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

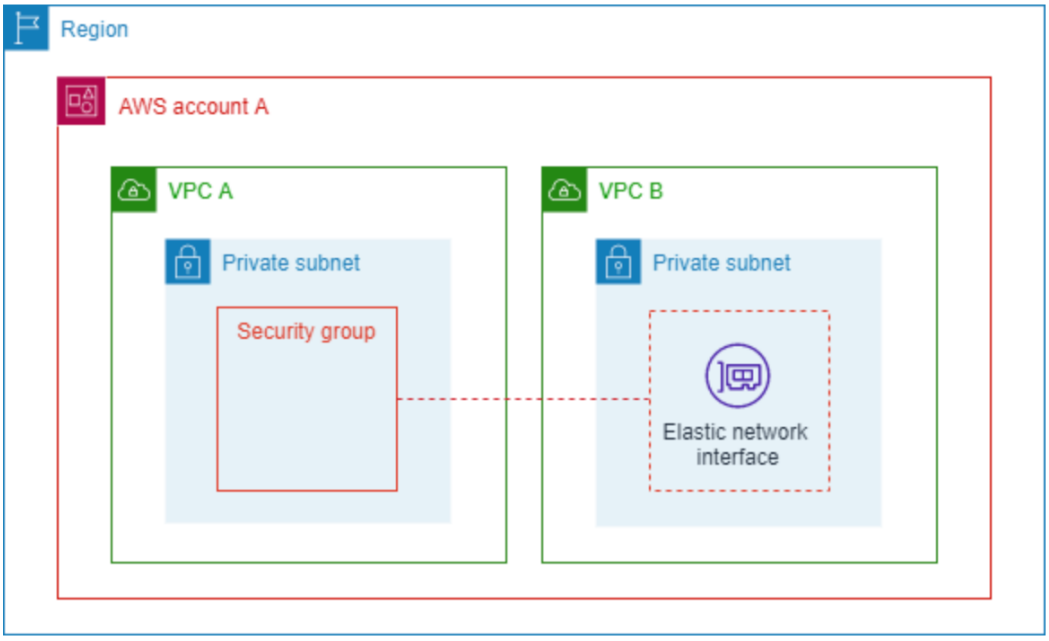
By

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

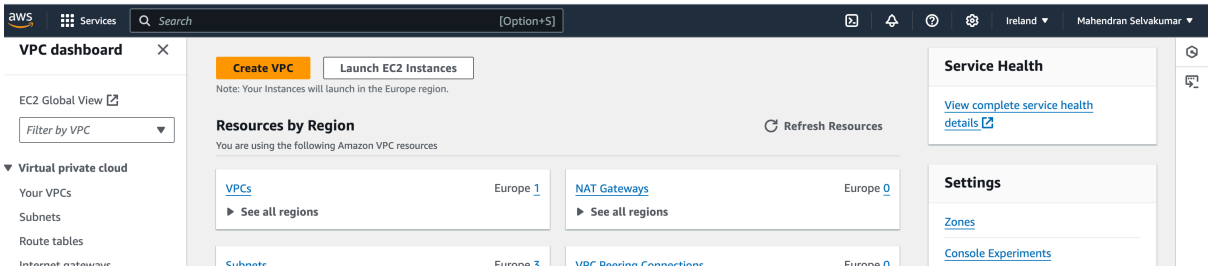
- **Ownership and Permissions**: To associate a security group with a VPC, you must either own the VPC or have one of its subnets shared with you.
- **Region Consistency**: Both the VPC and the security group must be in the same AWS Region.
- **Restrictions on Default Resources**:
  - Only non-default 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:

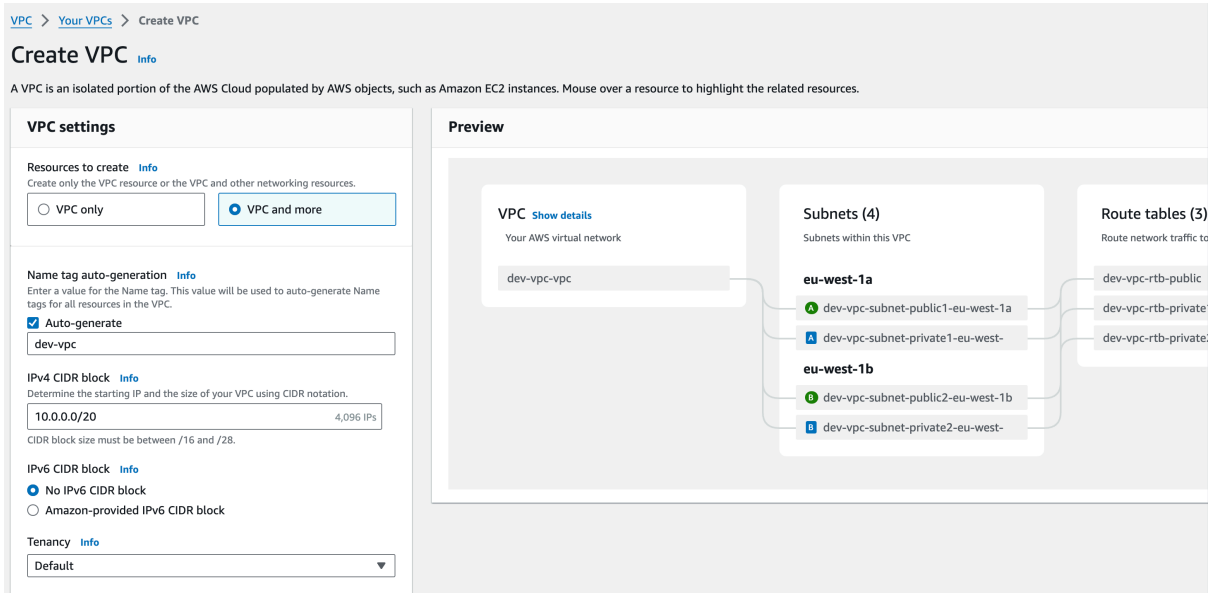
- Amazon API Gateway (REST APIs only)
- AWS Auto Scaling
- AWS CloudFormation
- Amazon EC2
- Amazon EFS
- Amazon EKS
- Amazon FSx
- AWS PrivateLink
- Amazon Route 53

Create Multiple VPC's:

