VPC- Challenge1

Use Case: Setting up Transit Gateway and VPC Endpoints for a Multi-VPC 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.

Objectives:

- Design and deploy a scalable network architecture using AWS Transit Gateway to simplify network connectivity between multiple VPCs.
- Configure VPC endpoints to securely access AWS services without internet gateways or NAT gateways, ensuring data privacy and minimizing exposure to external threats.

VPC- Challenge1

Objective

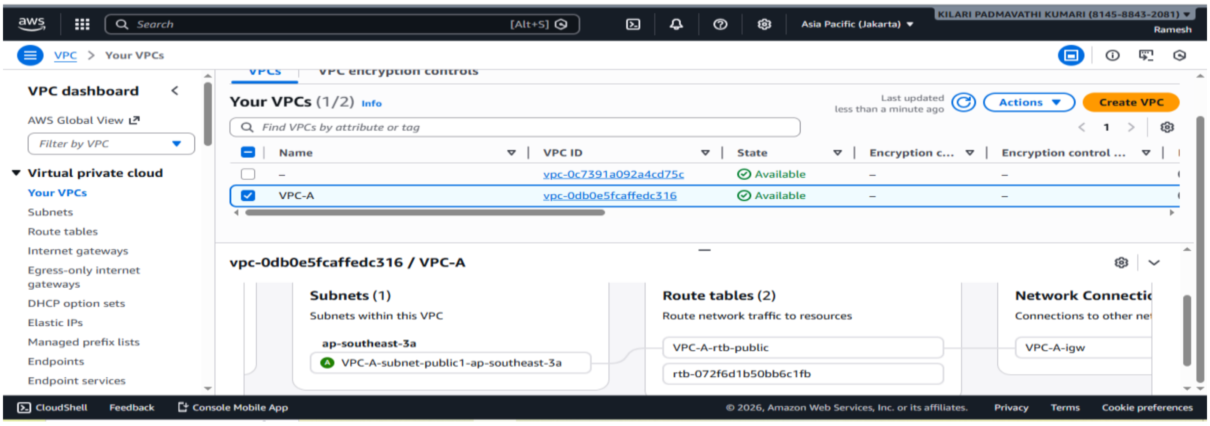
- To design a **centralized, scalable, and secure network architecture** that simplifies connectivity between multiple VPCs using **AWS Transit Gateway**, reducing operational complexity and enabling easy future expansion.

Design Components:

1. Transit Gateway
2. VPC Attachments
3. Transit Gateway Route Tables
4. VPC Route Tables

Deployment Steps

Firstly, create VPC , subnets and Route tables in 3 regions and CIDR should not overlap(Regions:-Jakarta, Malaysia, Melbourne)



Your VPCs (1/2) Info

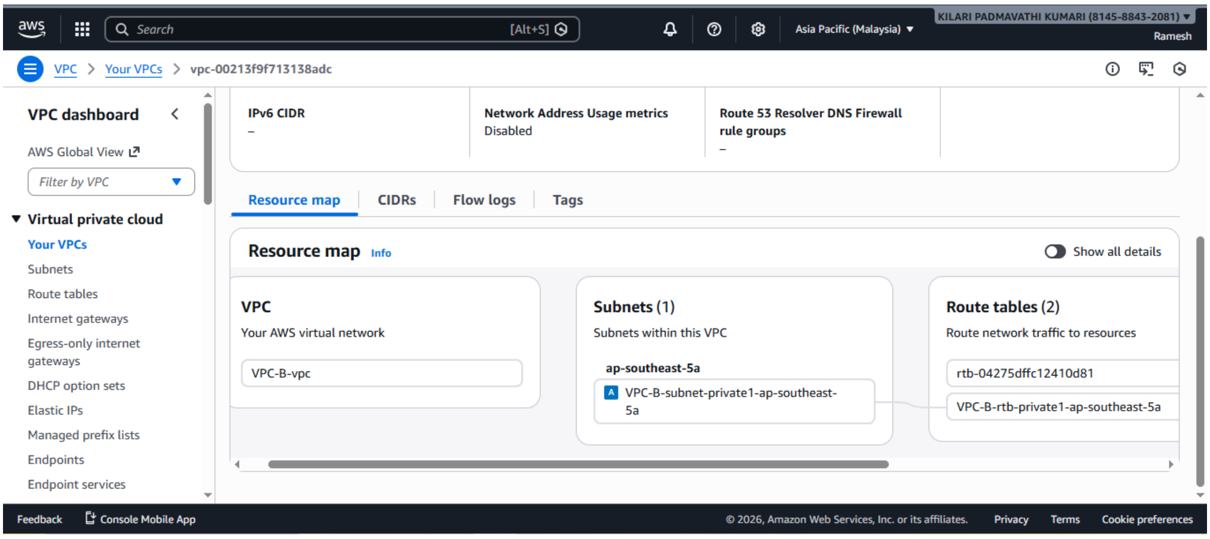
	Name	VPC ID	State	Encryption c...	Encryption control ...
☐	–	vpc-0c7391a092a4cd75c	Available	–	–
☑	VPC-A	vpc-0db0e5fcaffedc316	Available	–	–

vpc-0db0e5fcaffedc316 / VPC-A

Subnets (1)
Subnets within this VPC
ap-southeast-3a
VPC-A-subnet-public1-ap-southeast-3a

Route tables (2)
Route network traffic to resources
VPC-A-rtb-public
rtb-072f6d1b50bb6c1fb

Network Connecti
Connections to other ne
VPC-A-igw



IPv6 CIDR
–

Network Address Usage metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
–

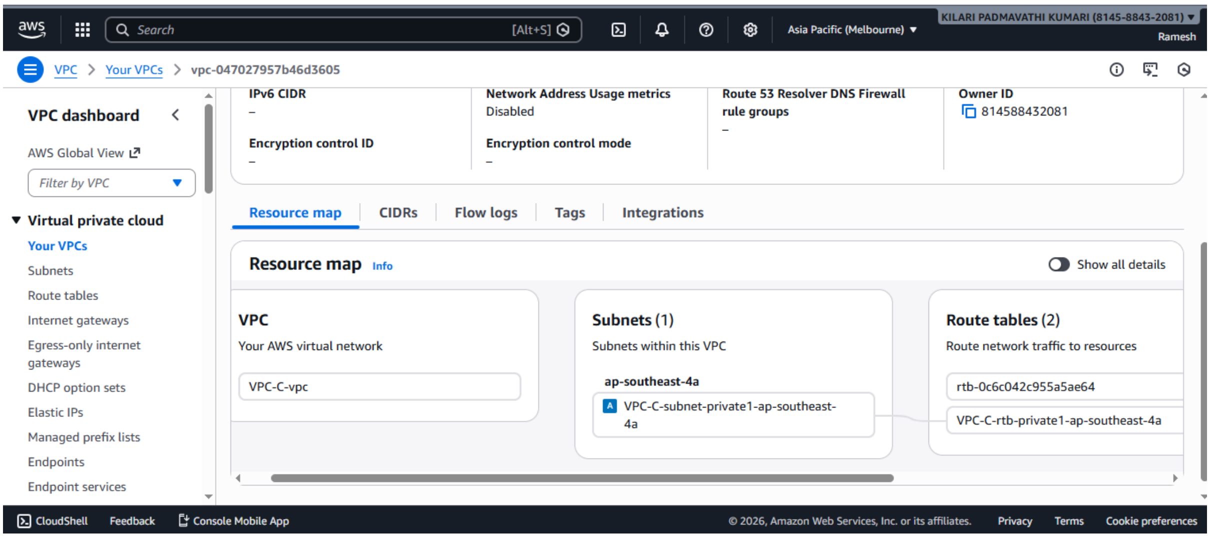
Resource map Info

VPC
Your AWS virtual network
VPC-B-vpc

Subnets (1)
Subnets within this VPC
ap-southeast-5a
VPC-B-subnet-private1-ap-southeast-5a

Route tables (2)
Route network traffic to resources
rtb-04275dffc12410d81
VPC-B-rtb-private1-ap-southeast-5a

VPC- Challenge1



IPv6 CIDR: –
Network Address Usage metrics: Disabled
Route 53 Resolver DNS Firewall rule groups: –
Owner ID: 814588432081
Encryption control ID: –
Encryption control mode: –

Resource map

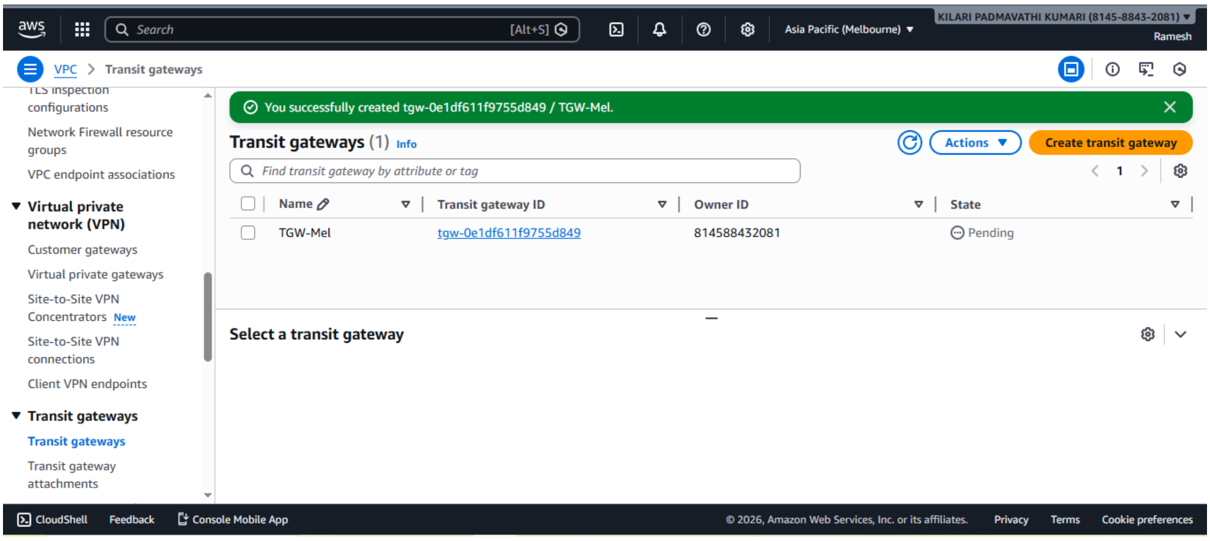
VPC — Your AWS virtual network: VPC-C-vpc

Subnets (1) — Subnets within this VPC: ap-southeast-4a — VPC-C-subnet-private1-ap-southeast-4a

Route tables (2) — Route network traffic to resources: rtb-0c6c042c955a5ae64; VPC-C-rtb-private1-ap-southeast-4a

Step 1: Create a Transit Gateway

- Enable DNS support if required
- Disable auto-accept (recommended for security)

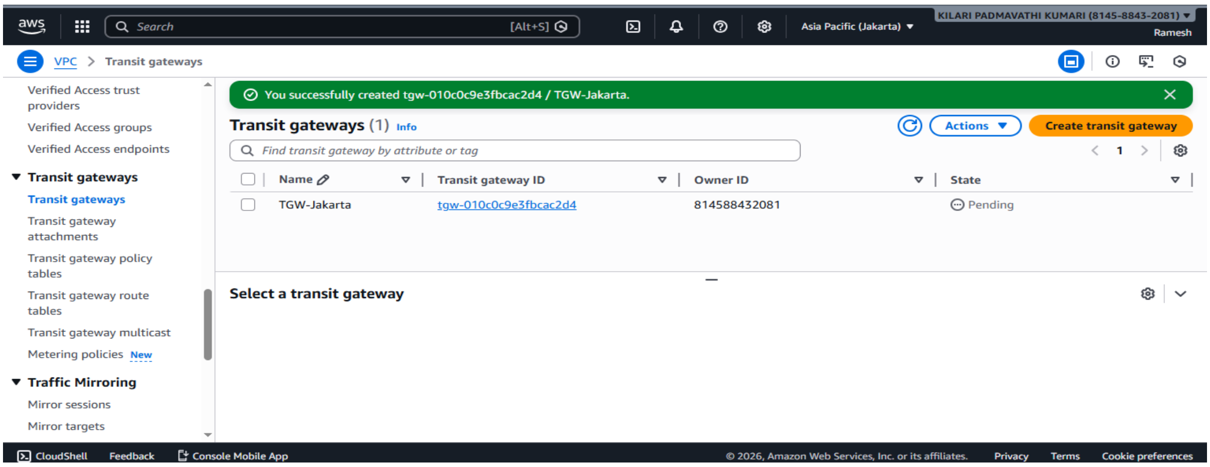

VPC > Transit gateways
TLS inspection configurations
Network Firewall resource groups
VPC endpoint associations
Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN Concentrators New
Site-to-Site VPN connections
Client VPN endpoints
Transit gateways
Transit gateways
Transit gateway attachments
Asia Pacific (Melbourne)
KILARI PADMAVATHI KUMARI (8145-8843-2081)
Ramesh
Actions
Create transit gateway
Find transit gateway by attribute or tag
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

You successfully created tgw-0e1df611f9755d849 / TGW-Mel.

