

ACCESS S3 OBJECTS FROM EC2 INSTANCE

➤ Create S3 bucket By giving name.

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

Amazon S3 / Buckets / Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type [Info](#)

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

sais3

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

- Now S3 bucket is successfully created.

General purpose buckets | Directory buckets

General purpose buckets (1) [Info](#) [All AWS Regions](#)

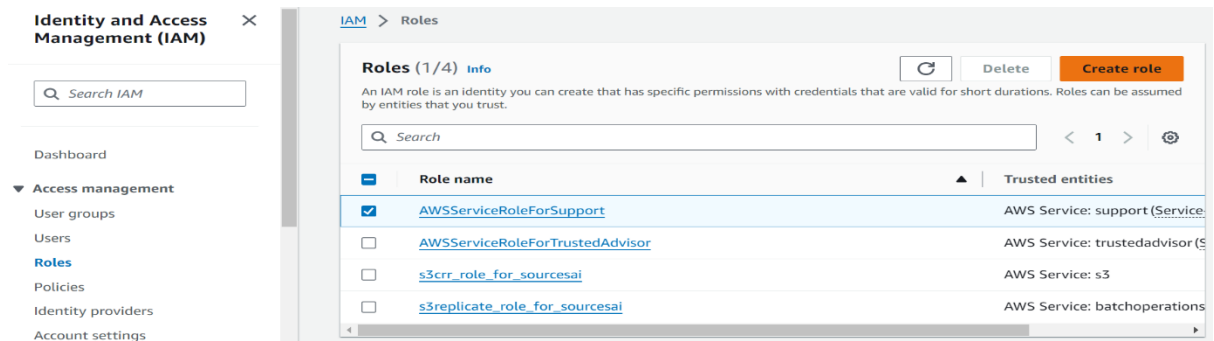
[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

< 1 > [Settings](#)

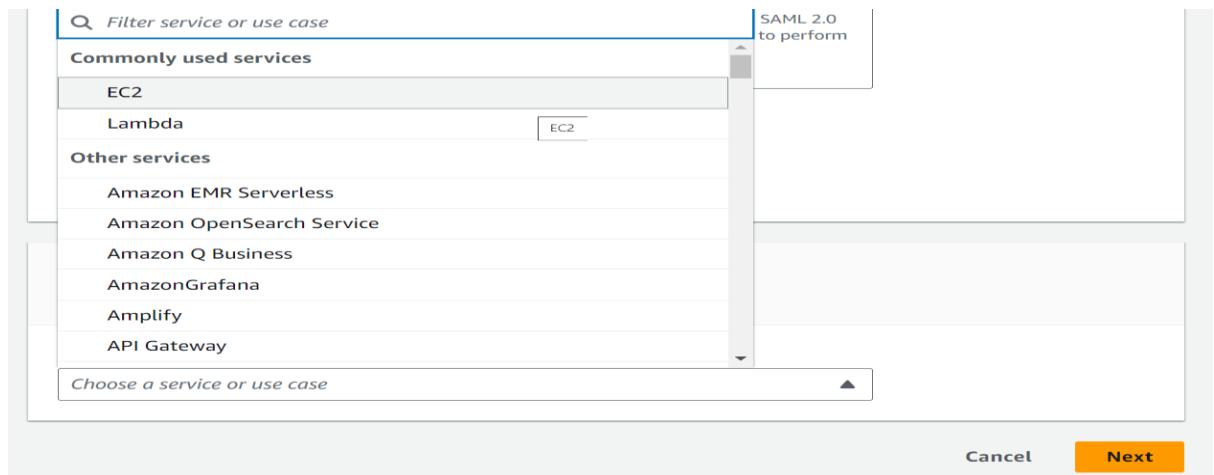
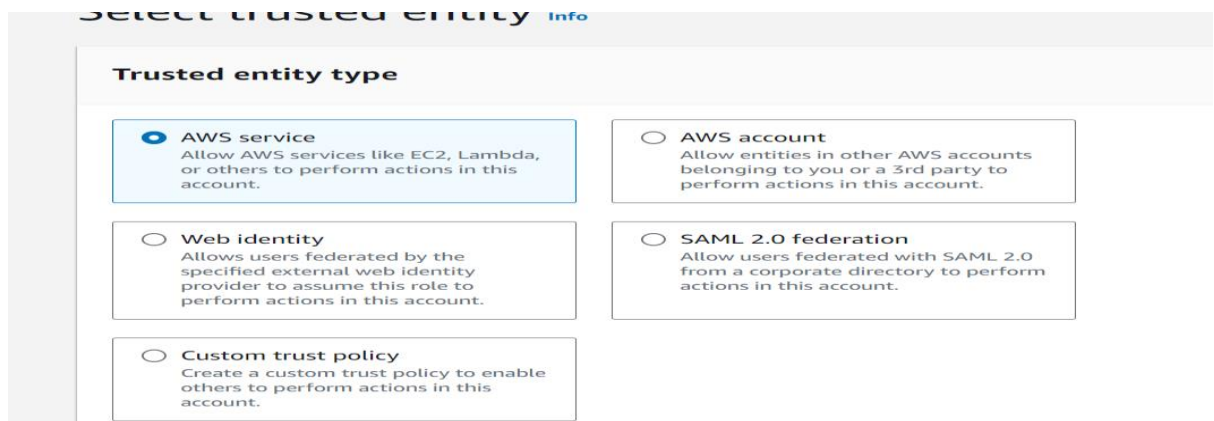
Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/> sais3	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 11, 2024, 10:34:54 (UTC+05:30)

➤ Create an IAM instance profile that grants access to Amazon S3.

