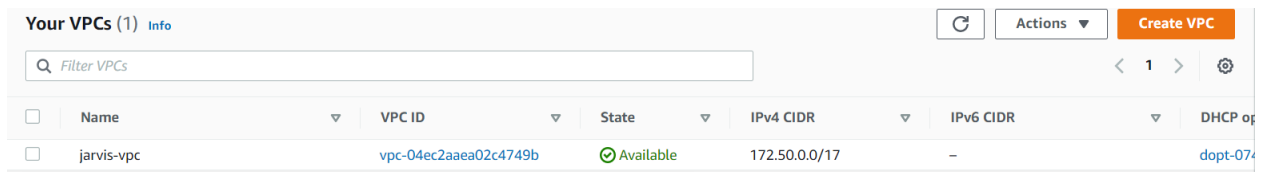


Why we use Endpoint in aws vpc.

1. Endpoint create a connection in between VPC & AWS service as like S3.
2. It enables to get privately access of specific AWS Services from your own VPC.
3. It doesn't require NAT Gateway, Internet Gateway or VPN Connection.
4. It is additional stage of security to our Database.

Firstly, create VPC

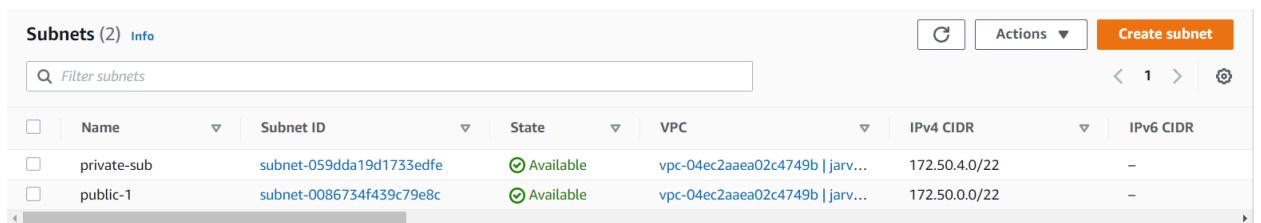


Your VPCs (1) Info

Filter VPCs

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP op
<input type="checkbox"/>	jarvis-vpc	vpc-04ec2aeea02c4749b	Available	172.50.0.0/17	-	dopt-074

Create 2 subnets for public and private instances

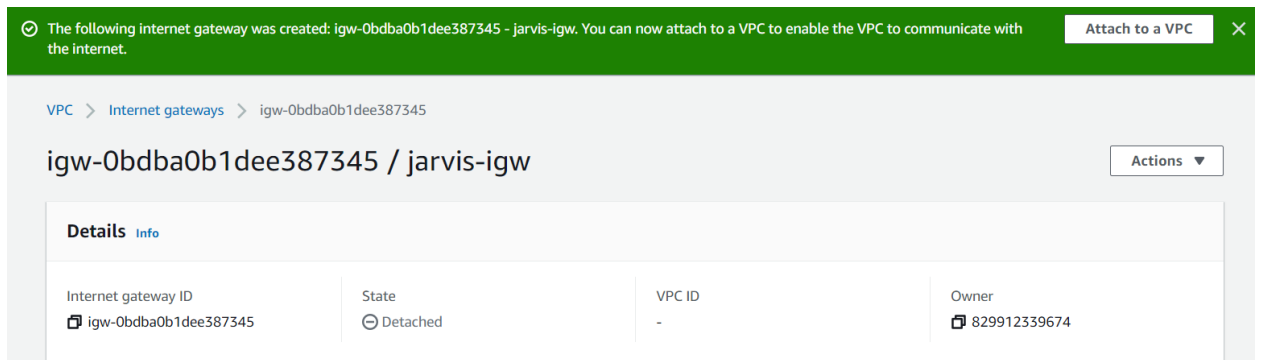


Subnets (2) Info

Filter subnets

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	private-sub	subnet-059dda19d1733edfe	Available	vpc-04ec2aeea02c4749b jarv...	172.50.4.0/22	-
<input type="checkbox"/>	public-1	subnet-0086734f439c79e8c	Available	vpc-04ec2aeea02c4749b jarv...	172.50.0.0/22	-