Transit gateways (1)

Name	Transit gateway ID	Owner ID	State
TGW-Mel	tgw-0e1df611f9755d849	814588432081	Pending

Select a transit gateway


VPC > Transit gateways
Verified Access trust providers
Verified Access groups
Verified Access endpoints
Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway multicast
Metering policies New
Traffic Mirroring
Mirror sessions
Mirror targets
Asia Pacific (Jakarta)
KILARI PADMAVATHI KUMARI (8145-8843-2081)
Ramesh
Actions
Create transit gateway
Find transit gateway by attribute or tag
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

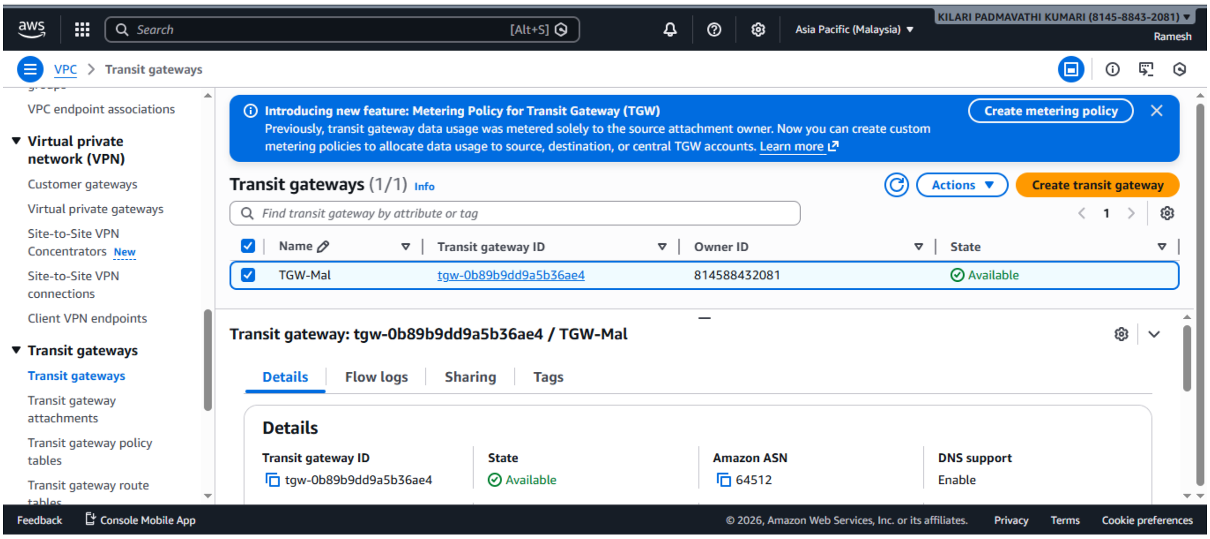
You successfully created tgw-010c0c9e3fbcac2d4 / TGW-Jakarta.

Transit gateways (1)

Name	Transit gateway ID	Owner ID	State
TGW-Jakarta	tgw-010c0c9e3fbcac2d4	814588432081	Pending

Select a transit gateway

VPC- Challenge1



aws
Search
[Alt+S]
Asia Pacific (Malaysia) ▼
KILARI PADMAVATHI KUMARI (8145-8843-2081) ▼
Ramesh
VPC > Transit gateways
VPC endpoint associations
▼ Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN Concentrators New
Site-to-Site VPN connections
Client VPN endpoints
▼ Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Create metering policy
Actions ▼
Create transit gateway
Details
Flow logs
Sharing
Tags
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Introducing new feature: Metering Policy for Transit Gateway (TGW)
Previously, transit gateway data usage was metered solely to the source attachment owner. Now you can create custom metering policies to allocate data usage to source, destination, or central TGW accounts. Learn more

Transit gateways (1/1) Info

☑	Name	Transit gateway ID	Owner ID	State
☑	TGW-Mal	tgw-0b89b9dd9a5b36ae4	814588432081	✓ Available

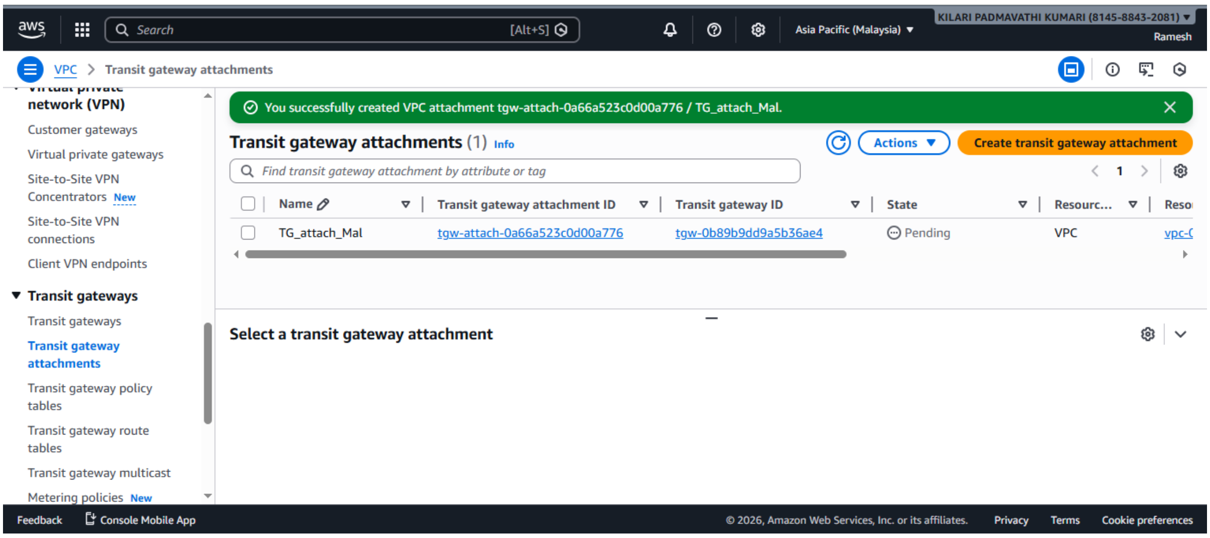
Transit gateway: tgw-0b89b9dd9a5b36ae4 / TGW-Mal

Details

Transit gateway ID	State	Amazon ASN	DNS support
tgw-0b89b9dd9a5b36ae4	✓ Available	64512	Enable

Step 2: Create VPC Attachments

- Attach each VPC to the TGW
- Select private subnets only
- One attachment per VPC



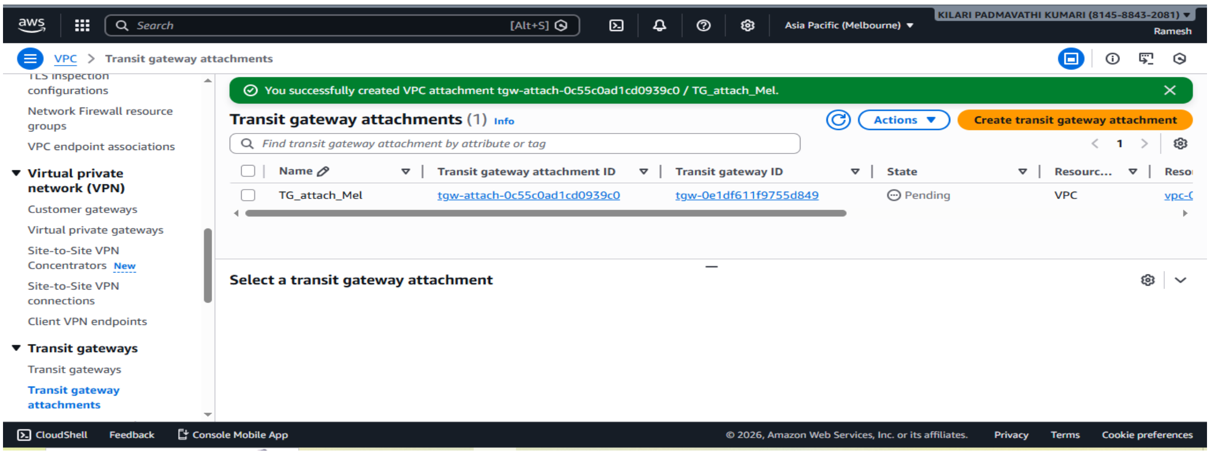
aws
Search
[Alt+S]
Asia Pacific (Malaysia) ▼
KILARI PADMAVATHI KUMARI (8145-8843-2081) ▼
Ramesh
VPC > Transit gateway attachments
network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN Concentrators New
Site-to-Site VPN connections
Client VPN endpoints
▼ Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway multicast
Metering policies New
Actions ▼
Create transit gateway attachment
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

✓ You successfully created VPC attachment tgw-attach-0a66a523c0d00a776 / TG_attach_Mal.

Transit gateway attachments (1) Info

□	Name	Transit gateway attachment ID	Transit gateway ID	State	Resourc...	Reso
□	TG_attach_Mal	tgw-attach-0a66a523c0d00a776	tgw-0b89b9dd9a5b36ae4	Pending	VPC	vpc-(

Select a transit gateway attachment



aws
Search
[Alt+S]
Asia Pacific (Melbourne) ▼
KILARI PADMAVATHI KUMARI (8145-8843-2081) ▼
Ramesh
VPC > Transit gateway attachments
TLS inspection configurations
Network Firewall resource groups
VPC endpoint associations
▼ Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN Concentrators New
Site-to-Site VPN connections
Client VPN endpoints
▼ Transit gateways
Transit gateways
Transit gateway attachments
Actions ▼
Create transit gateway attachment
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

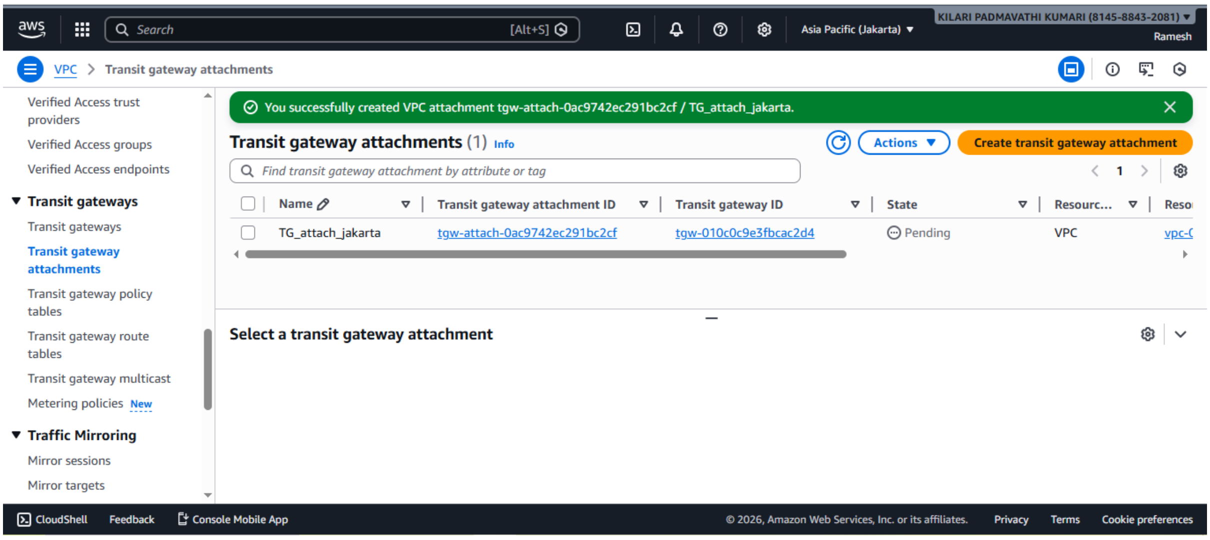
✓ You successfully created VPC attachment tgw-attach-0c55c0ad1cd0939c0 / TG_attach_Mel.

Transit gateway attachments (1) Info

□	Name	Transit gateway attachment ID	Transit gateway ID	State	Resourc...	Reso
□	TG_attach_Mel	tgw-attach-0c55c0ad1cd0939c0	tgw-0e1df611f9755d849	Pending	VPC	vpc-(

Select a transit gateway attachment

VPC- Challenge1


aws
Search [Alt+S]
Asia Pacific (Jakarta)
KILARI PADMAVATHI KUMARI (8145-8843-2081)
Ramesh
VPC > Transit gateway attachments
Verified Access trust providers
Verified Access groups
Verified Access endpoints
Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway multicast
Metering policies New
Traffic Mirroring
Mirror sessions
Mirror targets
Actions
Create transit gateway attachment
Find transit gateway attachment by attribute or tag
1
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

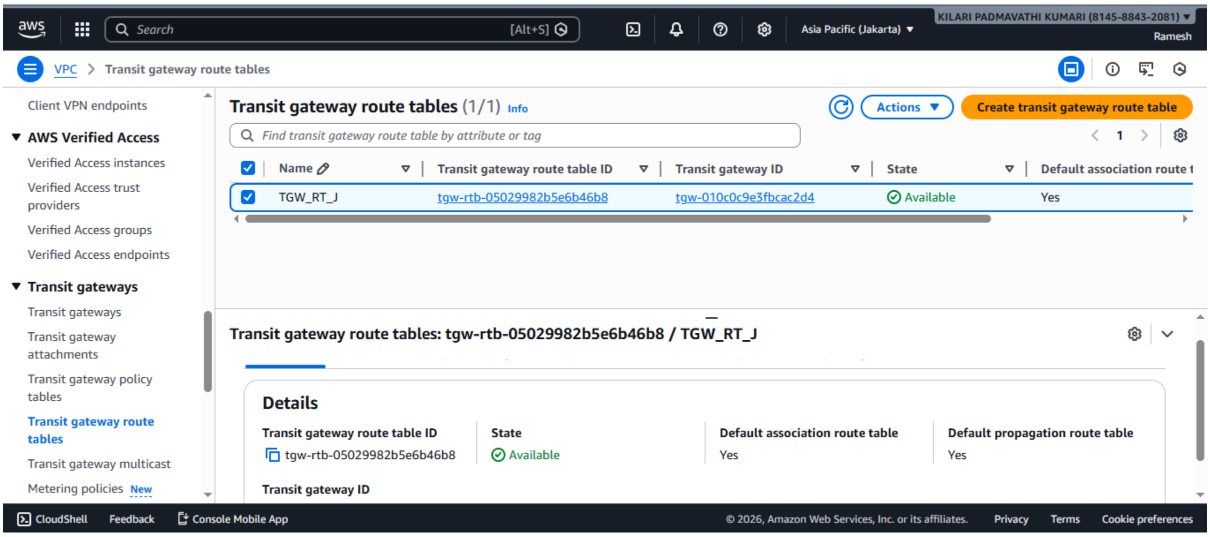
You successfully created VPC attachment tgw-attach-0ac9742ec291bc2cf / TG_attach_jakarta.

