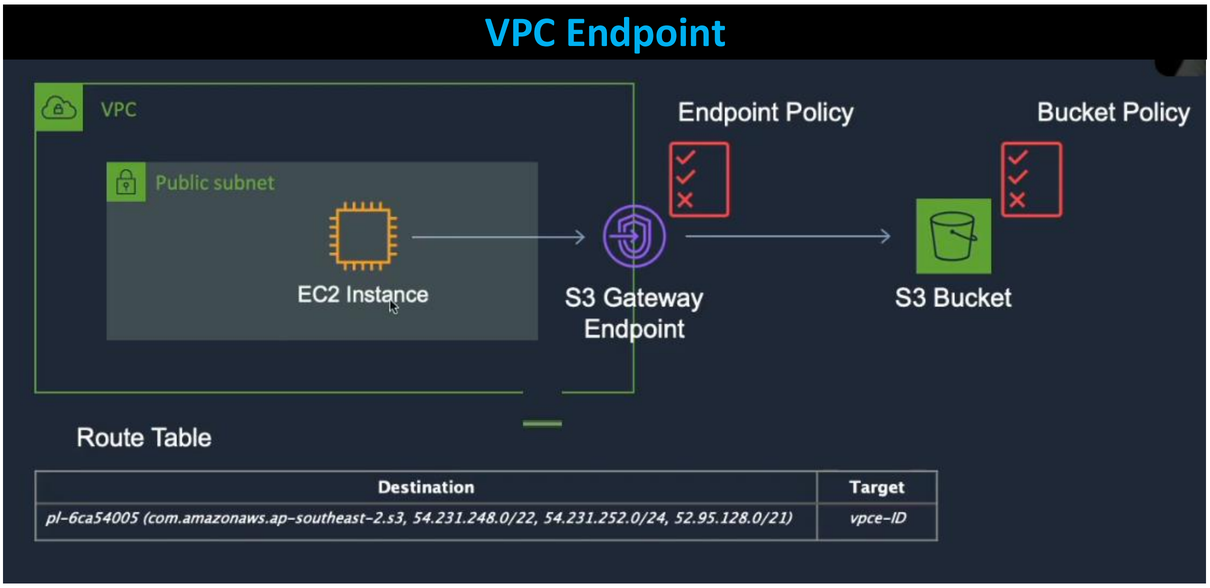
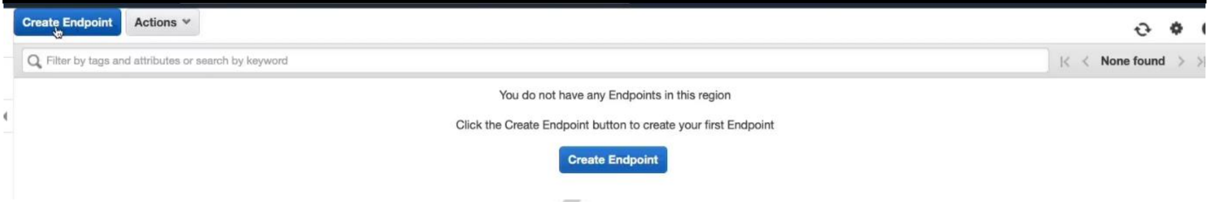
VPC Endpoint

VPC Endpoint



Destination	Target
pl-6ca54005 (com.amazonaws.ap-southeast-2.s3, 54.231.248.0/22, 54.231.252.0/24, 52.95.128.0/21)	*vpce-ID*

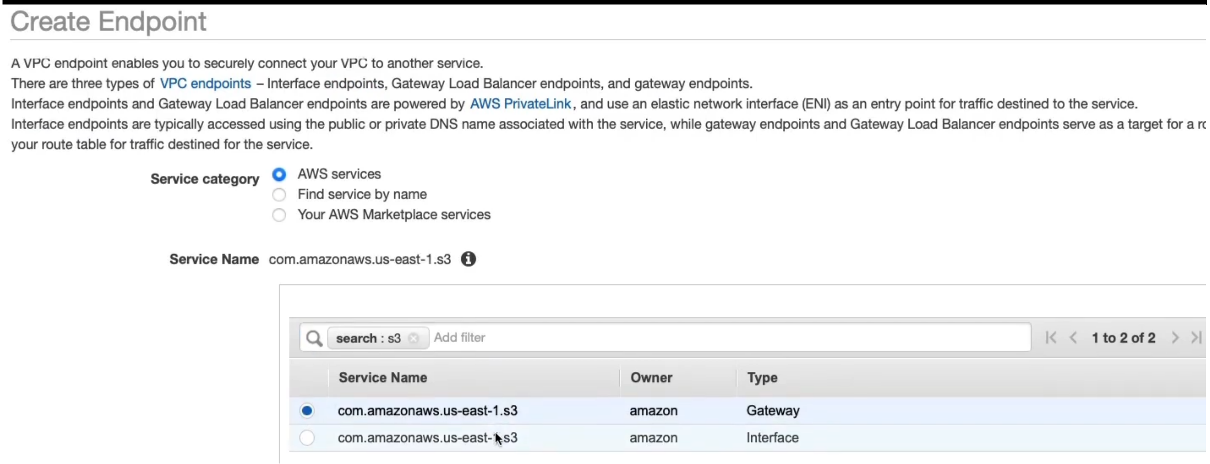
Create Endpoint



You do not have any Endpoints in this region

Click the Create Endpoint button to create your first Endpoint

Choose category and search service



Create Endpoint

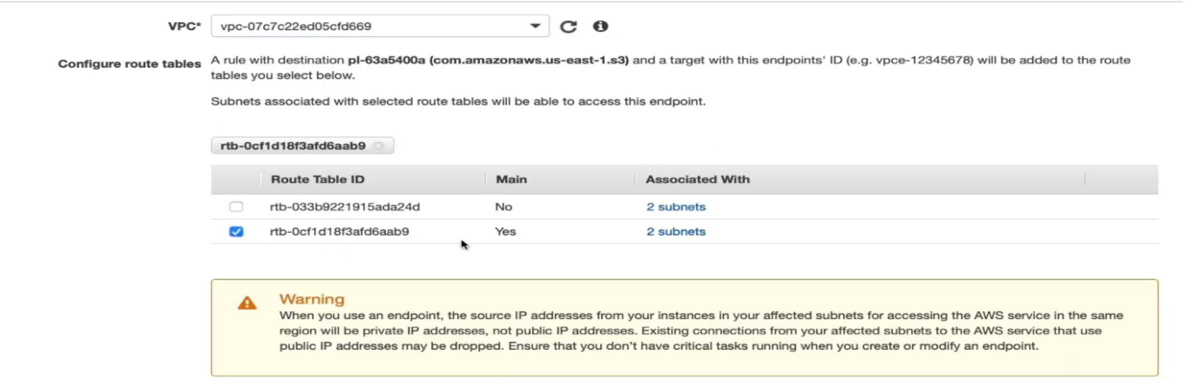
A VPC endpoint enables you to securely connect your VPC to another service.
There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and gateway endpoints.
Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an elastic network interface (ENI) as an entry point for traffic destined to the service.
Interface endpoints are typically accessed using the public or private DNS name associated with the service, while gateway endpoints and Gateway Load Balancer endpoints serve as a target for a ro
your route table for traffic destined for the service.

