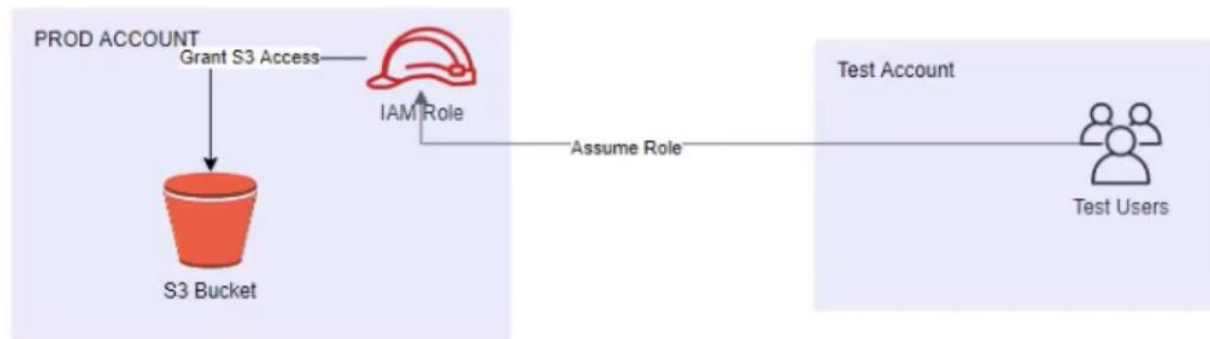


How can I provide cross-account access to objects that are in Amazon S3 buckets? Using AWS Console?



AWS:

Account1

The screenshot shows the AWS S3 console interface. The left sidebar contains navigation options under 'Amazon S3', including Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, Access analyzer for S3, Block Public Access settings for this account, Storage Lens, Dashboards, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3. The main content area displays an 'Account snapshot' section with a 'View Storage Lens dashboard' button. Below this is the 'Buckets (2)' section, which includes a search bar and a table of buckets.

Name	AWS Region	Access	Creation date
<input type="radio"/> crossaccount-s3-bucket-1	US East (N. Virginia) us-east-1	Objects can be public	February 16, 2022, 22:44:27 (UTC+05:30)
<input type="radio"/> crossaccount-s3-bucket-2	US East (N. Virginia) us-east-1	Objects can be public	February 16, 2022, 23:19:25 (UTC+05:30)

mx.massmutual.com x YouTube x How to enable Cross Acco... x S3 Management Console x IAM Management Console x IAM Management Console x +

console.aws.amazon.com/iamv2/home#/roles/details/cross-account-role?section=permissions

Search for services, features, blogs, docs, and more [Alt+S]

Global shivani

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

cross-account-role

Delete Edit

Summary

Creation date February 16, 2022, 22:56 (UTC+05:30)	ARN arn:aws:iam::738087856818:role/cross-account-role	Link to switch roles in console https://signin.aws.amazon.com/switchrole?roleName=cross-account-role&account=archana-access	Instance profile ARN arn:aws:iam::738087856818:instance-profile/cross-account-role
Last activity None	Maximum session duration 1 hour		

Permissions Trust relationships Tags Access Advisor Revoke sessions

Permissions policies (1)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

Policy name	Type	Description
<input type="checkbox"/> cross-account-policy	Customer managed	

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

mx.massmutual.com x YouTube x How to enable Cross Acco... x S3 Management Console x IAM Management Console x IAM Management Console x +

console.aws.amazon.com/iam/home#/policies/arn:aws:iam::738087856818:policy/cross-account-policy\$serviceLevelSummary

Search for services, features, blogs, docs, and more [Alt+S]

Global shivani

Identity and Access Management (IAM)

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

cross-account-policy

Delete policy

Summary

Policy ARN [arn:aws:iam::738087856818:policy/cross-account-policy](#)