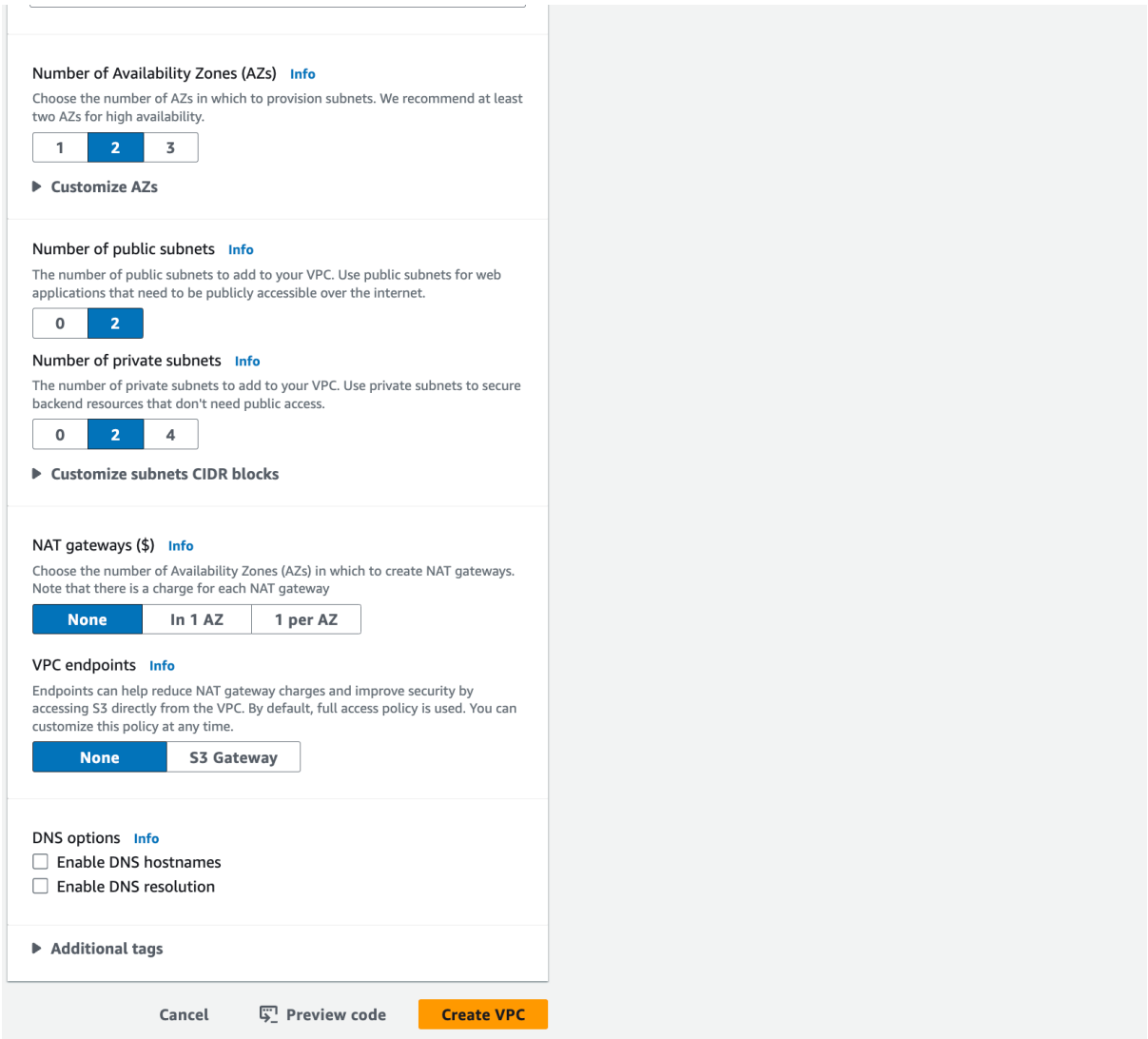
Navigate to **VPC**, then click **Create VPC**



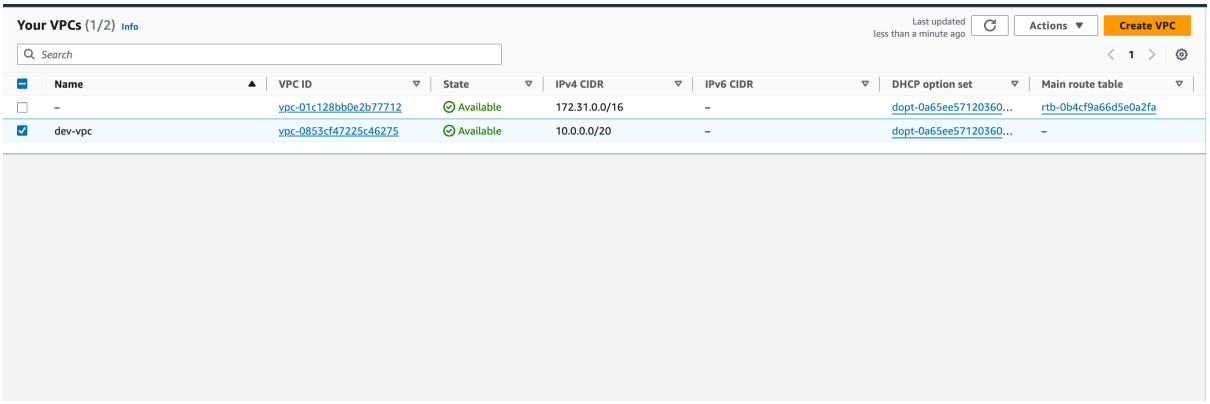
Select **VPC and More**, then enter the **Name** and specify the **IPv4 CIDR block**



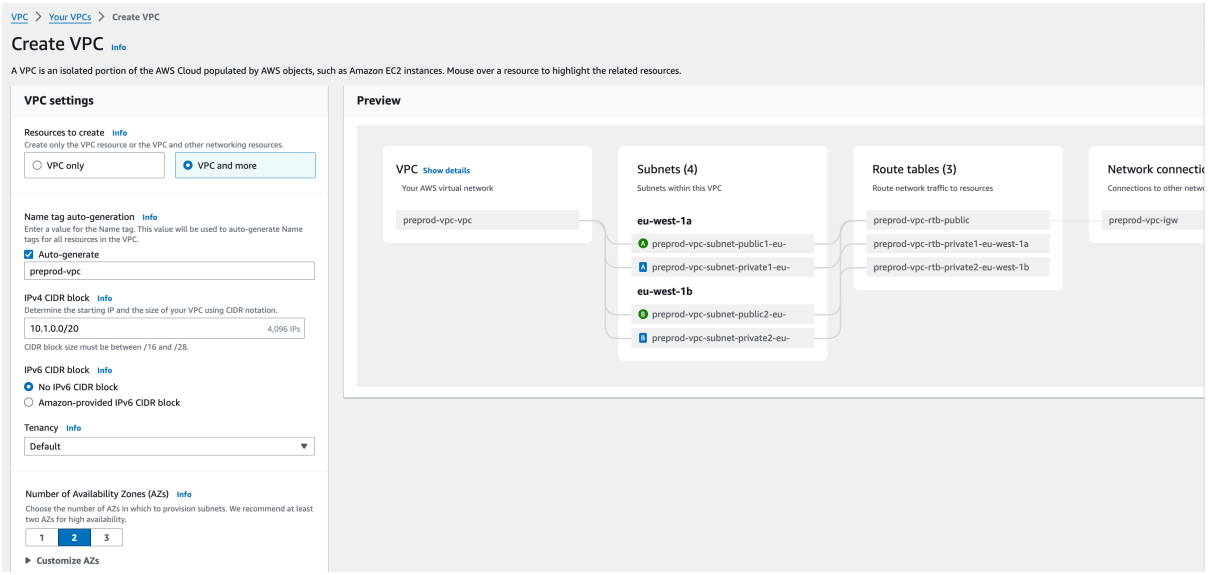
Leave the settings as default, select **None** for VPC Endpoints, and uncheck the **DNS Options**