Service category ● AWS services
○ Find service by name
○ Your AWS Marketplace services

Service Name com.amazonaws.us-east-1.s3

	Service Name	Owner	Type
●	com.amazonaws.us-east-1.s3	amazon	Gateway
○	com.amazonaws.us-east-1.s3	amazon	Interface

Select VPC and select subnet



VPC* vpc-07c7c22ed05cfd669

Configure route tables A rule with destination **pl-63a5400a (com.amazonaws.us-east-1.s3)** and a target with this endpoints' ID (e.g. vpce-12345678) will be added to the route tables you select below.

Subnets associated with selected route tables will be able to access this endpoint.

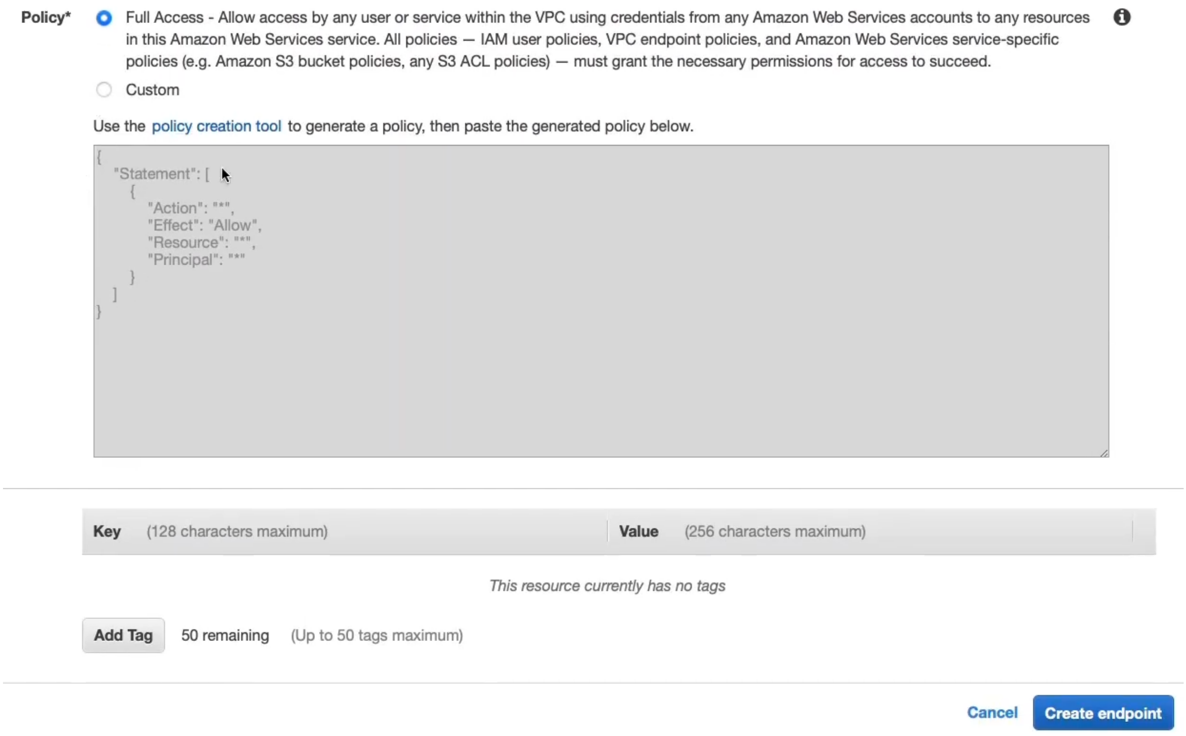
rtb-0cf1d18f3afd6aab9

	Route Table ID	Main	Associated With
□	rtb-033b9221915ada24d	No	2 subnets
☑	rtb-0cf1d18f3afd6aab9	Yes	2 subnets

Warning
When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

VPC Endpoint

Access policy



Policy* ● Full Access - Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

○ Custom

Use the policy creation tool to generate a policy, then paste the generated policy below.