Create internet gateway and attach to the vpc



The following internet gateway was created: igw-0bdba0b1dee387345 - jarvis-igw. You can now attach to a VPC to enable the VPC to communicate with the internet. Attach to a VPC X

VPC > Internet gateways > igw-0bdba0b1dee387345

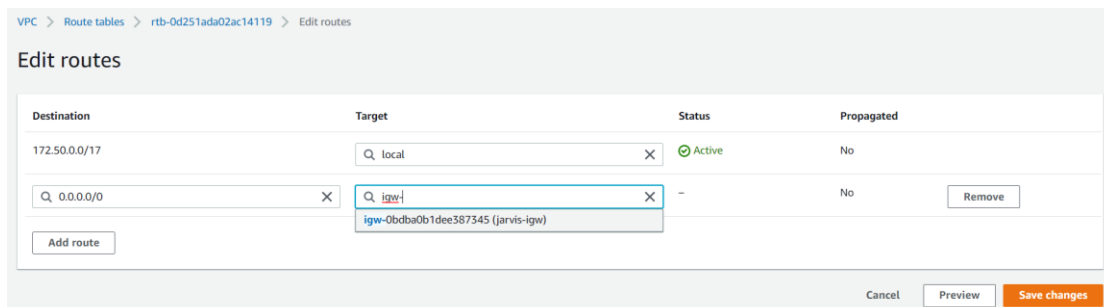
igw-0bdba0b1dee387345 / jarvis-igw

Actions

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0bdba0b1dee387345	Detached	-	829912339674

Do Jarvis-igw entry in default route table



VPC > Route tables > rtb-0d251ada02ac14119 > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.50.0.0/17	local	Active	No
0.0.0.0/0	igw-0bdba0b1dee387345 (jarvis-igw)	-	No

Add route

Cancel Preview Save changes

Now we create **End Point for AWS services**

1. Put End point name
2. Choose AWS service category
3. Services -> Type[Gateway] -> select S3 service
4. Select created VPC
5. Select default route table for created VPC

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.

Service category
Select the service category

☒ **AWS services**
Services provided by Amazon

☐ **PrivateLink Ready partner services**
Services with an AWS Service Ready designation

☐ **AWS Marketplace services**
Services that you've purchased through AWS Marketplace

☐ **Other endpoint services**
Find services shared with you by service name

Services (1/2)

Filter services

Type: Gateway X Clear filters

	Service Name	Owner	Type
<input type="radio"/>	com.amazonaws.ap-south-1.dynamodb	amazon	Gateway
<input checked="" type="radio"/>	com.amazonaws.ap-south-1.s3	amazon	Gateway

VPC

Select the VPC in which to create the endpoint.

VPC
The VPC in which to create your endpoint.

Route tables (1/1) [Info](#)

Filter route tables

<input checked="" type="checkbox"/>	Name	Route Table ID	Main
<input checked="" type="checkbox"/>	-	rtb-0d251ada02ac14119	Yes

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-0d251ada02ac14119 X

Created end point succsesfully

Endpoints (1) [Info](#)

Filter endpoints

Actions [Create endpoint](#)

<input type="checkbox"/>	Name	VPC endpoint ID	VPC ID	Service name	End
<input type="checkbox"/>	jarvis-endpoint	vpce-09b6ffd3fc1725fd8	vpc-04ec2aaea02c4749b jarvis-vpc	com.amazonaws.ap-south-1.s3	Gate

Now we create 2 instances one with pub/priv & second with only private IP

While creating publi IP **Auto assign Public IP** should be enable in Network setting