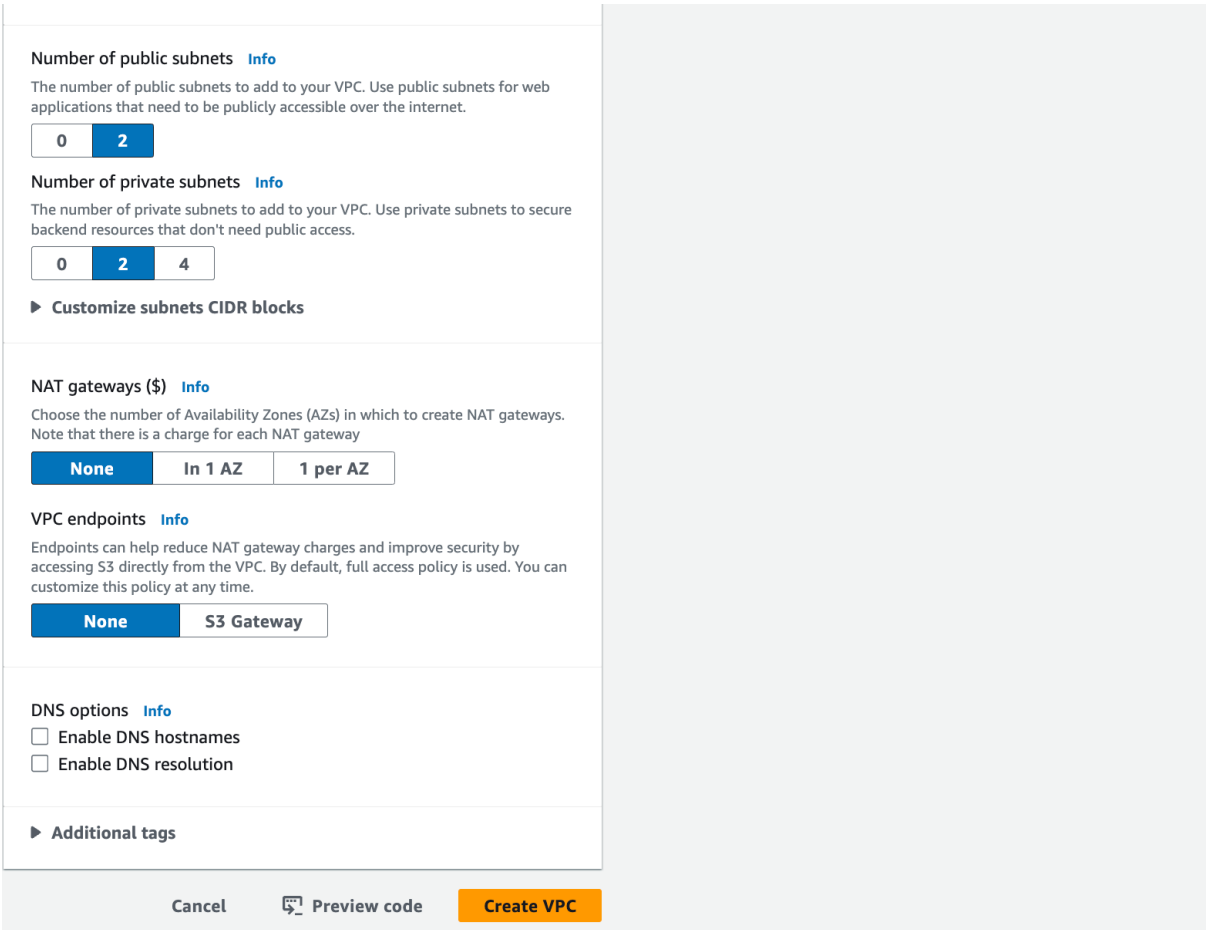
The VPC has now been successfully created and is named **dev-vpc**



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

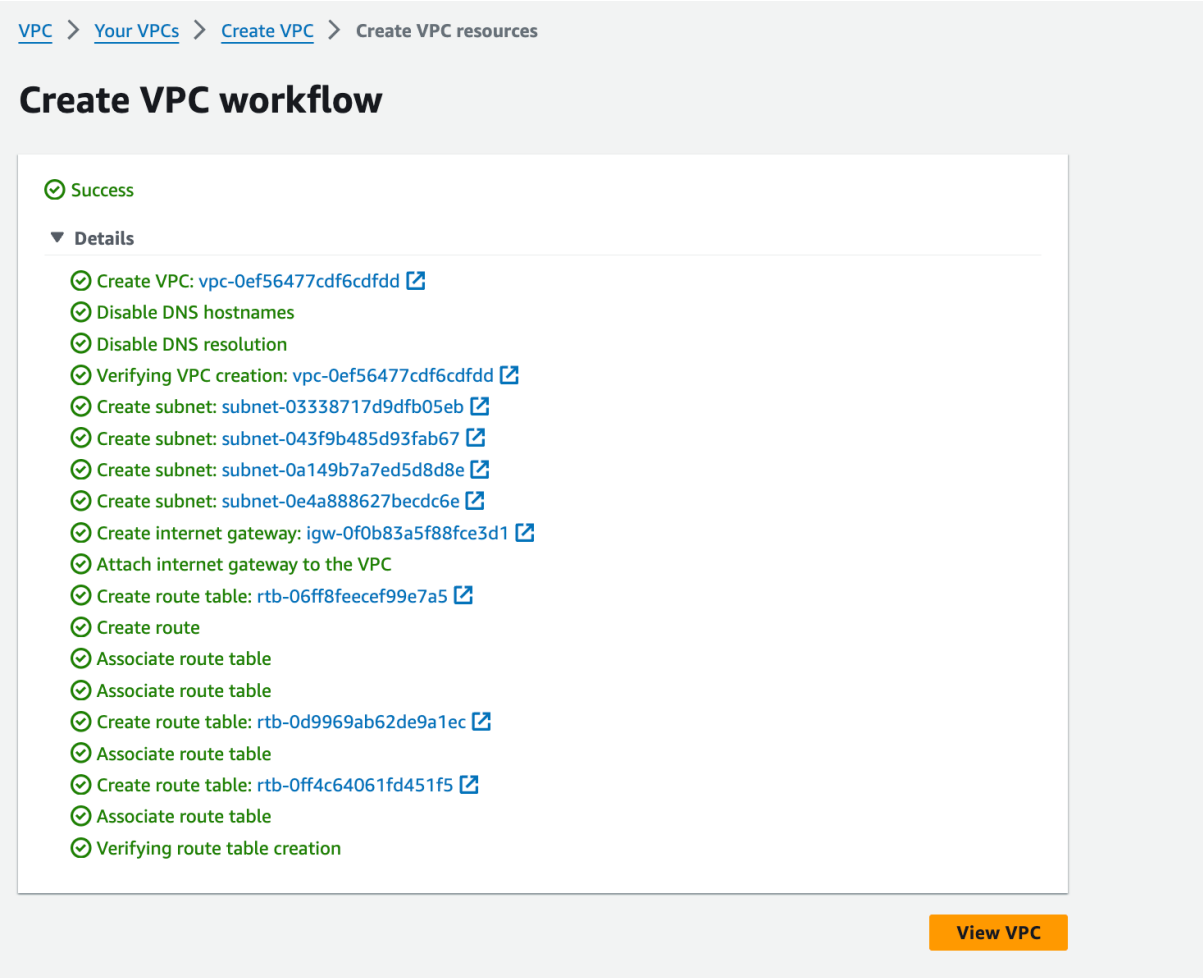


Leave the settings as default, select **None** for VPC Endpoints, uncheck the **DNS Options**, and then click **Create VPC**