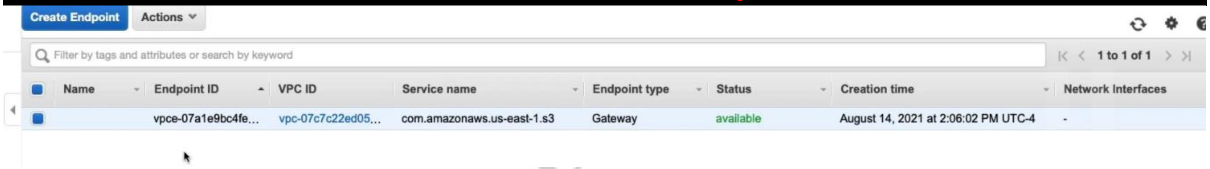
```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

Key (128 characters maximum)	Value (256 characters maximum)

This resource currently has no tags

Add Tag 50 remaining (Up to 50 tags maximum)

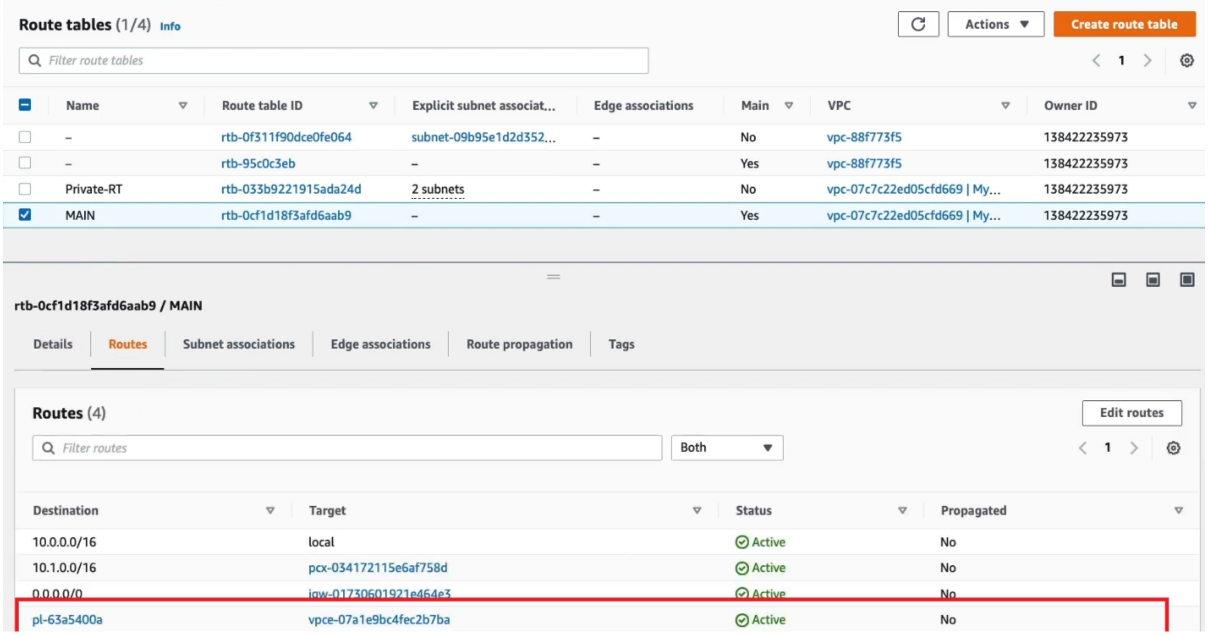
Create successfully



Filter by tags and attributes or search by keyword 1 to 1 of 1

Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status	Creation time	Network Interfaces
	vpce-07a1e9bc4fe...	vpc-07c7c22ed05...	com.amazonaws.us-east-1.s3	Gateway	available	August 14, 2021 at 2:06:02 PM UTC-4	-

Open route table and see automatic create one VPC endpoint



Route tables (1/4) Info

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
□	–	rtb-0f311f90dce0fe064	subnet-09b95e1d2d352...	–	No	vpc-88f773f5	138422235973
□	–	rtb-95c0c3eb	–	–	Yes	vpc-88f773f5	138422235973
□	Private-RT	rtb-033b9221915ada24d	2 subnets	–	No	vpc-07c7c22ed05cfd669 | My...	138422235973
☑	MAIN	rtb-0cf1d18f3afd6aab9	–	–	Yes	vpc-07c7c22ed05cfd669 | My...	138422235973

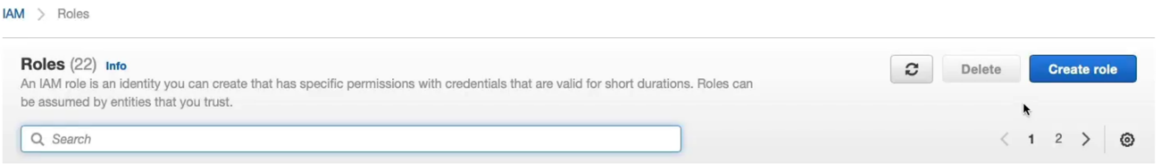
rtb-0cf1d18f3afd6aab9 / MAIN

Routes (4)

Destination	Target	Status	Propagated
10.0.0.0/16	local	✓ Active	No
10.1.0.0/16	pcx-034172115e6af758d	✓ Active	No
0.0.0.0/0	igw-01730601921e464e3	✓ Active	No
pl-63a5400a	vpce-07a1e9bc4fec2b7ba	✓ Active	No

VPC Endpoint

Create Role

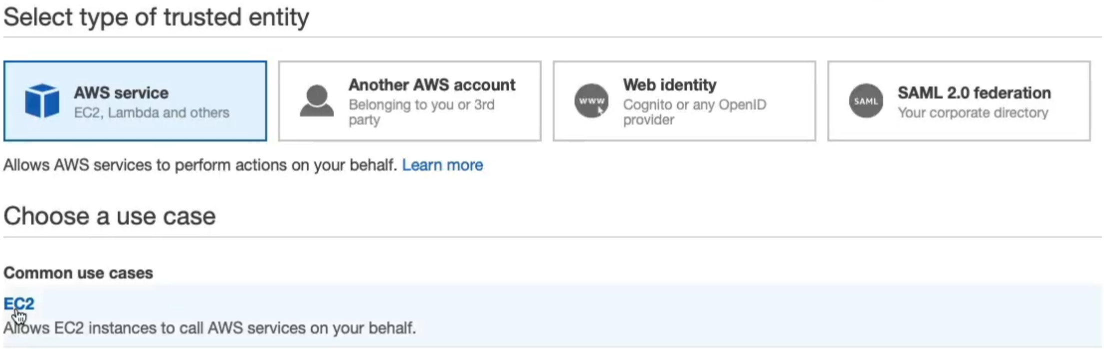


IAM > Roles