Network settings

VPC - *required* [Info](#)

vpc-04ec2aaea02c4749b (jarvis-vpc)
172.50.0.0/17

Subnet [Info](#)

subnet-0086734f439c79e8c public-1
VPC: vpc-04ec2aaea02c4749b Owner: 829912339674
Availability Zone: ap-south-1a IP addresses available: 1019

Auto-assign public IP [Info](#)

Enable

Made 2 instances


<input type="checkbox"/>	jarvis-pub-instance	i-08a17768d647c0013	Running	t2.micro	2/2 checks passed	No alarms	+	ap-south-1a	-
<input type="checkbox"/>	jarvis-priv instance	i-01a05efbd04d3434a	Running	t2.micro	2/2 checks passed	No alarms	+	ap-south-1b	-

Now create role for the private instacne of S3 full access

EC2 > Instances > i-01a05efbd04d3434a > Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID
 i-01a05efbd04d3434a (jarvis-priv instance)

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.



Choose IAM role

No IAM Role
Choose this option to detach an IAM role

ec2-to-s3
arn:aws:iam::829912339674:instance-profile/ec2-to-s3

Jarvis-cli-role
arn:aws:iam::829912339674:instance-profile/Jarvis-cli-role

jarvispolicy
arn:aws:iam::829912339674:instance-profile/jarvispolicy


 [Create new IAM role](#) 

the instance will be removed. Are you


Cancel [Save](#)

Make 1-2 buckets in S3 service in same region where VPC & Endpoint created





Amazon S3 > Buckets


 **Account snapshot**

[View Storage Lens dashboard](#)


Last updated: Apr 13, 2022 by Storage Lens. Metrics are generated every 24 hours. [Learn more](#) 

Buckets (2) [Info](#)

  Copy ARN  Empty  Delete [Create bucket](#)

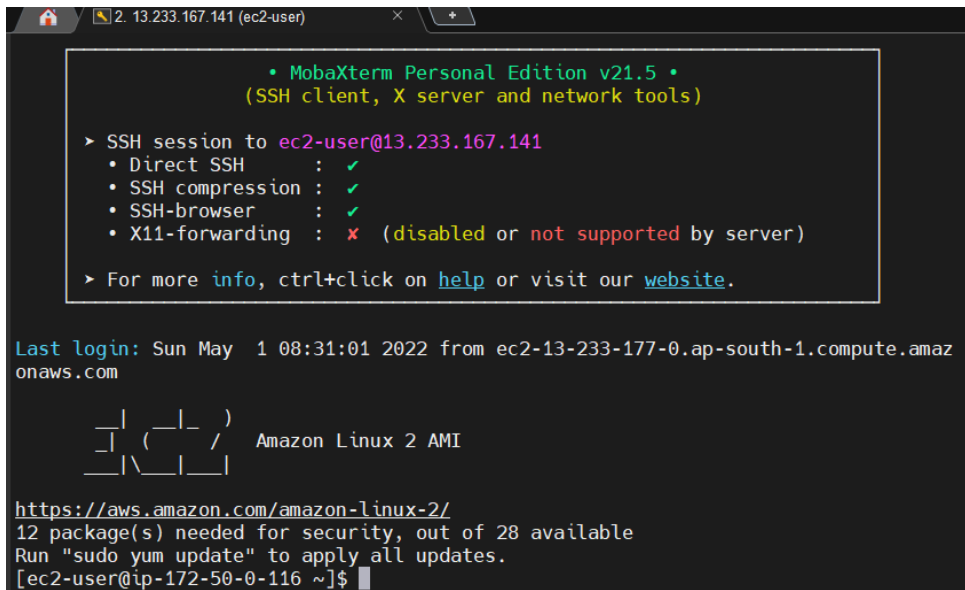
Buckets are containers for data stored in S3. [Learn more](#) 

