

Setting up Transit Gateway and VPC Endpoints for a MultiVPC Architecture.

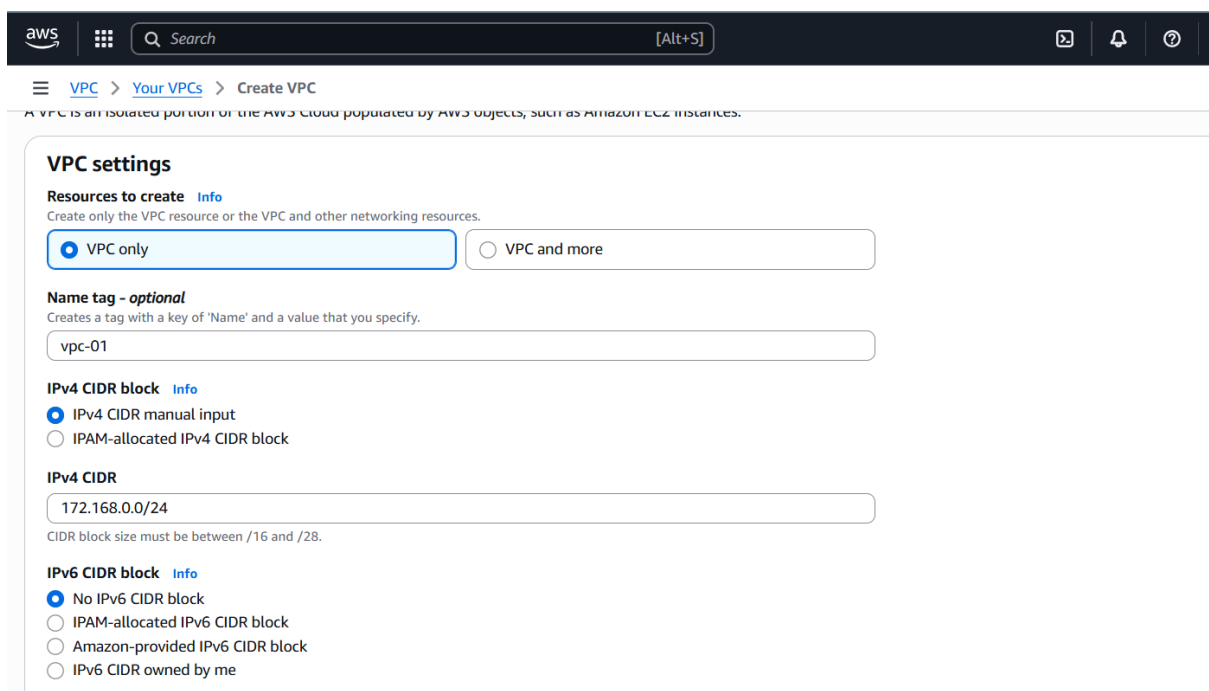
SCENARIO:

A large organization is migrating its on-premises infrastructure to the AWS cloud.

The organization's architecture involves multiple VPCs for different departments and applications, each requiring secure communication with centralized services and external resources.

The IT team needs to design and implement a scalable and efficient network architecture to accommodate the organization's growth and ensure robust connectivity between VPCs and external services.

Create 3 VPC's one for public and 2 for private.



The screenshot shows the AWS Management Console interface for creating a new VPC. The breadcrumb navigation at the top indicates the path: **VPC** > **Your VPCs** > **Create VPC**. Below the navigation bar, a descriptive line states: "A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances." The main content area is titled "VPC settings" and includes several configuration sections:

- Resources to create** (with an "Info" link): A note says "Create only the VPC resource or the VPC and other networking resources." There are two radio button options: "VPC only" (which is selected) and "VPC and more".
- Name tag - optional** (with an "Info" link): A note says "Creates a tag with a key of 'Name' and a value that you specify." A text input field contains the value "vpc-01".
- IPv4 CIDR block** (with an "Info" link): Two radio button options are present: "IPv4 CIDR manual input" (selected) and "IPAM-allocated IPv4 CIDR block". Below these, a text input field for the "IPv4 CIDR" contains the value "172.168.0.0/24". A small note below the field states: "CIDR block size must be between /16 and /28."
- IPv6 CIDR block** (with an "Info" link): Four radio button options are present: "No IPv6 CIDR block" (selected), "IPAM-allocated IPv6 CIDR block", "Amazon-provided IPv6 CIDR block", and "IPv6 CIDR owned by me".

