

# TRANSIT GATEWAY

---

Uso en estrategias multi VPC en AWS



**Carlos Cruzado**  
CLOUD SOLUTIONS ARCHITECT

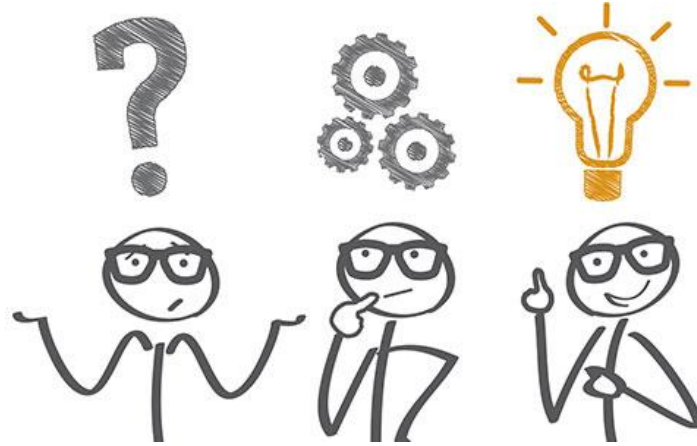
 /ccruzado

# Resumen



- Multi cuentas en AWS
- Uso de multi VPC
- VPC Peering
- Transit Gateway
- Demo

# Multi cuentas en AWS



## Problema

Necesidad de segmentar servicios para para supervisar los costos, controlar el acceso y proporcionar una gestión ambiental más fácil

## Solución

Uso de cuentas múltiples proporciona cuentas específicas para los servicios y usuarios dentro de una organización.

## Como hacerlo

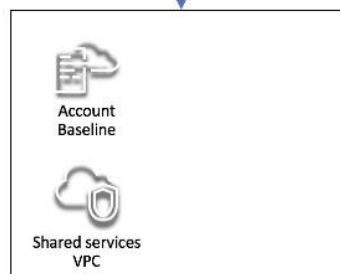
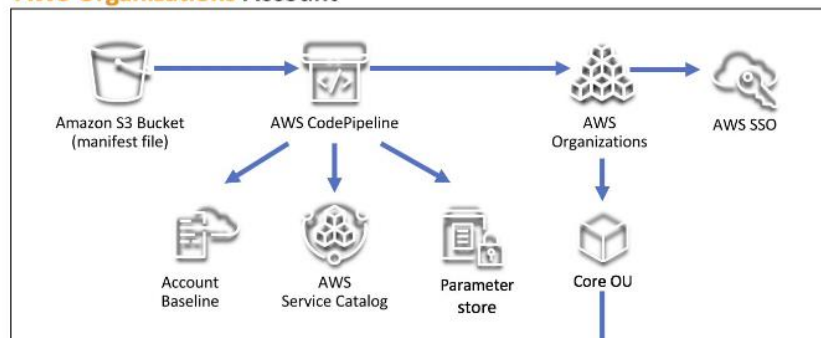
AWS proporciona herramientas para gestionar y configurar esta infraestructura, incluyendo **Landing Zone** y **Control Tower**

# Multi cuentas en AWS

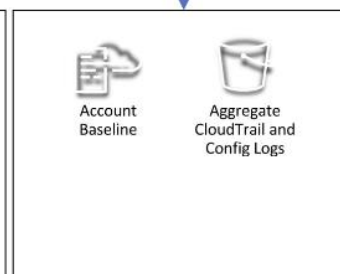
## Landing Zone / Control Tower

Automatizar la configuración e integración de los múltiples servicios del AWS para proporcionar un entorno básico, altamente controlado y de múltiples cuentas con gestión de identidades y evaluaciones (IAM), gobernanza, seguridad de los datos, diseño de redes y registro.