< 1 >



	Name ▲	AWS Region ▼	Access ▼	Creation date ▼
<input type="radio"/>	difvdsildsiu	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	May 1, 2022, 13:58:58 (UTC+05:30)
<input type="radio"/>	kjdfbgdfkj	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	April 28, 2022, 10:25:46 (UTC+05:30)

Connect public instance to Moba with public IP



```
2. 13.233.167.141 (ec2-user) x +

• MobaXterm Personal Edition v21.5 •
(SSH client, X server and network tools)

> SSH session to ec2-user@13.233.167.141
• Direct SSH : ✓
• SSH compression : ✓
• SSH-browser : ✓
• X11-forwarding : ✗ (disabled or not supported by server)

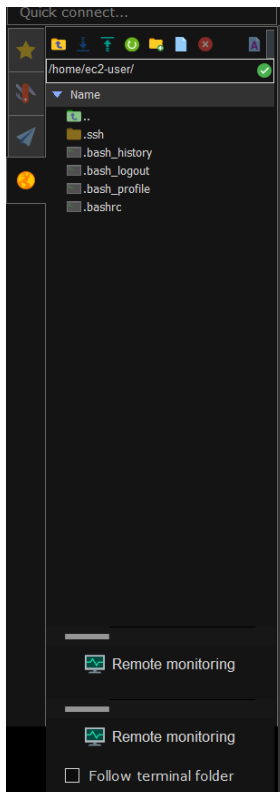
> For more info, ctrl+click on help or visit our website.

Last login: Sun May 1 08:31:01 2022 from ec2-13-233-177-0.ap-south-1.compute.amazonaws.com

 _ | _ | _ |
 _ | ( _ | /   Amazon Linux 2 AMI
 _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
12 package(s) needed for security, out of 28 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-50-0-116 ~]$
```

Upload key



Now we can get SSH of private instance via **Public IP**

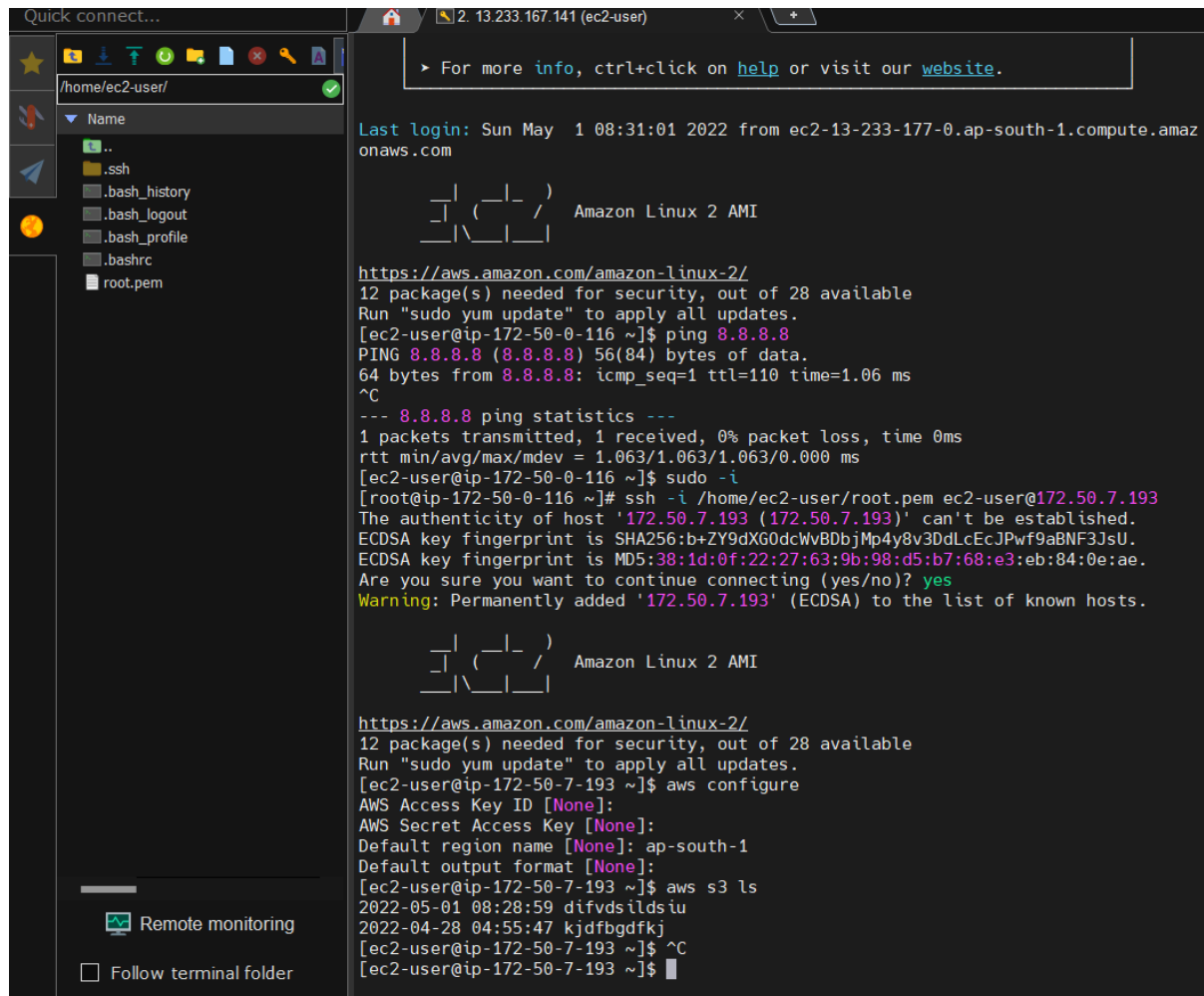
Switch to root

```
#sudo -i
```

```
#ssh -i /home/ec2-user/root.pem ec2-user@172.50.7.193
```

```
#aws configure [Provide same region]
```

```
#aws s3 ls
```



