How to Create Private Link Between Account

Contents

[1. Introduction 2](#_Toc182836233)

[2. Requirement 2](#_Toc182836234)

[**3.** **Account A** 3](#_Toc182836235)

[**3.1.** **Target Group – Account A** 3](#_Toc182836236)

[**3.2.** **NLB** 6](#_Toc182836237)

[**3.3.** **Endpoint Service – Account A** 9](#_Toc182836238)

[**3.3.1.** **Create endpoint service** 9](#_Toc182836239)

[**3.3.2.** **Allow Principle for endpoint service** 10](#_Toc182836240)

[**4.** **Account B** 11](#_Toc182836241)

[**4.1.** **Target Group** 11](#_Toc182836242)

[**4.2.** **NLB – Account B** 14](#_Toc182836243)

[**4.3.** **Endpoint Service – Account B** 17](#_Toc182836244)

[**4.3.1.** **Create endpoint service** 17](#_Toc182836245)

[**4.3.2.** **Allow Principle for endpoint service** 18](#_Toc182836246)

[**5.** **Create Endpoint** 19](#_Toc182836247)

[**5.1.** **How to get endpoint service name.** 19](#_Toc182836248)

[**5.2.** **Create Endpoint – Account-A** 19](#_Toc182836249)

[**5.3.** **Create Endpoint – Account-B** 21](#_Toc182836250)

[**6.** **Accept the Endpoint Request** 23](#_Toc182836251)

[**6.1.** **Accept Request – Account-A** 23](#_Toc182836252)

[**6.2.** **Accept Request – Account-B** 24](#_Toc182836253)

[**7.** **Update the Security Group of EC2** 24](#_Toc182836254)

[**8.** **How to Connect to Cross Account EC2.** 24](#_Toc182836255)

# Introduction

* AWS Private link provides private connectivity between VPCs, AWS services, and your on-premises networks without exposing your traffic to the public internet.
* In this account Private Link use for private connectivity between EC2 instances across 2 different accounts.
* Diagram

  Description automatically generated

# Requirement

* We need to create Private Link between AWS Account A to AWS Account B for following instances.