### AWS Organizations Account



### Shared Services Account



### Log Archive Account



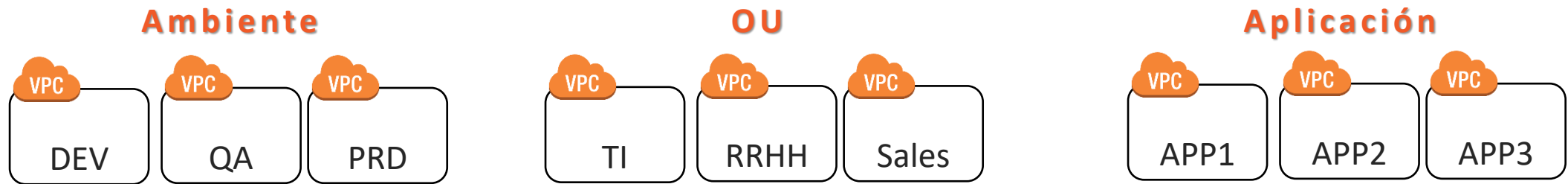
### Security Account



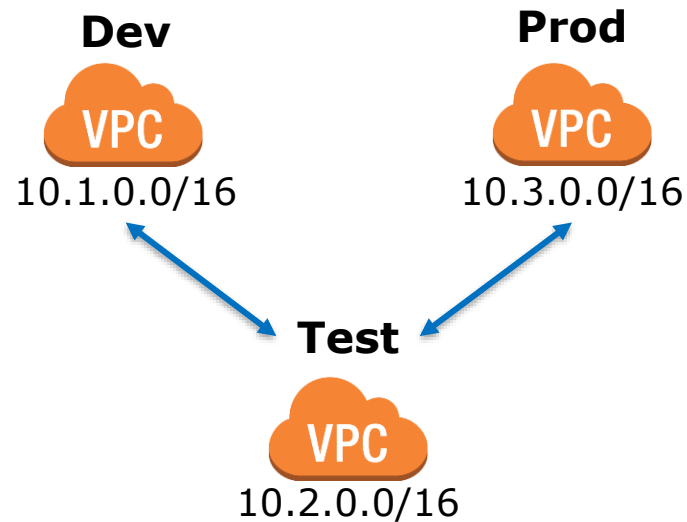
### Network Services Account

# Multi VPC en AWS

- La mayoría de los clientes comienzan con unos pocos VPC para desplegar su infraestructura.
- El número de VPC que un cliente posee está generalmente relacionado con su número de cuentas, usuarios, y entornos escenificados (PRD, DEV, QA).
- A medida que aumenta el uso de la nube, se multiplica el número de usuarios, unidades de negocio, aplicaciones y regiones con las que el cliente interactúa, lo que da lugar a la creación de nuevos VPC.



