



Access permission to another aws account

FIRST METHOD \Rightarrow S3

Amazon S3

Account snapshot
Last updated: Jul 14, 2021 by Storage Lens. Metrics are generated every 24 hours. [Learn more](#)

View Storage Lens dashboard

Total storage	Object count	Avg. object size	You can enable advanced metrics in the "default-account-dashboard" configuration.
27.9 KB	10	2.8 KB	

Buckets (2) [Info](#)

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

Find buckets by name

Name	AWS Region	Access	Creation date
different.account	US East (N. Virginia) us-east-1	Bucket and objects not public	July 18, 2021, 21:32:40 (UTC-04:00)
benimbucketim-all	US East (N. Virginia) us-east-1	Objects can be public	July 18, 2021, 21:50:50 (UTC-04:00)

Amazon S3 > different.account

different.account [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 this bucket.

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#)

Find objects by prefix

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	ec2.json	json

Access control list (ACL) [Learn more](#)

Grant basic read/write permissions to other AWS accounts.

Public access is blocked because Block Public Access settings are turned on for this bucket.
To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

The console displays combined access grants for duplicate grantees.
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee: [Objects](#) | [Bucket ACL](#)

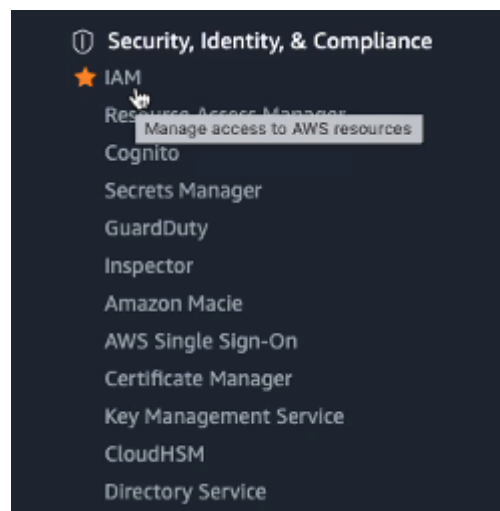
Access for other AWS accounts

Grantee	Objects	Bucket ACL	
<input type="text" value="Enter canonical ID"/> <input type="text" value="aaaaa"/> <input type="button" value="Add grantee"/>	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write	<input type="button" value="Remove"/>

Access for other AWS accounts

Grantee	Objects	Bucket ACL	
<input type="text" value="test@gmail.com"/> <input type="button" value="Add grantee"/>	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write	<input type="button" value="Remove"/>

SECOND METHOD \Rightarrow IAM ROLE



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)

🔍 Search IAM

IAM > Users

IAM users (2) [info](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.



Delete

Add users

🔍 Search

< 1 > ⓘ

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Console last sign-in	Access key age	Access key last used
--------------------------	-----------	--------	---------------	-----	----------------------	----------------	----------------------

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type* ☒ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ☒ Autogenerated password
☐ Custom password

Require password reset ☒ User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

Cancel

Next: Permissions

Add user

1 2 3 4 5

Set permissions



Add user to group



Copy permissions from existing user



Attach existing policies directly

Create policy



Filter policies <input type="text" value="s3"/>		Showing 6 results	
	Policy name	Type	Used as
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed	None
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	Permissions policy (3)
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS managed	None
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS managed	None

Add user

1 2 3 4 5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Name"/>	<input type="text" value="Test"/>	✕
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 49 more tags.

[Cancel](#)

[Previous](#)

[Next: Review](#)

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	test
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonS3FullAccess
Managed policy	IAMUserChangePassword

Tags

The new user will receive the following tag

Key	Value
Name	Test

Cancel

Previous

Create user

Add user

1 2 3 4 5

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://ali-lam.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Password	Email login instructions
▶	test	AKIA5JQIQMXIORX4T7KC	***** Show	***** Show	Send email