

# VPC ENDPOINT LAB

## Create a VPC

[VPC](#) > [Your VPCs](#) > [Create VPC](#)

## Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

### VPC settings

**Resources to create** [Info](#)  
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.

**IPv4 CIDR block** [Info](#)

☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

**IPv4 CIDR**

**IPv6 CIDR block** [Info](#)

☒ No IPv6 CIDR block ☐ IPAM-allocated IPv6 CIDR block ☐ Amazon-provided IPv6 CIDR block ☐ IPv6 CIDR owned by me

**Tenancy** [Info](#)

### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="vpc1"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

## Create Subnets one for public and one for private

- Public

### Create subnet Info

#### VPC

**VPC ID**  
Create subnets in this VPC.

vpc-0ae4ac7e18b0bb366 (vpc1) ▼

**Associated VPC CIDRs**

IPv4 CIDRs

10.0.0.0/16

#### Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

**Subnet 1 of 1**

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.

Public\_subnet

The name can be up to 256 characters long.

**Availability Zone** Info  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference ▼

**IPv4 CIDR block** Info

10.0.0.0/24 ✕

▼ Tags - *optional*

Key	Value - <i>optional</i>	
✕ Name ✕	✕ Public_subnet ✕	Remove

**Add new tag**

You can add 49 more tags.

**Remove**

**Add new subnet**

- Private

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

vpc-0ae4ac7e18b0bb366 (vpc1) ▼

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Private\_subnet

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference ▼

IPv4 CIDR block [Info](#)

10.0.1.0/24 ✕

▼ Tags - optional

Key

Value - optional

✕ Name ✕

✕ Private\_subnet ✕

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Create Internet Gateway and attach it to the VPC you have created

VPC > Internet gateways > Create internet gateway

## Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

### Internet gateway settings

**Name tag**  
Creates a tag with a key of 'Name' and a value that you specify.

**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)

You can add 50 more tags.

[Cancel](#) [Create internet gateway](#)

Select you Internet Gateway and click actions there you will find attach option, after clicking on it you can attach you IG to a VPC

VPC > Internet gateways > Attach to VPC (igw-00a29fd0f0d09ba8c)

## Attach to VPC (igw-00a29fd0f0d09ba8c) Info

**VPC**  
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

**Available VPCs**  
Attach the internet gateway to this VPC.

vpc-0ae4ac7e18b0bb366 - vpc1

► AWS Command Line Interface command

[Cancel](#) [Attach internet gateway](#)

You can see here your IG is attached to the VPC you have created

VPC > Internet gateways > igw-00a29fd0f0d09ba8c

## igw-00a29fd0f0d09ba8c / vpc1-ig

Actions ▾

**Details** Info

Internet gateway ID igw-00a29fd0f0d09ba8c	State Attached	VPC ID vpc-0ae4ac7e18b0bb366   vpc1	Owner 436117849909
----------------------------------------------	-------------------	----------------------------------------	-----------------------

**Tags** Manage tags

Search tags

Key	Value
Name	vpc1-ig

Go to route table and add Internet gateway to your main route table:

VPC > Route tables > rtb-0068b19517428a96b > Edit routes

## Edit routes

**Edit routes**

Destination	Target	Status
10.0.0.0/16	local	Active
Propagated		
No		

**Edit routes**

Destination	Target	Status
0.0.0.0/0	igw-00a29fd0f0d09ba8c	-
Propagated		
No		

Remove

Add route

Cancel Preview Save changes

Create another Route table for the VPC with no IG attached to it

VPC > Route tables > rtb-09ad37fce832d8184

rtb-09ad37fce832d8184 / vpc1-rt(Private)

Actions

DetailsInfo

Route table ID  
rtb-09ad37fce832d8184

VPC  
vpc-0ae4ac7e18b0bb366 | vpc1

Main  
No

Owner ID  
436117849909

Explicit subnet associations  
-

Edge associations  
-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Edit routes

Filter routes

Both

< 1 >

Destination

Target

Status

Propagated

10.0.0.0/16

local

Active

No

## Associate Subnets to the route table by edit subnet association:

- Here public subnet will be attached to the route table with IG such that main route table of vpc1
- And private subnet to the route table with no IG association

Below image shows the public subnet being associated to the route table with IG(click on the section of explicit subnet association to verify which subnet is attached to the route table)