1. Instance Name = hbl-aws-aps1-lentra-nonpcidss-prod-archive\_2-db-ec2-01

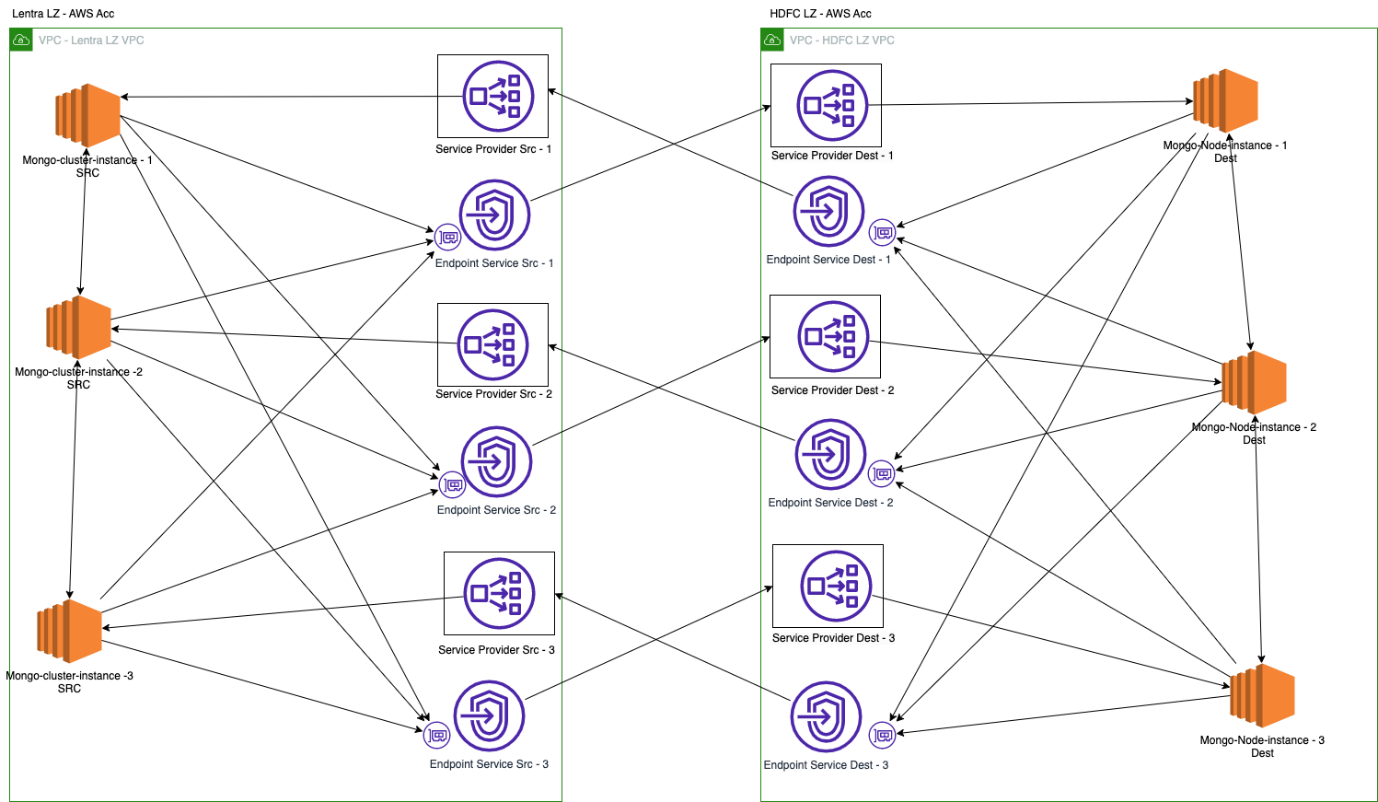
Instance id = i-09d1d25e01b3f99cb

Instance IP = 10.196.139.94

Availability zone =  ap-south-1b

Subnet ID = subnet-0a955270c51f28413

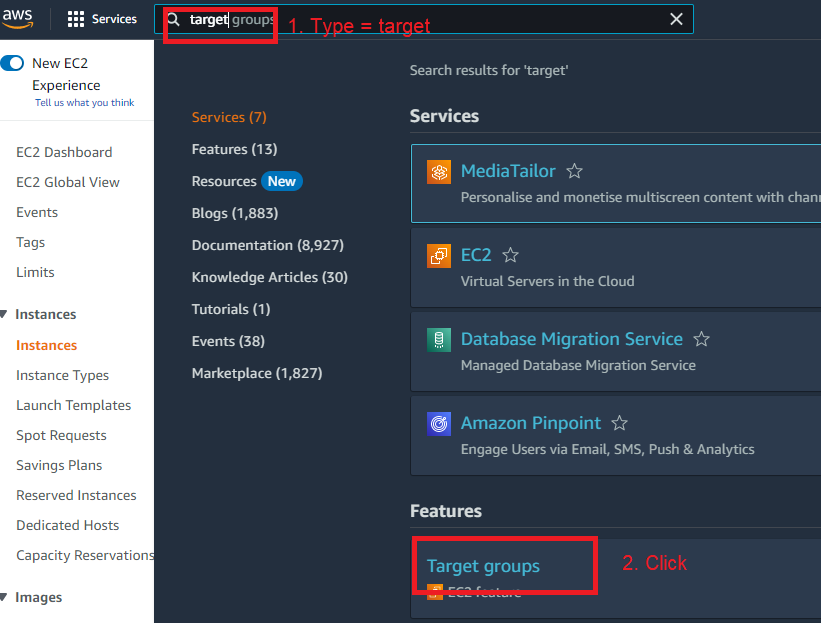
Availability Zone ID = aps1-az3 (From Subnet)



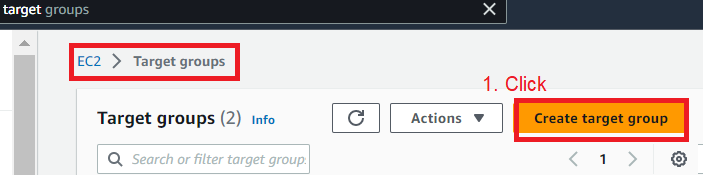
# **Account A**

## **Target Group – Account A**

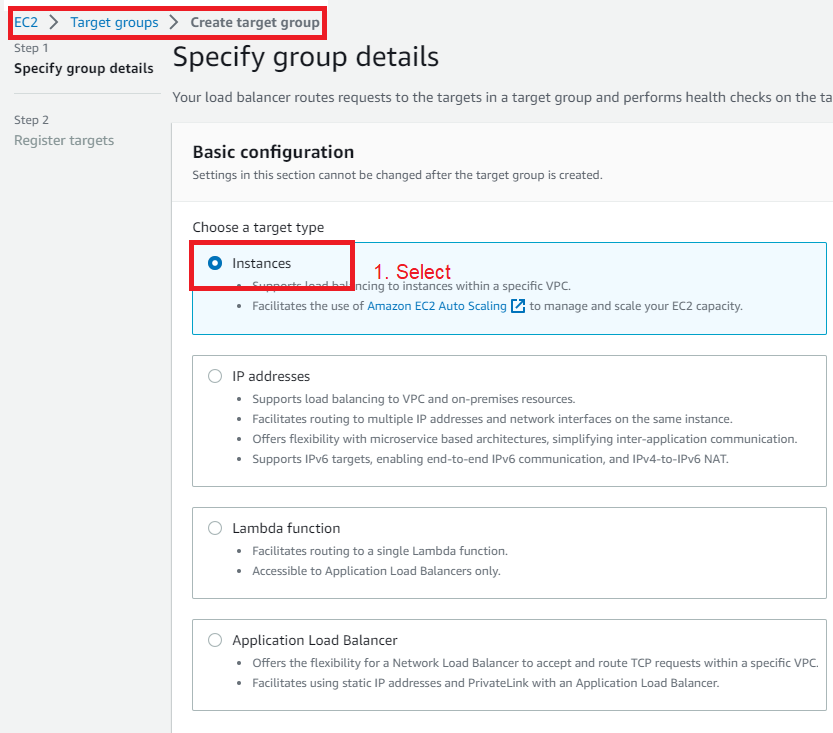
* We need to **create target group** for above instances.
* Type = **target** in search bar 🡪 Click on **Target Group**

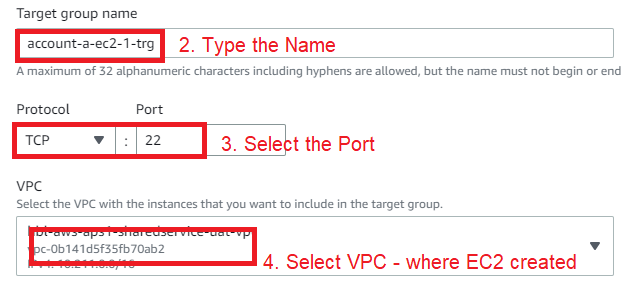


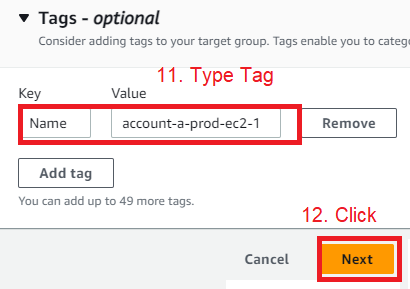
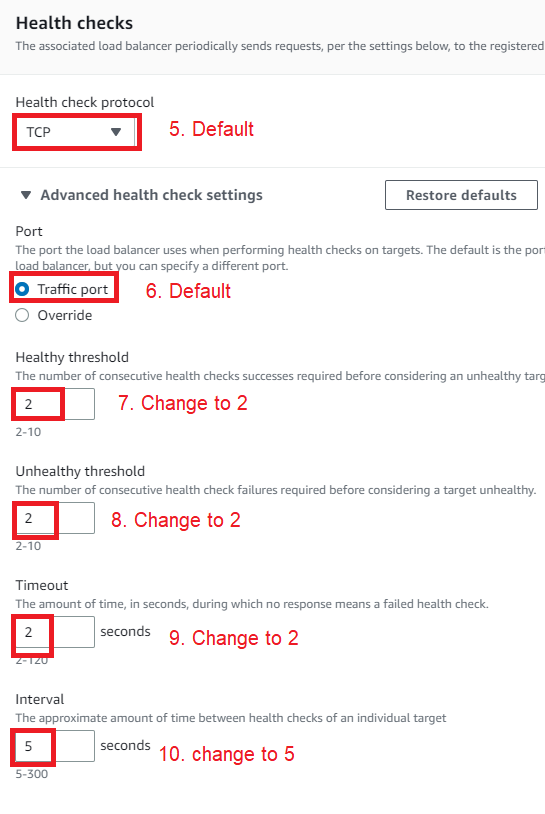
* Click on **Create target group**