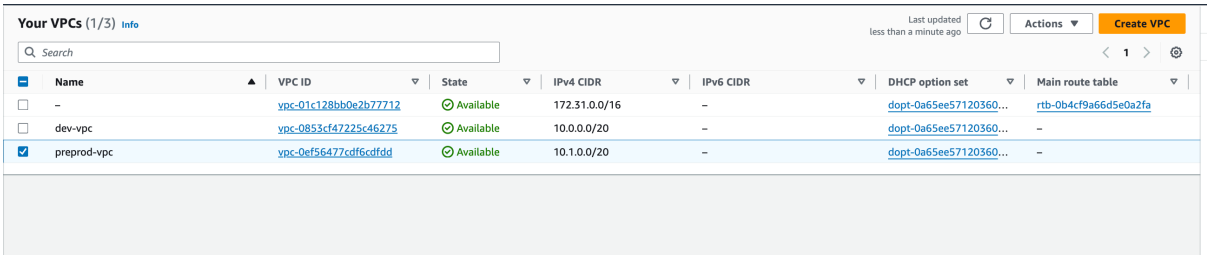


https://www.linkedin.com/in/mahendran-selvakumar-36444a77/

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

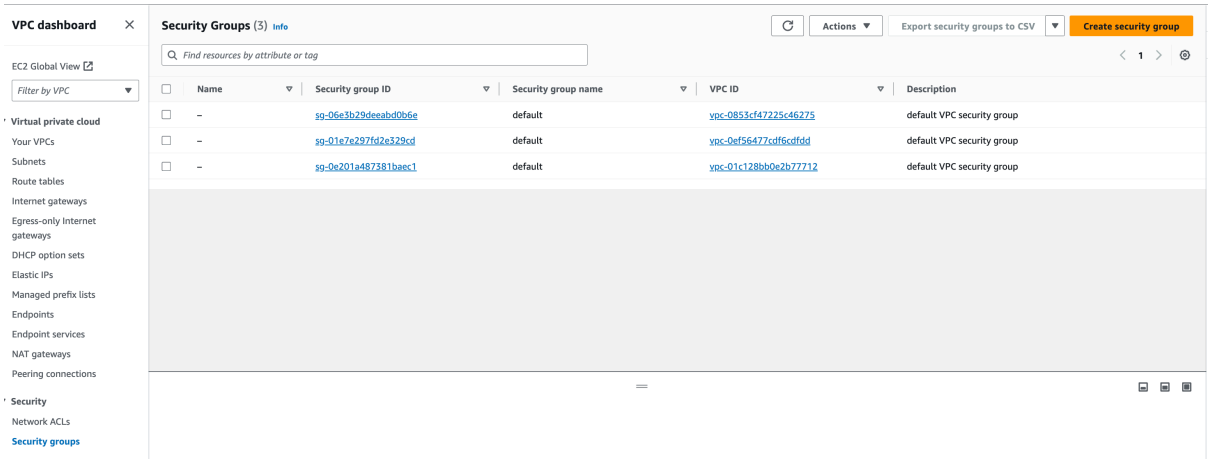


Another VPC has now been successfully created and is named **preprod-vpc**

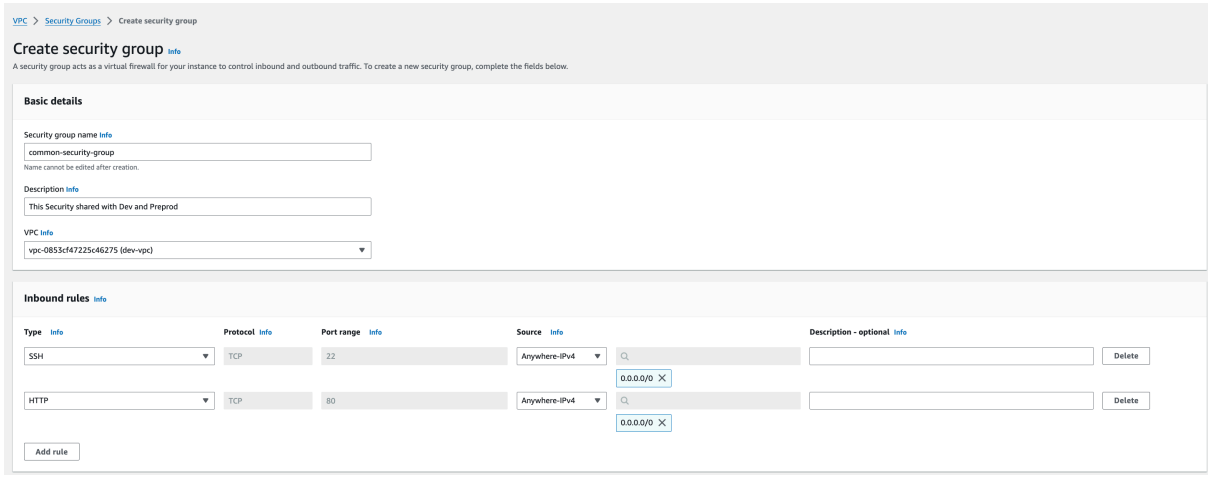


Associate a security group with another VPC

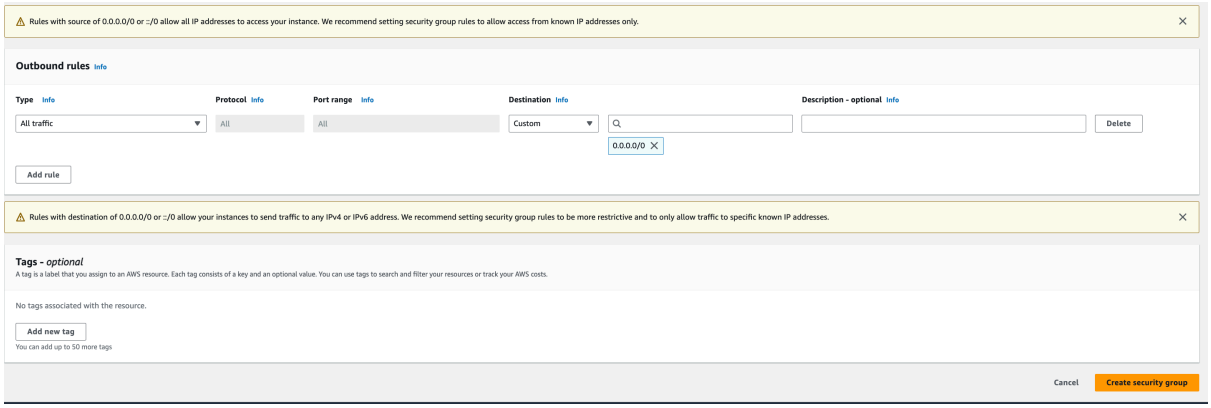
Navigate to **Security Groups** and click **Create Security Group**



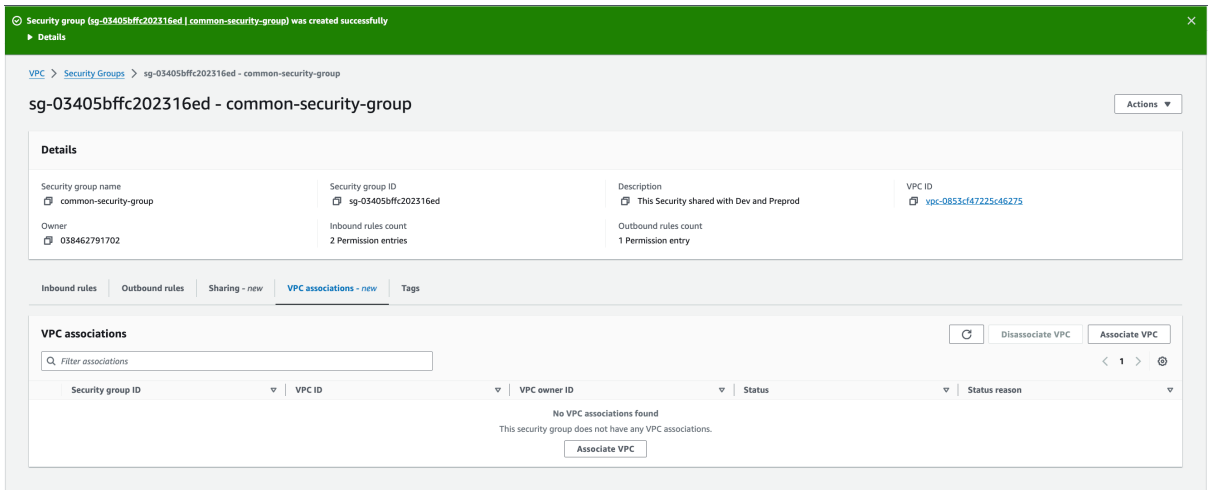
Provide the **Name**, **Description**, and select the **VPC**. Here, I have created inbound rules for **SSH** (port 22) and **HTTP** (port 80)



