longer available." The main area is titled "Summary" and shows the destination bucket: "s3://c185581a4806215l13009332t1w851725374142-bucket2-kzep4yvmu8ht". It details one succeeded upload: "1 file, 375.4 KB (100.00%)". There's also a failed section with "0 files, 0 B (0%)". Below this, there are tabs for "Files and folders" (which is selected) and "Configuration". The "Files and folders" tab displays a table with one row: "Image2.jpg" (image/jpeg, 375.4 KB, Status: Succeeded). The footer of the browser window includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

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

Analysis:

When we assumed the role, we temporarily gave up the devuser permissions and adopted the **BucketsAccessRole** permissions. This role had a specific policy allowing read/write access to these specific buckets, which devuser did not have natively.

```

1  {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Action": [
6                 "s3:GetObject",
7                 "s3:ListObjects",
8                 "s3:ListBucket"
9             ],
10            "Resource": [
11                "arn:aws:s3:::c185581a48062151130093321bd851725374142-bucket1-z04qm4kqh6ml/*",
12                "arn:aws:s3:::c185581a48062151130093321bd851725374142-bucket1-z04qm4kqh6ml/*"
13            ],
14            "Effect": "Allow"
15        }
16    ]
17 }

```

Policy editor

Visual **JSON** Actions

Edit statement Remove

Add actions

Choose a service

Included **S3**

Available

- AI Operations
- AMP
- API Gateway
- API Gateway V2
- ARC Region switch
- ARC Zonal Shift
- ASC

Add a resource **Add**

Add a condition (optional) **Add**

9748 of 10031 characters remaining

CloudShell Feedback Console Mobile App

Task 6: Understanding Resource -Based Policies

Action:

- While using the bucket -access-role, we navigated to **Bucket 2 -> Permissions** tab.
- Viewed the **Bucket Policy** .

Policy Analysis:

This is a Resource-Based Policy. Unlike the identity policy attached to a user, this policy is attached directly to the S3 bucket.

- It explicitly listed the **BucketsAccessRole** as a Principal.
- This confirms that access can be granted either by the user's IAM policy OR by the resource's policy (if in the same account), or requires both (if cross-account, though in this lab it was primarily about how the role was authorized).

The screenshot shows the AWS S3 Bucket policy configuration page. At the top, there are navigation links for 'Amazon S3' and 'Buckets'. The current view is for a specific bucket, indicated by the URL 'c185581a4806215l13009332t1w851725374142-bucket2-kzep4yvmu8ht'. On the right side of the header, the account ID '8517-2537-4142' and the role name 'BucketsAccessRole @ 851725374142' are displayed. Below the header, the title 'Bucket policy' is shown, along with 'Edit' and 'Delete' buttons. A note states: '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.' A 'Learn more' link is provided. The main content area displays the JSON policy code:

```
{  
    "Sid": "S3Write",  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "arn:aws:iam::851725374142:role/BucketsAccessRole"  
    },  
    "Action": [  
        "s3:GetObject",  
        "s3:PutObject"  
    ],  
    "Resource": "arn:aws:s3:::c185581a4806215l13009332t1w851725374142-bucket2-kzep4yvmu8ht/*"  
},  
{  
    "Sid": "ListBucket",  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "arn:aws:iam::851725374142:role/BucketsAccessRole"  
    },  
    "Action": "s3>ListBucket",  
    "Resource": "arn:aws:s3:::c185581a4806215l13009332t1w851725374142-bucket2-kzep4yvmu8ht"  
},
```

On the right side of the JSON code, there is a 'Copy' button. Below the JSON code, the section 'Object Ownership' is visible, which includes a note about controlling ownership of objects from other AWS accounts and the use of access control lists (ACLs). There are 'Edit' and 'Delete' buttons for this section as well. At the bottom of the page, there are links for 'CloudShell', 'Feedback', 'Privacy', 'Terms', and 'Cookie preferences'.

3. Challenge Task: Uploading to Bucket 3

Objective: Upload Image2.jpg to bucket3.