Transit gateway attachments (1) Info

□	Name	Transit gateway attachment ID	Transit gateway ID	State	Resourc...	Reso
□	TG_attach_jakarta	tgw-attach-0ac9742ec291bc2cf	tgw-010c0c9e3fbcac2d4	Pending	VPC	vpc-(

Select a transit gateway attachment

Step 3: Configure Transit Gateway Route Tables


aws
Search [Alt+S]
Asia Pacific (Jakarta)
KILARI PADMAVATHI KUMARI (8145-8843-2081)
Ramesh
VPC > Transit gateway route tables
Client VPN endpoints
AWS Verified Access
Verified Access instances
Verified Access trust providers
Verified Access groups
Verified Access endpoints
Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway multicast
Metering policies New
Actions
Create transit gateway route table
Find transit gateway route table by attribute or tag
1
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Transit gateway route tables (1/1) Info

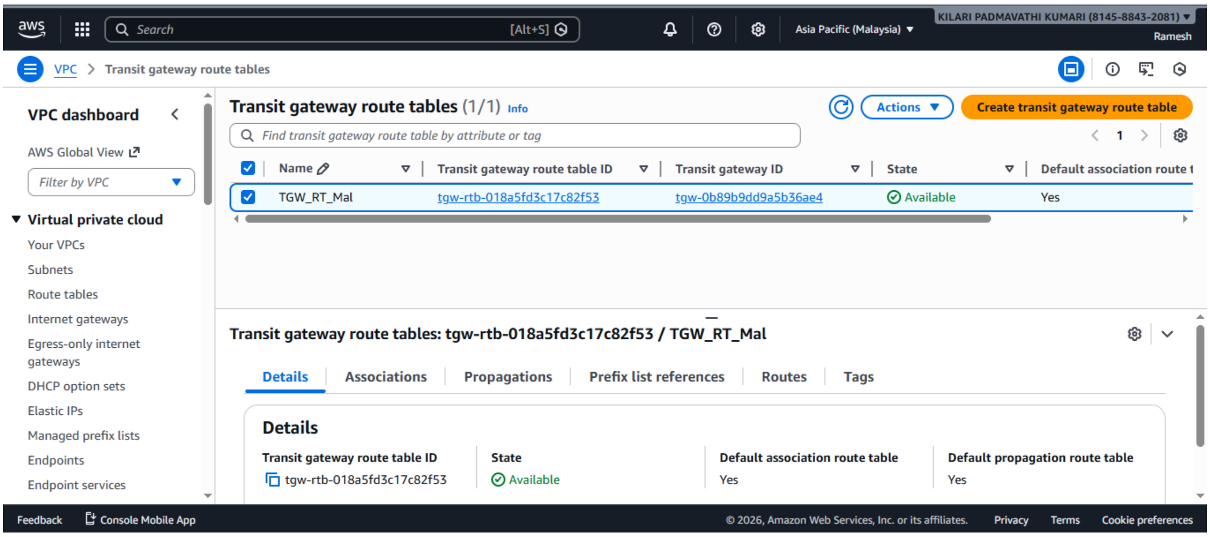
☑	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route t
☑	TGW_RT_J	tgw-rtb-05029982b5e6b46b8	tgw-010c0c9e3fbcac2d4	Available	Yes

Transit gateway route tables: tgw-rtb-05029982b5e6b46b8 / TGW_RT_J

Details

Transit gateway route table ID	State	Default association route table	Default propagation route table
tgw-rtb-05029982b5e6b46b8	Available	Yes	Yes

Transit gateway ID



Transit gateway route tables (1/1) Info

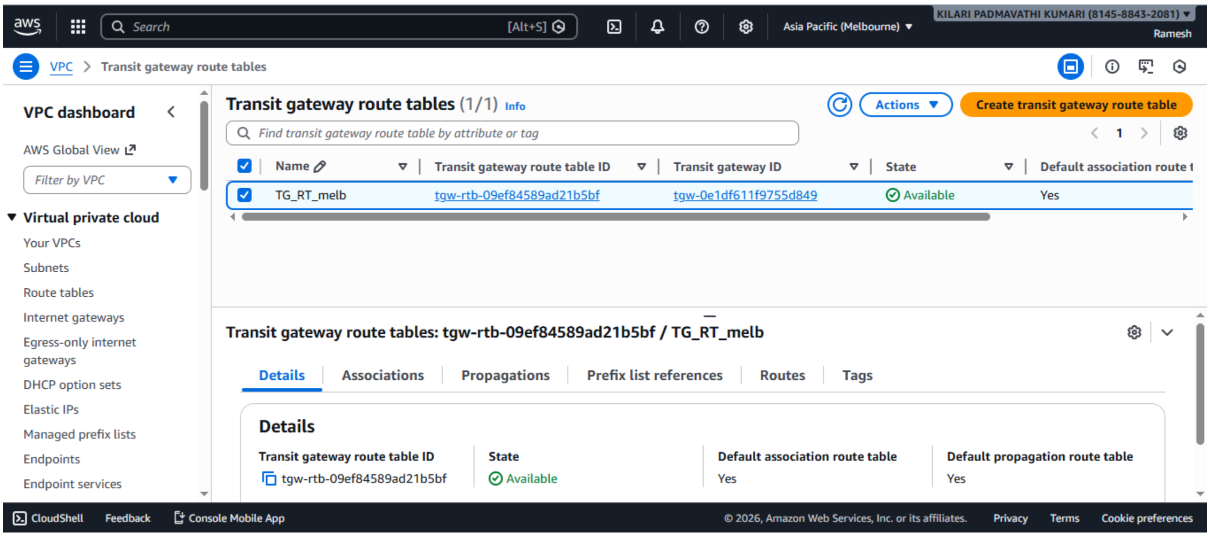
☑	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route t
☑	TGW_RT_Mal	tgw-rtb-018a5fd3c17c82f53	tgw-0b89b9dd9a5b36ae4	Available	Yes

Transit gateway route tables: tgw-rtb-018a5fd3c17c82f53 / TGW_RT_Mal

Details

Transit gateway route table ID	State	Default association route table	Default propagation route table
tgw-rtb-018a5fd3c17c82f53	Available	Yes	Yes

VPC- Challenge1



Transit gateway route tables (1/1) Info

☑	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route t
☑	TG_RT_melb	tgw-rtb-09ef84589ad21b5bf	tgw-0e1df611f9755d849	✓ Available	Yes

Transit gateway route tables: tgw-rtb-09ef84589ad21b5bf / TG_RT_melb

Details

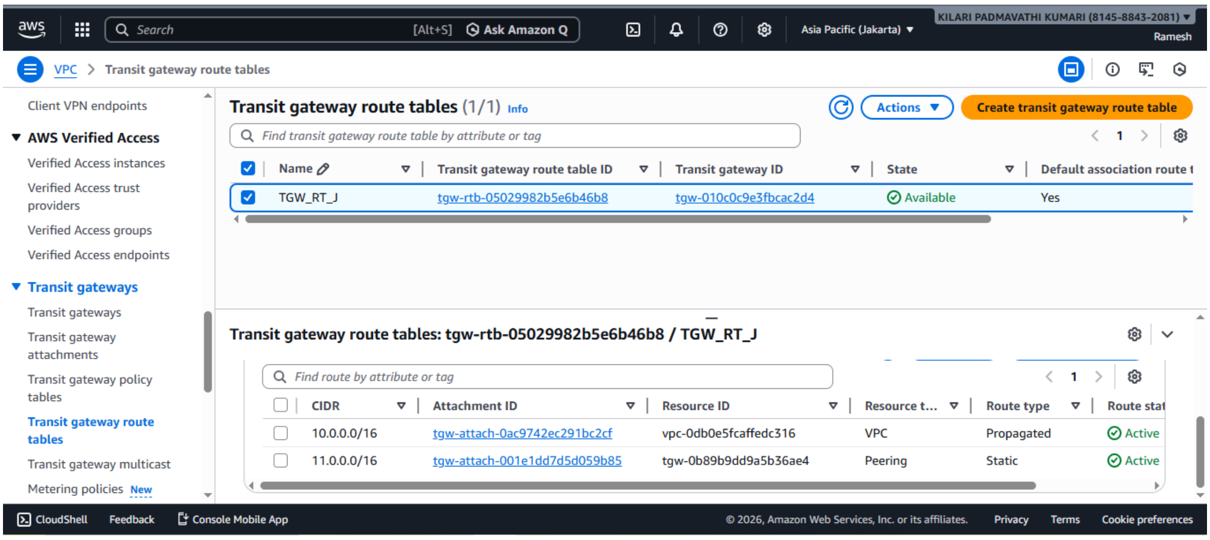
Transit gateway route table ID	State	Default association route table	Default propagation route table
tgw-rtb-09ef84589ad21b5bf	✓ Available	Yes	Yes

Step 4: Update VPC Route Tables

Add routes in private subnet route tables:

Destination: 10.0.1.0/16 (Remote VPC)

Target: Transit Gateway



aws
Search
[Alt+S]
Ask Amazon Q
Asia Pacific (Jakarta) ▼
KILARI PADMAVATHI KUMARI (8145-8843-2081) ▼
Ramesh
VPC > Transit gateway route tables
Client VPN endpoints
▼ AWS Verified Access
Verified Access instances
Verified Access trust providers
Verified Access groups
Verified Access endpoints
▼ Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway multicast
Metering policies New
Actions ▼
Create transit gateway route table
Find transit gateway route table by attribute or tag
1
Find route by attribute or tag
1
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

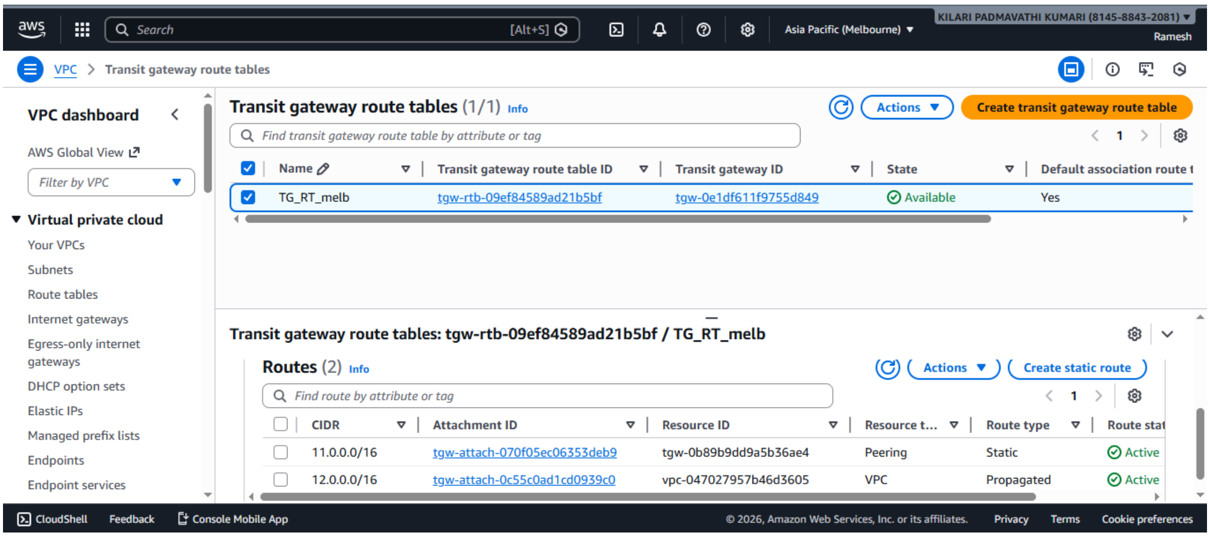
Transit gateway route tables (1/1) Info

☑	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route t
☑	TGW_RT_J	tgw-rtb-05029982b5e6b46b8	tgw-010c0c9e3fbcac2d4	✓ Available	Yes