Description

Permissions Policy usage Tags Policy versions Access Advisor

Policy summary {} JSON Edit policy

Filter

Service	Access level	Resource	Request condition
Allow (1 of 315 services) Show remaining 314			
S3	Limited: List, Write	Multiple	None

cross-account-role

Summary

Creation date February 16, 2022, 22:56 (UTC+05:30)	ARN arn:aws:iam:738087856818:role/cross-account-role	Link to switch roles in console https://signin.aws.amazon.com/switchrole?roleName=cross-account-role&account=archana-access	Instance profile ARN arn:aws:iam:738087856818:instance-profile/cross-account-role
Last activity None	Maximum session duration 1 hour		

Permissions **Trust relationships** **Tags** **Access Advisor** **Revoke sessions**

Trusted entities
Entities that can assume this role under specified conditions.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam:293955714039:root"  
8       },  
9       "Action": "sts:AssumeRole"  
10    }  
11  ]  
12 }
```

Account2:

cross-user

Summary

User ARN: [arn:aws:iam:293955714039:user/cross-user](#)

Path: /

Creation time: 2022-02-16 22:48 UTC+0530

Permissions **Groups** **Tags** **Security credentials** **Access Advisor**

Permissions policies (1 policy applied)

[Add permissions](#) [Add inline policy](#)

Policy name	Policy type
Attached directly	
user-assume-policy	Managed policy

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

S3 Management Console x IAM Management Console x New Tab x +

← → ↻ https://console.aws.amazon.com/iam/home#/policies/arn:aws:iam::293955714039:policy/user-assume-policy\$jsonEditor ☆ 🔒 [Alt+S] Global pokala vaibhaw

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles
- Policies**
- Identity providers
- Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Policies > user-assume-policy

Summary

Policy ARN: [arn:aws:iam::293955714039:policy/user-assume-policy](#)

Description

Permissions Policy usage Tags Policy versions Access Advisor

Policy summary {} JSON Edit policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Resource": "arn:aws:iam::738887856818:role/cross-account-role"
8     }
9   ]
10 }
```

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

S3 Management Console x IAM Management Console x New Tab x +

← → ↻ https://s3.console.aws.amazon.com/s3/home?region=us-east-1®ion=us-east-1 ☆ 🔒 IAM Global cross-account-role @ 738887856818

Amazon S3

- Buckets**
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- Access analyzer for S3
- Block Public Access settings for this account
- Storage Lens**
 - Dashboards
 - AWS Organizations settings
- Feature spotlight
- AWS Marketplace for S3

We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose **Provide feedback**.

Amazon S3

Account snapshot View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

Buckets (2) Info Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

	Name	AWS Region	Creation date
<input type="radio"/>	crossaccount-s3-bucket-1	US East (N. Virginia) us-east-1	February 16, 2022, 22:44:27 (UTC+05:30)
<input type="radio"/>	crossaccount-s3-bucket-2	US East (N. Virginia) us-east-1	February 16, 2022, 23:19:25 (UTC+05:30)

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Terraform:

The screenshot shows the Amazon S3 console interface. The left sidebar contains navigation options like Buckets, Access Points, and Storage Lens. The main content area displays the details for the bucket 'cross-account-bucket-user1890'. Under the 'Objects' tab, there is a table with one object: 'object-uploaded-via-prod-creds', which is 14.0 B in size and was last modified on February 22, 2022, at 19:02:04 (UTC+05:30). The console also shows a search bar for objects and various action buttons like 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'.