Roles (22) 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.

Select service



Select type of trusted entity

- **AWS service** EC2, Lambda and others
- **Another AWS account** Belonging to you or 3rd party
- **Web identity** Cognito or any OpenID provider
- **SAML 2.0 federation** Your corporate directory

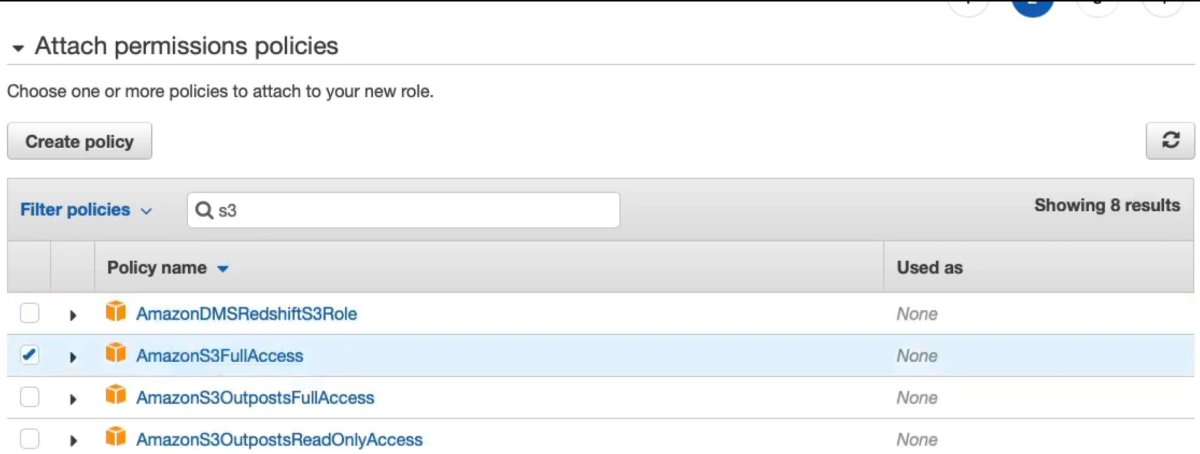
Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

Common use cases

EC2
Allows EC2 instances to call AWS services on your behalf.

Give permission



Attach permissions policies

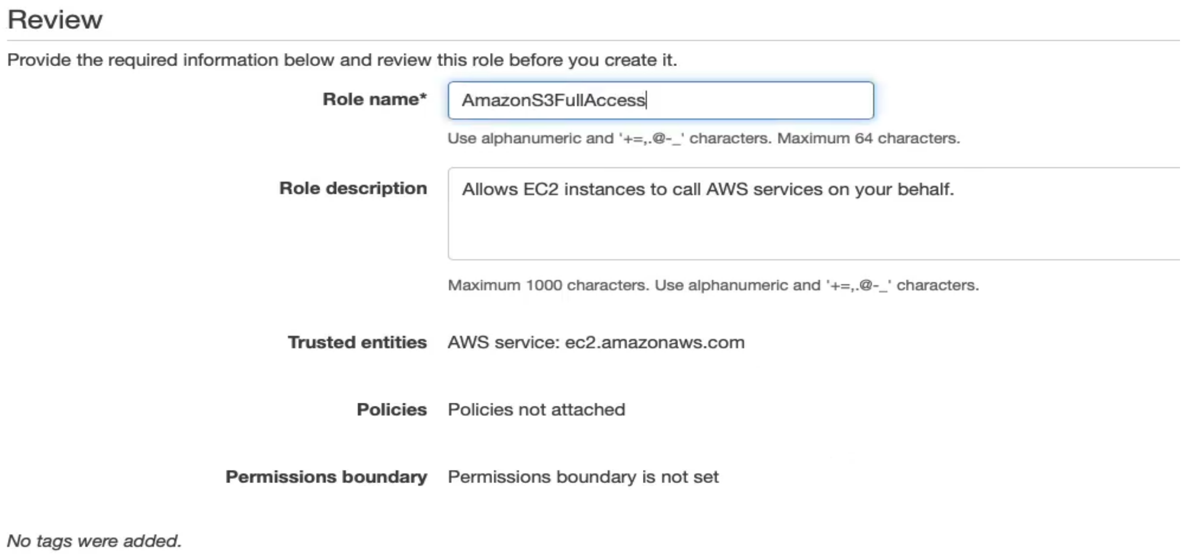
Choose one or more policies to attach to your new role.

s3

Showing 8 results

		Policy name	Used as
□	▸	AmazonDMSRedshiftS3Role	None
☑	▸	AmazonS3FullAccess	None
□	▸	AmazonS3OutpostsFullAccess	None
□	▸	AmazonS3OutpostsReadOnlyAccess	None

Check review



Review

Provide the required information below and review this role before you create it.

Role name* AmazonS3FullAccess

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

Role description Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

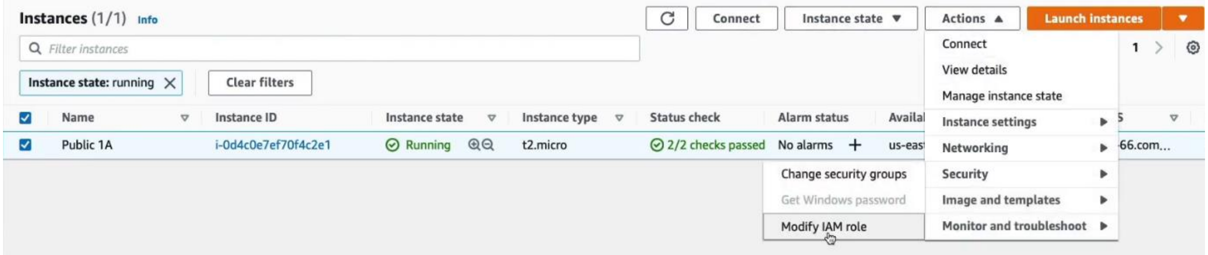
Policies Policies not attached

Permissions boundary Permissions boundary is not set

No tags were added.

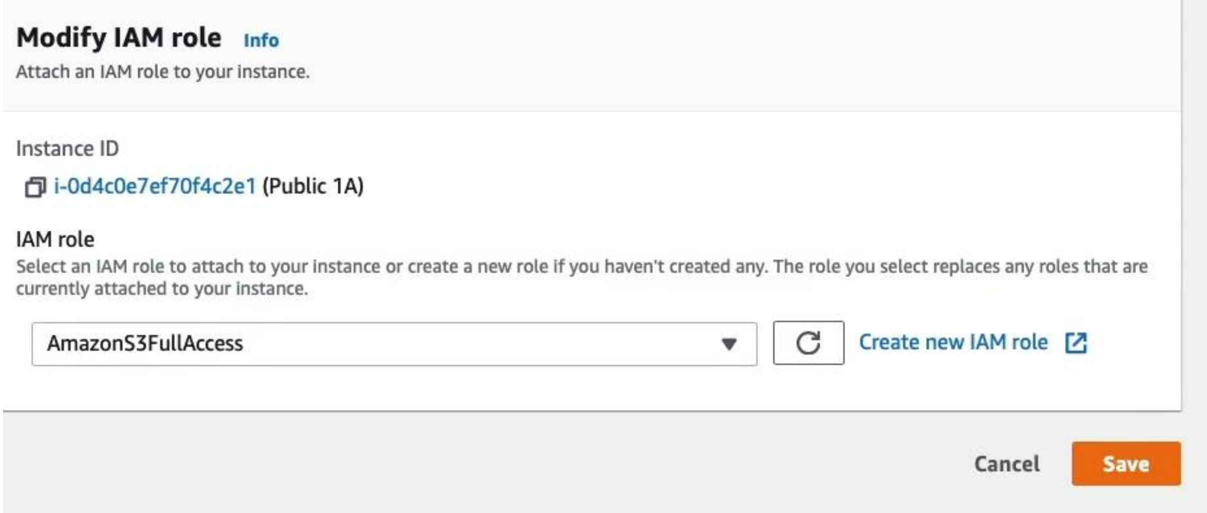
VPC Endpoint

Assign role to EC2



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availal
☑	Public 1A	i-0d4c0e7ef70f4c2e1	Running	t2.micro	2/2 checks passed	No alarms	us-east

Assign Role