Attempt 1: As 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	Failed
s3://c185581a4806215l13009332t1w851725374142-bucket3-nq4cmfzgodfh	0 files, 0 B (0%)	1 file, 375.4 KB (100.00%)

Files and folders **Configuration**

Files and folders (1 total, 375.4 KB)

Name	Folder	Type	Size	Status	Error
Image2.jpg	-	image/jpeg	375.4 KB	Failed	Access denied

- Result: Failed. No write permissions and devuser can't view bucket policy.

"arn:aws:s3:::c185581a4806215l13009332t1w851725374142-bucket3-nq4cmfzgodfh" because no identity-based policy allows the s3:GetBucketPublicAccessBlock action

Bucket policy

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](#).

Object Ownership

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](#).

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

CloudShell Feedback Console Mobile App Privacy Terms Cookie preferences

Attempt 2: As BucketAccessRole

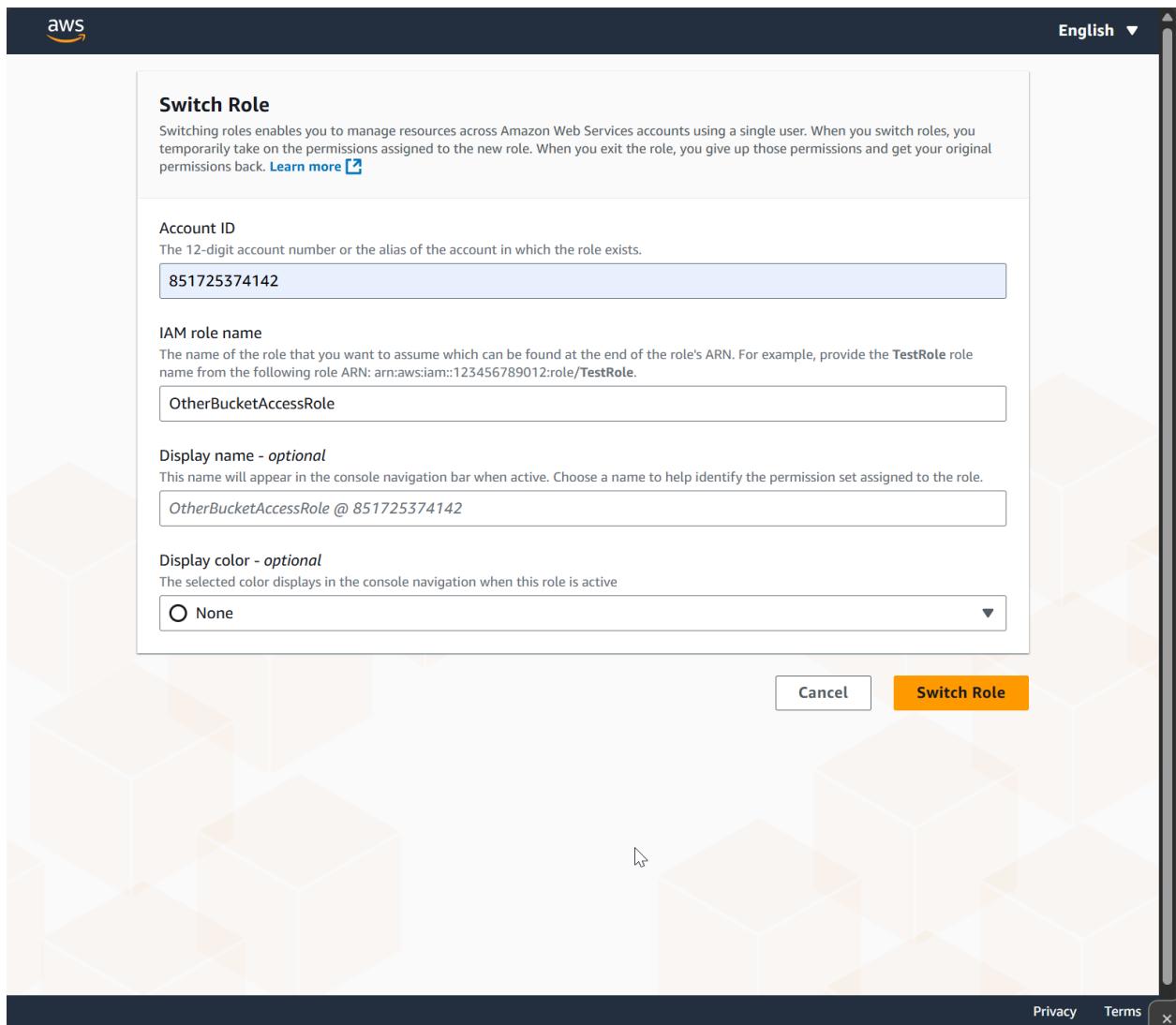
The screenshot shows the AWS S3 console with a bucket named 'c185581a4806215l13009332t1w851725374142-bucket3-nq4cmfzgodfh'. The 'Permissions' tab is active. A red box highlights a message: 'Insufficient permissions to list objects. After you or your AWS administrator has updated your permissions to allow the s3>ListBucket action, refresh the page. Learn more.'