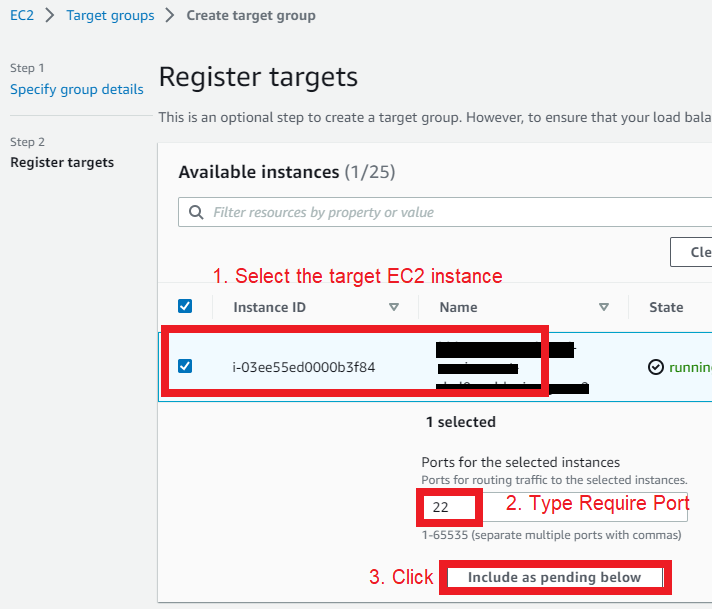
* Select the following



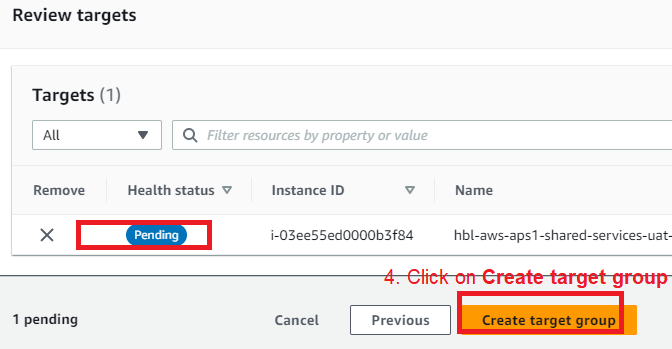




Select the Target **EC2** 🡪 Type the Require **Port** 🡪 Click on **Include as pending below**



Review the target group 🡪 Click on **Create target group**



## **NLB**

* We need to **create 5 Network Load Balancer** for above instances.
* Type = **load** in Search bar 🡪 Click on **Load Balansers**