VPC > Route tables > rtb-0068b19517428a96b

### rtb-0068b19517428a96b / vpc1-rt(Public)

Actions ▾

**Details** info

Route table ID rtb-0068b19517428a96b	Main Yes	Explicit subnet associations subnet-069b102ff3b5117be / public_subnet	Edge associations -
VPC vpc-0ae4ac7e18b0bb366   vpc1	Owner ID 436117849909		

Routes | Subnet associations | Edge associations | Route propagation | Tags

**Routes (2)** Edit routes

Filter routes Both < 1 > ⚙

Destination ▾	Target ▾	Status ▾	Propagated ▾
0.0.0.0/0	igw-00a29fd0f0d09ba8c	Active	No
10.0.0.0/16	local	Active	No

Similarly attach the private subnet to the route table with no IG associated to it.

VPC > Route tables > rtb-09ad37fce832d8184

rtb-09ad37fce832d8184 / vpc1-rt(Private) 

Actions

Details Info

Route table ID

rtb-09ad37fce832d8184

VPC

vpc-0ae4ac7e18b0bb366 | vpc1

Main

No

Owner ID

436117849909

Explicit subnet associations

subnet-0297148b8b63c1e77 / private\_subnet

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1) 

Edit routes

Filter routes

Both

< 1 >

Destination

Target

Status

Propagated

10.0.0.0/16

local

Active

No

Below image shows your private subnet associated with the route table with no IG associated to it

VPC > Route tables > rtb-09ad37fce832d8184

rtb-09ad37fce832d8184 / vpc1-rt(Private) 

Actions

Details Info

Route table ID

rtb-09ad37fce832d8184

VPC

vpc-0ae4ac7e18b0bb366 | vpc1

Main

No

Owner ID

436117849909

Explicit subnet associations

subnet-0297148b8b63c1e77 / private\_subnet

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1) 

Edit routes

Filter routes

Both

< 1 >

Destination

Target

Status

Propagated

10.0.0.0/16

local

Active

No



## Create VPC Endpoint

- Select the service category and name your endpoint Here we want to access our S3 service with the private subnet in the vpc1 and S3 comes
- under AWS services category

VPC > Endpoints > Create endpoint

### Create endpoint Info

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 route in your route table for traffic destined for the service.

#### Endpoint settings

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.

vpc1-endpoint

**Service category**  
Select the service category

<input checked="" type="radio"/> <b>AWS services</b> Services provided by Amazon	<input type="radio"/> <b>PrivateLink Ready partner services</b> Services with an AWS Service Ready designation
<input type="radio"/> <b>AWS Marketplace services</b> Services that you've purchased through AWS Marketplace	<input type="radio"/> <b>Other endpoint services</b> Find services shared with you by service name

- Select the service name and select endpoint gateway of S3 and select the route table with private subnet as we wanted to access our S3 service from the Private subnet

### Services (1/3)

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

Clear filters

	Service Name	Owner	Type
<input checked="" type="radio"/>	com.amazonaws.us-east-1.s3	amazon	Gateway
<input type="radio"/>	com.amazonaws.us-east-1.s3	amazon	Interface
<input type="radio"/>	com.amazonaws.us-east-1.s3-outposts	amazon	Interface

### VPC

Select the VPC in which to create the endpoint

VPC

The VPC in which to create your endpoint.

vpc-0ae4ac7e18b0bb366 (vpc1)

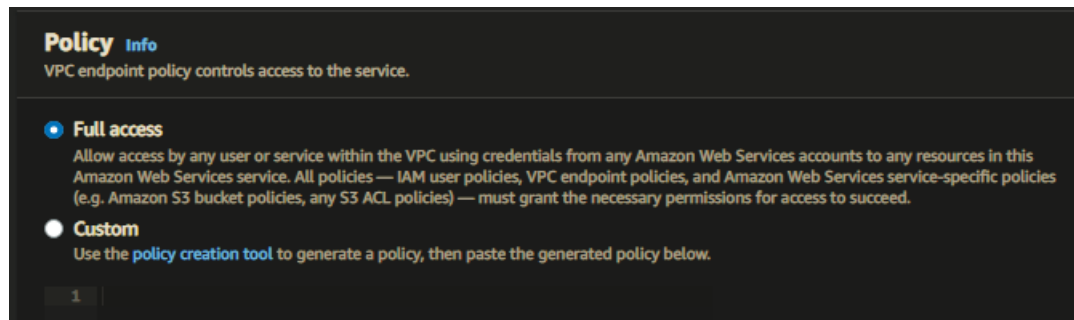
### Route tables (1/2)

	Name	Route Table ID	Main
<input type="checkbox"/>	vpc1-rt(Public)	rtb-0068b19517428a96b (vpc1-rt(Publ...	Yes
<input checked="" type="checkbox"/>	vpc1-rt(Private)	rtb-09ad37fce832d8184 (vpc1-rt(Privat...	No

ⓘ 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.