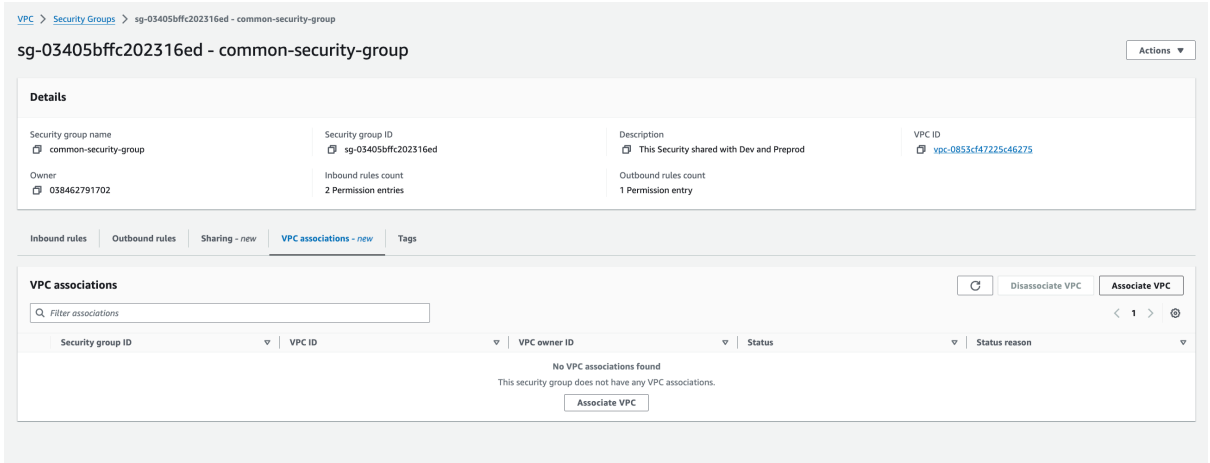
Click **Create Security Group** to finalize the creation of the security group



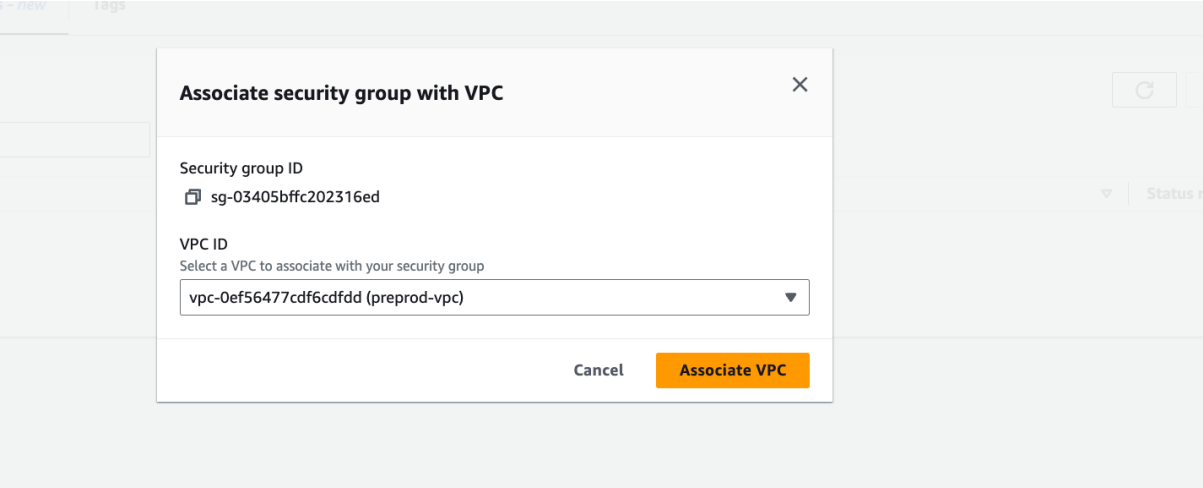
The security group has now been successfully created



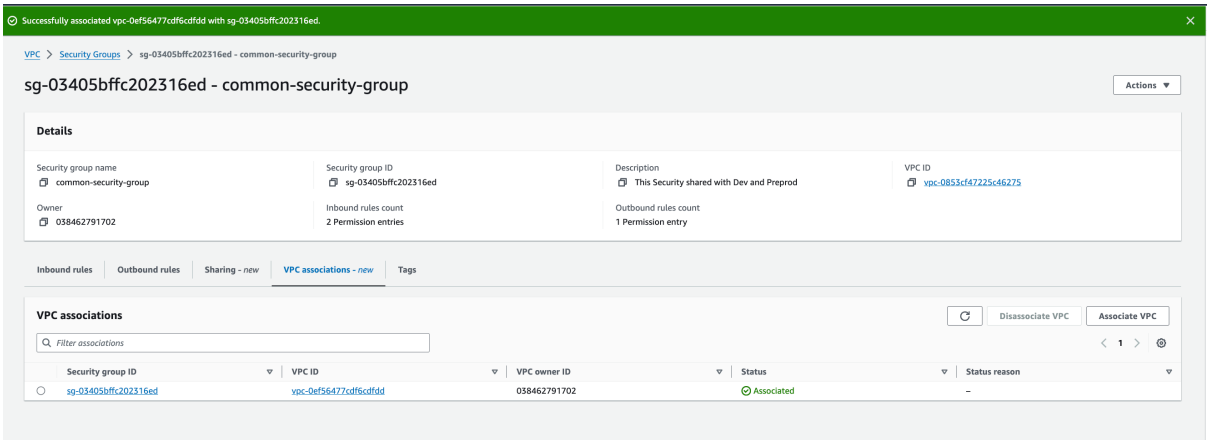
Navigate to the newly created security group and click **Associate VPC**



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



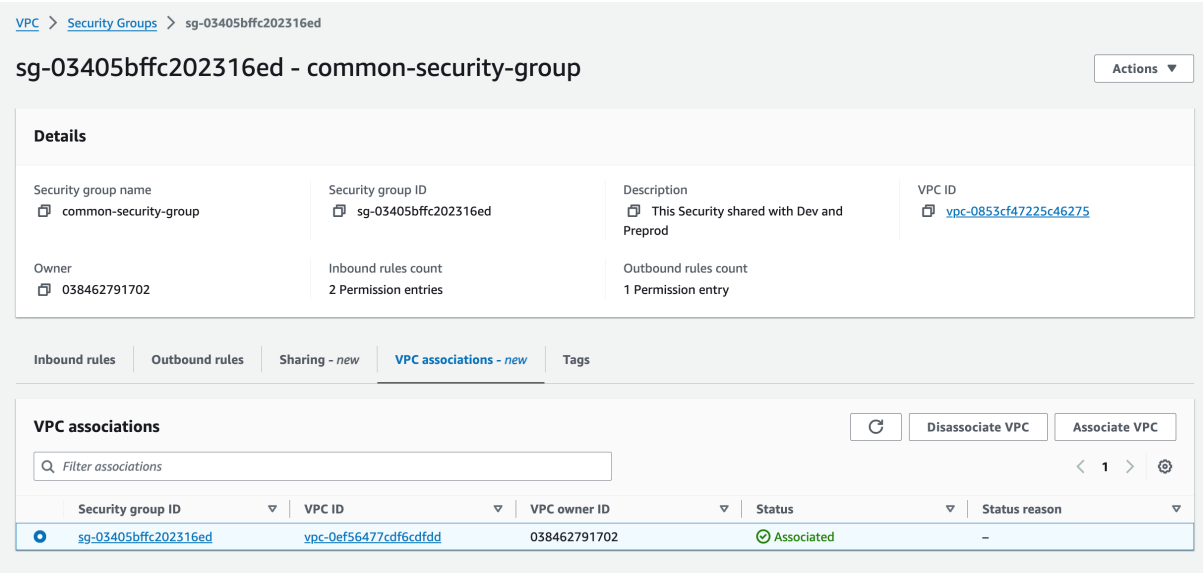
The security group is now successfully associated with another VPC