Modify IAM role Info

Attach an IAM role to your instance.

Instance ID

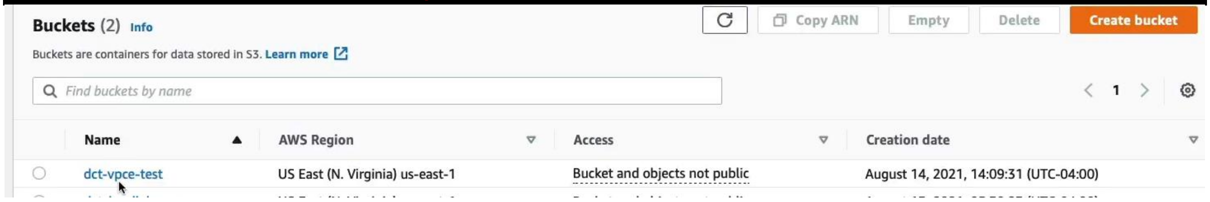
i-0d4c0e7ef70f4c2e1 (Public 1A)

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.

AmazonS3FullAccess

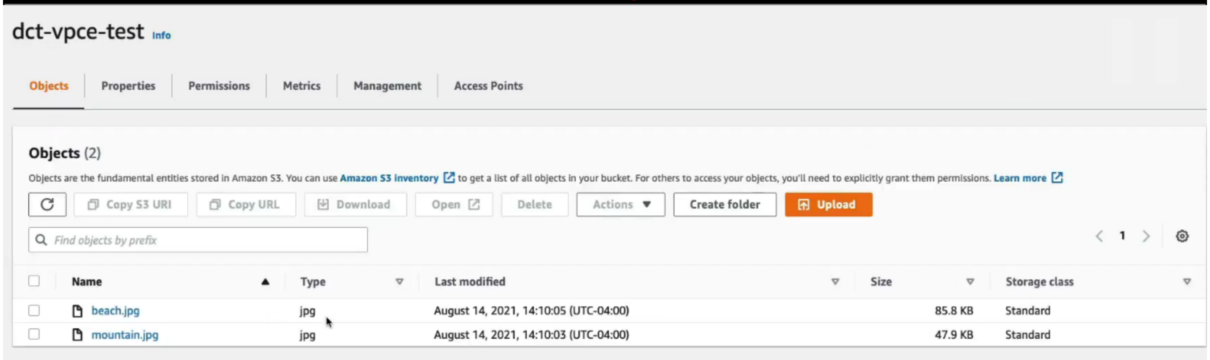
Open S3 and create bucket



Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	dct-vpce-test	US East (N. Virginia) us-east-1	Bucket and objects not public	August 14, 2021, 14:09:31 (UTC-04:00)

Add object



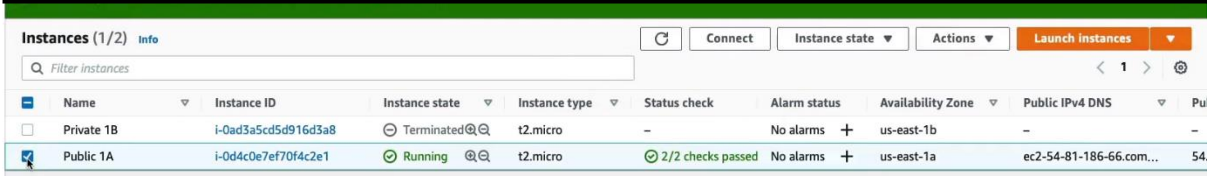
Objects (2)

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

□	Name	Type	Last modified	Size	Storage class
□	beach.jpg	jpg	August 14, 2021, 14:10:05 (UTC-04:00)	85.8 KB	Standard
□	mountain.jpg	jpg	August 14, 2021, 14:10:03 (UTC-04:00)	47.9 KB	Standard

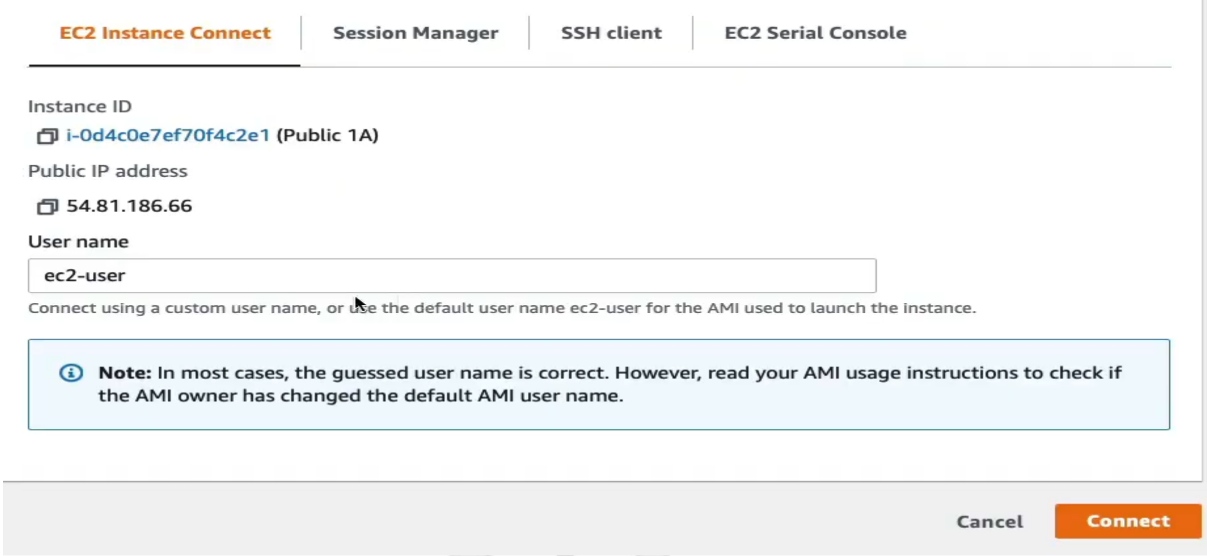
VPC Endpoint

connect



☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Pu
☐	Private 1B	i-0ad3a5cd5d916d3a8	Terminated	t2.micro	–	No alarms +	us-east-1b	–	–
☑	Public 1A	i-0d4c0e7ef70f4c2e1	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1a	ec2-54-81-186-66.com...	54.

Direct coonect



Instance ID

i-0d4c0e7ef70f4c2e1 (Public 1A)

Public IP address

54.81.186.66

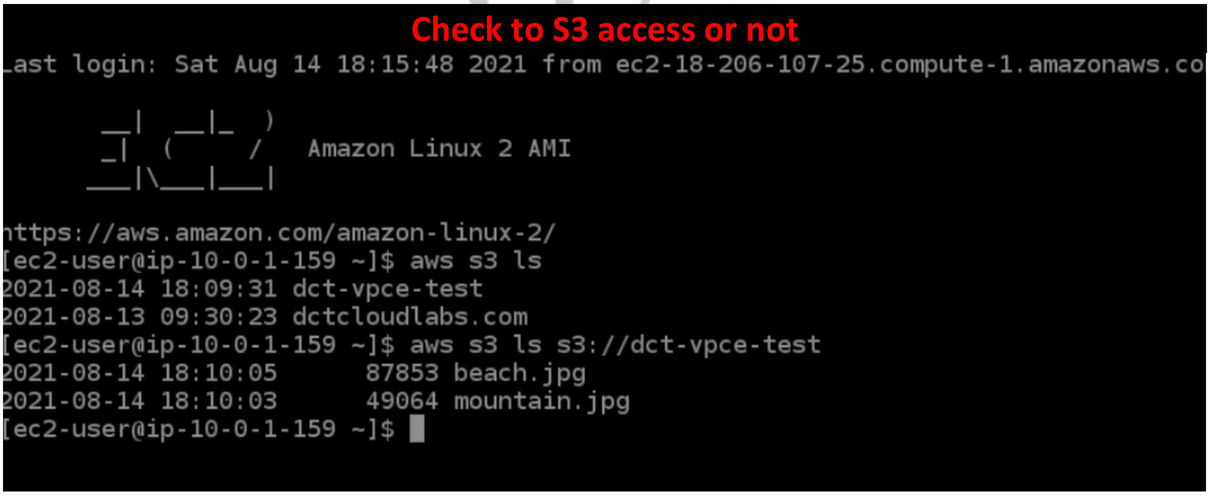
User name

ec2-user

Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.

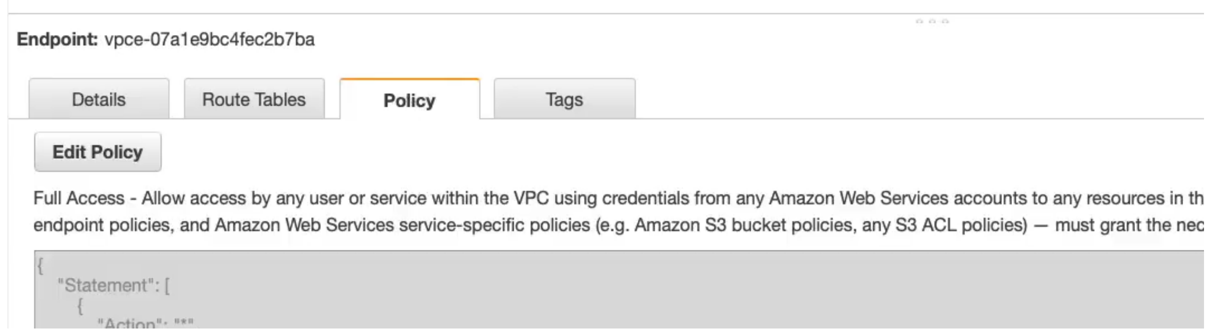
Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Check to S3 access or not



