

VPC Endpoint

VPC endpoints enable you to connect your VPC resources to supported AWS services and other VPCs without requiring an internet gateway, NAT gateway, VPN or a DC connection.

This runbook simulates the Gateway VPC endpoints:

- Gateway endpoints provide access to S3 and DynamoDB to resources in a private subnet without using public addressing.

Prerequisite

- VPC
- min 1 public subnet (you will need a jump box in a public subnet)
- min 1 private subnet (Don't include NAT Gateway in private route table)

TIP: You can use the VPC launch wizard to create the above networking configuration

1. Create a Security group and give it a name **Bastion-SG**. Open port 22 to the internet.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
<input type="text" value="SSH"/>	TCP	22	<input type="text" value="Anywh..."/> <input type="text" value="0.0.0.0/0"/> <input type="text" value="0.0.0.0/0"/>	

Add rule

2. Create another Security group with the name **Appserver-SG**. Open port 22 to Bastion-SG

VPC > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>
SSH	TCP	22	Custom

CIDR blocks

Security Groups

Bastion-SG | [sg-09ab8f30692464474](#)

Prefix lists

sg-09ab8f30692464474 X

sg-09ab8f30692464474 X

- create a keypair for ssh named e.g **bastion**
- Create 1 instance in the public subnet **of the VPC-endpoint VPC** using Amazon linux 2 AMI and give it a name **JJtech-Bastion**. Attach the Bastion security group (Bastion-SG) to the instance

▼ Network settings

Info

Network settings for public Bastion EC2

VPC - required

Info

vpc-043f791cd9e850e74 (VPC-endpoint-vpc)

10.0.0.0/16

↻

Subnet

Info

subnet-031367af84f1ec8d5

VPC-endpoint-subnet-public1-us-east-1a

VPC: vpc-043f791cd9e850e74 Owner: 945685952191 Availability Zone: us-east-1a

IP addresses available: 4091 CIDR: 10.0.0.0/20

↻

Create new su

Auto-assign public IP

Info

Enable

↻

Additional charges apply when outside of free tier allowance

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 yo instance.

☐ Create security group

☒ Select existing security group

Common security groups

Info

Select security groups

↻

Bastion-SG sg-09ab8f30692464474

×

VPC: vpc-043f791cd9e850e74

↻

Compare secur group rules

- Create another instance in the private subnet **of the VPC-endpoint VPC** using Amazon linux 2 AMI and give it a name **JJtech-AppServer**. Use the Appserver-SG created above

▼ Network settings

Info

Network settings for private AppServer EC2

VPC - required

Info

vpc-043f791cd9e850e74 (VPC-endpoint-vpc)

10.0.0.0/16

↻

Subnet

Info

subnet-0ec3f6aa425e610ef

VPC-endpoint-subnet-private1-us-east-1a

VPC: vpc-043f791cd9e850e74 Owner: 945685952191 Availability Zone: us-east-1a

IP addresses available: 4090 CIDR: 10.0.128.0/20

↻

Create new subnet

Auto-assign public IP

Info

Disable

↻

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

Common security groups

Info

Select security groups

↻

Appserver-SG sg-0cec28bf68e586b15

×

VPC: vpc-043f791cd9e850e74

↻

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

6. SSH into the Bastion server

Instances (1/4) Info									
Filter instances									
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 address
<input checked="" type="checkbox"/>	Bastion	i-00f677f3e88fecb12	Running	t2.micro	2/2 checks passed	No alarms	us-east-2a	ec2-3-14-246-131.us-east-2.compute.amazonaws.com	3.14.246.131
<input type="checkbox"/>	Webserver	i-0a5bebfff10570066	Running	t2.micro	Initializing	No alarms	us-east-2b	-	-
<input type="checkbox"/>	-	i-03be371f7d42c3aff	Stopped	t2.micro	-	No alarms	us-east-2a	-	-
<input type="checkbox"/>	-	i-07b4108e2c1251b0b	Stopped	t2.micro	-	No alarms	us-east-2b	-	-

Instance: i-00f677f3e88fecb12 (Bastion)