# VPC Peering

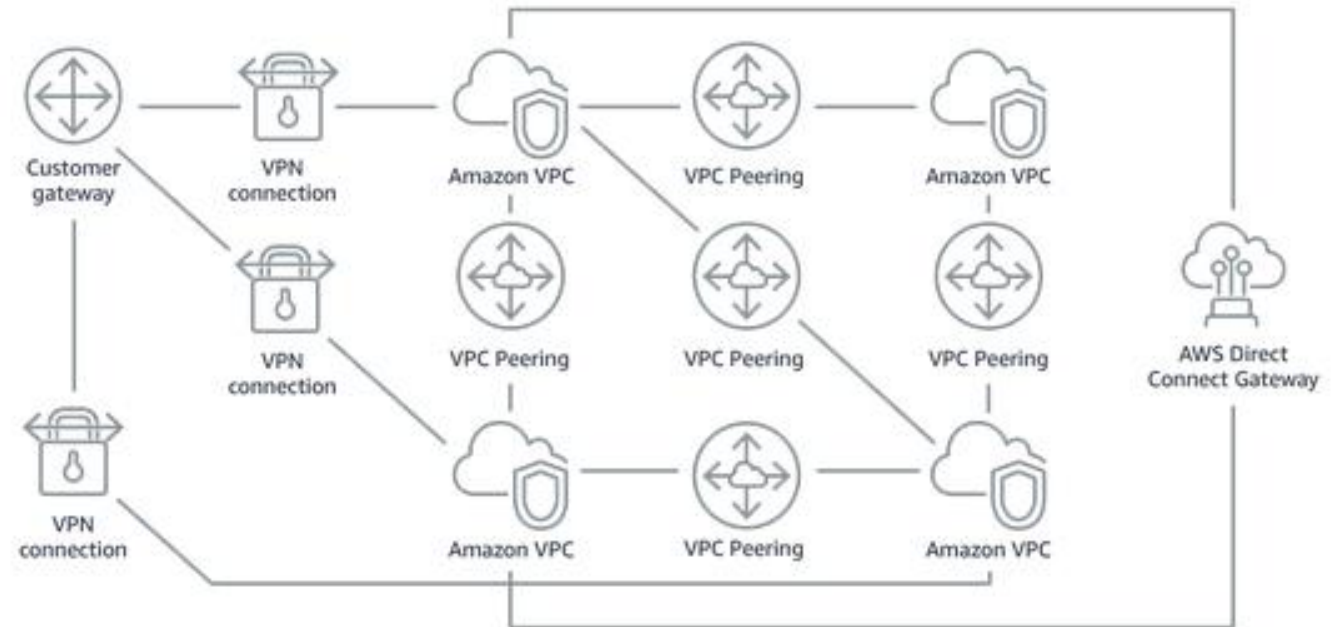


- Usar direcciones IP privadas
- Soporte intra e inter regiones
- CIDR no deben sobreponerse
- No tiene transitividad
- Puede establecerse entre diferentes cuentas
- Conexiones altamente disponibles
- No hay cuellos de botella en el ancho de banda
- El tráfico siempre se mantiene en el backbone de AWS

# VPC Peering

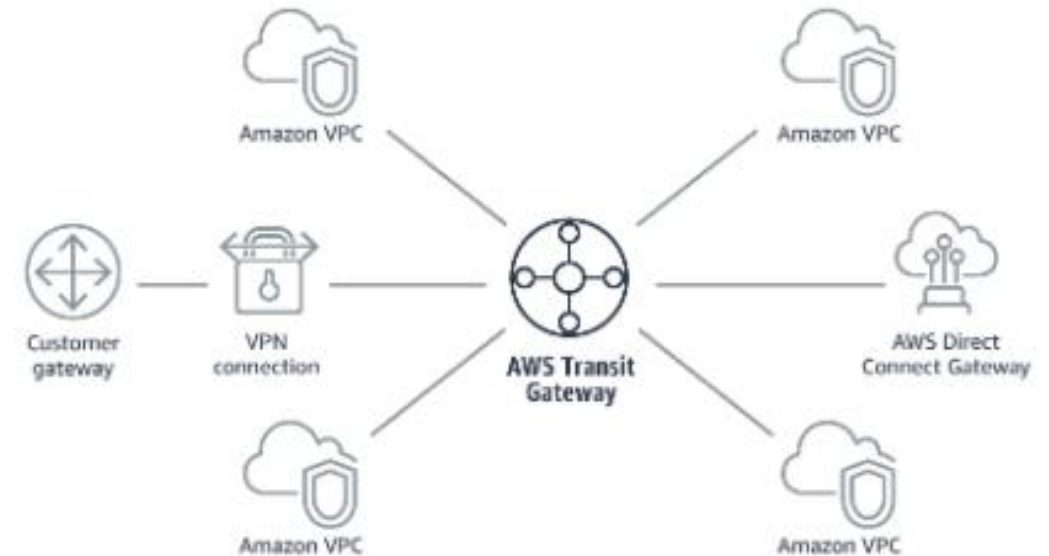


Complejidad aumenta con la escala. Se debe dar mantenimiento las tablas de enrutamiento de cada VPC.