Transit gateway route tables: tgw-rtb-05029982b5e6b46b8 / TGW_RT_J

□	CIDR	Attachment ID	Resource ID	Resource t...	Route type	Route stat
□	10.0.0.0/16	tgw-attach-0ac9742ec291bc2cf	vpc-0db0e5fcaffedc316	VPC	Propagated	✓ Active
□	11.0.0.0/16	tgw-attach-001e1dd7d5d059b85	tgw-0b89b9dd9a5b36ae4	Peering	Static	✓ Active

VPC- Challenge1



VPC > Transit gateway route tables

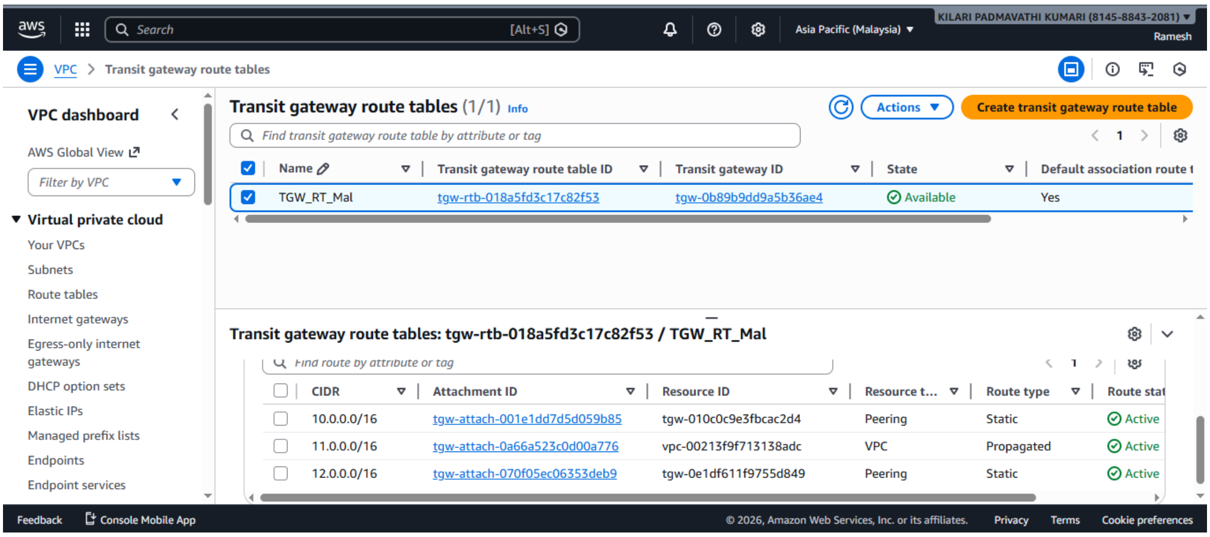
Transit gateway route tables (1/1) Info

☑	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route t
☑	TG_RT_melb	tgw-rtb-09ef84589ad21b5bf	tgw-0e1df611f9755d849	✓ Available	Yes

Transit gateway route tables: tgw-rtb-09ef84589ad21b5bf / TG_RT_melb

Routes (2) Info

□	CIDR	Attachment ID	Resource ID	Resource t...	Route type	Route stat
□	11.0.0.0/16	tgw-attach-070f05ec06353deb9	tgw-0b89b9dd9a5b36ae4	Peering	Static	✓ Active
□	12.0.0.0/16	tgw-attach-0c55c0ad1cd0939c0	vpc-047027957b46d3605	VPC	Propagated	✓ Active



VPC > Transit gateway route tables

Transit gateway route tables (1/1) Info

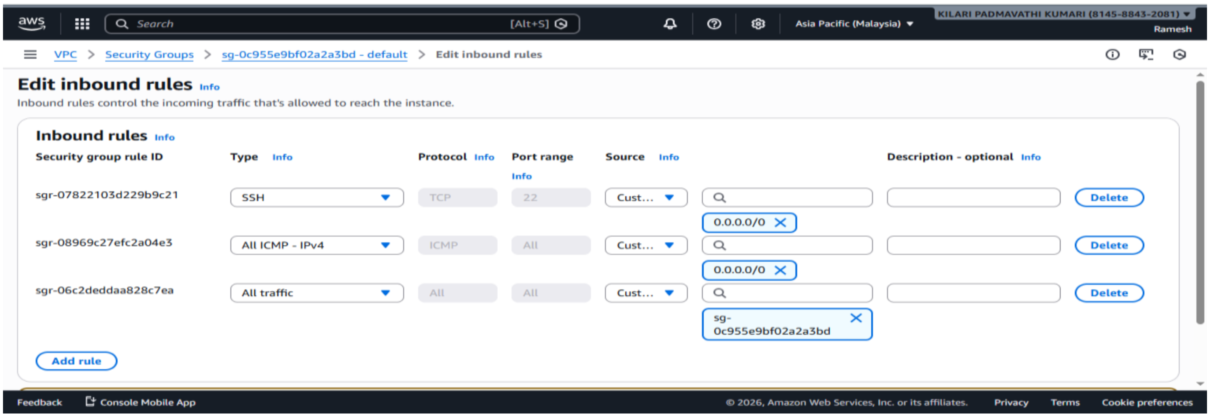
☑	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route t
☑	TGW_RT_Mal	tgw-rtb-018a5fd3c17c82f53	tgw-0b89b9dd9a5b36ae4	✓ Available	Yes

Transit gateway route tables: tgw-rtb-018a5fd3c17c82f53 / TGW_RT_Mal

□	CIDR	Attachment ID	Resource ID	Resource t...	Route type	Route stat
□	10.0.0.0/16	tgw-attach-001e1dd7d5d059b85	tgw-010c0c9e3fbcac2d4	Peering	Static	✓ Active
□	11.0.0.0/16	tgw-attach-0a66a523c0d00a776	vpc-00213f9f713138adc	VPC	Propagated	✓ Active
□	12.0.0.0/16	tgw-attach-070f05ec06353deb9	tgw-0e1df611f9755d849	Peering	Static	✓ Active

Step 5: Security Configuration

- Use **Security Groups** and **NACLs**(follow these rules for all 3 regions)
- Restrict TGW routes to required CIDRs



VPC > Security Groups > sg-0c955e9bf02a2a3bd - default > Edit inbound rules

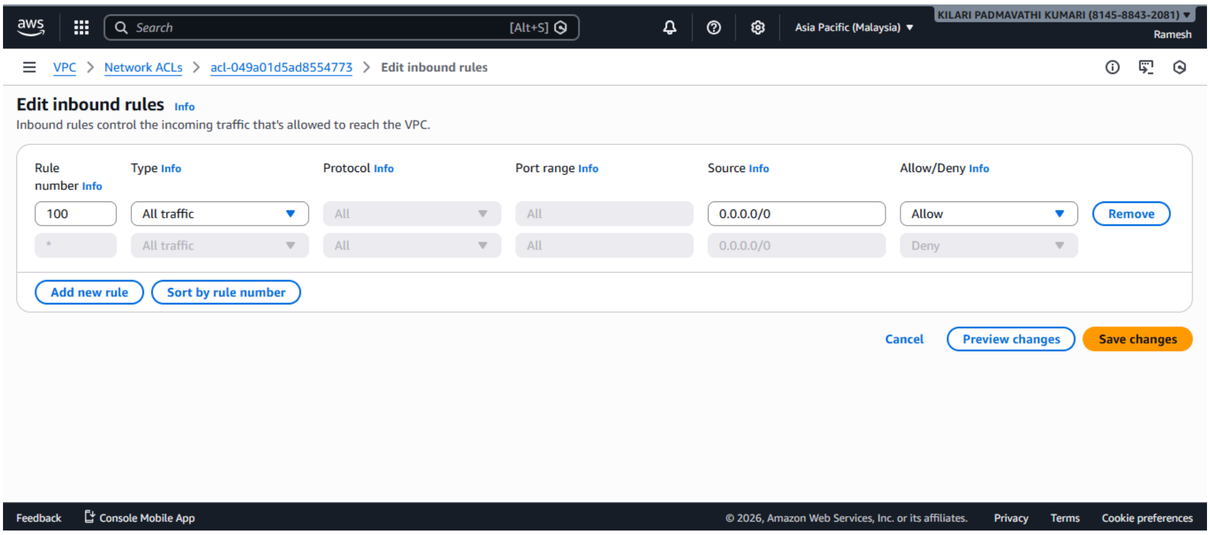
Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-07822103d229b9c21	SSH	TCP	22	Cust...	0.0.0.0/0	
sgr-08969c27efc2a04e3	All ICMP - IPv4	ICMP	All	Cust...	0.0.0.0/0	
sgr-06c2deddaa828c7ea	All traffic	All	All	Cust...	sg-0c955e9bf02a2a3bd	

VPC- Challenge1



aws
Search [Alt+S]
Asia Pacific (Malaysia) ▼
KILARI PADMAVATHI KUMARI (8145-8843-2081) ▼
Ramesh
VPC > Network ACLs > acl-049a01d5ad8554773 > Edit inbound rules

Edit inbound rules Info

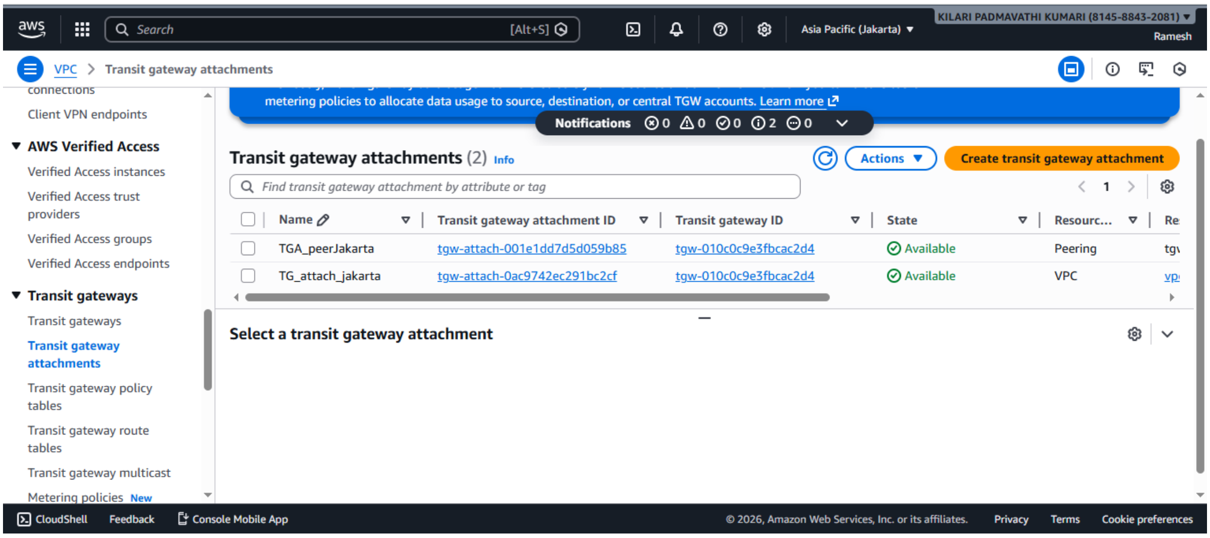
Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number Info	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info	
100	All traffic	All	All	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

Add new rule
Sort by rule number
Cancel
Preview changes
Save changes
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 6: High Availability

- TGW is **regionally highly available**
- Use multiple subnets (AZs) per attachment
- For multi-region:
  - Use **TGW Peering**



aws
Search [Alt+S]
Asia Pacific (Jakarta) ▼
KILARI PADMAVATHI KUMARI (8145-8843-2081) ▼
Ramesh
VPC > Transit gateway attachments
connections
Client VPN endpoints
▼ AWS Verified Access
Verified Access instances
Verified Access trust providers
Verified Access groups
Verified Access endpoints
▼ Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway multicast
Metering policies New
Notifications ⊗ 0 ⚠ 0 ⊘ 0 ⓘ 2 ⊖ 0
Actions ▼
Create transit gateway attachment
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

metering policies to allocate data usage to source, destination, or central TGW accounts. Learn more

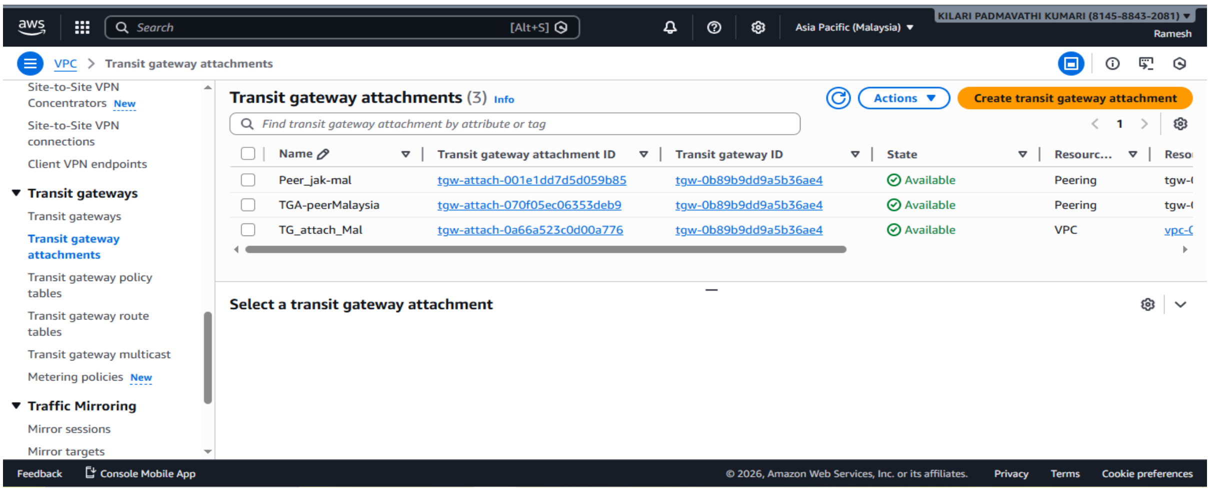
Transit gateway attachments (2) Info

Find transit gateway attachment by attribute or tag

□	Name	Transit gateway attachment ID	Transit gateway ID	State	Resourc...	Re
□	TGA_peerJakarta	tgw-attach-001e1dd7d5d059b85	tgw-010c0c9e3fbcac2d4	✓ Available	Peering	tg\
□	TG_attach_jakarta	tgw-attach-0ac9742ec291bc2cf	tgw-010c0c9e3fbcac2d4	✓ Available	VPC	vp