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
<div>▼ Instance summary Info</div> <div> <div>Instance ID</div> <div>i-00f677f3e88fecb12 (Bastion)</div> </div> <div> <div>IPv6 address</div> <div>-</div> </div> <div> <div>Private IPv4 DNS</div> <div>ip-10-0-0-82.us-east-2.compute.internal</div> </div> <div> <div>VPC ID</div> <div>vpc-04cca9b16ba32ce56 (Endpoint)</div> </div> <div> <div>Subnet ID</div> <div>subnet-0621ab913a4a7607 (Endpoint-Pub)</div> </div> <div> <div>Public IPv4 address</div> <div>3.14.246.131 open address</div> </div> <div> <div>Instance state</div> <div>Running</div> </div> <div> <div>Instance type</div> <div>t2.micro</div> </div> <div> <div>AWS Compute Optimizer finding</div> <div>No recommendations available for this instance.</div> </div> <div> <div>Private IPv4 addresses</div> <div>10.0.0.82</div> </div> <div> <div>Public IPv4 DNS</div> <div>ec2-3-14-246-131.us-east-2.compute.amazonaws.com</div> </div> <div> <div>Elastic IP addresses</div> <div>-</div> </div> <div> <div>IAM Role</div> <div>EC2-SSM-Mandatory</div> </div>						

```

ec2-user@ip-10-0-0-82:~
$ cd Downloads/
suskan04@10230-LT-X0317 MINGW64 ~/Downloads
$ chmod 400 endpointkey.pem
suskan04@10230-LT-X0317 MINGW64 ~/Downloads
$ ssh -i "endpointkey.pem" ec2-user@ec2-3-14-246-131.us-east-2.compute.amazonaws.com
The authenticity of host 'ec2-3-14-246-131.us-east-2.compute.amazonaws.com (3.14.246.131)' can't be established.
ED25519 key fingerprint is SHA256:CBMD1XBS1ojW7q5i+Pi34UuiyZ66kA2mkForHrzdYDA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-3-14-246-131.us-east-2.compute.amazonaws.com' (ED25519) to the list of known hosts.

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

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
11 package(s) needed for security, out of 35 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-82 ~]$

```

7. While in the Bastion server SSH into the Appserver.

- Create a file bastion.pem
- copy the content of the pem file from the downloads folder to the bastion.pem

c. Windows users:

- i. Open file explorer and open file using notepad. Copy content to bastion.pem

Instances (1/4) Info

Filter instances

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 address
<input type="checkbox"/>	Bastion	i-00f677f3e88fecb12	Running	t2.micro	2/2 checks passed	No alarms	us-east-2a	ec2-3-14-246-131.us-e...	3.14.246.131
<input checked="" type="checkbox"/>	Webserver	i-0a5bebf10570066	Running	t2.micro	Initializing	No alarms	us-east-2b	-	-
<input type="checkbox"/>	-	i-03be371f7d42c3aff	Stopped	t2.micro	-	No alarms	us-east-2a	-	-
<input type="checkbox"/>	-	i-07b4108e2c1251b0b	Stopped	t2.micro	-	No alarms	us-east-2b	-	-

Instance: i-0a5bebf10570066 (Webserver)

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

Instance summary Info

Instance ID

i-0a5bebf10570066 (Webserver)

IPv6 address

-

Private IPv4 DNS

ip-10-0-1-98.us-east-2.compute.internal

VPC ID

vpc-04cca9b16ba32ce56 (Endpoint)

Subnet ID

Public IPv4 address

-

Instance state

Running

Instance type

t2.micro

AWS Compute Optimizer finding

No recommendations available for this instance.