Graphical user interface, text, application, chat or text message

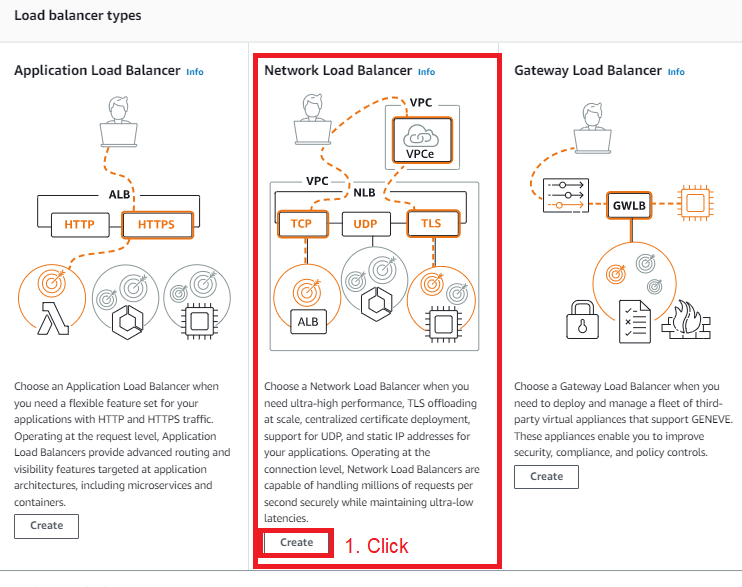
Description automatically generated

* Click on **Create load Balancers**

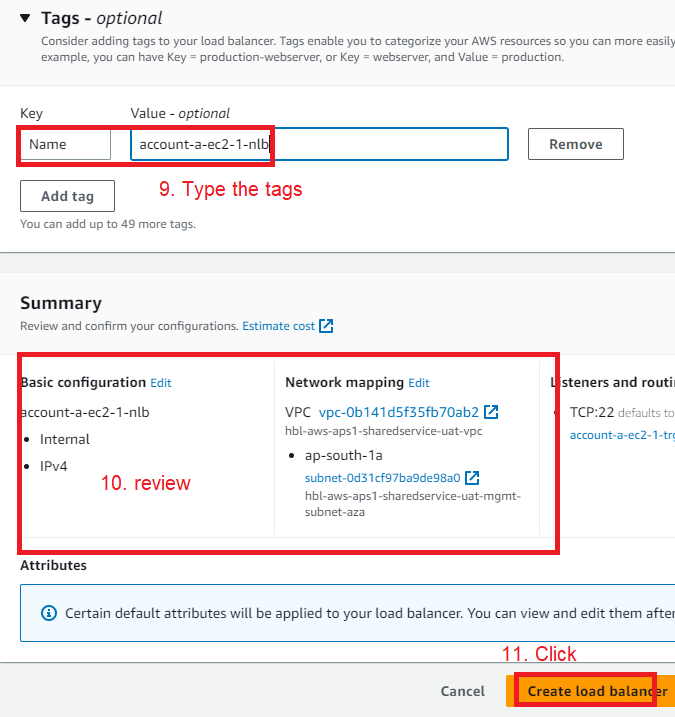
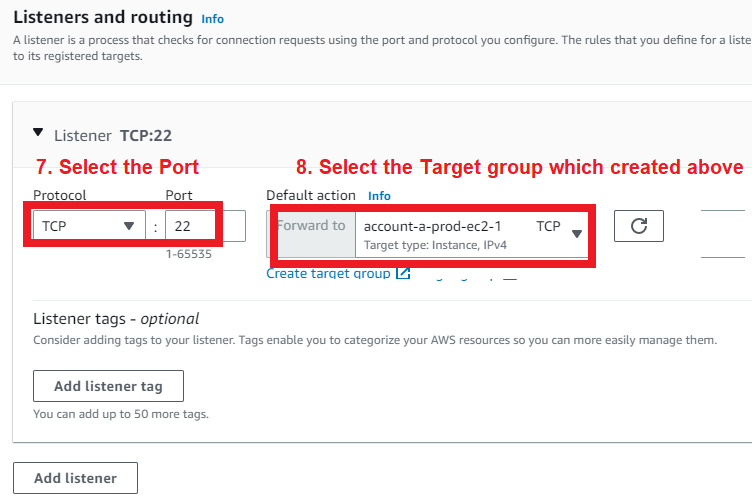
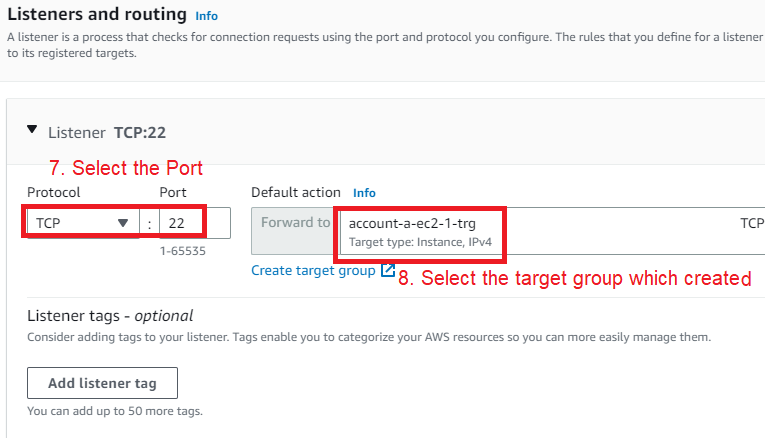
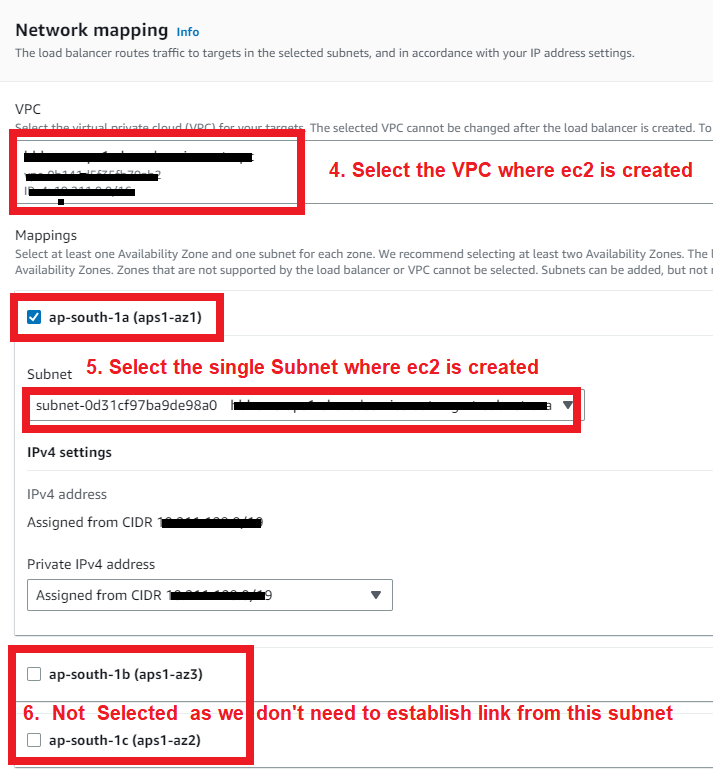
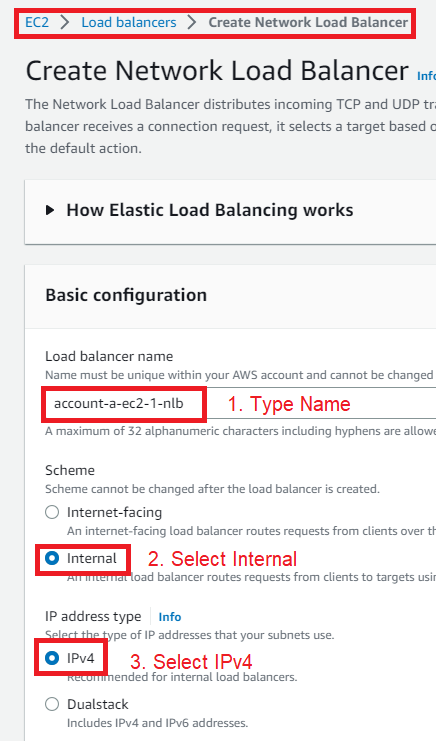
Graphical user interface, application