- Result: Failed. The role's policy did not include permissions for bucket3 but we can read the bucket policy .

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "S3Write",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::851725374142:role/OtherBucketAccessRole"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::c185581a4806215l13009332t1w851725374142-bucket3-nq4cmfzgodfh/*"
    },
    {
      "Sid": "ListBucket",
      "Effect": "Allow",
      "Principal": "*"
    }
  ]
}
```

Solution:

1. We identified a second role available in the account: **OtherBucketAccessRole**.
2. We used the **Switch Role** feature again to switch from **BucketsAccessRole** to **OtherBucketAccessRole**.



3. Navigated to bucket3.
4. Clicked **Upload**, selected Image2.jpg, and submitted.
5. Result: Success .

Explanation:

The **OtherBucketAccessRole** had a policy that specifically allowed **s3:PutObject** on the **bucket3** resource. By assuming this specific role, we gained the necessary credentials to complete the challenge.

aws | Search [Alt+S] | United States (N. Virginia) | Account ID: 8517-2537-4142
OtherBucketAccessRole @ 851725374142

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	
Destination	Succeeded 1 file, 375.4 KB (100.00%)
s3://c185581a4806215l13009332t1w851725374142-bucket3-nq4cmfzgodfh	Failed 0 files, 0 B (0%)

Files and folders Configuration

Files and folders (1 total, 375.4 KB)

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

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

Analysis of OtherBucketAccessRole Policy

Step 1 **Modify permissions in GrantBucket1Access**

Step 2 Review and save

Modify permissions in GrantBucket1Access Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```

1 Version: "2012-10-17",
2 Statement: [
3   {
4     Action: [
5       "s3:GetObject",
6       "s3:ListObjects",
7       "s3:PutObject",
8       "s3:ListBucket"
9     ],
10    Resource: [
11      "arn:aws:s3:::c185581a4806215l13009332t1w851725374142-bucket3-nq4cmfzgodfh",
12      "arn:aws:s3:::c185581a4806215l13009332t1w851725374142-bucket3-nq4cmfzgodfh/*"
13    ],
14    Effect: "Allow"
15  }
16 ]
17
18
  
```

Visual JSON Actions ▾

Edit statement Remove

Add actions

Choose a service

Included S3

Available AI Operations AMP API Gateway

Inferred Policy Analysis:

Component	Observation/Inference
Principal	The devuser was allowed to assume this role (defined in the role's Trust Policy).
Allowed Actions (S3)	include <code>s3:PutObject</code> and <code>s3:GetObject</code> and <code>s3>ListBucket</code> .
Resource Scope	The permissions were explicitly scoped to <code>bucket3</code> (<code>arn:aws:s3:::c185581a4806215l13009332t1w851725374142-bucket3-nq4cmfzgodfh</code>).
Key Difference	Unlike the <code>BucketsAccessRole</code> , this role granted the specific write permissions necessary to interact with <code>bucket3</code> , confirming the principle of least privilege where each role serves a targeted function.

This analysis confirms that the role's identity policy was the key mechanism enabling the successful upload to the restricted `bucket3`.

4. Conclusion

In this lab, we successfully demonstrated the flexibility of AWS access control.

1. **Identity Policies** attached to devuser provided basic entry access but restricted powerful actions like creating EC2 instances or writing to arbitrary buckets.
2. **IAM Roles** allowed us to elevate permissions temporarily to perform specific tasks (managing specific buckets) without permanently granting those privileges to the user.
3. **Resource Policies** on the S3 buckets acted as a second layer of access control, defining exactly which principals (users/roles) could interact with the bucket data.