Private IPv4 addresses

10.0.1.98

Public IPv4 DNS

-

Elastic IP addresses

-

IAM Role

EC2-SSM-Mandatory

```
ec2-user@ip-10-0-1-98:~  
[ec2-user@ip-10-0-0-82 ~]$ vi bastion.pem  
[ec2-user@ip-10-0-0-82 ~]$ cat bastion.pem  
-----BEGIN RSA PRIVATE KEY-----  
MIIEpAIBAAKCAQEAsAqAF100tcJjzo6bT8hoUaoM6K4JDjUOLzIikR0ER9VVo8kE  
ksyz3YB8xIYIARffBj/iSw/CL1UMPYcCqeJddHpp7eXi4RUPv/mvQ+R31VAWNrkq  
Jaw4sFIm7xxX19rNYSZF8RkXnA/ZgYoMv5Yx1oulsE83Cz3+LXbJWljLwWpBPPCZ  
hCId/+WC9kv46KMJ4yGiaeHUoR2uHBSPh8Ktt1+L CbzkXAs3biYiyuhCNxtQlV  
GQkgfbJw/1kyRoHzLajSz5p+6+3vt9TJXtkAS00jLmodvkD0lve78pnhZlCr7wzm  
AVA4+1ITRfaa+iv/LFQeKrrFb6Jm4xGDlUlaAwIDAQABAoIBAA0A0YV/gRELuion  
FIH46xkSp/Eepa6BFon8bwV1wMXfKQKTHQq+f2Zx50b60trv+TOQv/5aPXl6gmB  
Nwk1UXWQtNIE8ER/MbKT1gXfkbQHPHy8gAhXvNQIvSdbiIFAf3qT+gZcPAoigYW3  
7Elx5ixaE9p5fy8tXOAuraAmfQXB+8Dm8IkERpC7RV7+ZkxL/2n4h+6L124k8wv8  
Czma1b8fPIXYaEBJj1oi67ifCyqXACDEWB5p5V6qWCJpSpmHFT7YdRBzqmdsDZV9  
cCZ+QDM0XYMb80TnM0Xehtii7XQAVVco1sC476HM1x//1U3Q7t7ZSivxaf90woVy  
oRiZXkECgYEA2oPT75E5BxH+PZw6/qz/ReXWhczi22PGvGZAEgy6ov5RE248S6Mm  
QVVCzjPiviXUA38v50pH/RLworaQrMlHfdAN9ZHkEfzYgecq75ltJ+bVhOQbjZUv  
BN10wW8rusu3p3SC2QbKVZ0S+e7nppp6rnG55FIDYrTw0Fh6lhx/G+0CgYEAzj1p  
mXLhECpbDsupwqGSJw0+k52xxHFCnevsRly1QmGKiBfI58nNiSs5V3nttfKMjzj9  
t4Bd7GEK0e8AiLmmaAEPqNTTjVSrUACpCwJkTe153Nc1nM0ifG4veByjIzc0RiqQd  
1lL5z1X4YrXl0S0zLu0jeygTvTw9iv/zP9A/768CgYAFfPYfuDgEc3E9PuVEbDf1  
G4atyZ20FzVwmejwAMUXPufuYwBkre5SCcApyafS0sT+aX1cg8MXGhGF8ivkCxiE  
mNEg788YnI8bhCDR77qMHAIU2l3oyoZpyt0i5eXlRSSRsh1vMfp2+AD4AgYTayHV  
q8mNcHnhSsYZlX90sdyHaQKBgQDHdu3i0w2t/+kBbkhJTSq1S1HzQtjjPQdI5Rwn  
ERLdmKj65sYQJ0T6HSvgRrR4/JS1EGGSUDyGmY0H2veRRLwgFY821k8m/Xz8hbLD  
M0l7WFHDX10mGFWJtsSN+Av9vw/wHrocXz0EK4mHLpVg077Y4qECQ8iThOegv9rr  
JOYxUQKBgQDYIitAKV9fB0aGNv4xt6zXFU/kcRx3Z0gdw9dtmLTxG4GGGjOND3mf  
9d6R+o842thDBSmZzOCz6fwQBgnSqhrQytjwvEtmTaTe9iUkuz/2bp6pfN8OvnO  
3ejeZU72afB9gR8RxZSheBD6x+Nb5gpjgSrRzn+rJjU406JSR4o9ig==  
-----END RSA PRIVATE KEY-----  
[ec2-user@ip-10-0-0-82 ~]$ chmod 400 bastion.pem  
[ec2-user@ip-10-0-0-82 ~]$ ssh -i bastion.pem ec2-user@10.0.1.98  
  
  _ | _ | _ )  
  _ | ( _ /   Amazon Linux 2 AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
11 package(s) needed for security, out of 35 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-10-0-1-98 ~]$ |
```

From the above screen you see that you are now in the private instance.

Note:

Steps 6 and 7 could be achieved using **SSH agent forwarding**

- Add the private key to the ssh agent. Change into the directory with the private key
 - **ssh-add [bastion.pem]**
- **ssh -A [username]@[server-public-address]** to ssh into the public bastion host