```
ast login: Sat Aug 14 18:15:48 2021 from ec2-18-206-107-25.compute-1.amazonaws.co

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

ttps://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-159 ~]$ aws s3 ls
2021-08-14 18:09:31 dct-vpce-test
2021-08-13 09:30:23 dctcloudlabs.com
[ec2-user@ip-10-0-1-159 ~]$ aws s3 ls s3://dct-vpce-test
2021-08-14 18:10:05      87853 beach.jpg
2021-08-14 18:10:03      49064 mountain.jpg
[ec2-user@ip-10-0-1-159 ~]$ 
```

If Change Endpoint policy change then cheeked



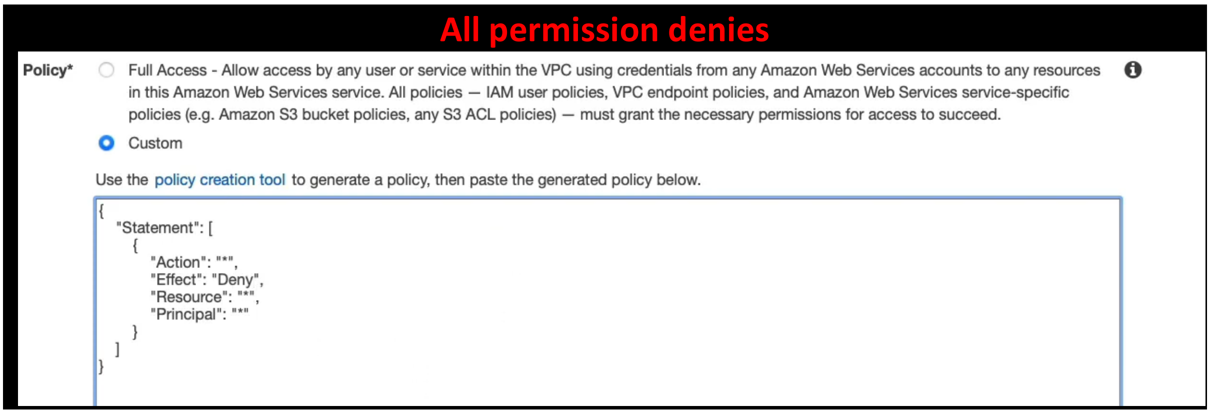
Endpoint: vpce-07a1e9bc4fec2b7ba

Full Access - Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in th endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the nec

```
{
  "Statement": [
    {
      "Action": "*"
```

VPC Endpoint

All permission denies



Policy*

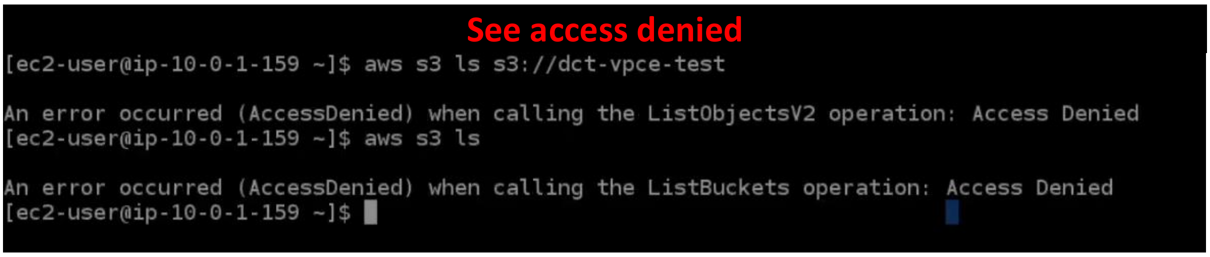
○ Full Access - Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

● Custom

Use the policy creation tool to generate a policy, then paste the generated policy below.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

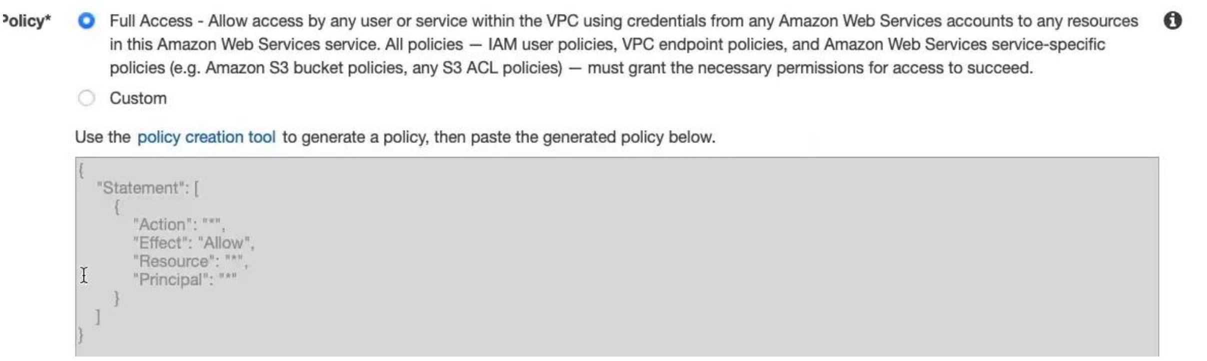
See access denied