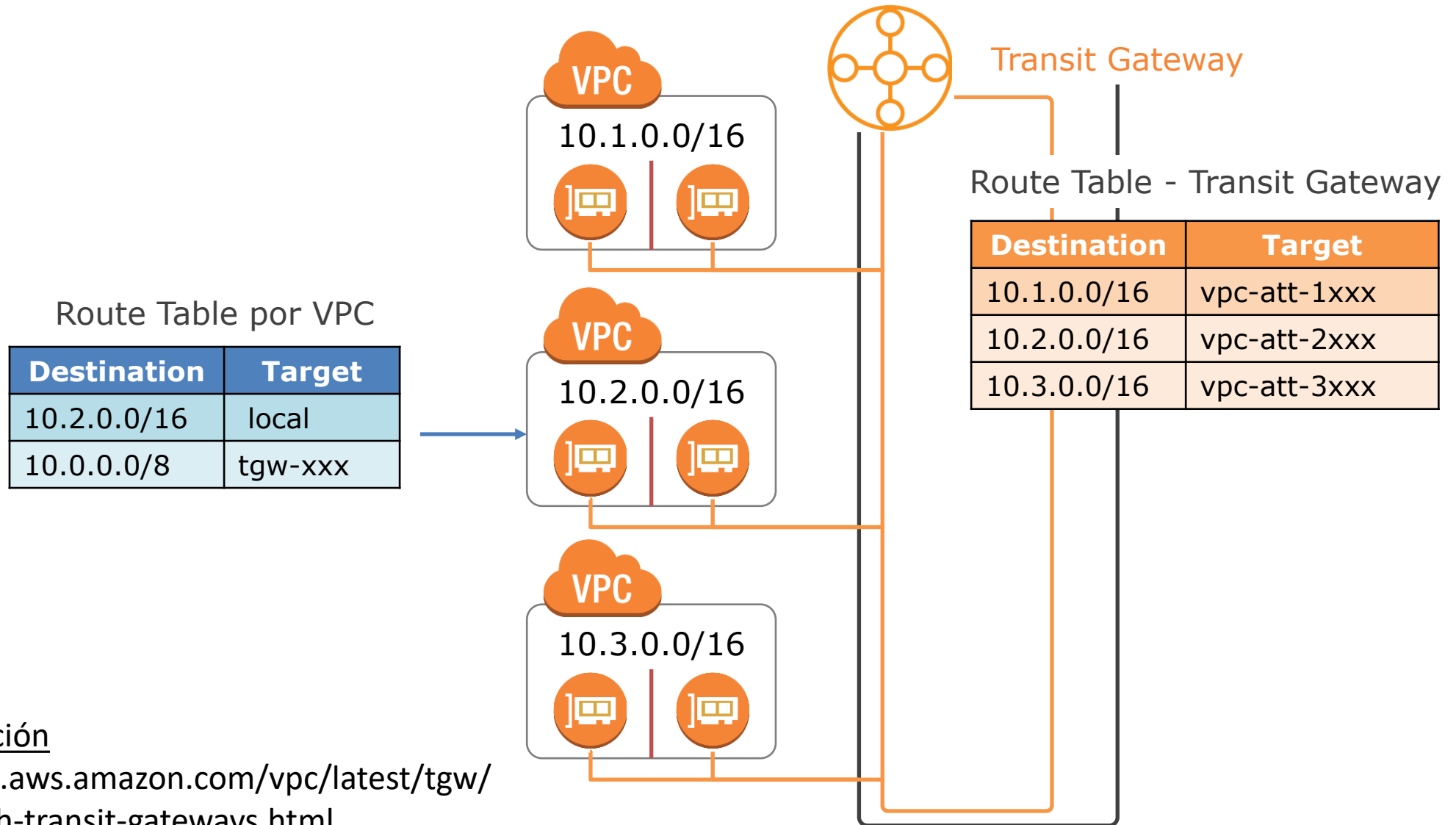
# Transit Gateway

- Actúa como hub para que todo el tráfico fluya entre las redes simplificando la conectividad
- Servicio de enrutamiento totalmente gestionado, altamente disponible y flexible
- Soporte intra e inter regiones, conexiones VPN y Direct Connect.