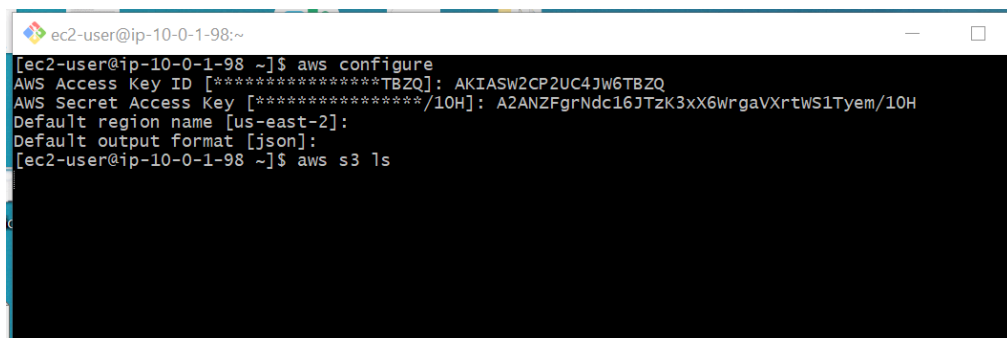
- `ssh -A [ec2-user]@[3.87.73.227]`
- **You should be in the public bastion host. confirm this by comparing its private IP with the private IP on the AWS console**

from the bastion host, you can confirm the ssh key from your local has been forwarded into the bastion host using the command

ssh-add -L

- **ssh into the private server from the bastion host using**
 - `ssh [ec2-user]@[private-IP-of-Appserver]`
e.g `ssh ec2-user@10.0.132.120`

8. Since this is an amazon linux instance it comes with AWS CLI already Run aws configure and give the accesskey and secret key and try to access s3
 - a. Run aws s3 ls
 - b. It will not list the buckets in your account. You will notice that it will time out. To make connection possible we need to create a VPC endpoint



```

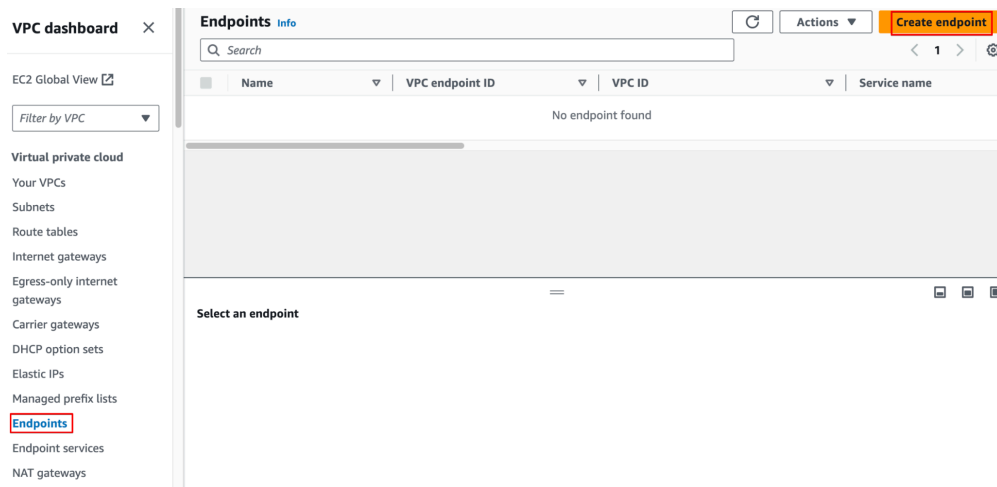
ec2-user@ip-10-0-1-98:~
[ec2-user@ip-10-0-1-98 ~]$ aws configure
AWS Access Key ID [*****]: AKIASW2CP2UC4JW6TBZQ
AWS Secret Access Key [*****]: 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
Default region name [us-east-2]:
Default output format [json]:
[ec2-user@ip-10-0-1-98 ~]$ aws s3 ls

```

9. Creating Gateway endpoint:

Now we will create a VPC endpoint for S3.

Go to the VPC console, select **Endpoints** from drop down menu and click on create Endpoint



10. Enter configuration details:

- Name the Endpoint (e.g s3GatewayEndpoint) to be created
- Under **Service category**, select **AWS services** and under **Services**, search for s3 and select the s3 service endpoint.

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 the AWS Marketplace

☐ **EC2 Instance Connect Endpoint**
An elastic network interface that allow you to connect to resources in a private subnet

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

Services (1/2)

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

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

- Choose the vpc and select the private subnet route table since we will be accessing S3 from the private subnet.