```
[ec2-user@ip-10-0-1-159 ~]$ aws s3 ls s3://dct-vpce-test

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
[ec2-user@ip-10-0-1-159 ~]$ aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets operation: Access Denied
[ec2-user@ip-10-0-1-159 ~]$
```

Allows me to access S3 services even if I give full permissions to the Endpoint and deny permissions to the S3 Bucket

ACCESS FULL PERMISSION



Policy*

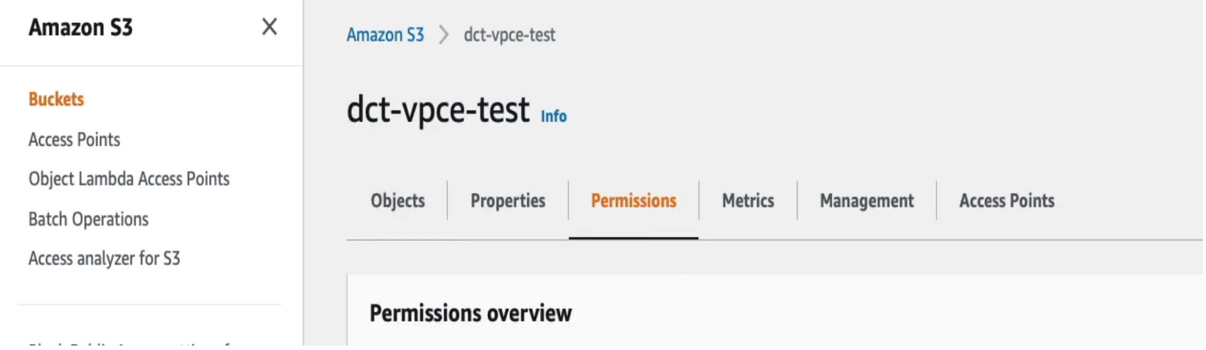
● Full Access - Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

○ Custom

Use the policy creation tool to generate a policy, then paste the generated policy below.

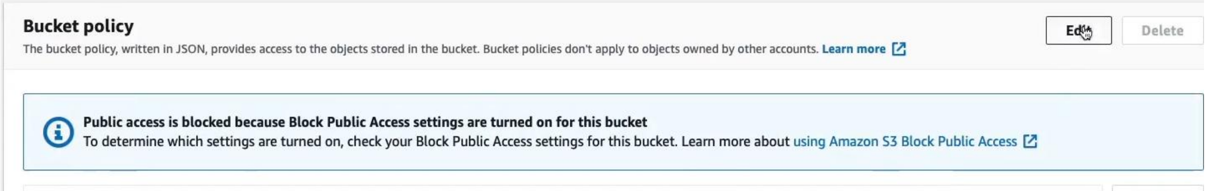
```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