Select a transit gateway attachment

VPC- Challenge1



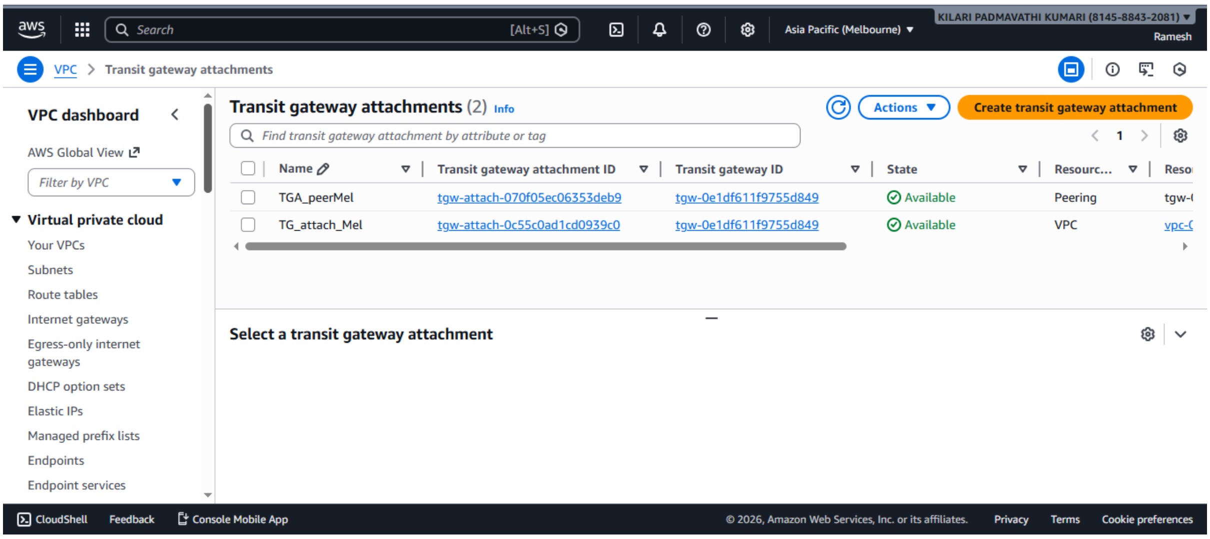
aws
Search [Alt+S]
Asia Pacific (Malaysia)
KILARI PADMAVATHI KUMARI (8145-8843-2081)
Ramesh
VPC > Transit gateway attachments
Site-to-Site VPN Concentrators New
Site-to-Site VPN connections
Client VPN endpoints
Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway multicast
Metering policies New
Traffic Mirroring
Mirror sessions
Mirror targets
Actions
Create transit gateway attachment
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Transit gateway attachments (3) Info

Find transit gateway attachment by attribute or tag

	Name	Transit gateway attachment ID	Transit gateway ID	State	Resourc...	Reso
□	Peer_jak-mal	tgw-attach-001e1dd7d5d059b85	tgw-0b89b9dd9a5b36ae4	✓ Available	Peering	tgw-(
□	TGA-peerMalaysia	tgw-attach-070f05ec06353deb9	tgw-0b89b9dd9a5b36ae4	✓ Available	Peering	tgw-(
□	TG_attach_Mal	tgw-attach-0a66a523c0d00a776	tgw-0b89b9dd9a5b36ae4	✓ Available	VPC	vpc-(

Select a transit gateway attachment



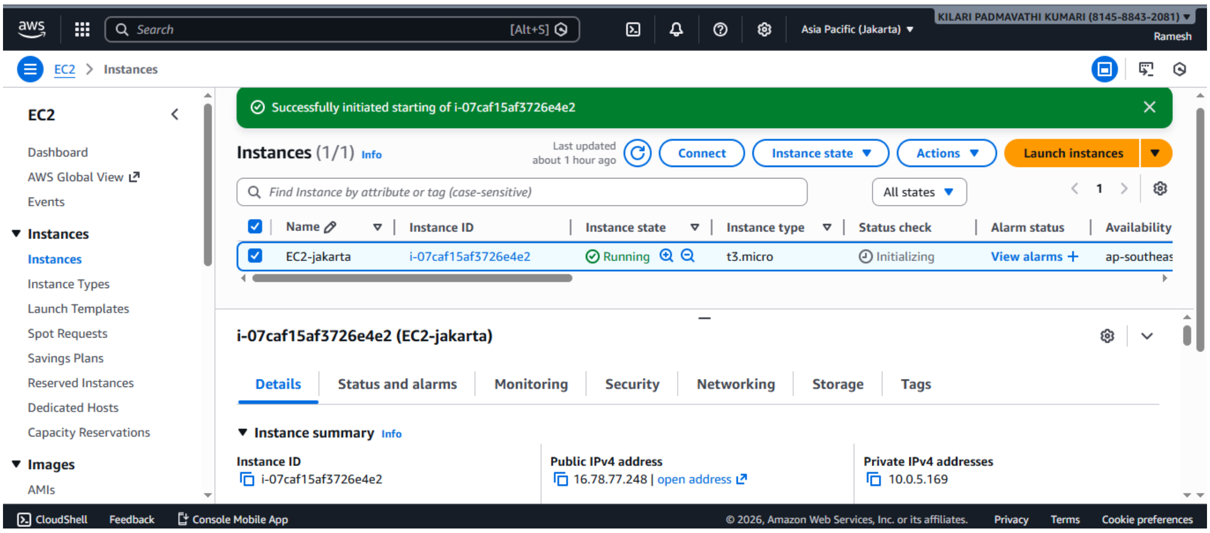
Transit gateway attachments (2) Info

Find transit gateway attachment by attribute or tag

	Name	Transit gateway attachment ID	Transit gateway ID	State	Resourc...	Reso
□	TGA_peerMel	tgw-attach-070f05ec06353deb9	tgw-0e1df611f9755d849	✓ Available	Peering	tgw-(
□	TG_attach_Mel	tgw-attach-0c55c0ad1cd0939c0	tgw-0e1df611f9755d849	✓ Available	VPC	vpc-(

Select a transit gateway attachment

Create EC2 instance for checking connectivity.



✓ Successfully initiated starting of i-07caf15af3726e4e2

Instances (1/1) Info

Last updated about 1 hour ago

Find Instance by attribute or tag (case-sensitive)

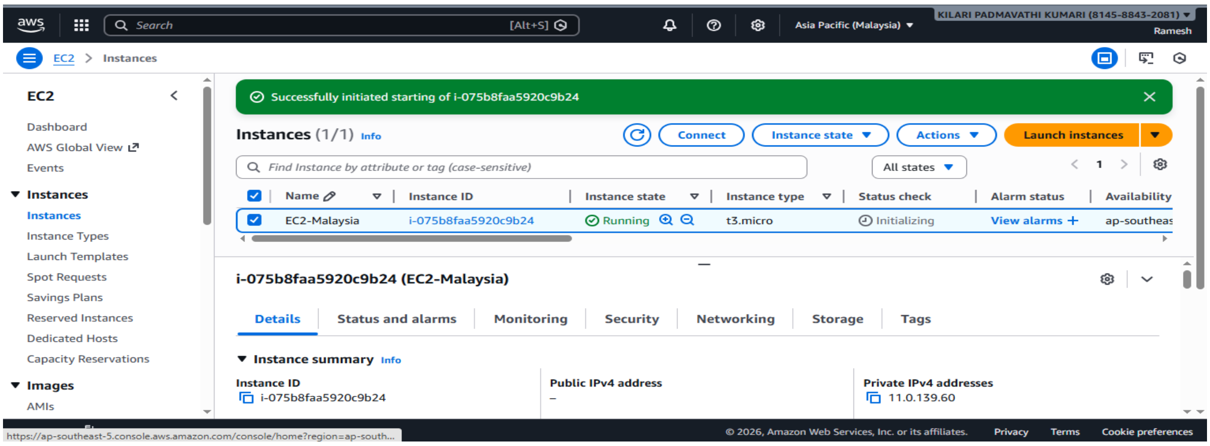
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
☑	EC2-jakarta	i-07caf15af3726e4e2	✓ Running	t3.micro	Initializing	View alarms +	ap-southeas

i-07caf15af3726e4e2 (EC2-jakarta)

▼ Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-07caf15af3726e4e2	16.78.77.248 | open address	10.0.5.169

VPC- Challenge1



Successfully initiated starting of i-075b8faa5920c9b24

Instances (1/1) Info

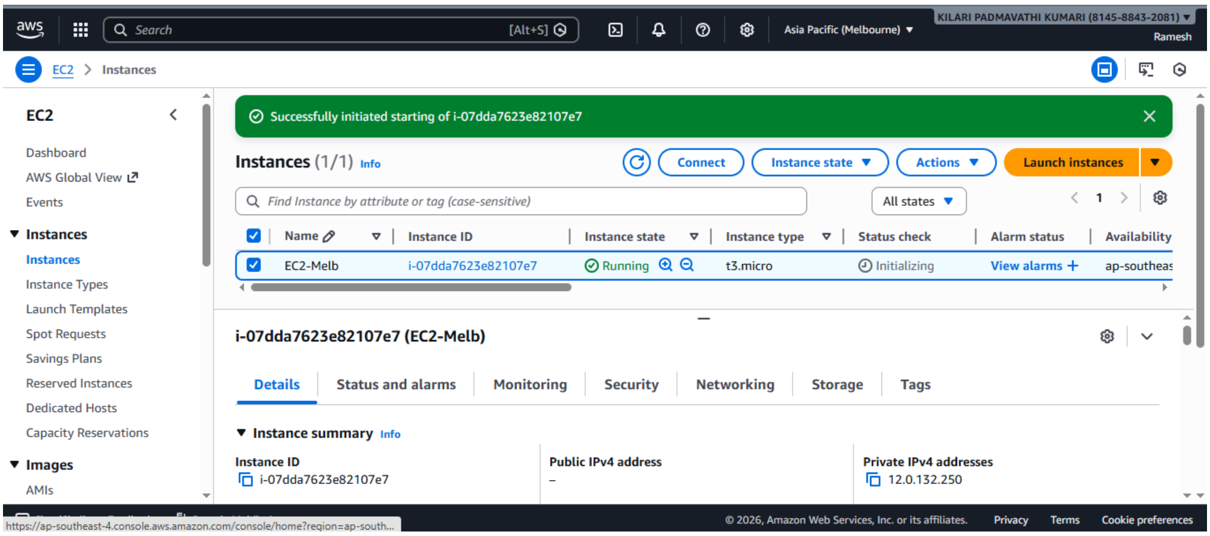
Find Instance by attribute or tag (case-sensitive)

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
☑	EC2-Malaysia	i-075b8faa5920c9b24	Running	t3.micro	Initializing	View alarms +	ap-southeas

i-075b8faa5920c9b24 (EC2-Malaysia)

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-075b8faa5920c9b24	–	11.0.139.60



Successfully initiated starting of i-07dda7623e82107e7

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
☑	EC2-Melb	i-07dda7623e82107e7	Running	t3.micro	Initializing	View alarms +	ap-southeas

i-07dda7623e82107e7 (EC2-Melb)