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options like Identity and Access Management (IAM), Access management, and Access reports. The main content area displays the details for the role 'EKS-Role1'. Under the 'Permissions' tab, there is a table with one policy: 'EKS-Policy1', which is a Customer inline policy. The console also shows a search bar for policies and various action buttons like 'Simulate', 'Remove', and 'Add permissions'. The summary section provides details about the role's creation date, ARN, last activity, and maximum session duration.

mx.massmutual.com x terraform-aws-e2-instanc... x S3 bucket with cross-accou... x IAM Management Console x How to enable Cross Acco... x aws_iam_user_policy | Reso... x +

console.aws.amazon.com/iam/home#/roles/EKS-Rol1\$jsonEditor?policyName=EKS-Policy1&step=edit

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global shivani

Edit EKS-Policy1

1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor JSON Import managed policy

```
1 {
2   "Statement": [
3     {
4       "Action": [
5         "s3:PutObject",
6         "s3:CreateBucket",
7         "s3:ListBucket",
8         "s3:ListAllMyBuckets",
9         "s3:DeleteObject",
10        "s3:DeleteBucket"
11      ],
12      "Effect": "Allow",
13      "Resource": "*",
14      "Sid": "VisualEditor0"
15    }
16  ],
17  "Version": "2012-10-17"
18 }
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

IAM Management Console x New Tab x +

https://console.aws.amazon.com/iam/home#/users/EKS-User1

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global pokala vaibhaw

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users**
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analizers
 - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Users > EKS-User1

Summary

Delete user ⓘ

User ARN: arn:aws:iam:293955714039:user:EKS-User1 ⓘ

Path: /

Creation time: 2022-02-22 17:54 UTC+0530

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (1 policy applied)

Add permissions Add inline policy

Policy name	Policy type
Attached directly	
EKS-Policy1	Inline policy

Policy summary {} JSON Edit policy Simulate policy

```
1 {
2   "Statement": [
3     {
4       "Action": "sts:AssumeRole",
5       "Effect": "Allow",
6       "Resource": "arn:aws:iam:738887856818:role/EKS-Rol1",
7       "Sid": "VisualEditor0"
8     }
9   ]
10 }
```

Amazon S3 Management Console - IAM User: EKS-User1 @ 2939-5571-4039

Account ID: 2939-5571-4039
IAM user: EKS-User1

Account
Organization
Service Quotas
Billing Dashboard
Security credentials

Role history
EKS-Role1 @ 738087856818
cross-account-role @ 73808785...

Switch role Sign out

Amazon S3

Account snapshot
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

Buckets (0) Info
Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Name AWS Region Creation date

You don't have permissions to list buckets
After you or your AWS administrator have updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. [Learn more about identity and access management in Amazon S3](#)

cross-account-bucket-user1890 - IAM Role: EKS-Role1 @ 738087856818

Currently active as: EKS-Role1
Account ID: 73808-8785-6818

Account
Organization
Service Quotas
Billing Dashboard

Signed in as: EKS-User1
Account ID: 2939-5571-4039

Switch back

Role history
EKS-Role1 @ 738087856818
cross-account-role @ 73808785...

Switch role Sign out

Amazon S3 > cross-account-bucket-user1890

cross-account-bucket-user1890 Info

Objects Properties Permissions Metrics Management Access Points

Objects (1)
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your bucket, you must grant them permissions. [Learn more](#)

Copy S3 URI Copy URL Download Open Delete Actions Create

Find objects by prefix Show versions

Name	Type	Last modified
object-uploaded-via-prod-creds	-	February 22, 2022, 19:02:04 (UTC+05:30)

The screenshot displays the Amazon S3 console for a bucket named 'cross-account-bucket-user1890'. The 'Objects' tab is active, showing a list of objects. A single object, 'object-uploaded-via-prod-creds', is listed with a size of 14.0 B and a storage class of 'Standard'. The object was last modified on February 22, 2022, at 19:02:04 (UTC+05:30). The console interface includes a left sidebar with navigation options like Buckets, Access Points, and Storage Lens. The top navigation bar shows the AWS logo and a search bar. The bottom status bar indicates the page is from 2022 and includes links for Privacy, Terms, and Cookie preferences.

Name	Type	Last modified	Size	Storage class
object-uploaded-via-prod-creds	-	February 22, 2022, 19:02:04 (UTC+05:30)	14.0 B	Standard