Click bucket permission



VPC Endpoint

Edit bucket policy

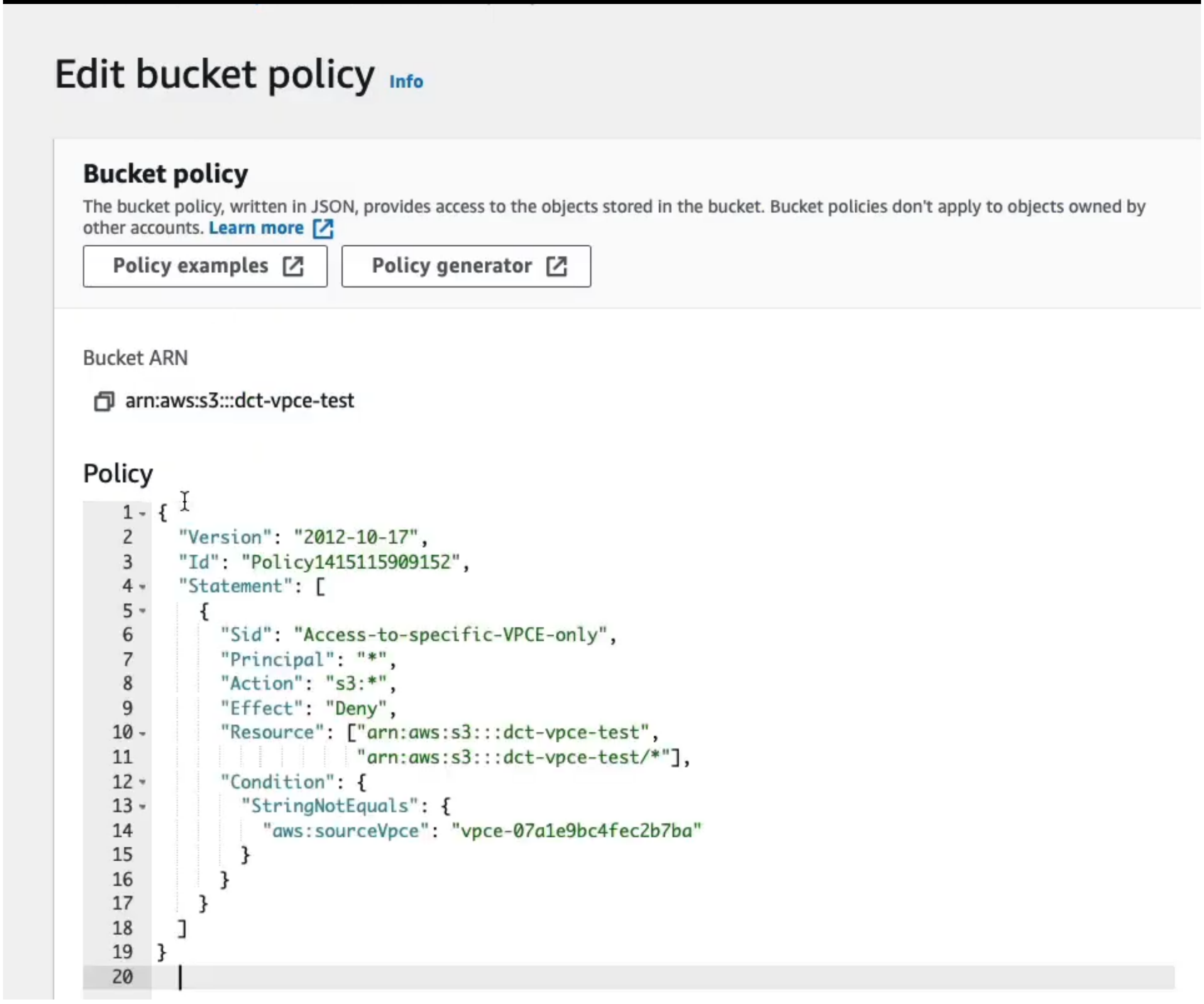


Bucket policy

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. Learn more

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

Permission deny



Edit bucket policy Info

Bucket policy

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. Learn more

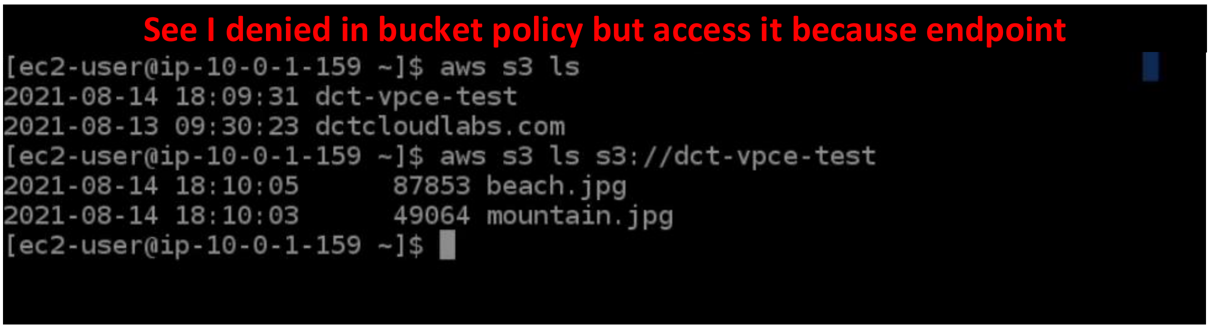
Bucket ARN

arn:aws:s3:::dct-vpce-test

Policy

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::dct-vpce-test",
                   "arn:aws:s3:::dct-vpce-test/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-07a1e9bc4fec2b7ba"
        }
      }
    }
  ]
}

```

See I denied in bucket policy but access it because endpoint

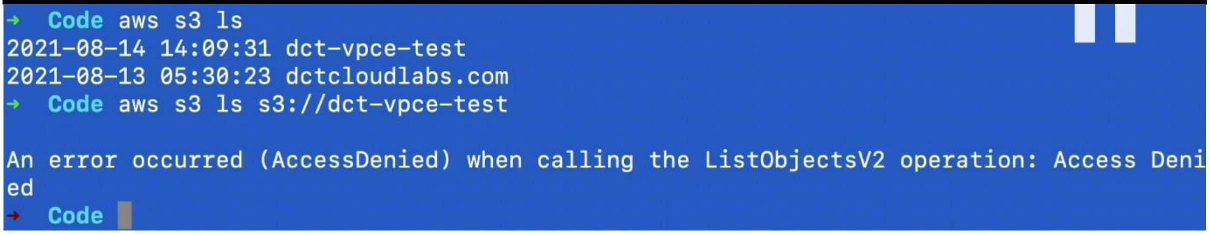


```
[ec2-user@ip-10-0-1-159 ~]$ aws s3 ls
2021-08-14 18:09:31 dct-vpce-test
2021-08-13 09:30:23 dctcloudlabs.com
[ec2-user@ip-10-0-1-159 ~]$ aws s3 ls s3://dct-vpce-test
2021-08-14 18:10:05      87853 beach.jpg
2021-08-14 18:10:03      49064 mountain.jpg
[ec2-user@ip-10-0-1-159 ~]$
```

it means I am getting access from endpoint not bucket

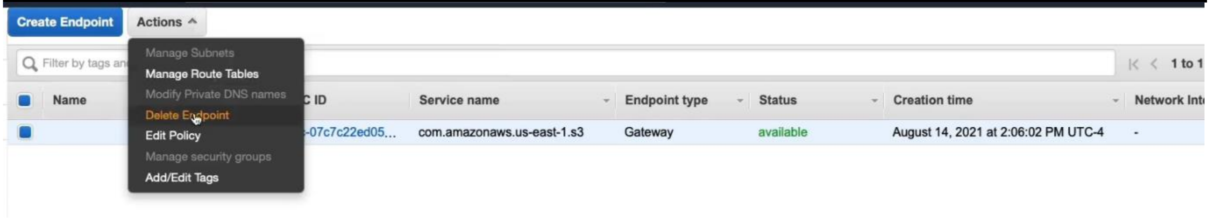
VPC Endpoint

If I had not configured the endpoints, and then denied the bucket permissions, I would not have been allowed to access S3 →see result without Endpoint configure result



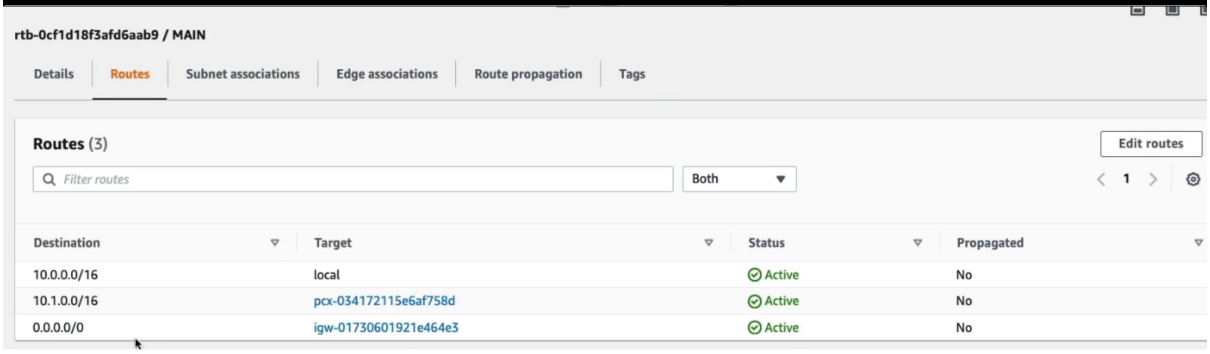
```
→  Code aws s3 ls
2021-08-14 14:09:31 dct-vpce-test
2021-08-13 05:30:23 dctcloudlabs.com
→  Code aws s3 ls s3://dct-vpce-test

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Deni
ed
→  Code
```

If I delete the endpoint, the entry will be deleted from the route table automatically.



Name	C ID	Service name	Endpoint type	Status	Creation time	Network Int
	-07c7c22ed05...	com.amazonaws.us-east-1.s3	Gateway	available	August 14, 2021 at 2:06:02 PM UTC-4	-

Auto delete



Routes (3)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
10.1.0.0/16	pcx-034172115e6af758d	Active	No
0.0.0.0/0	igw-01730601921e464e3	Active	No