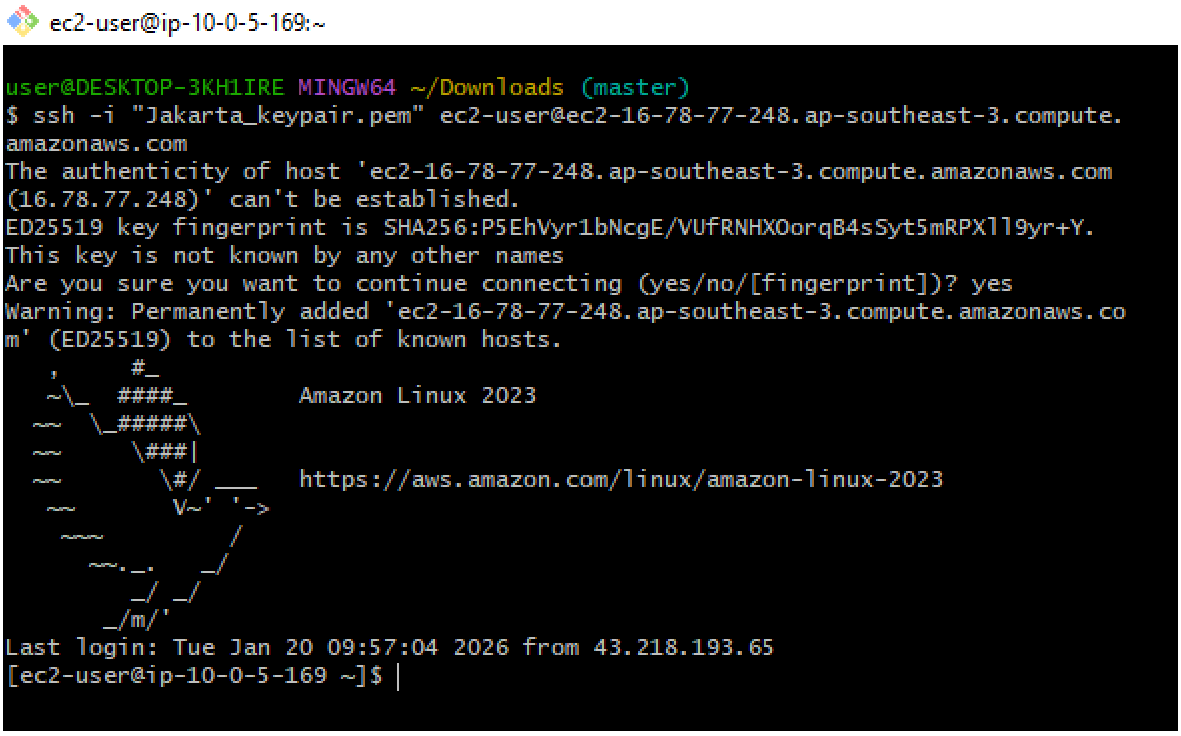
Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-07dda7623e82107e7	–	12.0.132.250

VPC- Challenge1

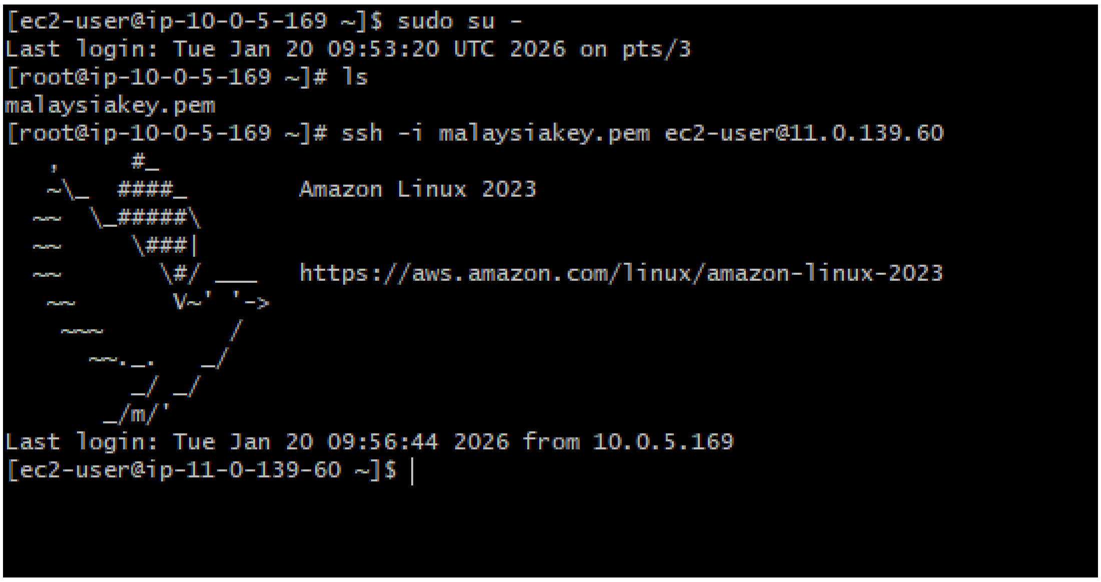
Connection: To Verify

Ec2 instance for Jakarta region



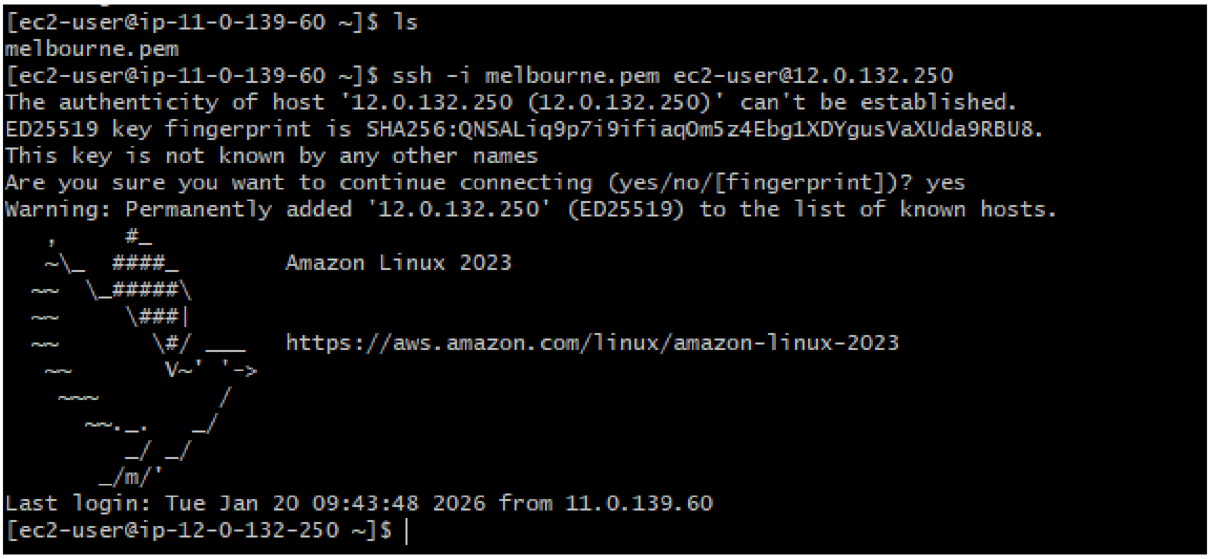
ec2-user@ip-10-0-5-169:~

```
user@DESKTOP-3KH1IRE MINGW64 ~/Downloads (master)
$ ssh -i "Jakarta_keypair.pem" ec2-user@ec2-16-78-77-248.ap-southeast-3.compute.
amazonaws.com
The authenticity of host 'ec2-16-78-77-248.ap-southeast-3.compute.amazonaws.com
(16.78.77.248)' can't be established.
ED25519 key fingerprint is SHA256:P5EhVyr1bNcgE/VUfRNHXOorqB4sSyt5mRPXll9yr+Y.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-16-78-77-248.ap-southeast-3.compute.amazonaws.co
m' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jan 20 09:57:04 2026 from 43.218.193.65
[ec2-user@ip-10-0-5-169 ~]$ |
```

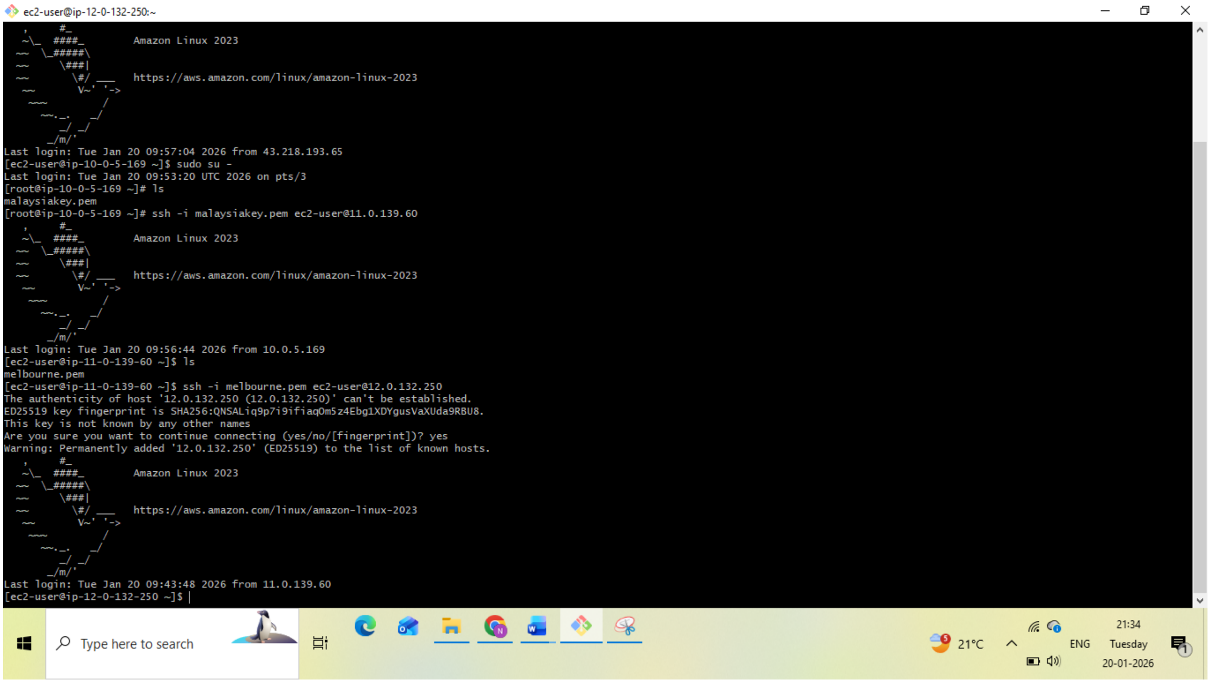


```
[ec2-user@ip-10-0-5-169 ~]$ sudo su -
Last login: Tue Jan 20 09:53:20 UTC 2026 on pts/3
[root@ip-10-0-5-169 ~]# ls
malaysiakey.pem
[root@ip-10-0-5-169 ~]# ssh -i malaysiakey.pem ec2-user@11.0.139.60
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jan 20 09:56:44 2026 from 10.0.5.169
[ec2-user@ip-11-0-139-60 ~]$ |
```

VPC- Challenge1



```
[ec2-user@ip-11-0-139-60 ~]$ ls
melbourne.pem
[ec2-user@ip-11-0-139-60 ~]$ ssh -i melbourne.pem ec2-user@12.0.132.250
The authenticity of host '12.0.132.250 (12.0.132.250)' can't be established.
ED25519 key fingerprint is SHA256:QNSALiq9p7i9ifiaqOm5z4Ebg1XDYgusVaXUda9RBU8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '12.0.132.250' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jan 20 09:43:48 2026 from 11.0.139.60
[ec2-user@ip-12-0-132-250 ~]$ |
```