Description automatically generated

* Click on NLB



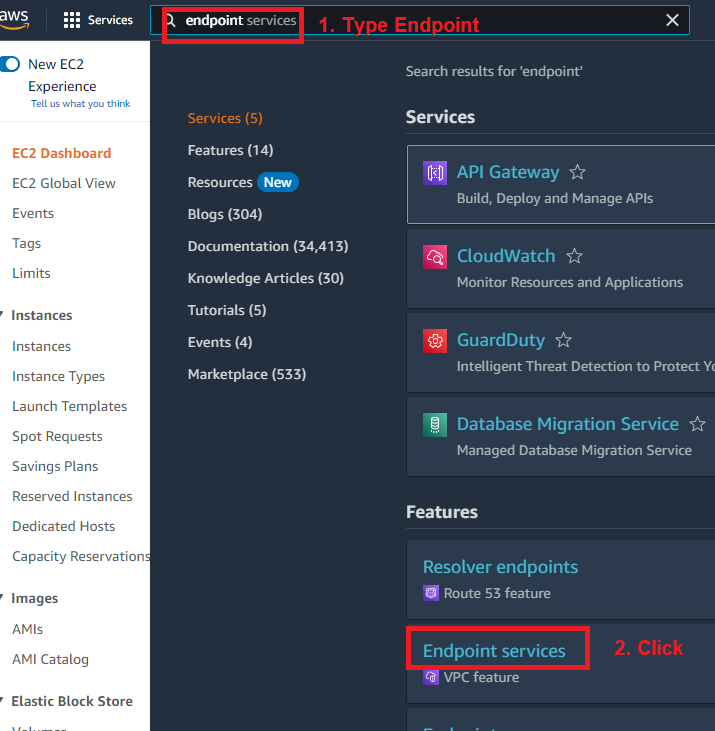
* Select the Following



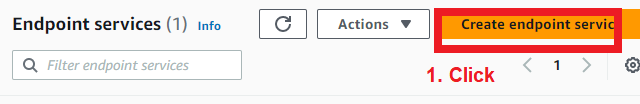
## **Endpoint Service – Account A**

### **Create endpoint service**

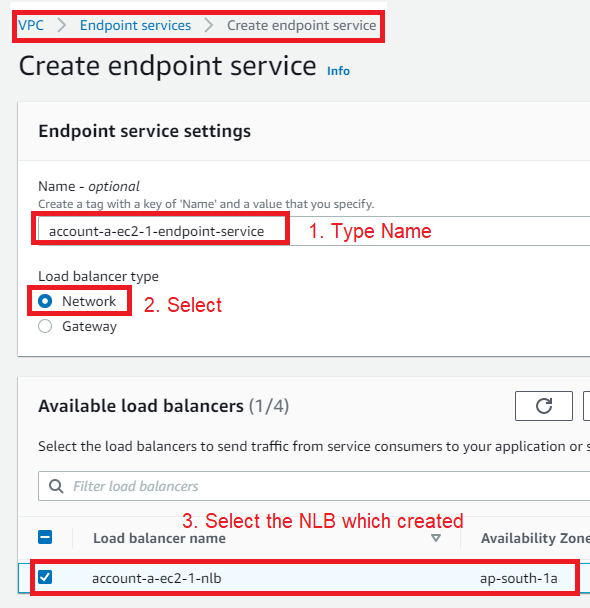
* We need to **endpoint Service** for endpoint traffic.
* Type = **endpoint** in search bar 🡪 Click **Endpoint Service**

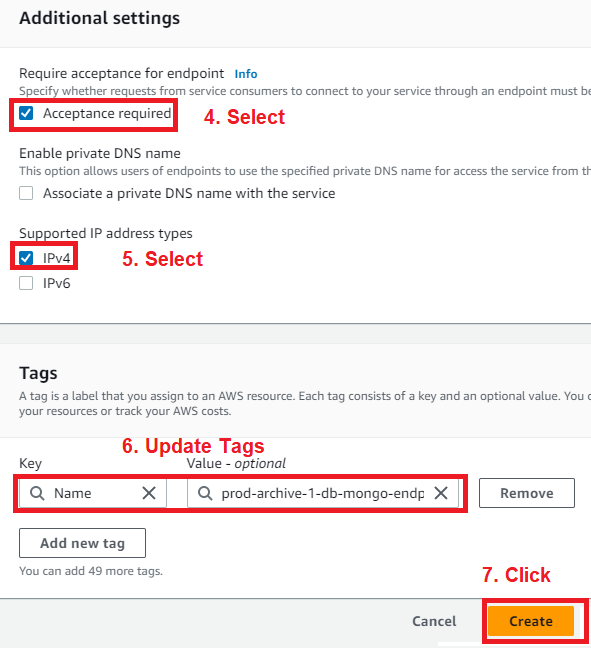


* Click on Create endpoint services.



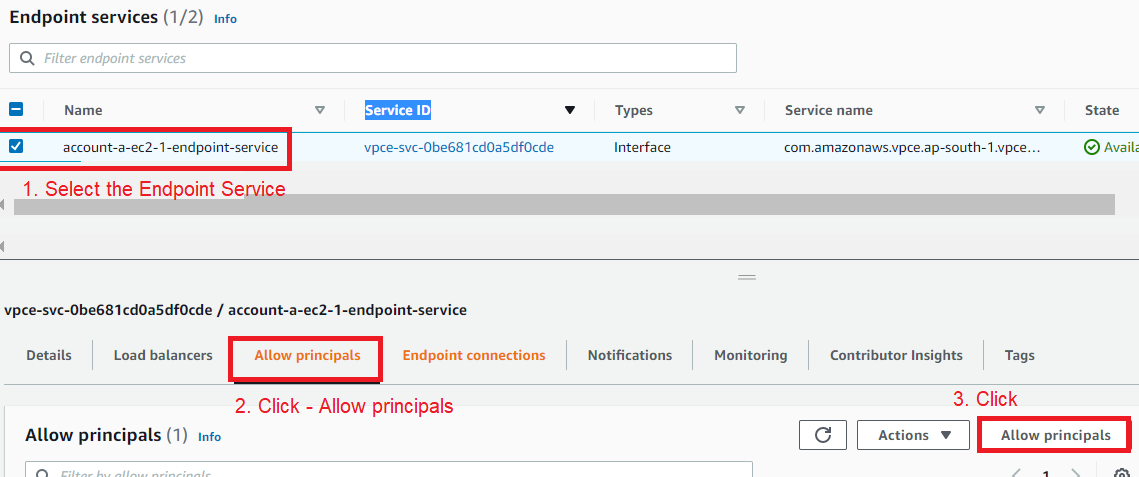
* Select the Following



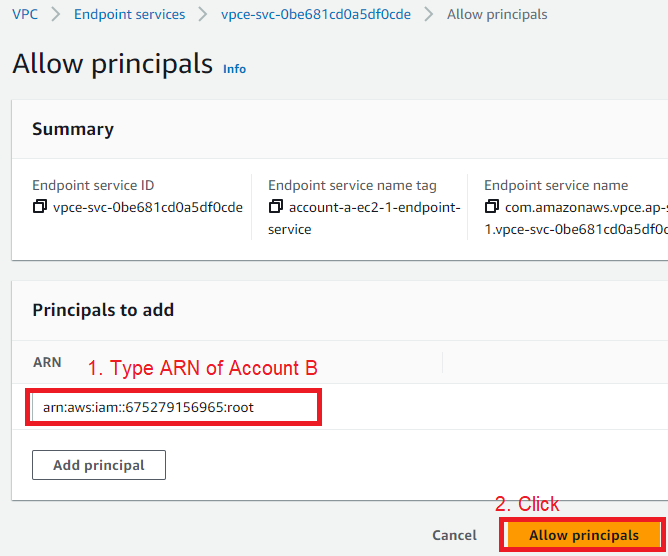


### **Allow Principle for endpoint service**

* Select the Created **Endpoint Service** 🡪 Click on **Allow principals** 🡪 Click **Allow principals**



