



Step-by-Step Guide: Associating Security Groups with Multiple VPCs and Sharing Security Groups with AWS Organizations



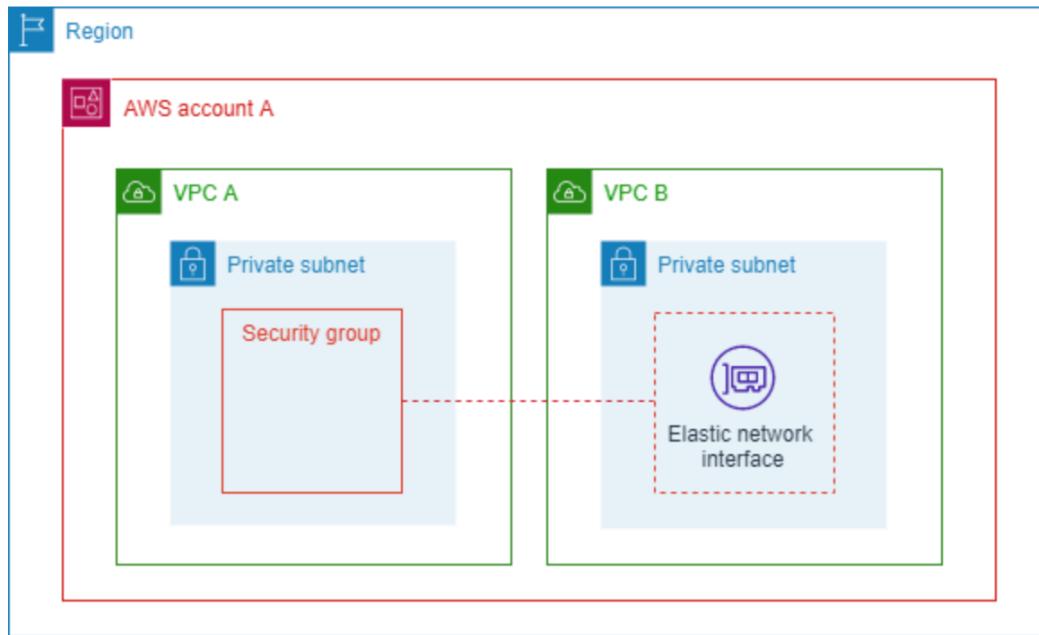
By
Mahendran Selvakumar

<https://devopstronaut.com/>

<https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>



Associate security groups with multiple VPCs:



Requirements for the Security Group VPC Associations Feature

- Ownership and Permissions:** To associate a security group with a VPC, you must either own the VPC or have one of its subnets shared with you.
- Region Consistency:** Both the VPC and the security group must be in the same AWS Region.
- Restrictions on Default Resources:**
 - Only non-default security groups are eligible for this feature.
 - Security groups created in a default VPC cannot be used; only security groups associated with non-default VPCs are supported.
- Visibility:** Both the security group owner and the VPC owner can view the security group VPC associations.

Supported Services for Security Group VPC Associations

This feature is compatible with the following AWS services:

- Amazon API Gateway (REST APIs only)
- AWS Auto Scaling
- AWS CloudFormation
- Amazon EC2
- Amazon EFS
- Amazon EKS
- Amazon FSx
- AWS PrivateLink
- Amazon Route 53



Create Multiple VPC's:

Navigate to **VPC**, then click **Create VPC**

The screenshot shows the AWS VPC dashboard. At the top, there is a search bar and a note: "Note: Your Instances will launch in the Europe region." Below this is a section titled "Resources by Region" with tabs for "VPCs" (Europe 1), "NAT Gateways" (Europe 0), and "Subnets" (Europe 3). On the right side, there are sections for "Service Health" and "Settings". A large orange "Create VPC" button is prominently displayed at the top left of the main content area.

Select **VPC and More**, then enter the **Name** and specify the **IPv4 CIDR block**

The screenshot shows the "Create VPC" wizard. In the "VPC settings" section, under "Resources to create", the "VPC and more" option is selected. Under "Name tag auto-generation", "Auto-generate" is checked and "dev-vpc" is entered. Under "IPv4 CIDR block", "10.0.0.0/20" is specified. In the "Preview" section, a diagram illustrates the VPC structure: a central "VPC" box labeled "dev-vpc-vpc" is connected to four "Subnets (4)" boxes (eu-west-1a, eu-west-1b, eu-west-1c, eu-west-1d) and three "Route tables (3)" boxes (dev-vpc-rtb-public, dev-vpc-rtb-private1, dev-vpc-rtb-private2). Each subnet is associated with a specific route table.