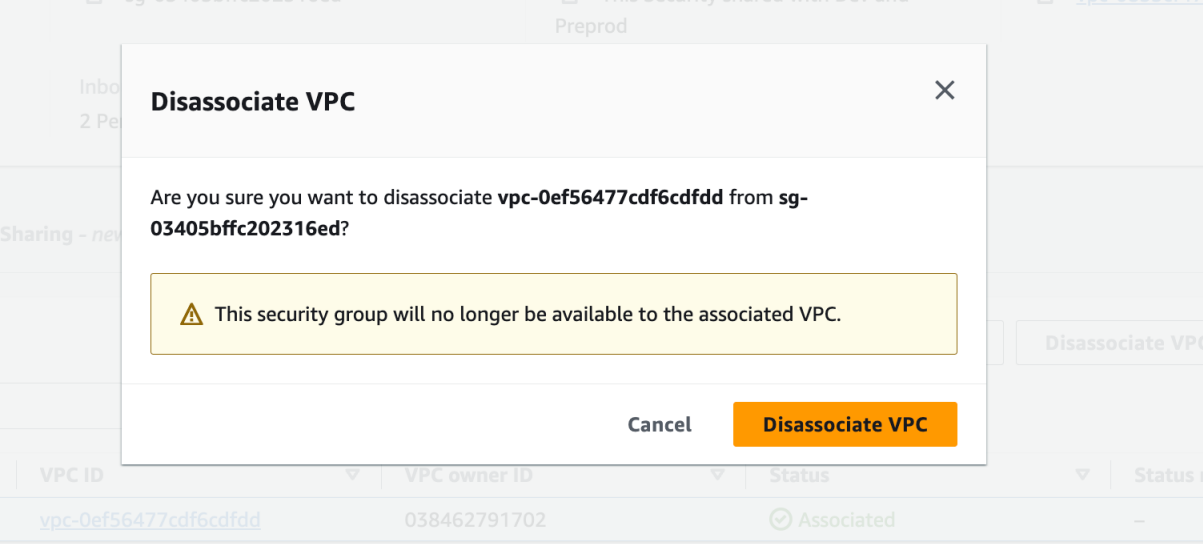
Now we can create an EC2 instance using the shared security group

Disassociate a security group from another VPC:

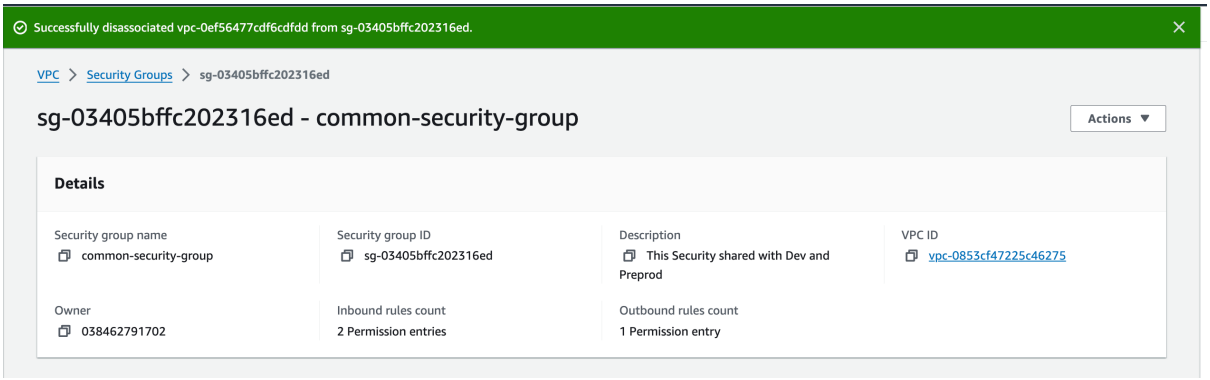
Select the security group, navigate to **VPC Associations**, choose the associated VPC, and then click **Disassociate VPC**



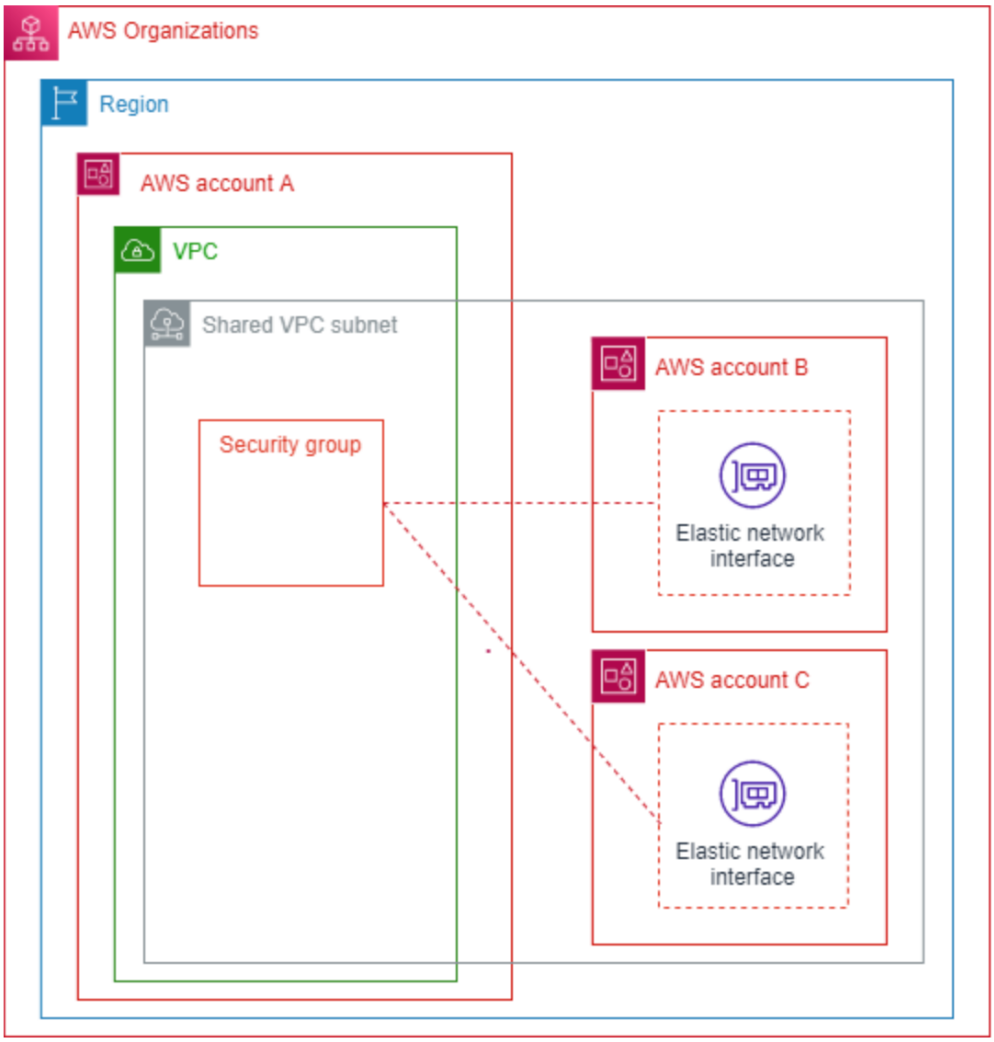
Click **Disassociate VPC**



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.