Your VPCs (3/5) [Info](#)

Last updated less than a minute ago [Actions](#) [Create VPC](#)

Find VPCs by attribute or tag

<input type="checkbox"/>	Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	my-vpc	vpc-0b3ab1c3d8a1c0bdb	Available	Off	10.0.0.0/16	-
<input checked="" type="checkbox"/>	vpc-01	vpc-0af726d176c49904e	Available	Off	172.168.0.0/24	-
<input checked="" type="checkbox"/>	vpc-02	vpc-0b96ede37d17a943c	Available	Off	10.0.1.0/28	-
<input checked="" type="checkbox"/>	vpc-03	vpc-0f6b4aea545ed4a65	Available	Off	10.0.0.0/28	-

VPCs: vpc-0af726d176c49904e, vpc-0b96ede37d17a943c, vpc-0f6b4aea545ed4a65

VPC dashboard

AWS Global View

Filter by VPC

Virtual private cloud

- Your VPCs
- Subnets**
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP option sets

You have successfully created 1 subnet: subnet-0578113227cc73af7

Last updated less than a minute ago

Subnets (3/8) info

Find subnets by attribute or tag

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
vpc-1-subnet	subnet-0420ecddb617afb9	Available	vpc-0af726d176c49904e vpc-01	Off	172.168.0.0
vpc-2-subnet	subnet-03044c10e4caa8517	Available	vpc-0b96ede37d17a943c vpc-02	Off	10.0.1.0/28
vpc-3-subnet	subnet-0578113227cc73af7	Available	vpc-0f6b4aea545ed4a65 vpc-03	Off	10.0.0.0/28

Subnets: subnet-0420ecddb617afb9, subnet-03044c10e4caa8517, subnet-0578113227cc73af7

☰ VPC > Transit gateways > Create transit gateway

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts:

Name tag

my-tg

Set the description of your transit gateway to help you identify it in the future.

description

Amazon side Autonomous System Number (ASN) | Info

- ✓ DNS support [Info](#)
- ✓ Security Group Referencing support [Info](#)
- ✓ VPN ECMP support [Info](#)
- ✓ Default route table association [Info](#)

Create transit gateway attachments for three vpc's. and give the subnet associations, for public subnet attach the internet gateway.

ay attachments

You can visualize and monitor your Transit Gateway(s) from the [AWS Network Manager](#). Register your Transit Gateway by creating a [global network](#) to get started.

Transit gateway attachments (3/3) Info

Find transit gateway attachment by attribute or tag

<input checked="" type="checkbox"/>	Name	Transit gateway attachment ID	Transit gateway ID	State	Resource type	Resource
<input checked="" type="checkbox"/>	vpc-tga1	tgw-attach-00142779ec62afb98	tgw-04639e643a6fbbe0d	Pending	VPC	vpc-0af7
<input checked="" type="checkbox"/>	vpc-tga2	tgw-attach-05cadd678e417fa1a	tgw-04639e643a6fbbe0d	Pending	VPC	vpc-0b9
<input checked="" type="checkbox"/>	vpc-tga3	tgw-attach-0efa3c2dcc6557a80	tgw-04639e643a6fbbe0d	Pending	VPC	vpc-0f6

Transit gateway attachment IDs

tgw-attach-0efa3c2dcc6557a80, tgw-attach-05cadd678e417fa1a, tgw-attach-00142779ec62afb98

Create 3 instances with the 3 vpc's.

Instances (3/4) Info

Last updated less than a minute ago

Connect Instance state Actions Launch instances

Find Instance by attribute or tag (case-sensitive)

All states

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/>	my-vpc-1	i-06fe0f2d7d054cf38	Running	t3.micro	Initializing	View alarms +	eu-north-1c	-
<input checked="" type="checkbox"/>	vpc-3-instance	i-00299d1d857ebebfb	Running	t3.micro	-	View alarms +	eu-north-1c	-
<input type="checkbox"/>	peering-europe	i-001bcffa94af95490	Stopped	t3.micro	-	View alarms +	eu-north-1a	-
<input checked="" type="checkbox"/>	vpc-2-instance	i-00a2341e815728c75	Running	t3.micro	Initializing	View alarms +	eu-north-1a	-

3 instances selected

Monitoring

Configure CloudWatch agent

Alarm recommendations Investigate with AI - new 1h 3h 12h 1d 3d 1w Custom UTC timezone Explore related

Go to first subnet and edit routes add remaining two vpc's cidr range .

Go to aws configure and give the security key and password .

```
[root@ip-172-31-36-222 ~]# aws configure
AWS Access Key ID [None]: AKIATNTADWLTSYF63H5C
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
[root@ip-172-31-36-222 ~]# aws s3 ls
2025-09-29 10:11:05 bucketnew57
2025-09-29 11:34:52 n-virginia-bucket6
2025-10-01 09:35:38 vpc-challenge7
[root@ip-172-31-36-222 ~]#
```

Copy the pem key in local and create a file and paste the pem key in that file.