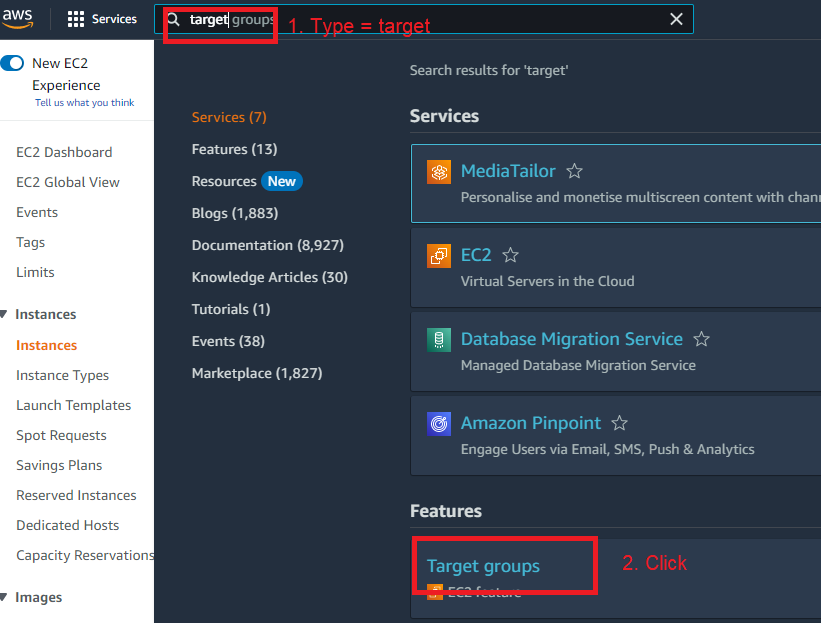
* Type the **ARN of Account B** 🡪 Click **Allow principals**



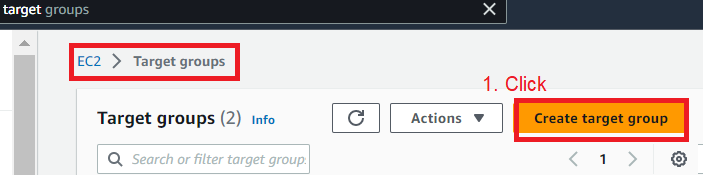
# **Account B**

## **Target Group**

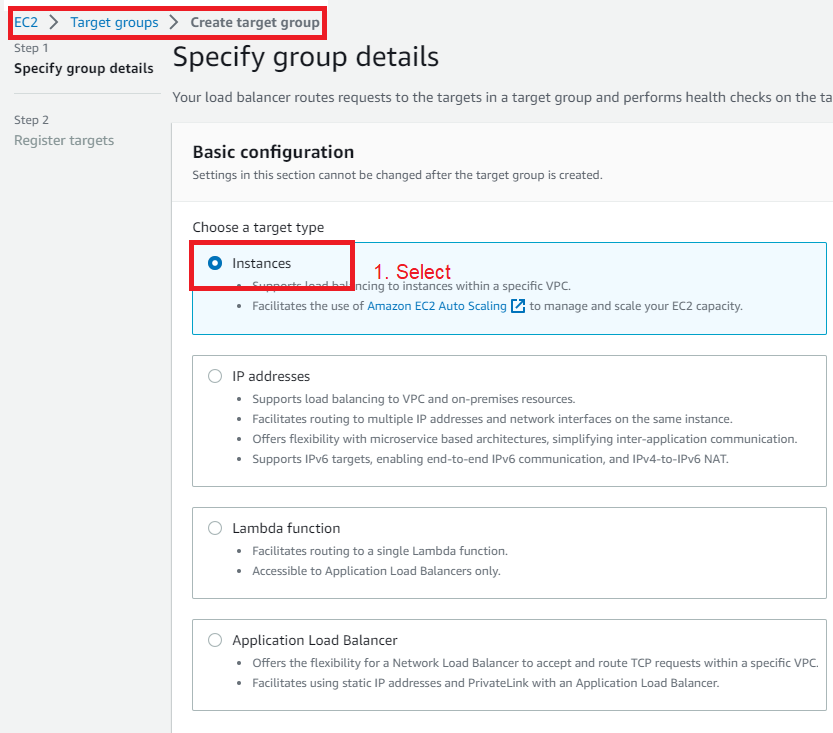
* We need to **create target group** for above instances.
* Type = **target** in search bar 🡪 Click on **Target Group**