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jan 20 09:57:04 2026 from 43.218.193.65
[ec2-user@ip-10-0-5-169 ~]$ sudo su -
Last login: Tue Jan 20 09:53:20 UTC 2026 on pts/3
[root@ip-10-0-5-169 ~]# ls
malaysiakey.pem
[root@ip-10-0-5-169 ~]# ssh -i malaysiakey.pem ec2-user@11.0.139.60
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jan 20 09:56:44 2026 from 10.0.5.169
[ec2-user@ip-11-0-139-60 ~]$ ls
melbourne.pem
[ec2-user@ip-11-0-139-60 ~]$ ssh -i melbourne.pem ec2-user@12.0.132.250
The authenticity of host '12.0.132.250 (12.0.132.250)' can't be established.
ED25519 key fingerprint is SHA256:QNSALiq9p7i9ifiaqOm5z4Ebg1XDYgusVaXUda9RBU8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '12.0.132.250' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jan 20 09:43:48 2026 from 11.0.139.60
[ec2-user@ip-12-0-132-250 ~]$ |
```

Conclusion

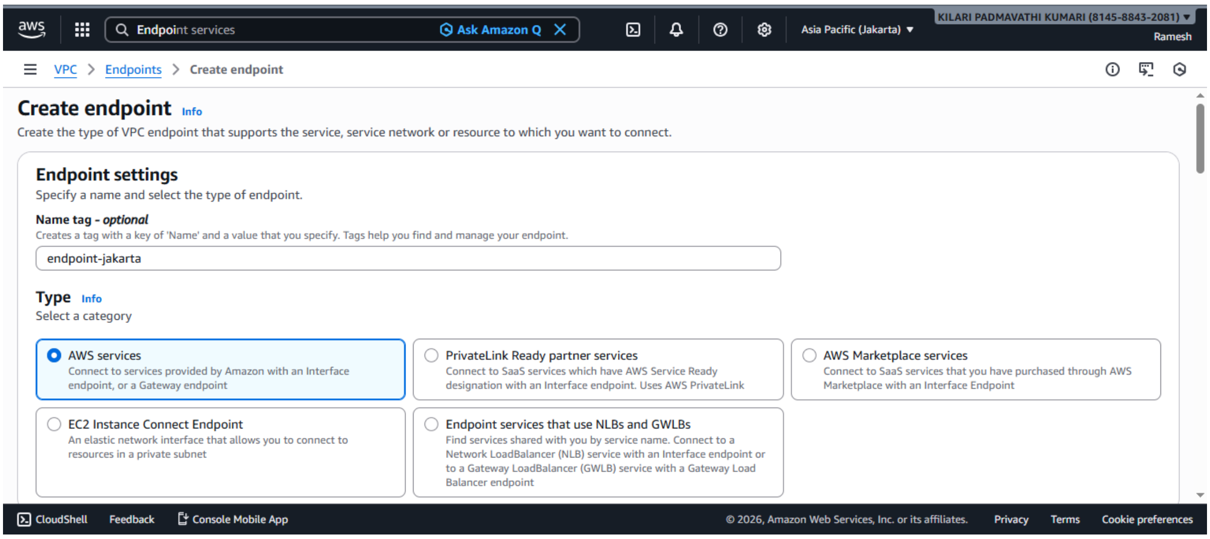
- By using **AWS Transit Gateway**, we can design a **scalable, secure, and centralized network architecture** that simplifies VPC connectivity, reduces operational overhead, and supports future growth without re-architecting the network.

VPC- Challenge1

- Configure VPC endpoints to securely access AWS services without internet gateways or NAT gateways, ensuring data privacy and minimizing exposure to external threats.

  Objective:

  - Implemented **VPC Gateway and Interface Endpoints (PrivateLink)** to enable secure, private access to AWS services without Internet or NAT Gateways.
  - Ensured **data privacy and reduced attack surface** by keeping all service traffic on the AWS private backbone using Private DNS and endpoint policies.
  - Optimized **security and cost** by eliminating public IP dependencies and enforcing least-privilege access controls.


aws
Endpoint services
Ask Amazon Q
Asia Pacific (Jakarta) ▾
KILARI PADMAVATHI KUMARI (8145-8843-2081) ▾
Ramesh
VPC > Endpoints > Create endpoint
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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.

endpoint-jakarta

Type Info

Select a category

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

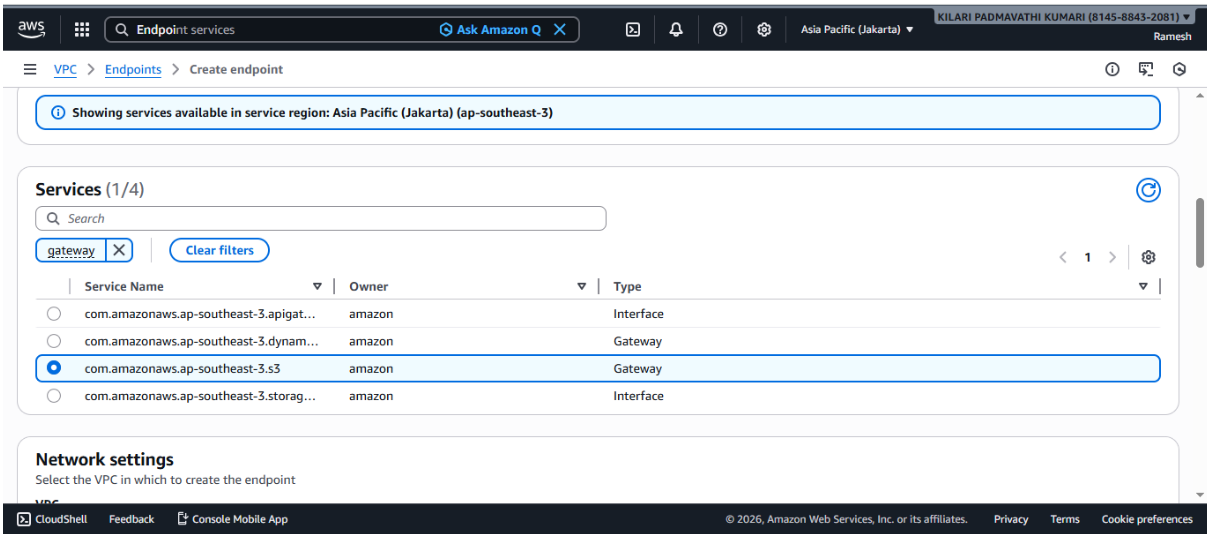
○ PrivateLink Ready partner services
Connect to SaaS services which have AWS Service Ready designation with an Interface endpoint. Uses AWS PrivateLink

○ AWS Marketplace services
Connect to SaaS services that you have purchased through AWS Marketplace with an Interface Endpoint

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

○ 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- Challenge1



Showing services available in service region: Asia Pacific (Jakarta) (ap-southeast-3)

Services (1/4)

gateway ☒

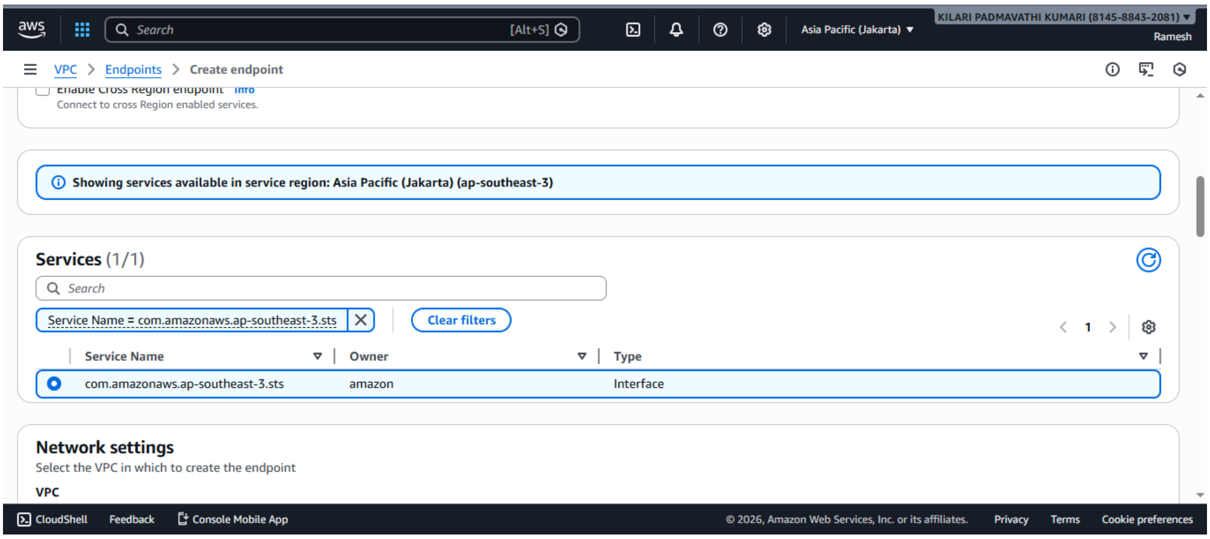
	Service Name	Owner	Type
○	com.amazonaws.ap-southeast-3.apigat...	amazon	Interface
○	com.amazonaws.ap-southeast-3.dynam...	amazon	Gateway
●	com.amazonaws.ap-southeast-3.s3	amazon	Gateway
○	com.amazonaws.ap-southeast-3.storag...	amazon	Interface

Network settings

Select the VPC in which to create the endpoint

Create gateway for s3

or


Search
[Alt+S]
Asia Pacific (Jakarta)
KILARI PADMAVATHI KUMARI (8145-8843-2081)
Ramesh
VPC > Endpoints > Create endpoint
Search
Clear filters
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

□ Enable Cross Region endpoint Info

Connect to cross Region enabled services.

Showing services available in service region: Asia Pacific (Jakarta) (ap-southeast-3)

Services (1/1)

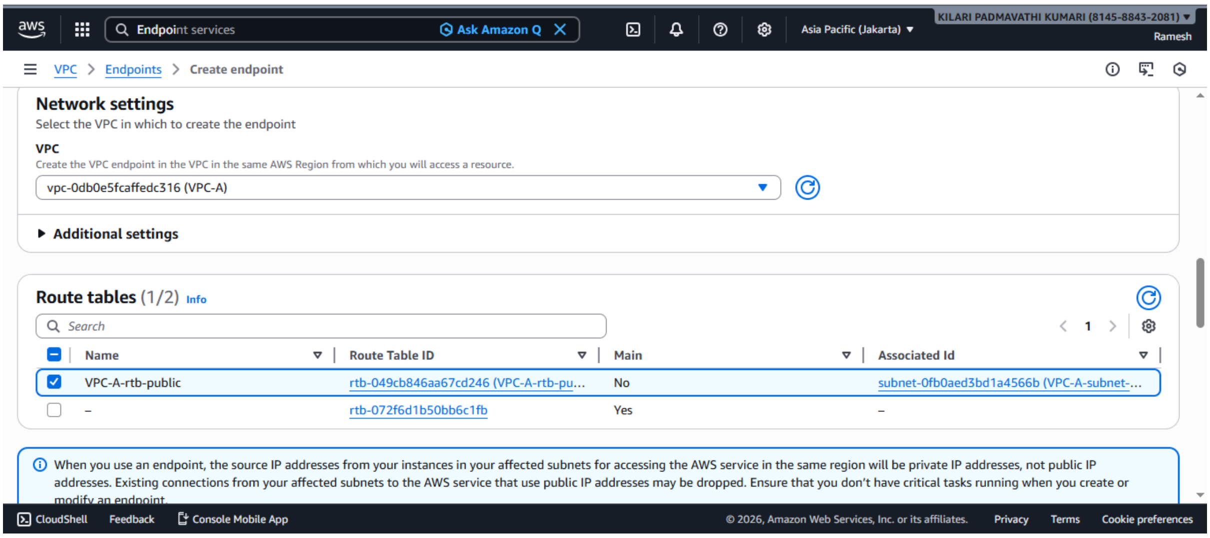
Service Name = com.amazonaws.ap-southeast-3.sts ☒

	Service Name	Owner	Type
●	com.amazonaws.ap-southeast-3.sts	amazon	Interface

Network settings

Select the VPC in which to create the endpoint

VPC



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-0db0e5fcaffedc316 (VPC-A)

▸ Additional settings

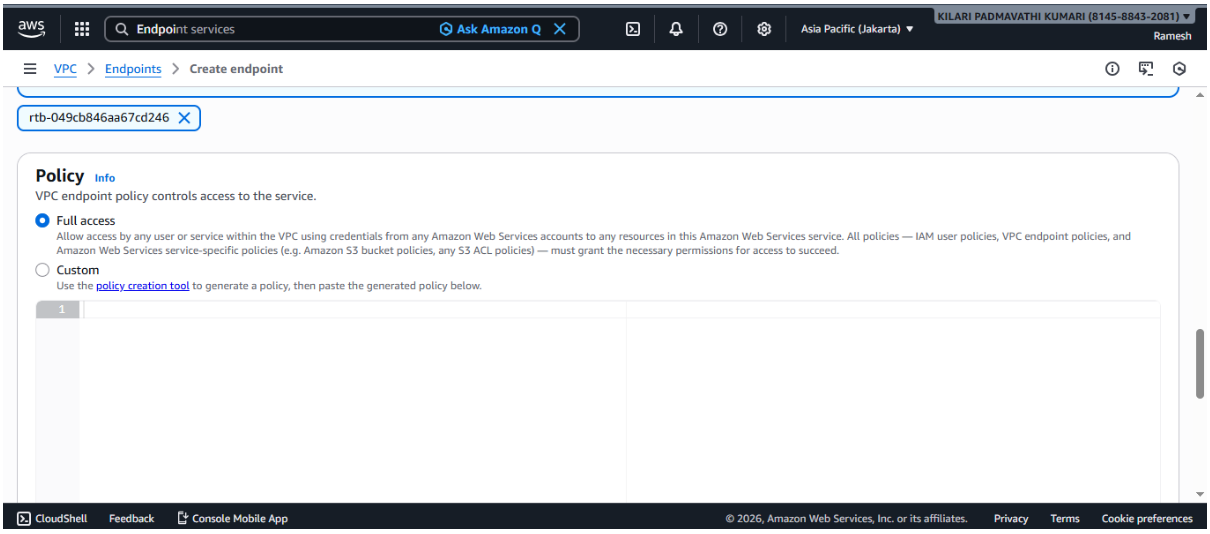
Route tables (1/2) Info

	Name	Route Table ID	Main	Associated Id
☑	VPC-A-rtb-public	rtb-049cb846aa67cd246 (VPC-A-rtb-pu...	No	subnet-0fb0aed3bd1a4566b (VPC-A-subnet-...
□	–	rtb-072f6d1b50bb6c1fb	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.

VPC- Challenge1

- Add VPC to network



rtb-049cb846aa67cd246

Policy Info

VPC endpoint policy controls access to the service.

● Full access

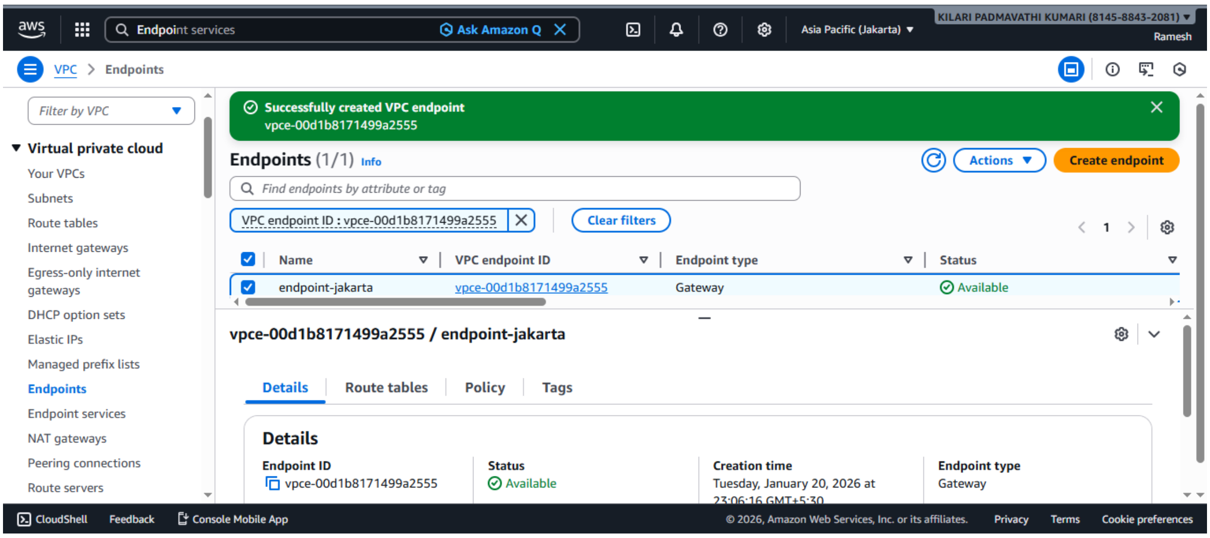
Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, 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.

Endpoint services
Ask Amazon Q
Asia Pacific (Jakarta)
KILARI PADMAVATHI KUMARI (8145-8843-2081)
Ramesh
VPC > Endpoints > Create endpoint
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

- In policy give full access and click on create endpoint.



Successfully created VPC endpoint vpce-00d1b8171499a2555

Endpoints (1/1) Info

VPC endpoint ID : vpce-00d1b8171499a2555

☑	Name	VPC endpoint ID	Endpoint type	Status
☑	endpoint-jakarta	vpce-00d1b8171499a2555	Gateway	✓ Available

vpce-00d1b8171499a2555 / endpoint-jakarta

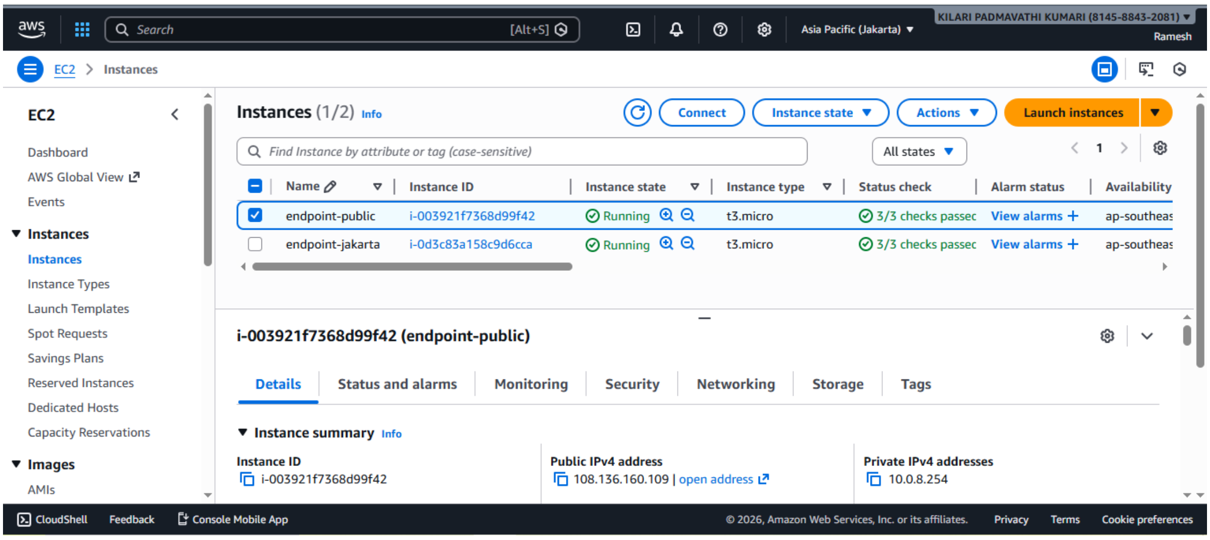
Details | Route tables | Policy | Tags

Details

Endpoint ID	Status	Creation time	Endpoint type
vpce-00d1b8171499a2555	✓ Available	Tuesday, January 20, 2026 at 23:06:16 GMT+5:30	Gateway

- The above image shows endpoint created successfully.

VPC- Challenge1



Instances (1/2) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
☑	endpoint-public	i-003921f7368d99f42	Running	t3.micro	3/3 checks passec	View alarms +	ap-southeas
□	endpoint-jakarta	i-0d3c83a158c9d6cca	Running	t3.micro	3/3 checks passec	View alarms +	ap-southeas

i-003921f7368d99f42 (endpoint-public)

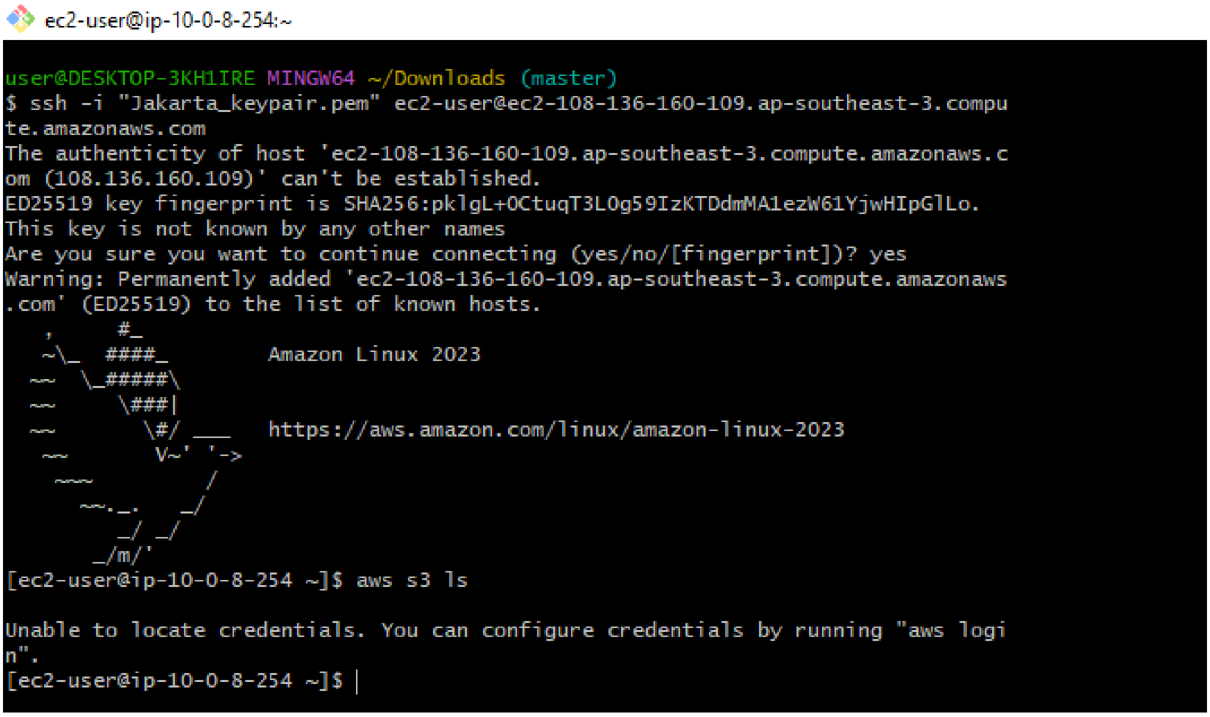
Instance summary Info

Instance ID: i-003921f7368d99f42

Public IPv4 address: 108.136.160.109 | open address

Private IPv4 addresses: 10.0.8.254

- Create two instance to check connectivity one is public and other one is private
- Connectivity check:-

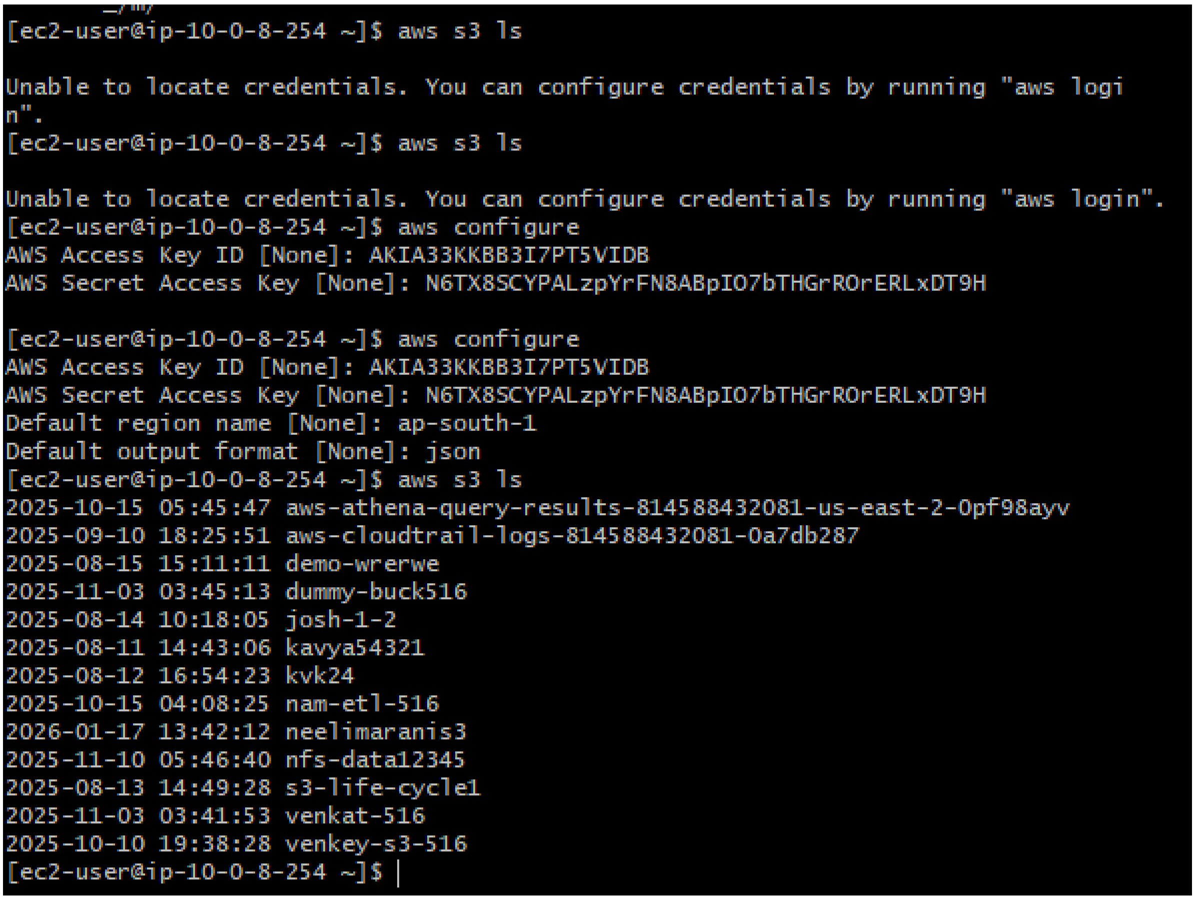


ec2-user@ip-10-0-8-254:~