Leave the settings as default, select **None** for VPC Endpoints, and uncheck the **DNS Options**



Number of Availability Zones (AZs) [Info](#)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 **2** **3**

► **Customize AZs**

Number of public subnets [Info](#)
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 **2**

Number of private subnets [Info](#)
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 **2** **4**

► **Customize subnets CIDR blocks**

NAT gateways (\$) [Info](#)
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.

None **In 1 AZ** **1 per AZ**

VPC endpoints [Info](#)
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None **S3 Gateway**

DNS options [Info](#)
 Enable DNS hostnames
 Enable DNS resolution

► **Additional tags**

Create VPC

The VPC has now been successfully created and is named **dev-vpc**

Your VPCs (1/2) Info									Last updated less than a minute ago	Actions	Create VPC
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table					
-	vpc-01c128bb0e2b77712	Available	172.31.0.0/16	-	dopt-0a65ee57120360...	rtb-0b4cf9a66d5e0a2fa					
<input checked="" type="checkbox"/> dev-vpc	vpc-0853cf47225c46275	Available	10.0.0.0/20	-	dopt-0a65ee57120360...	-					



Select VPC and More, then provide the Name and enter the IPv4 CIDR block

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.
 VPC only VPC and more

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
 Auto-generate
preprod-vpc

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.
10.1.0.0/20 4,096 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
 No IPv6 CIDR block
 Amazon-provided IPv6 CIDR block

Tenancy [Info](#)
Default

Number of Availability Zones (AZs) [Info](#)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
1 **2** 3
► Customize AZs

Preview

VPC [Show details](#)
Your AWS virtual network
preprod-vpc-vpc

Subnets (4)
Subnets within this VPC
eu-west-1a
preprod-vpc-subnet-public1-eu-
preprod-vpc-subnet-private1-eu-
eu-west-1b
preprod-vpc-subnet-public2-eu-
preprod-vpc-subnet-private2-eu-

Route tables (3)
Route network traffic to resources
preprod-vpc-rtb-public
preprod-vpc-rtb-private1-eu-west-1a
preprod-vpc-rtb-private2-eu-west-1b

Network connectivity
Connections to other networks
preprod-vpc-lgw

Leave the settings as default, select **None** for VPC Endpoints, uncheck the **DNS Options**, and then click **Create VPC**

Number of public subnets [Info](#)
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.
0 2

Number of private subnets [Info](#)
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.
0 2 4

► **Customize subnets CIDR blocks**

NAT gateways (\$) [Info](#)
Choose the number of Availability Zones (AZs) in which to create NAT gateways.
Note that there is a charge for each NAT gateway
None In 1 AZ 1 per AZ

VPC endpoints [Info](#)
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.
None S3 Gateway

DNS options [Info](#)
 Enable DNS hostnames
 Enable DNS resolution

► **Additional tags**

Create VPC

<https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>



The VPC will be created. Click **View VPC** to see the newly created VPC

VPC > Your VPCs > Create VPC > Create VPC resources

Create VPC workflow

Success

Details

- ✓ Create VPC: vpc-0ef56477cdf6cdfdd []
- ✓ Disable DNS hostnames
- ✓ Disable DNS resolution
- ✓ Verifying VPC creation: vpc-0ef56477cdf6cdfdd []
- ✓ Create subnet: subnet-03338717d9dfb05eb []
- ✓ Create subnet: subnet-043f9b485d93fab67 []
- ✓ Create subnet: subnet-0a149b7a7ed5d8d8e []
- ✓ Create subnet: subnet-0e4a888627becdc6e []
- ✓ Create internet gateway: igw-0f0b83a5f88fce3d1 []
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-06ff8fecef99e7a5 []
- ✓ Create route
- ✓ Associate route table
- ✓ Associate route table
- ✓ Create route table: rtb-0d9969ab62de9a1ec []
- ✓ Associate route table
- ✓ Create route table: rtb-0ff4c64061fd451f5 []
- ✓ Associate route table
- ✓ Verifying route table creation