# Transit Gateway



Documentación

<https://docs.aws.amazon.com/vpc/latest/tgw/working-with-transit-gateways.html>

# Demo



## Creación de Transit Gateway

- Creación de VPC en diferentes cuentas
- Creación de Transit Gateway
- Creación de EC2

aws Services

CloudFormation > Stacks > lab-networking

Stacks (1)

Filter by stack name

Active View nested

lab-networking  
2020-10-09 11:07:55 UTC-0500  
CREATE\_COMPLETE

### lab-networking

Delete Update Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change sets

#### Resources (31)

Search resources

Logical ID	Physical ID	Type	Status	Status reason
Database1RouteTableAssociation	rtbassoc-0e23b66c8f2a1f600	AWS::EC2::SubnetRouteTable Association	CREATE_COMPLETE	-
Database2RouteTableAssociation	rtbassoc-0d3883b0ec57a7c95	AWS::EC2::SubnetRouteTable Association	CREATE_COMPLETE	-
DatabaseRouteTable	rtb-0e01d43c5132a6e85	AWS::EC2::RouteTable	CREATE_COMPLETE	-
DatabaseSubnet1	subnet-09ff5f784560cb2a6	AWS::EC2::Subnet	CREATE_COMPLETE	-
DatabaseSubnet2	subnet-02cd727dc27098b41	AWS::EC2::Subnet	CREATE_COMPLETE	-
DatabaseSubnetGroup	db-sngroup	AWS::RDS::DBSubnetGroup	CREATE_COMPLETE	-
DefaultDatabaseRoute	lab-n-Defau-MRJAT3UMTFY5	AWS::EC2::Route	CREATE_COMPLETE	-
DefaultPrivateRoute	lab-n-Defau-Z20X5AI8AE04	AWS::EC2::Route	CREATE_COMPLETE	-
DefaultPublicRoute	lab-n-Defau-1QM8GHSV6WHY	AWS::EC2::Route	CREATE_COMPLETE	-
InternetGateway	igw-0ed74aca76838ff2d	AWS::EC2::InternetGateway	CREATE_COMPLETE	-
InternetGatewayAttachment	lab-n-Inter-UAPOPCOVLSDJ	AWS::EC2::VPCGatewayAttac hment	CREATE_COMPLETE	-
NatGateway	nat-0bd977d2fee12d13a	AWS::EC2::NatGateway	CREATE_COMPLETE	-

Feedback English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

## 1. Creación de VPC en diferentes cuentas

aws

Services

carlos.cruzado@bwit.pe @ pe-bwit-admin

Ohio

Support

New VPC Experience

Tell us what you think

Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables

Network Manager

TRAFFIC MIRRORING

Mirror Sessions

Mirror Targets

Mirror Filters

Create Transit Gateway

Actions

Filter by tags and attributes or search by keyword

1 to 1 of 1

Name	Transit Gateway ID	Owner ID	State
TG	tgw-0c8b80d2264a5e7b2	027340862068	available

Transit Gateway: tgw-0c8b80d2264a5e7b2

Details

Tags

Sharing

Transit Gateway ID	tgw-0c8b80d2264a5e7b2	Owner account ID	027340862068
State	available	Amazon ASN	64512
DNS support	enable	VPN ECMP support	enable
Auto accept shared attachments	enable	Default association route table	enable
Association route table ID	tgw-rtb-02eaf41cf392e854d	Default propagation route table	enable
Propagation route table ID	tgw-rtb-02eaf41cf392e854d		