The screenshot shows a terminal window with a file explorer on the left and a terminal on the right. The file explorer shows the contents of the /home/ec2-user/ directory, including .ssh, .bash_history, .bash_logout, .bash_profile, .bashrc, and root.pem. The terminal window shows the following commands and output:

```
Last login: Sun May 1 08:31:01 2022 from ec2-13-233-177-0.ap-south-1.compute.amazonaws.com

_ _ | ( _ _ | _ )
_ | ( _ _ | _ ) /
_ | \ _ _ | _ |

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
12 package(s) needed for security, out of 28 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-50-0-116 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=1.06 ms
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.063/1.063/1.063/0.000 ms
[ec2-user@ip-172-50-0-116 ~]$ sudo -i
[root@ip-172-50-0-116 ~]# ssh -i /home/ec2-user/root.pem ec2-user@172.50.7.193
The authenticity of host '172.50.7.193 (172.50.7.193)' can't be established.
ECDSA key fingerprint is SHA256:b+ZY9dXG0dcWvBDbjMp4y8v3DdLcEcJPwf9aBNF3JsU.
ECDSA key fingerprint is MD5:38:1d:0f:22:27:63:9b:98:d5:b7:68:e3:eb:84:0e:ae.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.50.7.193' (ECDSA) to the list of known hosts.

_ _ | ( _ _ | _ )
_ | ( _ _ | _ ) /
_ | \ _ _ | _ |

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
12 package(s) needed for security, out of 28 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-50-7-193 ~]$ aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]: ap-south-1
Default output format [None]:
[ec2-user@ip-172-50-7-193 ~]$ aws s3 ls
2022-05-01 08:28:59 difvdsildsiu
2022-04-28 04:55:47 kjdfbgdfkj
[ec2-user@ip-172-50-7-193 ~]$ ^C
[ec2-user@ip-172-50-7-193 ~]$
```

Now we can successfully access aws s3 buckets without internet.