View VPC

Another VPC has now been successfully created and is named **preprod-vpc**

Your VPCs (1/3) Info		Actions Create VPC						
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table		
-	vpc-01c128bb0e2b77712	Available	172.31.0.0/16	-	dopt-0a65ee57120360...	rtb-0b4cf9a66d5e0a2fa		
dev-vpc	vpc-0853cf47225c46275	Available	10.0.0.0/20	-	dopt-0a65ee57120360...	-		
<input checked="" type="checkbox"/> preprod-vpc	vpc-0ef56477cdf6cdfdd	Available	10.1.0.0/20	-	dopt-0a65ee57120360...	-		



Associate a security group with another VPC

Navigate to **Security Groups** and click **Create Security Group**

Name	Security group ID	Security group name	VPC ID	Description
-	sg-06e5b29eeahd0b6e	default	vpc-0853cf47225c46275	default VPC security group
-	sg-01e7e297fd2e329cd	default	vpc-0ef56477cf66cdffdd	default VPC security group
-	sg-0e201ad87381baec1	default	vpc-01c128bb0e2b77712	default VPC security group

Provide the **Name**, **Description**, and select the **VPC**. Here, I have created inbound rules for **SSH** (port 22) and **HTTP** (port 80)

Basic details

Security group name **Info**
common-security-group
Name cannot be edited after creation.

Description **Info**
This Security shared with Dev and Preprod

VPC **Info**
vpc-0853cf47225c46275 (dev-vpc)

Inbound rules **Info**

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	Anywhere-IPv4	0.0.0.0/0
HTTP	TCP	80	Anywhere-IPv4	0.0.0.0/0

Click **Create Security Group** to finalize the creation of the security group



⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. X

Outbound rules Info

Type	Info	Protocol	Info	Port range	Info	Destination	Info	Description - optional	Info
All traffic	▼	All		All		Custom	▼	Q	
0.0.0.0/0 X									

Add rule

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses. X

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags

Create security group

The security group has now been successfully created

⌚ Security group (sg-03405bffc202316ed | common-security-group) was created successfully X

► Details

VPC > Security Groups > sg-03405bffc202316ed - common-security-group

sg-03405bffc202316ed - common-security-group Actions ▾

Details

Security group name common-security-group	Security group ID sg-03405bffc202316ed	Description This Security shared with Dev and Preprod	VPC ID vpc-0853cf47225c46275
Owner 038462791702	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

VPC associations

Q Filter associations

Security group ID	VPC ID	VPC owner ID	Status	Status reason
No VPC associations found				
This security group does not have any VPC associations.				

Associate VPC

Navigate to the newly created security group and click **Associate VPC**

VPC > Security Groups > sg-03405bffc202316ed - common-security-group

sg-03405bffc202316ed - common-security-group Actions ▾

Details

Security group name common-security-group	Security group ID sg-03405bffc202316ed	Description This Security shared with Dev and Preprod	VPC ID vpc-0853cf47225c46275
Owner 038462791702	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