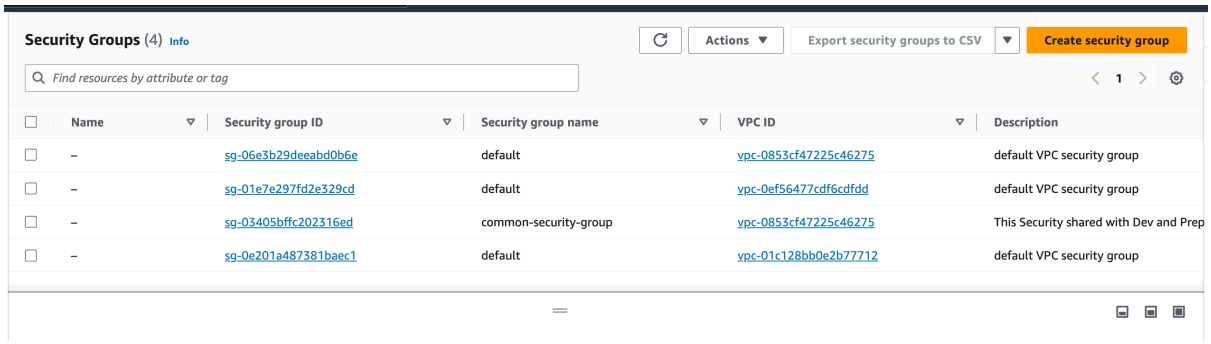
Supported Services for Shared Security Groups

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

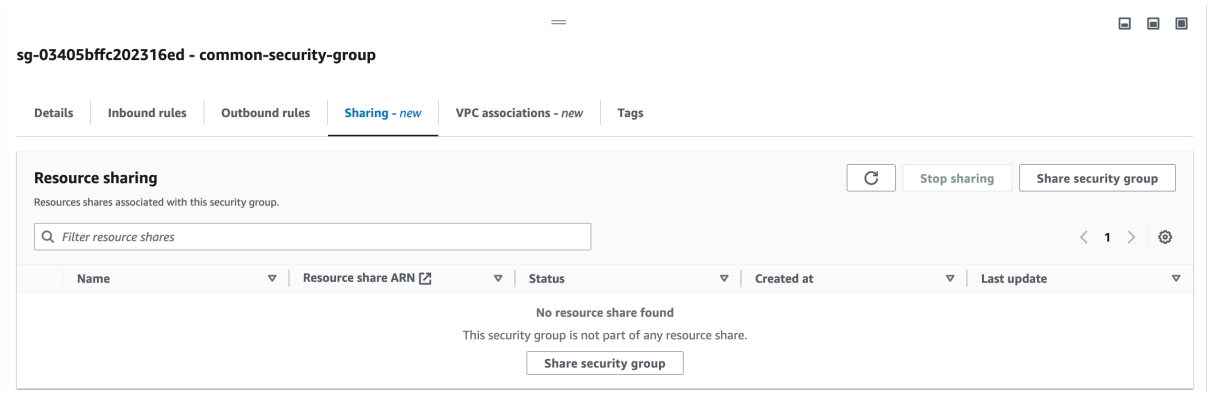
- Amazon API Gateway
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Amazon EMR
- Amazon FSx
- Amazon ElastiCache
- AWS Elastic Beanstalk
- AWS Glue
- Amazon MQ
- Amazon SageMaker

Share a security group with organization:

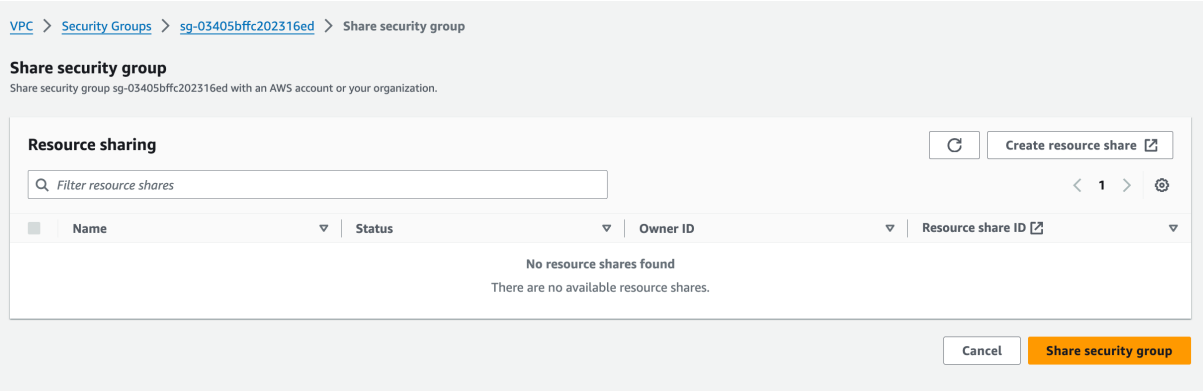
Select the security group that you want to share with your organizations



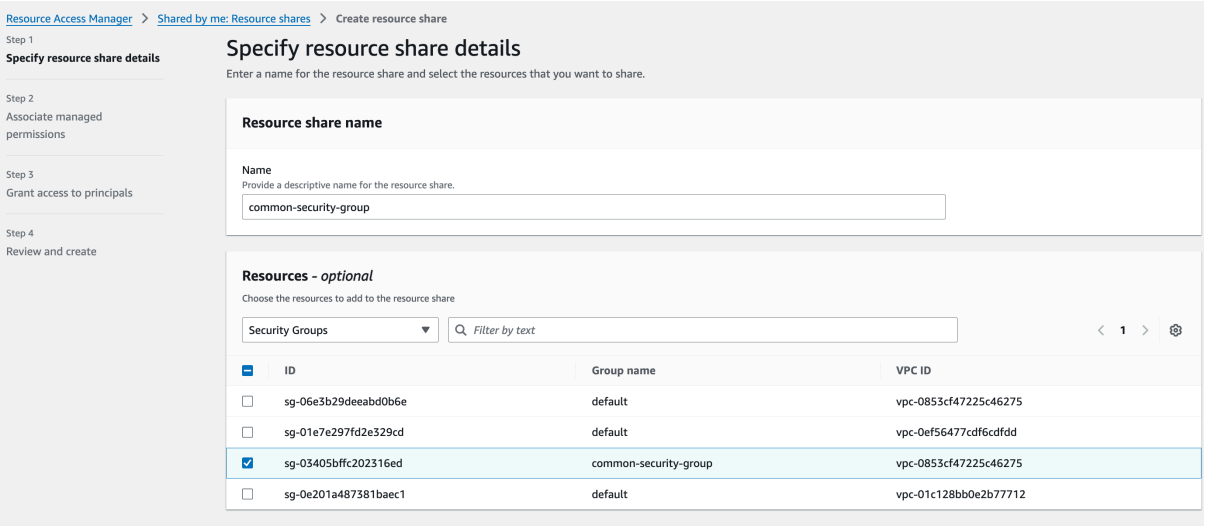
Navigate to the **Sharing** tab and click **Share Security Group**