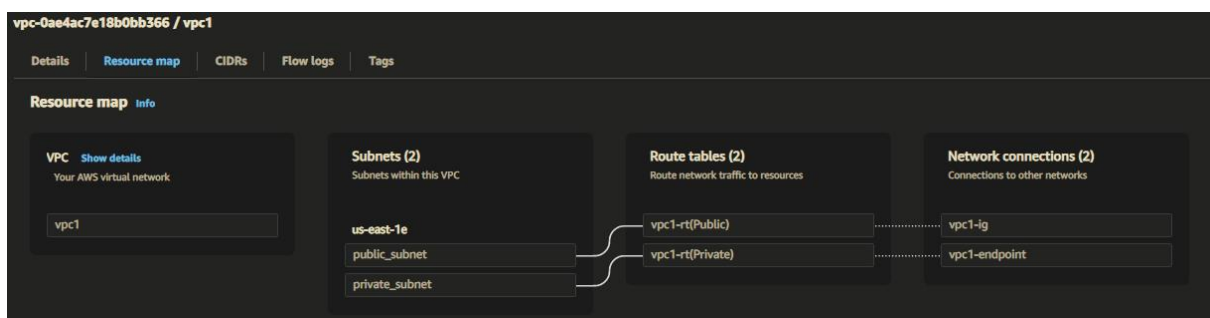
rtb-09ad37fce832d8184

- you can make or select the default full access policy here we are selecting s3 full access policy and click on create VPC endpoint.



Check the resource map you will see the routes you have created

- Below you can see how you have associated your public subnet to the IG and private subnet with no IG



- Edit network settings while creating EC2 instances, select public subnet and enable auto-assign public IP to make ec2 publicly accessible and select private subnet for private ec2 and disable auto-assign public IP. Create common security group vpc1-sg for both instances

**▼ Network settings** [Info](#)

---

**VPC - required** [Info](#)

vpc-0ae4ac7e18b0bb366 (vpc1) ▼ ↻

**Subnet** [Info](#)

subnet-069b102ff3b5117be public\_subnet ▼ ↻ [Create new subnet](#)

**Auto-assign public IP** [Info](#)

Enable ▼

**Firewall (security groups)** [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

+ Create security group ● Select existing security group

**Security group name - required**

vpc1-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and .\_-/#,@!+=&;[]\*~`

**Description - required** [Info](#)

launch-wizard-2 created 2023-02-19T13:42:10.581Z

**Inbound security groups rules**

**▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)** [Remove](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
ssh ▼	TCP	22

Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere ▼	<input type="text"/> Add CIDR, prefix list or security group <span>0.0.0.0/0 ✕</span>	<i>e.g. SSH for admin desktop</i>

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

Add security group rule

Create an IAM role for S3 access:

Go to IAM service console and select roles and then select create IAM roles and in Use case select EC2 instances and select S3 in use cases for other AWS services.

IAM > Roles > Create role

## Select trusted entity [Info](#)

### Trusted entity type

☒ **AWS service**  
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**  
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**  
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**  
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**  
Create a custom trust policy to enable others to perform actions in this account.

### Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

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

☐ **Lambda**  
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

S3

▼

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

Select the S3 full Access in the add permissions and click next there in Role details make your role name and create role

IAM > Roles > Create role

Step 1  
Select trusted entity

Step 2  
Add permissions

Step 3  
Name, review, and create

## Add permissions Info

Permissions policies (Selected 1/814)  
Info  
Choose one or more policies to attach to your new role.

9 matches

s3 ✕

Clear filters

< 1 > ⚙

	Policy name <a href="#">↗</a>	Type <a href="#">▼</a>	Description
<input type="checkbox"/>	AmazonDMSRedsh...	AWS m...	Provides access to manage S3 settings f...
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS m...	Provides full access to all buckets via the ...
<input type="checkbox"/>	QuickSightAccessF...	AWS m...	Policy used by QuickSight team to access...
<input type="checkbox"/>	AmazonS3ReadOnl...	AWS m...	Provides read only access to all buckets v...
<input type="checkbox"/>	AmazonS3Outposts...	AWS m...	Provides full access to Amazon S3 on Ou...
<input type="checkbox"/>	AWSBackupService...	AWS m...	Policy containing permissions necessary f...
<input type="checkbox"/>	AWSBackupService...	AWS m...	Policy containing permissions necessary f...
<input type="checkbox"/>	AmazonS3ObjectLa...	AWS m...	Provides AWS Lambda functions permissi...
<input type="checkbox"/>	AmazonS3Outposts...	AWS m...	Provides read only access to Amazon S3 ...