VPC associations

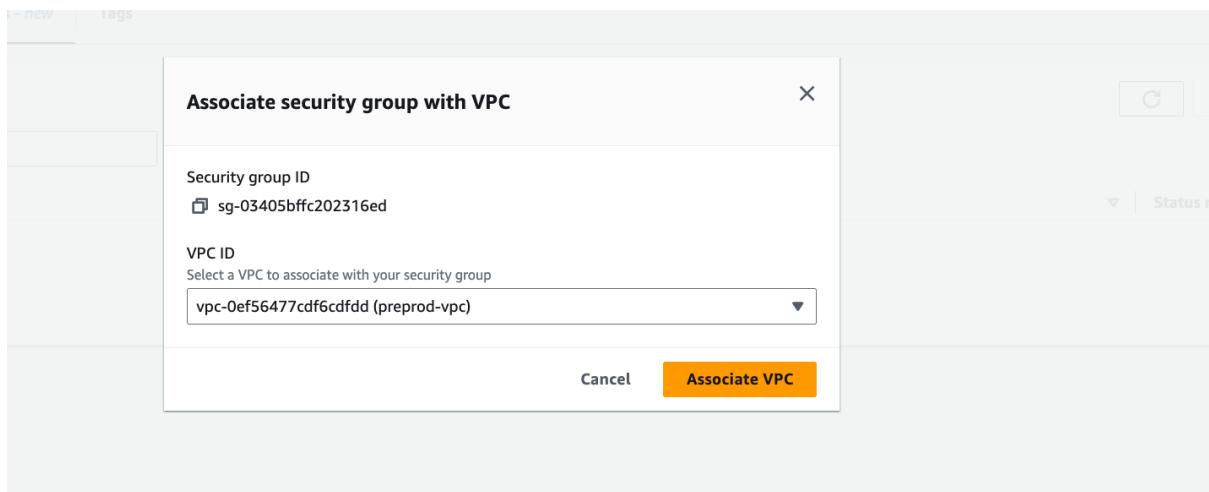
Q Filter associations

Security group ID	VPC ID	VPC owner ID	Status	Status reason
No VPC associations found				
This security group does not have any VPC associations.				

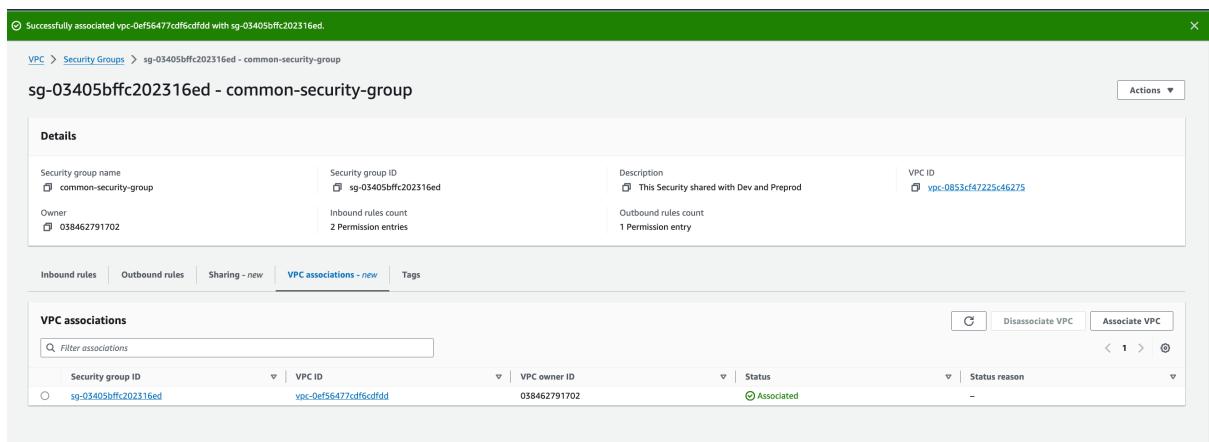
Associate VPC



Select another VPC from the **VPC ID** dropdown menu and click **Associate VPC**



The security group is now successfully associated with another VPC



Now we can create an EC2 instance using the shared security group

Disassociate a security group from another VPC:

Select the security group, navigate to **VPC Associations**, choose the associated VPC, and then click **Disassociate VPC**



VPC > Security Groups > sg-03405bffc202316ed

sg-03405bffc202316ed - common-security-group

Actions ▾

Details

Security group name common-security-group	Security group ID sg-03405bffc202316ed	Description This Security shared with Dev and Preprod	VPC ID vpc-0853cf47225c46275
Owner 038462791702	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

