

5. Create a new IAM role and policy to access only S3 bucket from AWS EC2 instance display the output using AWS S3 cli

AWS console:

The screenshot displays the AWS Management Console interface. The top navigation bar shows the user is logged in as 'shivani' in the 'us-east-2' region. The left sidebar contains navigation links for various AWS services, including EC2, S3, IAM, and CloudWatch.

The main content area is divided into two sections. The top section, titled 'Instances (1/1) Info', shows a table with one instance: 'i-00be39e685a70ffea'. The instance is in the 'Running' state, using the 't2.micro' instance type, and has '2/2 checks passed'. Below this table, the 'Instance: i-00be39e685a70ffea' details are shown, including its Public IPv4 address (3.17.64.90), Private IPv4 addresses (172.31.36.156), and Public IPv4 DNS (ec2-3-17-64-90.us-east-2.compute.amazonaws.com).

The bottom section, titled 'Amazon S3', shows a notification that a bucket named 'access3toec2' has been successfully created. Below the notification, the 'Buckets (1) Info' section shows a table with one bucket: 'access3toec2'. The bucket is in the 'US East (Ohio) us-east-2' region, has 'Objects can be public' access, and was created on 'January 24, 2022, 13:52:22 (UTC+05:30)'.

mx.massmutual.com x Instances | EC2 Management Co x S3 Management Console x IAM Management Console x Connect S3 Bucket to EC2 Instan x +

console.aws.amazon.com/iam/home#/roles/EC2-TO-S3

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)

Search IAM

New feature to generate a policy based on CloudTrail events.
AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this role.

Roles > EC2-TO-S3 Delete role

Summary

Role ARN	arn:aws:iam:738087856818:role/EC2-TO-S3
Role description	Allows EC2 instances to call access s3 bucket on your behalf. Edit
Instance Profile ARNs	arn:aws:iam:738087856818:instance-profile/EC2-TO-S3
Path	/
Creation time	2022-01-24 13:31 UTC+0530
Last activity	Not accessed in the tracking period
Maximum session duration	1 hour Edit

Permissions Trust relationships Tags (1) Access Advisor Revoke sessions

Permissions policies (1 policy applied)

[Attach policies](#) [Add inline policy](#)

Policy name	Policy type
AmazonS3FullAccess	AWS managed policy

Permissions boundaries (not set)

Feedback English (US)

Type here to search

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

25°C Sunny 13:54 24-01-2022

```
ec2-user@ip-172-31-36-156~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
  
Amazon Linux 2 AMI  
  
https://aws.amazon.com/amazon-linux-2/  
11 package(s) needed for security, out of 15 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-31-36-156 ~]$ aws s3 ls  
2022-01-24 08:22:22 accesss3toec2  
[ec2-user@ip-172-31-36-156 ~]$ ls  
[ec2-user@ip-172-31-36-156 ~]$ touch file1.txt  
[ec2-user@ip-172-31-36-156 ~]$ vi file1.txt  
[ec2-user@ip-172-31-36-156 ~]$ ls  
file1.txt  
[ec2-user@ip-172-31-36-156 ~]$ aws s3 cp file1.txt s3://accesss3toec2  
upload: ./file1.txt to s3://accesss3toec2/file1.txt  
[ec2-user@ip-172-31-36-156 ~]$ touch file2.txt  
[ec2-user@ip-172-31-36-156 ~]$ vi file2.txt  
[ec2-user@ip-172-31-36-156 ~]$ ls  
file1.txt file2.txt  
[ec2-user@ip-172-31-36-156 ~]$ ^C  
[ec2-user@ip-172-31-36-156 ~]$ aws s3 cp file2.txt s3://accesss3toec2  
upload: ./file2.txt to s3://accesss3toec2/file2.txt  
[ec2-user@ip-172-31-36-156 ~]$
```

Type here to search

25°C Sunny 14:00 24-01-2022

mx.massmutual.com

Instances | EC2 Management Console

access3toec2 - S3 bucket

IAM Management Console

Connect S3 Bucket to EC2

Copy files from EC2 to S3

s3.console.aws.amazon.com/s3/buckets/access3toec2?region=us-east-2&tab=objects

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

Globalshivani

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

Amazon S3 > access3toec2

access3toec2

ObjectsPropertiesPermissionsMetricsManagementAccess Points

Objects (2)

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 objects, you'll need to explicitly grant them permissions. [Learn more](#)

Refresh

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	file1.txt	txt	January 24, 2022, 13:58:49 (UTC+05:30)	24.0 B	Standard
<input type="checkbox"/>	file2.txt	txt	January 24, 2022, 14:00:34 (UTC+05:30)	207.0 B	Standard

FeedbackEnglish (US)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. PrivacyTermsCookie preferences

Type here to search

25°C Sunny

14:00

24-01-2022