```
user@DESKTOP-3KH1IRE MINGW64 ~/Downloads (master)
$ ssh -i "Jakarta_keypair.pem" ec2-user@ec2-108-136-160-109.ap-southeast-3.compu
te.amazonaws.com
The authenticity of host 'ec2-108-136-160-109.ap-southeast-3.compute.amazonaws.c
om (108.136.160.109)' can't be established.
ED25519 key fingerprint is SHA256:pklgL+OCtuqT3L0g59IzKTDdmMA1ezW61YjwHIpGlLo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-108-136-160-109.ap-southeast-3.compute.amazonaws
.com' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-8-254 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws logi
n".
[ec2-user@ip-10-0-8-254 ~]$ |
```

VPC- Challenge1



```
       _/m/
[ec2-user@ip-10-0-8-254 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws logi
n".
[ec2-user@ip-10-0-8-254 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws login".
[ec2-user@ip-10-0-8-254 ~]$ aws configure
AWS Access Key ID [None]: AKIA33KKBB3I7PT5VIDB
AWS Secret Access Key [None]: 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

[ec2-user@ip-10-0-8-254 ~]$ aws configure
AWS Access Key ID [None]: AKIA33KKBB3I7PT5VIDB
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: json
[ec2-user@ip-10-0-8-254 ~]$ aws s3 ls
2025-10-15 05:45:47 aws-athena-query-results-814588432081-us-east-2-0pf98ayv
2025-09-10 18:25:51 aws-cloudtrail-logs-814588432081-0a7db287
2025-08-15 15:11:11 demo-wrerwe
2025-11-03 03:45:13 dummy-buck516
2025-08-14 10:18:05 josh-1-2
2025-08-11 14:43:06 kavya54321
2025-08-12 16:54:23 kvk24
2025-10-15 04:08:25 nam-etl-516
2026-01-17 13:42:12 neelimaranis3
2025-11-10 05:46:40 nfs-data12345
2025-08-13 14:49:28 s3-life-cycle1
2025-11-03 03:41:53 venkat-516
2025-10-10 19:38:28 venkey-s3-516
[ec2-user@ip-10-0-8-254 ~]$ 
```