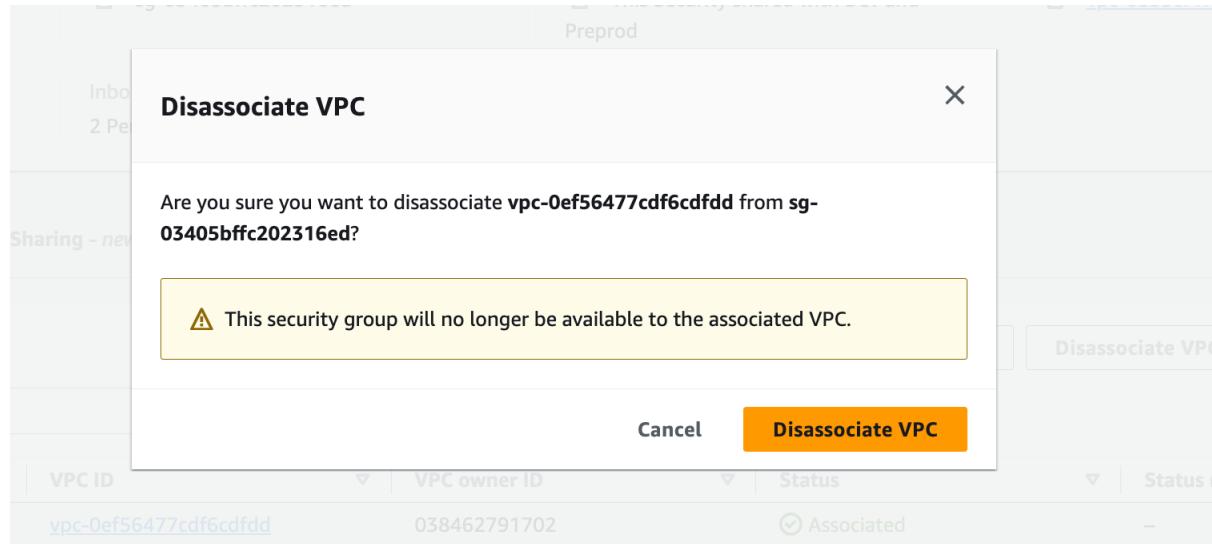
Inbound rules Outbound rules Sharing - new [VPC associations - new](#) Tags

VPC associations

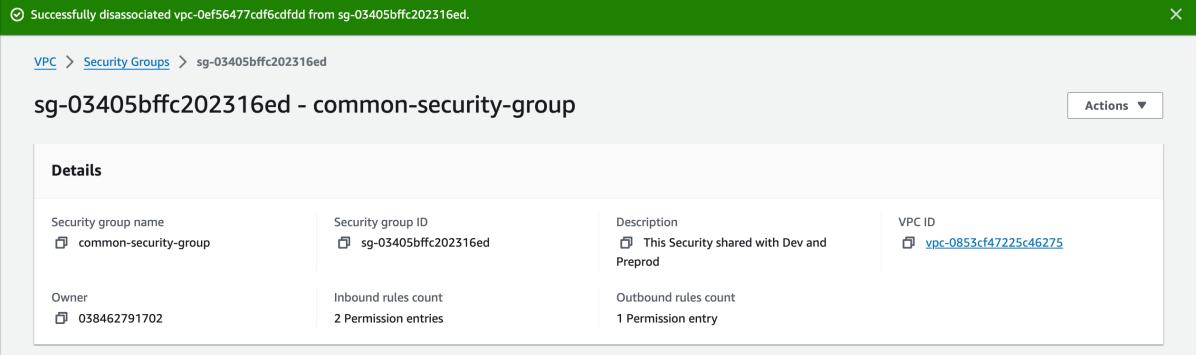
[C](#) Disassociate VPC Associate VPC
< 1 > ⚙

Security group ID	VPC ID	VPC owner ID	Status	Status reason
sg-03405bffc202316ed	vpc-0ef56477cdf6cdfdd	038462791702	Associated	-