- Goto Identity Access Management (IAM) console.
- In the navigation panel, under Access management, choose Roles.
- Choose Create role.



- Under Trusted entity type, choose AWS service, and then choose EC2.
- Choose Next.



- Create a custom policy that provides the minimum required permissions to access your S3 bucket.
- **Note:** It's a security best practice to create a policy with the minimum required permissions. However, to allow EC2 access to all your S3 buckets, use the AmazonS3ReadOnlyAccess or AmazonS3FullAccess managed IAM policy.
- Choose Next.

Add permissions [Info](#)

Permissions policies (949) [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type

All types 1 match

<input type="checkbox"/>	Policy name Info	Type	Description
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...

[Set permissions boundary - optional](#)

[Cancel](#) [Previous](#) [Next](#)

- Enter a role name, and then choose Create role.

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+=,.,@-_' characters.

Description
Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,.,@-/\[()!#\$%&^*()';:""

[View role](#)

Roles (1/5) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

[Delete](#) [Create role](#)

<input type="checkbox"/>	Role name	Trusted entities
<input checked="" type="checkbox"/>	s3accessstoec2	AWS Service: ec2
<input type="checkbox"/>	s3crr_role_for_sourcesai	AWS Service: s3
<input type="checkbox"/>	s3replicate_role_for_sourcesai	AWS Service: batchoperations

➤ Attach IAM profile to EC2 instance.

- Open the Amazon EC2 console.
- In the navigation panel, launch instance.

[EC2](#) > [Instances](#) > Launch an instance

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

[Add additional tags](#)

Instances (1) [Info](#)

Last updated less than a minute ago [Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

[All states](#) [< 1 >](#) [Settings](#)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/>	sai	i-069fdadf5ff2d6ca8	Running	t2.micro	Initializing	View alarm

- Select the instance that you want to attach the IAM role.
- Choose the Actions tab, and then choose Security.

Instances (1/1) [Info](#)

Last updated less than a minute ago [Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

[All states](#) [< 1 >](#) [Settings](#)

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
<input checked="" type="checkbox"/>	sai	i-069fdadf5ff2d6ca8	Running	t2.micro	Initializing	View alarm

i-069fdadf5ff2d6ca8 (sai)

- Change security groups
- Get Windows password
- Modify IAM role

Actions

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security**
- Image and templates
- Monitor and troubleshoot

- Choose Modify IAM role and update it.

[EC2](#) > [Instances](#) > [i-069fdadf5ff2d6ca8](#) > [Modify IAM role](#)

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID
i-069fdadf5ff2d6ca8 (sai)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

s3accessstoec2 [Refresh](#) [Create new IAM role](#)

[Cancel](#) [Update IAM role](#)

- Select the IAM role, and then choose Save. The IAM role is assigned to your EC2 instance.
- **Verify access to S3 buckets.**
- Select EC2 instance and connect it to web.

i-069fdadf5ff2d6ca8 (sai)

Connection Type

☒ **Connect using EC2 Instance Connect**
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

☐ **Connect using EC2 Instance Connect Endpoint**
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address
54.205.150.2

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

ec2-user

Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

[Cancel](#) [Connect](#)

Note: If you receive errors when you run AWS Command Line Interface (AWS CLI) commands, then see [Troubleshoot AWS CLI errors](#). Also, make sure that you're using the most recent AWS CLI version.

- Install the AWS CLI on your EC2 instance.
- Run the following commands to verify access to your S3 buckets:
 - ✓ `Aws s3 ls`

[illegible]

- ✓ Nano sample.txt – opens the GNU nano 5.8 interface. – for saving the text message use ctrl O enter ctrl x.

```
GNU nano 5.8
this is s3 to ec2 connection
```

- ✓ ls
- ✓ aws s3 cp sample.txt s3://name of bucket/samplefromec2.txt

```

Last login: Wed Sep 11 05:21:18 2024 from 18.206.107.28
[ec2-user@ip-172-31-94-91 ~]$ aws s3 ls
2024-09-11 05:04:54 saiss3
[ec2-user@ip-172-31-94-91 ~]$ aws --version
aws-cli/2.15.30 Python/3.9.16 Linux/6.1.106-116.188.amzn2023.x86_64 source/x86_64.amzn.2023 prompt/off
[ec2-user@ip-172-31-94-91 ~]$ pwd
/home/ec2-user
[ec2-user@ip-172-31-94-91 ~]$ nano sample.txt
[ec2-user@ip-172-31-94-91 ~]$ ls
sample.txt  sample.txt.save
[ec2-user@ip-172-31-94-91 ~]$ aws s3 cp sample.txt s3://name of bucket/samplefromec2.txt

Unknown options: of,bucket/samplefromec2.txt
[ec2-user@ip-172-31-94-91 ~]$ nano sample.txt
[ec2-user@ip-172-31-94-91 ~]$ ls
sample.txt  sample.txt.save
[ec2-user@ip-172-31-94-91 ~]$ aws s3 cp sample.txt s3://saiss3/samplefromec2.txt
upload: ./sample.txt to s3://saiss3/samplefromec2.txt

```