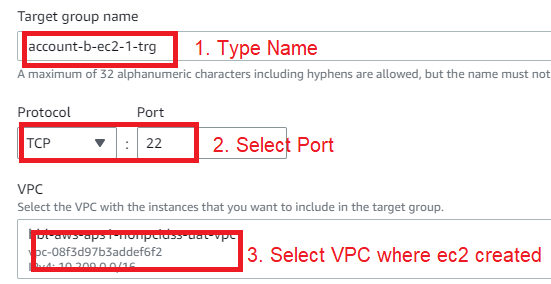


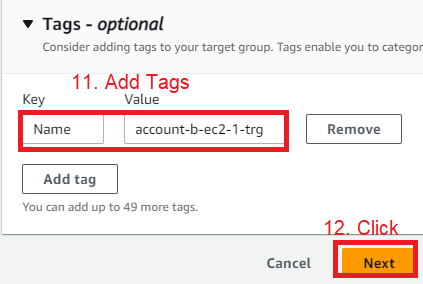
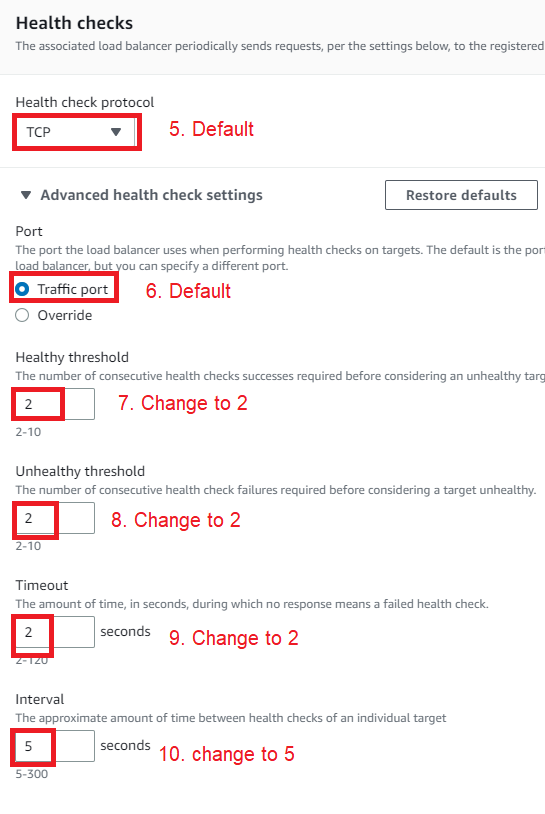
* Click on **Create target group**



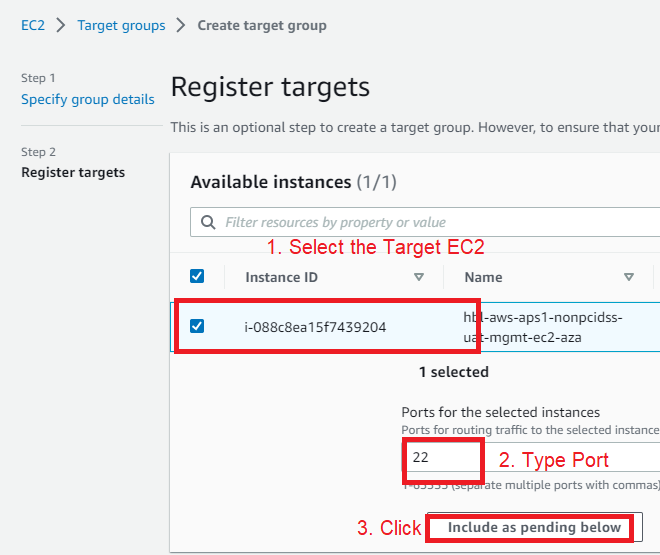
* Select the following



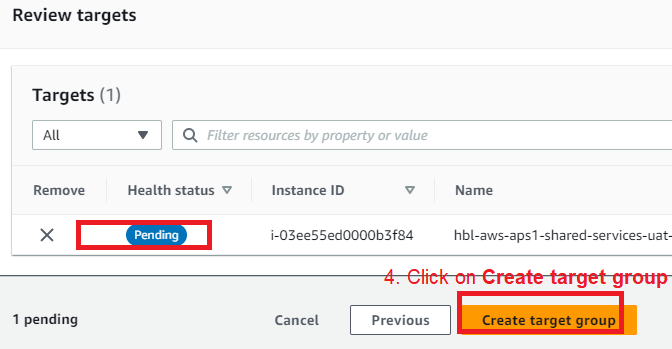




Select the Target **EC2** 🡪 Type the Require **Port** 🡪 Click on **Include as pending below**



Review the target group 🡪 Click on **Create target group**



## **NLB – Account B**

* We need to **create 5 Network Load Balancer** for above instances.
* Type = **load** in Search bar 🡪 Click on **Load Balansers**