Click Disassociate VPC

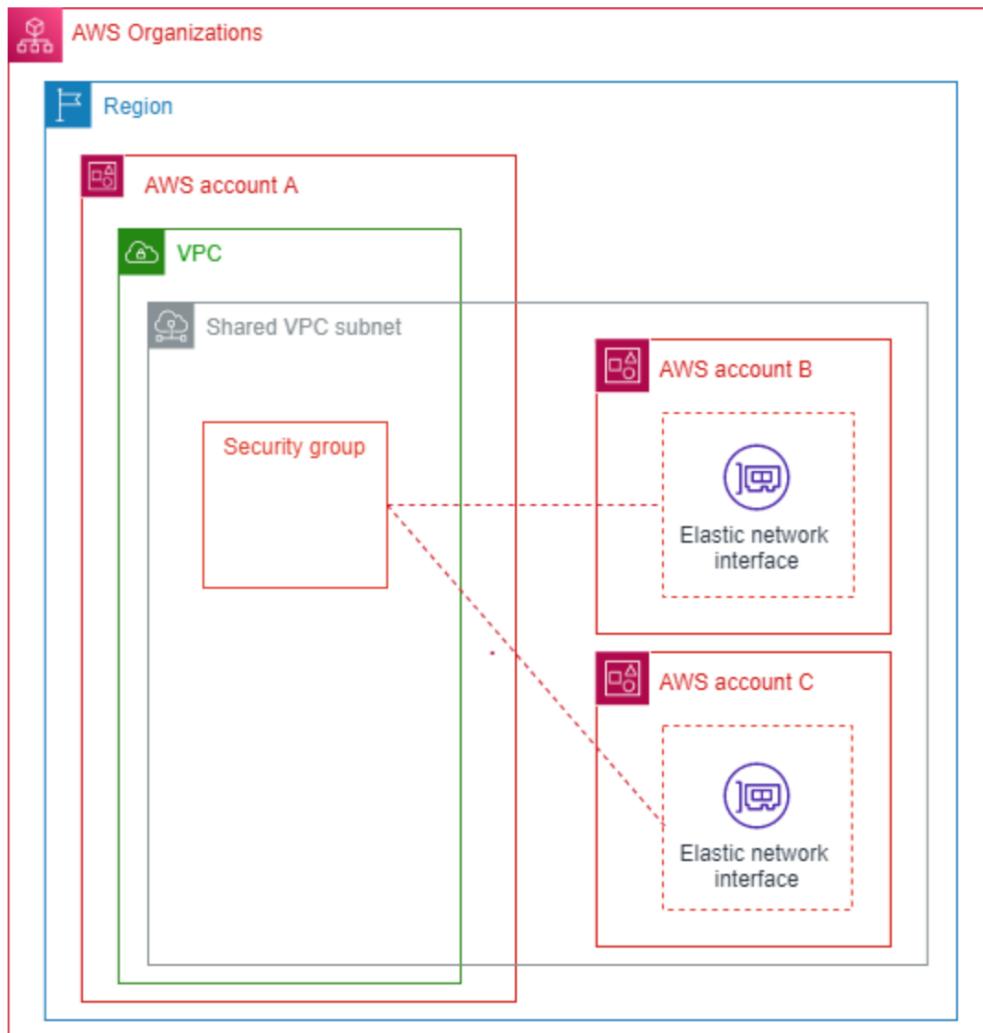


The VPC has now been successfully disassociated from the security group





Share security groups with AWS Organizations:



Requirements of the Shared Security Group Feature

- **Organizational Scope:** This feature is limited to accounts within the same AWS Organization. Resource sharing must be enabled within AWS Organizations.
- **Ownership:** The account sharing the security group must own both the **VPC** and the **security group**.
- **Restrictions on Default Resources:**
 - Default security groups cannot be shared.
 - Security groups in a default VPC are also not shareable.
- **Participant Accounts:** While participant accounts can create security groups in a shared VPC, they cannot share these security groups with others.



Supported Services for Shared Security Groups

The Shared Security Group feature is supported by the following AWS services:

- Amazon API Gateway
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Amazon EMR
- Amazon FSx
- Amazon ElastiCache
- AWS Elastic Beanstalk
- AWS Glue
- Amazon MQ
- Amazon SageMaker

Share a security group with organization:

Select the security group that you want to share with your organizations

Name	Security group ID	Security group name	VPC ID	Description
-	sg-06e3b29deabd0b6e	default	vpc-0853cf47225c46275	default VPC security group
-	sg-01e7e297fd2e529cd	default	vpc-0ef56477cdf6cdffd	default VPC security group
-	sg-03405bffc202316ed	common-security-group	vpc-0853cf47225c46275	This Security shared with Dev and Prep
-	sg-0e201a487381baec1	default	vpc-01c128bb0e2b77712	default VPC security group

Navigate to the **Sharing** tab and click **Share Security Group**

sg-03405bffc202316ed - common-security-group

Sharing - new

Resource sharing

No resource share found

This security group is not part of any resource share.

Share security group



Click Create Resource Share

VPC > Security Groups > sg-03405bffc202316ed > Share security group

Share security group

Share security group sg-03405bffc202316ed with an AWS account or your organization.

Resource sharing

Filter resource shares

No resource shares found
There are no available resource shares.