▶ Set permissions boundary - optional Info

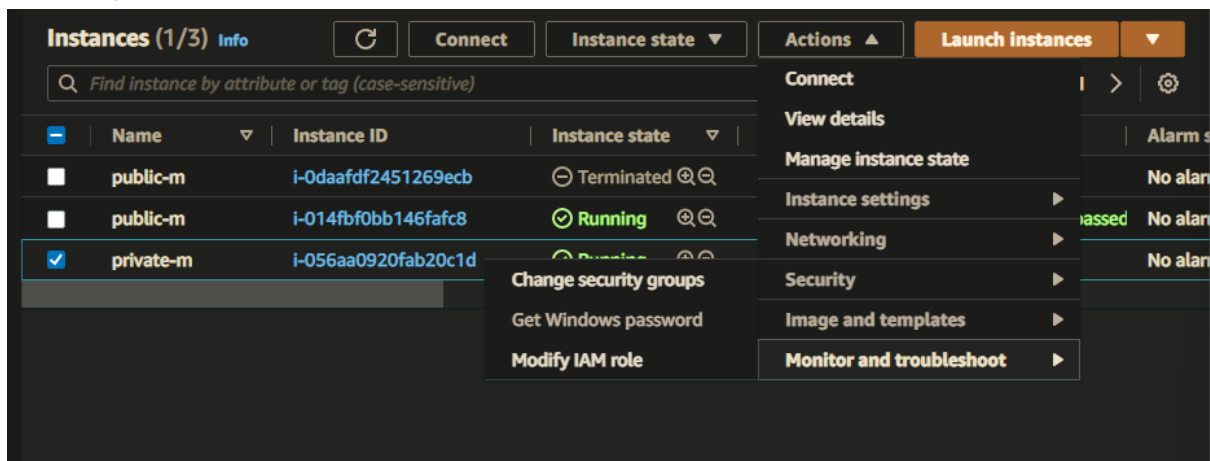
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Cancel

Previous

Next

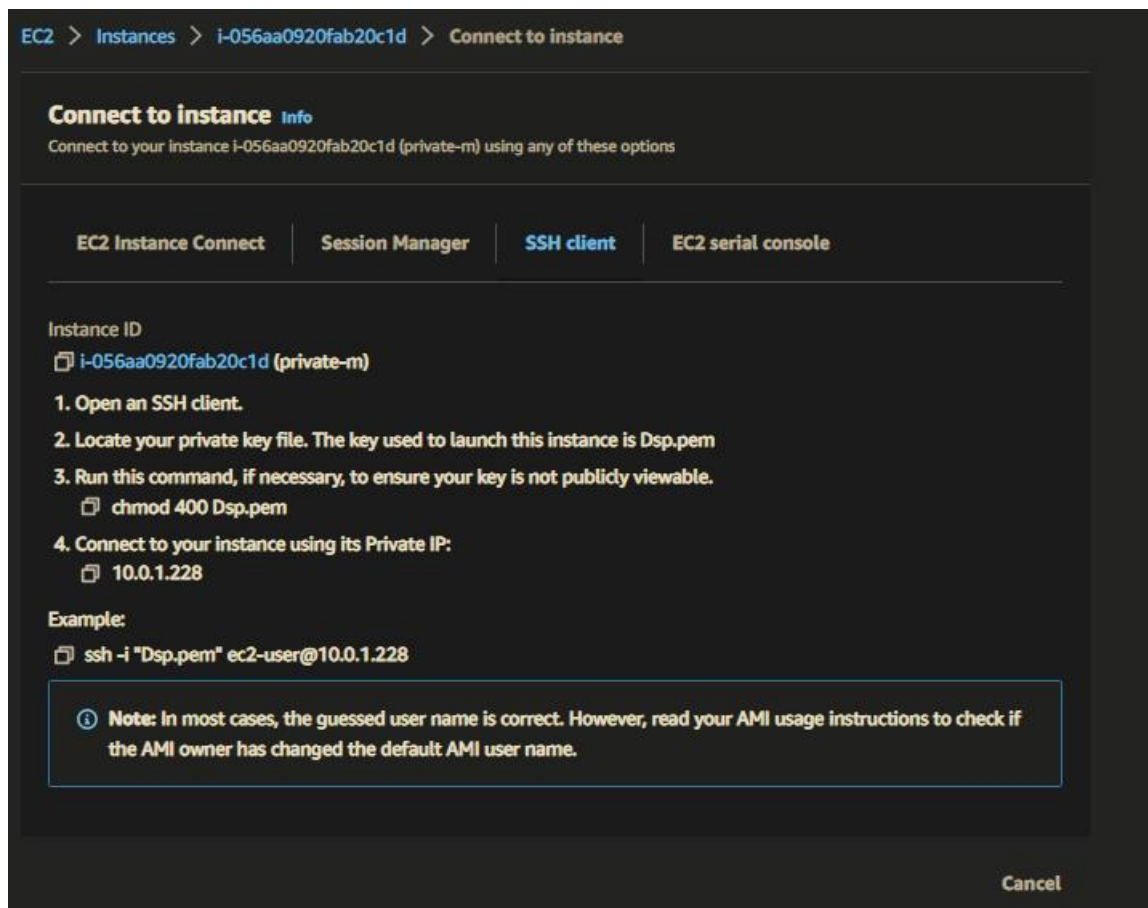
Modify IAM role for the Private Instance:



- Open Public instance using putty and enter `sudo su -` command to switch to root user

```
root@ip-10-0-0-151:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
  
  _ |  _ | _ )  
  _ | (  _ /  Amazon Linux 2 AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-0-151 ~]$ sudo su -  
[root@ip-10-0-0-151 ~]#
```

- Now you have to access your private subnet from the public subnet for that go to private Ec2 instance we have created and click on connect and then click on SSH client, you will see the following procedure there



Execute following in your linux CLI :

- vi Dsp.pem
- open your .pem file of your key assigned to the instance in Notepad and copy the key
- In CLI press I you will enter into insert mode and now paste the copied key.
- Now copy the commands from the connect to instance ,as shown in the image above
- After successful connection you will see the following

```
[root@ip-10-0-0-151 ~]#  
[root@ip-10-0-0-151 ~]# chmod 400 Dsp.pem  
[root@ip-10-0-0-151 ~]# ssh -i "Dsp.pem" ec2-user@10.0.1.228  
The authenticity of host '10.0.1.228 (10.0.1.228)' can't be established.  
ECDSA key fingerprint is SHA256:K1NgxRCZ5ulTRGeiKXoTuU9qGle0Be724ymqPpQm3vk.  
ECDSA key fingerprint is MD5:8f:4f:d1:e4:e8:c7:82:48:81:69:9e:f3:df:00:cb:bf.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.0.1.228' (ECDSA) to the list of known hosts.  
  
  _ | _ | _ )  
  _ | ( _ | /  Amazon Linux 2 AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-1-228 ~]$
```



- Type “sudo su –” command and switch to root user
- Now you can access you S3 and upload or download files from the S3 using private subnet or say private instance with use of VPC endpoint Gateway

- Create dummy files using “touch file1” command

```
[root@ip-10-0-1-228 ~]# touch file1
[root@ip-10-0-1-228 ~]# touch file2
```

- Type “aws s3 ls” command this will show you the list of buckets you have in your S3.below you can see I have dsp2 bucket in my S3

```
[root@ip-10-0-1-228 ~]# aws s3 ls
2023-02-19 14:34:06 dsp2
```

- Type “aws s3 cp /root/file1 s3://dsp2” command it will copy the file1 and upload it to the S3 bucket dsp2.

```
[root@ip-10-0-1-228 ~]# aws s3 cp /root/file1 s3://dsp2
upload: ./file1 to s3://dsp2/file1
```

- Now go to your S3 bucket and check for the file1, you would see you file being uploaded to the bucket dsp2

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

↻

📄 Copy S3 URI

📄 Copy URL

⬇️ Download

🔗 Open

Delete

⌵ Actions

Create folder

⬆️ Upload

< 1 >

⚙️

<input type="checkbox"/>	Name ▲	Type ▼	Last modified ▼	Size ▼	Storage class ▼
<input type="checkbox"/>	📄 file1	-	February 19, 2023, 20:14:29 (UTC+05:30)	0 B	Standard