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

## 2. Crear Transit Gateway



aws

Services

New VPC Experience

Tell us what you think

Endpoints

Endpoint Services

NAT Gateways New

Peering Connections

SECURITY

Network ACLs

Security Groups New

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables

Network Manager

TRAFFIC MIRRORING

Mirror Sessions New

Mirror Targets New

Mirror Filters New

Settings New

Create Transit Gateway Attachment

Actions

Filter by tags and attributes or search by keyword

1 to 1 of 1

	Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State	Associated route table ID	Association state
	TG CUENTA...	tgw-attach-0851a9d28bb47b72d	tgw-0c8b80d2264a5e7b2	VPC	vpc-01b83daf57ea24802	available	tgw-rtb-02eaf41cf392e854d	associated

Transit Gateway Attachment: tgw-attach-0851a9d28bb47b72d

Details

Tags

Transit Gateway attachment ID

tgw-attach-0851a9d28bb47b72d

Transit Gateway ID

tgw-0c8b80d2264a5e7b2

Resource type

VPC

Resource ID

vpc-01b83daf57ea24802

Association state

associated

Subnet IDs

subnet-0f110e99b65571563  
 subnet-06dc8de915d2f982f

Transit Gateway owner ID

027340862068

Resource owner account ID

027340862068

State

available

Associated route table

tgw-rtb-02eaf41cf392e854d

DNS support

enable

IPv6 support

disable

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

### 3. Crear Transit Gateway Attachment

The screenshot displays the AWS Resource Access Manager (RAM) console. The left sidebar shows the navigation menu with 'Resource Access Manager' selected. The main content area is titled 'Resource shares (1)' and shows a table with one resource share. The table has columns for Name, ID, Owner, Allow external principals, and Status. The resource share 'TG' is listed with ID '9b8ddb42-12d6-4045-9c4a-f7aff5fed073' and is in an 'Active' status.

Resource Access Manager

Resource shares (1)

Resource shares owned by your account

Filter by attributes or search by keyword

	Name	ID	Owner	Allow external principals	Status
<input type="radio"/>	TG	9b8ddb42-12d6-4045-9c4a-f7aff5fed073	027340862068	Yes	Active

#### 4. Compartir Transit Gateway con Resource Access Manager (RAM)

The screenshot displays the AWS Resource Access Manager (RAM) console. The left sidebar shows the navigation menu with 'Resource Access Manager' selected. Under 'Shared with me', 'Resource shares' is highlighted. The main content area shows 'Resource shares (1)' with a search bar and a table of shares. The table has columns for Name, ID, Owner, and Status. One share is listed with Name 'TG', ID '9b8ddb42-12d6-4045-9c4a-f7aff5fed073', Owner '027340862068', and Status 'Active'.

aws Services ▾

ccruzadogu ▾ Ohio ▾ Support ▾

Resource Access Manager ✕

Resource Access Manager > Shared with me : Resource shares

**Resource shares (1)** ⌂ Leave resource share

Resource shares my account has access to

< 1 > ⚙

	Name	ID	Owner	Status
<input type="radio"/>	TG	9b8ddb42-12d6-4045-9c4a-f7aff5fed073	027340862068	Active

Feedback English (US) ▾

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

5. Aceptar el recurso de Transit Gateway en la otra cuenta

aws

Services

New VPC Experience

Tell us what you think

Endpoints

Endpoint Services

NAT Gateways New

Peering Connections

SECURITY

Network ACLs

Security Groups New

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables

Network Manager

TRAFFIC MIRRORING

Mirror Sessions New

Mirror Targets New

Mirror Filters New

Settings New

Feedback

English (US)

Create Transit Gateway Attachment

Actions

Filter by tags and attributes or search by keyword

Name

Transit Gateway attachment ID

Transit Gateway ID

Resource type

Resource ID

State

Associated route table ID

Association state

TG CUENTA...