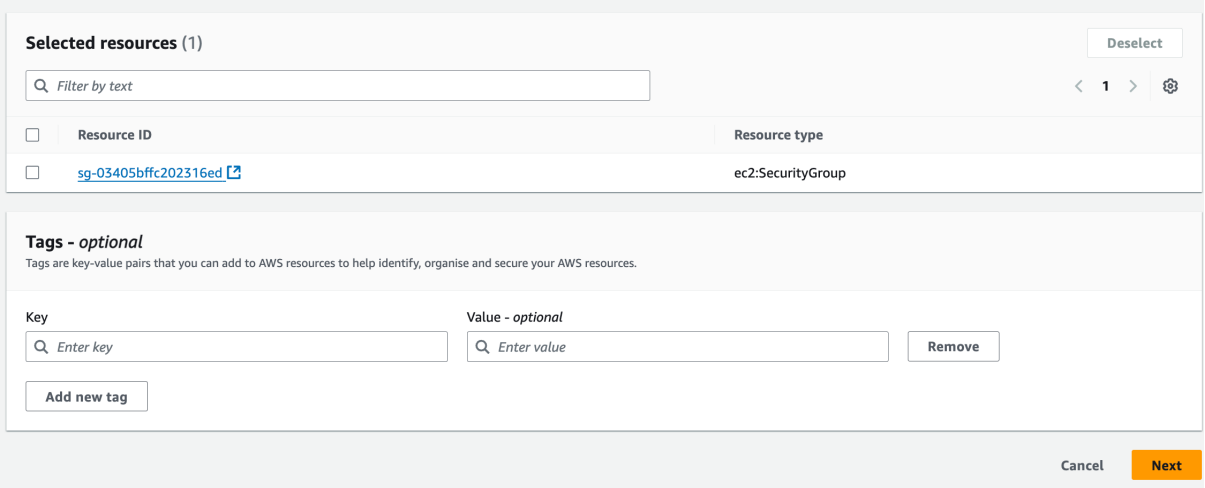
Click **Create Resource Share**



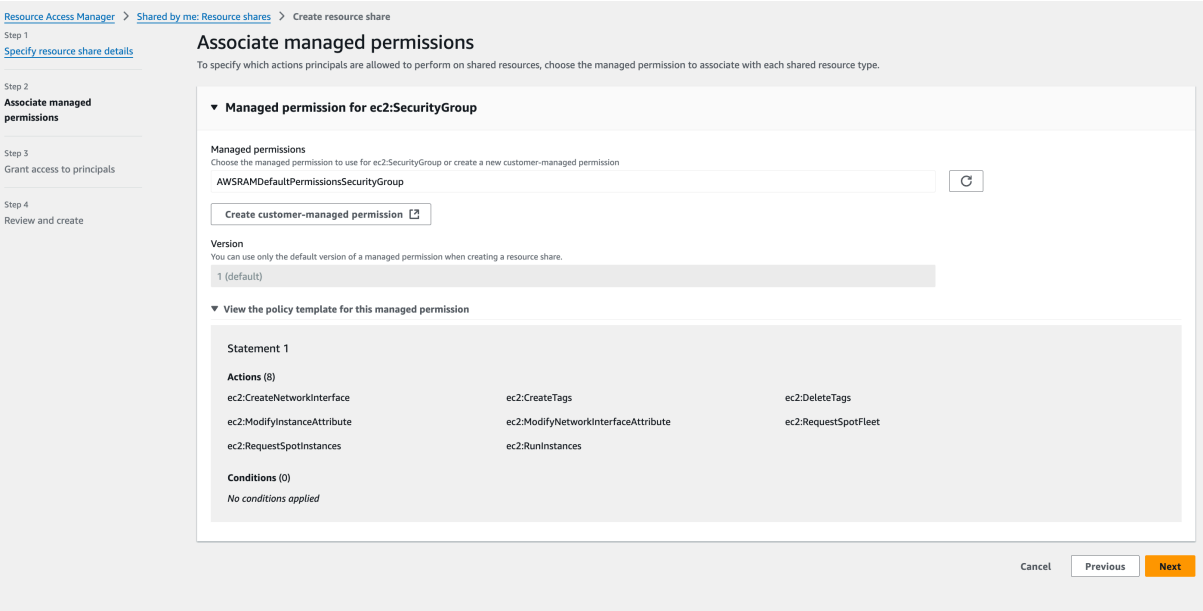
Provide a name for the resource share, choose **Security Group** as the resource type, and select the security group you wish to share with your organizations



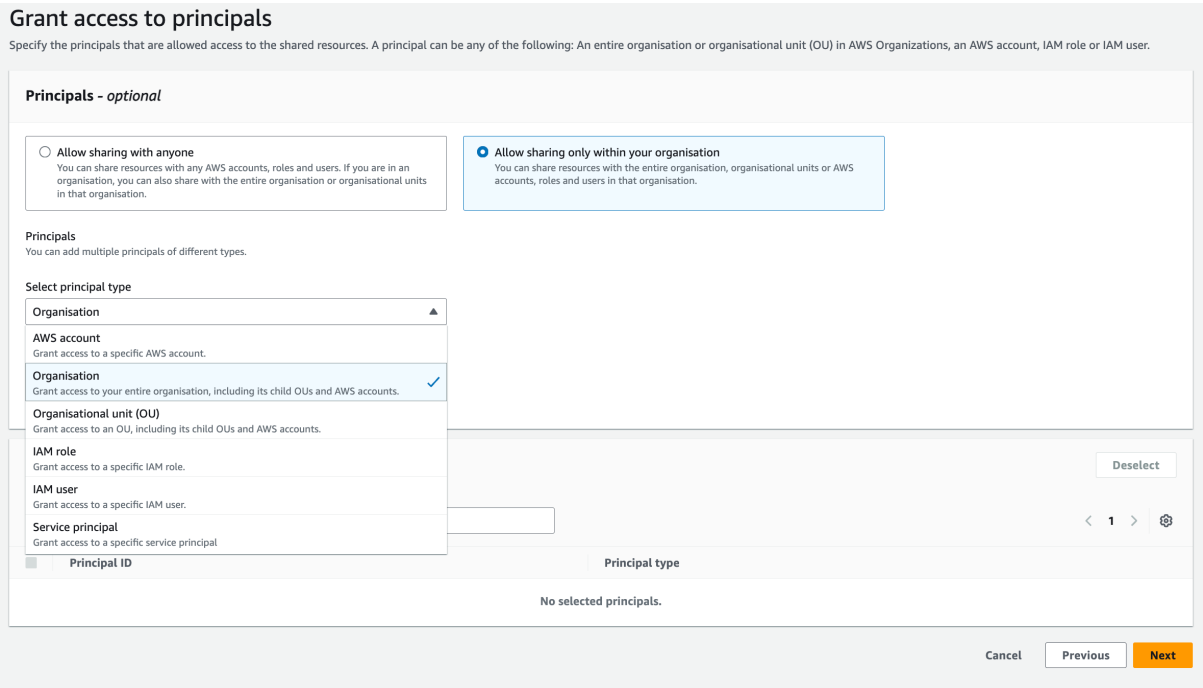
Click **Next** to associate managed permissions



Click **Next** to Grant access to principals



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



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

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

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/