VPC
Select the VPC in which to create the endpoint

VPC
The VPC in which to create your endpoint.

vpc-043f791cd9e850e74 (VPC-endpoint-vpc)

Route tables (1/3) [Info](#)

<input type="checkbox"/>	Name	Route Table ID	Main	Associated Id
<input type="checkbox"/>	-	rtb-003966be8555fba3b	Yes	-
<input checked="" type="checkbox"/>	VPC-endpoint-rtb-private1-us-east-1a	rtb-043edbd9bfa0e20db (VPC-endpoint...	No	subnet-0ec3f6aa425e610ef (VPC-endpoint-subnet-private1-us-east-1a)
<input type="checkbox"/>	VPC-endpoint-rtb-public	rtb-0b53e3432581b8afb (VPC-endpoint...	No	subnet-031367af84f1ec8d5 (VPC-endpoint-subnet-public1-us-east-1a)

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.

b-043edbd9bfa0e20db

Policy [Info](#)
VPC endpoint policy controls access to the service.

Full access

11. Click on **create endpoint** and you will see the endpoint created in the console.

12. Next check the private subnet route table and you will notice that a route has been added for the VPC endpoint as shown below.

Route tables (1/1) [Info](#) **Actions** **Create route table**

Route table ID: rtb-07a75dced274d25e9

Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Ow...												
rtb-07a75dced274d25e9 / private-rt-endpoint																	
<div> <div>Details</div> <div>Routes</div> <div>Subnet associations</div> <div>Edge associations</div> <div>Route propagation</div> <div>Tags</div> </div>																	
<p>Routes (2) </p> <p><input type="text" value="Filter routes"/> Both </p> <table border="1"> <thead> <tr> <th>Destination</th> <th>Target</th> <th>Status</th> <th>Propagated</th> </tr> </thead> <tbody> <tr> <td>10.0.0.0/16</td> <td>local</td> <td>Active</td> <td>No</td> </tr> <tr> <td>pl-63a5400a</td> <td>vpce-0677b0a6414ff2fc3</td> <td>Active</td> <td>No</td> </tr> </tbody> </table>						Destination	Target	Status	Propagated	10.0.0.0/16	local	Active	No	pl-63a5400a	vpce-0677b0a6414ff2fc3	Active	No
Destination	Target	Status	Propagated														
10.0.0.0/16	local	Active	No														
pl-63a5400a	vpce-0677b0a6414ff2fc3	Active	No														

13. Finally try the command to access S3 and you will notice that you now have access to S3.

\$ aws s3 ls

```
ec2-user@ip-10-0-1-98:~  
suskan04@10230-LT-X0317 MINGW64 ~/Downloads  
comh -i "endpointkey.pem" ec2-user@ec2-3-14-246-131.us-east-2.compute.amazonaws.  
Last login: Mon Sep 27 23:00:28 2021 from ads1-76-198-95-106.dsl.bkfd14.sbcglobal.net  
  
  _| _| _| _|  
  _| ( _| _| _| Amazon Linux 2 AMI  
  _| \ _| _| _|  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-0-82 ~]$ ssh -i bastion.pem ec2-user@10.0.1.98  
Last login: Mon Sep 27 23:43:52 2021 from ip-10-0-0-82.us-east-2.compute.internal  
  
  _| _| _| _|  
  _| ( _| _| _| Amazon Linux 2 AMI  
  _| \ _| _| _|  
  
https://aws.amazon.com/amazon-linux-2/  
11 package(s) needed for security, out of 35 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-10-0-1-98 ~]$ aws s3 ls  
2021-08-09 16:43:25 amazon-connect-8c32434d8a62  
2021-08-09 10:55:35 amazon-connect-f2604b5e259c  
2021-05-06 04:04:05 aws-application-discovery-service-6cku1wlkpsr0ns8r6g8ldtg43  
2021-08-27 19:43:40 aws-cloudtrail-logs-186433656069-09cc2ce6  
2021-03-30 13:03:59 aws-glue-scripts-186433656069-us-east-2  
2021-03-30 13:04:00 aws-glue-temporary-186433656069-us-east-2  
2021-04-09 07:21:33 aws-logs-186433656069-us-east-2  
2021-08-09 11:02:05 catchupbucket  
2021-08-06 09:25:02 central-logging-bucket123  
2021-08-09 10:55:29 cf-templates-n4mkzpvylu80-us-east-1  
2021-03-05 14:11:17 cf-templates-n4mkzpvylu80-us-east-2  
2021-06-13 16:32:46 cf-templates-n4mkzpvylu80-us-west-2  
2021-08-09 10:55:36 cloudtrail-awslogs-186433656069-soelvou9-isengard-do-not-delete  
2021-03-05 14:39:26 config-bucket-186433656069
```

Now you can see all the buckets are visible from the private server. That is because you created a gateway endpoint 🤔