tgw-attach-06ecec0c1ab57829f

tgw-0c8b80d2264a5e7b2

VPC

vpc-06e481466060f84b5

available

tgw-rtb-02eaf41cf392e854d

associated

Transit Gateway Attachment: tgw-attach-06ecec0c1ab57829f

Details

Tags

Transit Gateway attachment ID

tgw-attach-06ecec0c1ab57829f

Transit Gateway ID

tgw-0c8b80d2264a5e7b2

Resource type

VPC

Resource ID

vpc-06e481466060f84b5

Association state

associated

Subnet IDs

subnet-0c154303caa82085f

subnet-00e111dc3509d31ca

Transit Gateway owner ID

027340862068 (shared)

Resource owner account ID

843517460043

State

available

Associated route table

tgw-rtb-02eaf41cf392e854d

DNS support

enable

IPv6 support

disable

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

## 6. Crear Transit Gateway Attachment en cuenta adicional





aws

Services

carlos.cruzado@bwit.pe @ pe-bwit-admin

Ohio

Support

New VPC Experience

Tell us what you think

Endpoints

Endpoint Services

NAT Gateways New

Peering Connections

SECURITY

Network ACLs

Security Groups New

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables

Network Manager

TRAFFIC MIRRORING

Mirror Sessions New

Mirror Targets New

Mirror Filters New

Settings New

Create Transit Gateway Route Table

Actions

Filter by tags and attributes or search by keyword

<<

<

1 to 1 of 1

>

>>

	Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
<input checked="" type="checkbox"/>		tgw-rtb-02eaf41cf392e854d	tgw-0c8b80d2264a5e7b2	available	Yes	Yes

Transit Gateway Route Table: tgw-rtb-02eaf41cf392e854d

Details

Associations

Propagations

Prefix list references

Routes

Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create static route

Replace static route

Delete static route

Filter by attributes or search by keyword

<<

<

1 to 2 of 2

>

>>

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state	Prefix List ID
<input type="checkbox"/>	10.0.0.0/16	tgw-attach-0851a9d28bb47b72d   vpc-01b83daf57ea24802	VPC	propagated	active	-
<input type="checkbox"/>	10.1.0.0/16	tgw-attach-06ecec0c1ab57829f   vpc-06e481466060f84b5	VPC	propagated	active	-

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

## 7. Verificar el Transit Gateway Route Table

The logo for the AWS User Group Peru, featuring the AWS logo and the text "USER GROUP PERU" with a stylized map of Peru.

aws

Services

carlos.cruzado@bwit.pe @ pe-bwit-admin

Ohio

Support

New VPC Experience

Tell us what you think

VPC Dashboard

New

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN

Create route table

Actions

Filter by tags and attributes or search by keyword

1 to 4 of 4

	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
<input type="checkbox"/>		rtb-0b6e99bdd1b8a5f90	-	-	Yes	vpc-01b83daf57ea24802  ...	027340862068
<input type="checkbox"/>	RT DB 01	rtb-0e01d43c5132a6e85	2 subnets	-	No	vpc-01b83daf57ea24802  ...	027340862068
<input checked="" type="checkbox"/>	RT PRI	rtb-05196aec359cb0a5b	2 subnets	-	No	vpc-01b83daf57ea24802  ...	027340862068
<input type="checkbox"/>	RT PUB	rtb-084827b1bbc715ae6	2 subnets	-	No	vpc-01b83daf57ea24802  ...	027340862068

Route Table: rtb-05196aec359cb0a5b

Summary

Routes

Subnet Associations

Edge Associations

Route Propagation

Tags

Edit routes

View

All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-0bd977d2fee12d13a	active	No
10.0.0.0/8	tgw-0c8b80d2264a5e7b2	active	No

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

## 8. Modificar Route Table para comunicarse entre VPC a través de Transit Gateway

The logo for the AWS User Group in Peru, featuring the AWS logo and the word "PERU" with a map of Peru.



Preguntas?