Cancel Share security group

Provide a name for the resource share, choose **Security Group** as the resource type, and select the security group you wish to share with your organizations

Resource Access Manager > Shared by me: Resource shares > Create resource share

Step 1 Specify resource share details

Step 2 Associate managed permissions

Step 3 Grant access to principals

Step 4 Review and create

Specify resource share details

Enter a name for the resource share and select the resources that you want to share.

Resource share name

Name
Provide a descriptive name for the resource share.
common-security-group

Resources - optional

Choose the resources to add to the resource share

Security Groups Filter by text

ID	Group name	VPC ID
sg-06e3b29deab0b6e	default	vpc-0853cf47225c46275
sg-01e7e297fd2e329cd	default	vpc-0ef56477cdf6cdfdd
<input checked="" type="checkbox"/> sg-03405bffc202316ed	common-security-group	vpc-0853cf47225c46275
sg-0e201a487381baec1	default	vpc-01c128bb0e2b77712

Cancel Next

Click **Next** to associate managed permissions

Selected resources (1)

Filter by text

Resource ID	Resource type
sg-03405bffc202316ed	ec2:SecurityGroup

Tags - optional

Tags are key-value pairs that you can add to AWS resources to help identify, organise and secure your AWS resources.

Key	Value - optional
Enter key	Enter value

Add new tag

Cancel Next



Click **Next** to Grant access to principals

Resource Access Manager > Shared by me: Resource shares > Create resource share

Step 1
Specify resource share details

Step 2
Associate managed permissions

Step 3
Grant access to principals

Step 4
Review and create

Managed permission for ec2:SecurityGroup

To specify which actions principals are allowed to perform on shared resources, choose the managed permission to associate with each shared resource type.

Managed permissions

Choose the managed permission to use for ec2:SecurityGroup or create a new customer-managed permission

AWSRAMDefaultPermissionsSecurityGroup

Create customer-managed permission

Version

You can use only the default version of a managed permission when creating a resource share.

1 (default)

View the policy template for this managed permission

Statement 1

Actions (8)

ec2:CreateNetworkInterface	ec2:CreateTags	ec2:DeleteTags
ec2:ModifyInstanceAttribute	ec2:ModifyNetworkInterfaceAttribute	ec2:RequestSpotFleet
ec2:RequestSpotInstances	ec2:RunInstances	

Conditions (0)

No conditions applied

Cancel Previous Next

Choose **Allow sharing within your organization**, select the principals, and then click **Next**

Grant access to principals

Specify the principals that are allowed access to the shared resources. A principal can be any of the following: An entire organisation or organisational unit (OU) in AWS Organizations, an AWS account, IAM role or IAM user.

Principals - optional

Allow sharing with anyone
You can share resources with any AWS accounts, roles and users. If you are in an organisation, you can also share with the entire organisation or organisational units in that organisation.

Allow sharing only within your organisation
You can share resources with the entire organisation, organisational units or AWS accounts, roles and users in that organisation.

Principals
You can add multiple principals of different types.

Select principal type

Organisation	▲
AWS account	Grant access to a specific AWS account.
Organisation	Grant access to your entire organisation, including its child OUs and AWS accounts. <input checked="" type="checkbox"/>
Organisational unit (OU)	Grant access to an OU, including its child OUs and AWS accounts.
IAM role	Grant access to a specific IAM role.
IAM user	Grant access to a specific IAM user.
Service principal	Grant access to a specific service principal.

Principal type

Principal ID

No selected principals.

Deselect

< 1 > ⚙

Cancel Previous Next

Choose **Add**, then select **Next**. Click **Create Resource Share**. Under **Shared Resources**, wait until the status displays as "Associated".



Return to the VPC console and open the security group list. Select the security group you shared and go to the **Sharing** tab. Here, your AWS RAM resource should appear. If it does not, the resource share creation may have failed, and you may need to attempt the process again.

Conclusion:

This guide outlines the steps for effectively associating security groups with multiple VPCs and sharing them across AWS Organizations. By following these procedures, users can enhance their security posture and streamline resource management, ensuring secure access while promoting collaboration across accounts. Understanding and utilizing these features optimizes your AWS environment for improved security and resource accessibility.

Keep Learning, Keep Securing!!

Feel free to reach out to me, if you have any other queries or suggestions Stay connected on LinkedIn: [Mahendran Selvakumar](#)

Stay connected on Medium: <https://devopstronaut.com/>