Add permission to that file `chmod 400 test.pem`

```
Ssh -i test.pem ec2-user@<private ip>
```

```
[root@ip-172-31-36-222 ~]# vi test.pem  
[root@ip-172-31-36-222 ~]# chmod 400 test.pem  
[root@ip-172-31-36-222 ~]# ssh -i test.pem ec2-user@172.31.36.222  
The authenticity of host '172.31.36.222 (172.31.36.222)' can't be established.  
ED25519 key fingerprint is SHA256:4w+Vu2Fuk9B7oyo77R7k9udiFTt6LnLXKRf2teKboSE.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '172.31.36.222' (ED25519) to the list of known hosts.
```

```
#_
##### Amazon Linux 2023
~\#####
~~\####|
~~\###|
~~\#/ https://aws.amazon.com/linux/amazon-linux-2023
~~V~'->
~~~~
~~~~.-.
~/m/'
```

```
Last login: wed Oct 1 09:38:21 2025 from 103.143.169.218  
[ec2-user@ip-172-31-36-222 ~]$
```

After that aws configure.

```
Last login: Wed Oct 1 09:58:21 2025 from 105.175.105.210
[ec2-user@ip-172-31-36-222 ~]$ aws configure
AWS Access Key ID [None]: AKIATNTADWLTSYF63H5C
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
[ec2-user@ip-172-31-36-222 ~]$
```

- Now go to vpc
- Navigate to end points
- Select aws service
- Then select s3 and end point type expres
- Then select gateway
- Create end point the end point has been created
- Now you can access the s3 from the private instance : aws s3 ls

Create an end point.

VPC
Endpoints
Create endpoint

Create endpoint Info

Create the type of VPC endpoint that supports the service, service network or resource to which you want to connect.

Endpoint settings

Specify a name and select the type of endpoint.

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify. Tags help you find and manage your endpoint.

Type Info
Select a category

☒ **AWS services**
Connect to services provided by Amazon with an Interface endpoint, or a Gateway endpoint

☐ **PrivateLink Ready partner services**
Connect to SaaS services which have AWS Service Ready designation with an Interface endpoint. Uses AWS PrivateLink

☐ **AWS Marketplace**
Connect to SaaS with an Interface

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

☐ **Resources**
Connect to resources like Amazon Relational Database Services (RDS) with a Resource endpoint. Uses AWS PrivateLink

☐ **Service network**
Connect to VPC I Uses AWS Privati

☐ **Endpoint services that use NLBs and GWLBs**
Find services shared with you by service name. Connect to a Network LoadBalancer (NLB) service with an Interface endpoint or to a Gateway LoadBalancer (GWLB) service with a Gateway Load Balancer endpoint

VPC
Endpoints
Create endpoint

Services (1/1)

Service Name = com.amazonaws.eu-north-1.s3express
Clear filters

Service Name	Owner	Type	Service R
com.amazonaws.eu-north-1.s3express	amazon	Gateway	eu-north-

Network settings

Select the VPC in which to create the endpoint

VPC
Create the VPC endpoint in the VPC in the same AWS Region from which you will access a resource.

vpc-0db9d4fb39c8bc078 (default vpc)

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

Q Search

<input type="checkbox"/>	Name	Route Table ID	Main	Associated Id
<input type="checkbox"/>	-	rtb-0b42283383e9a976a	Yes	subnet-0446b22818aa451b1 (default-public-subnet)
<input type="checkbox"/>	default-public-subnet	rtb-08080318cb07dc856 (default-publi...	No	subnet-0cc304f411ffbe14c (default-public-subnet)
<input checked="" type="checkbox"/>	default-private-subnet	rtb-04fa92c9c736f604a (default-privat...	No	subnet-05523948fb6f25c67 (default-private-subnet)

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 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-04fa92c9c736f604a](#) X

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

☒ Full access

If we see in the routetable the endpoint is created for private subnet.

VPC dashboard < **Route tables**

AWS Global View [?](#)

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Security

Network ACLs

Security groups

Route tables (1/6) [Info](#)

Last updated less than a minute ago

Find route tables by attribute or tag

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-0b42283383e9a976a	-	-	Yes	vpc-0db9d...
<input type="checkbox"/>	pri-route-table-task0	rtb-00d57739fabcd9da	-	-	No	vpc-0b3ab...
<input type="checkbox"/>	-	rtb-0729da802662a0c5f	-	-	Yes	vpc-0b3ab...
<input checked="" type="checkbox"/>	default-private-subnet	rtb-04fa92c9c736f604a	subnet-05523948fb6f25...	-	No	vpc-0db9d...
<input type="checkbox"/>	default-public-subnet	rtb-08080318cb07dc856	subnet-0cc304f411ffbe1	-	No	vpc-0db9d...

rtb-04fa92c9c736f604a / default-private-subnet

Details **Routes** Subnet associations Edge associations Route propagation Tags

Routes (2)

Filter routes

Destination	Target	Status	Propagated	Route Origin
pl-05ed086c	vpce-04dadd688d236484f	Active	No	Create Route
172.31.0.0/16	local	Active	No	Create Route Table

```
[root@ip-172-31-36-222 ~]# aws configure
AWS Access Key ID [None]: AKIATNTADWLTSYF63H5C
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
[root@ip-172-31-36-222 ~]# aws s3 ls
2025-09-29 10:11:05 bucketnew57
2025-09-29 11:34:52 n-virginia-bucket6
2025-10-01 09:35:38 vpc-challenge7
[root@ip-172-31-36-222 ~]#
```