Graphical user interface, text, application, chat or text message

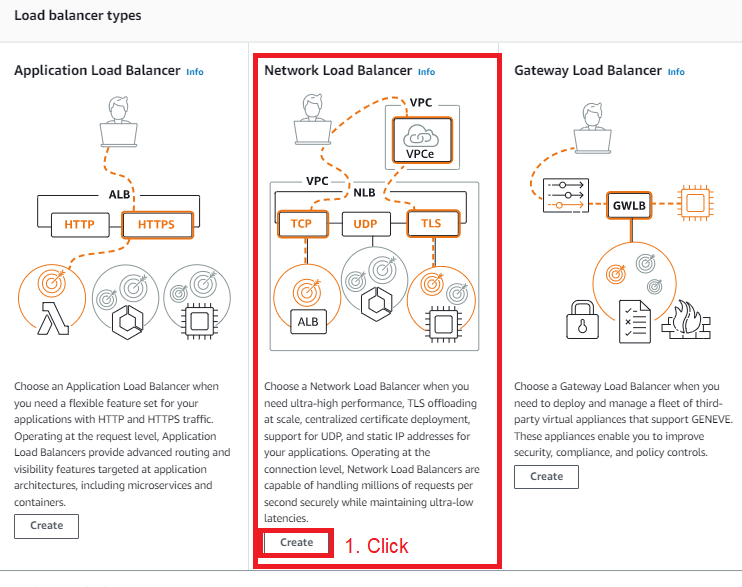
Description automatically generated

* Click on **Create load Balancers**

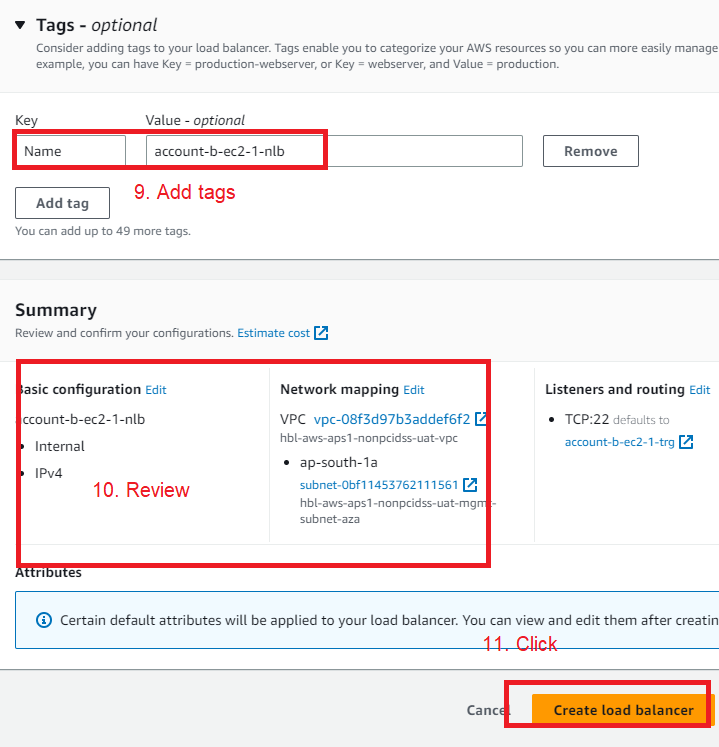
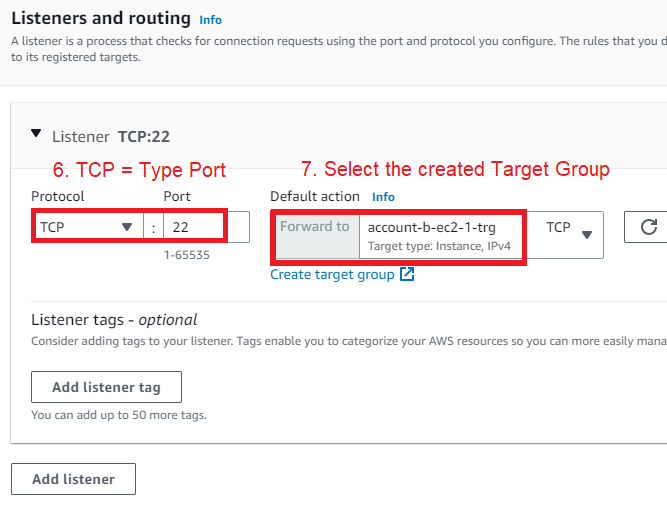
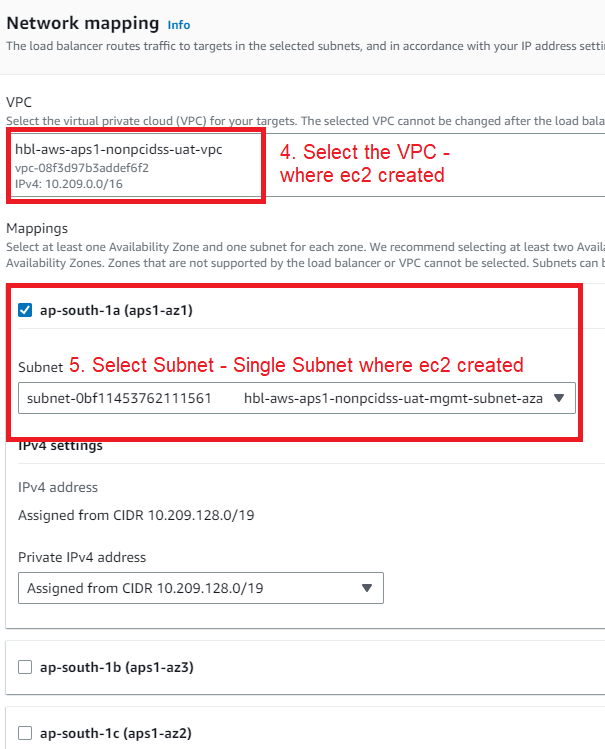
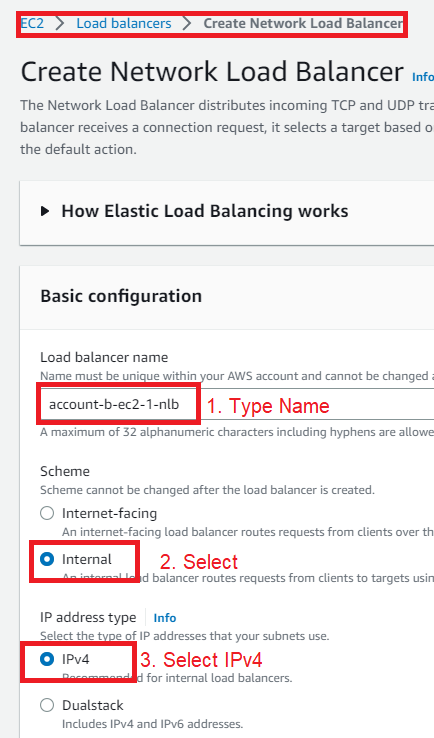
Graphical user interface, application

Description automatically generated

* Click on NLB



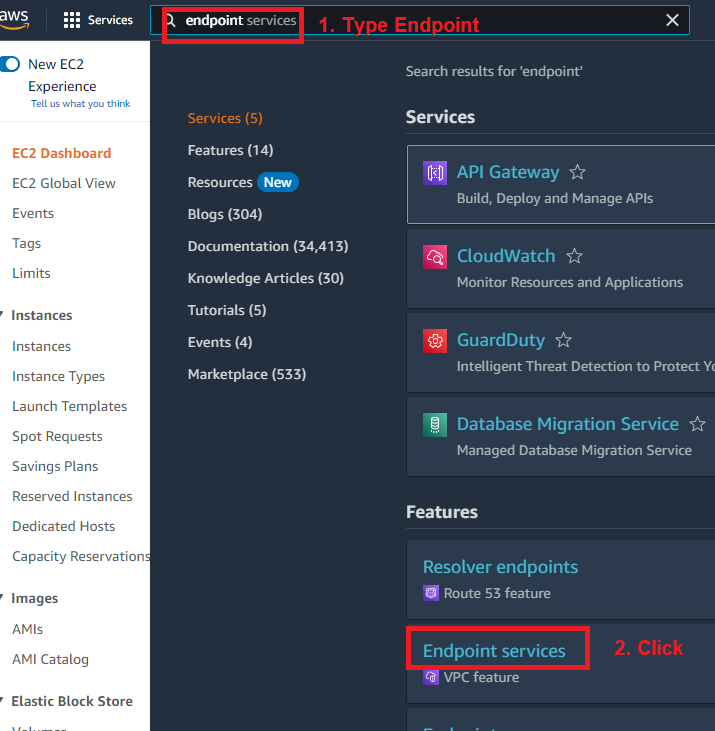
* Select the Following



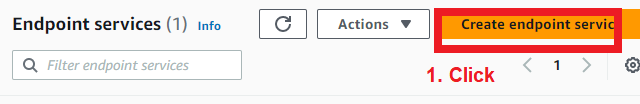
## **Endpoint Service – Account B**

### **Create endpoint service**

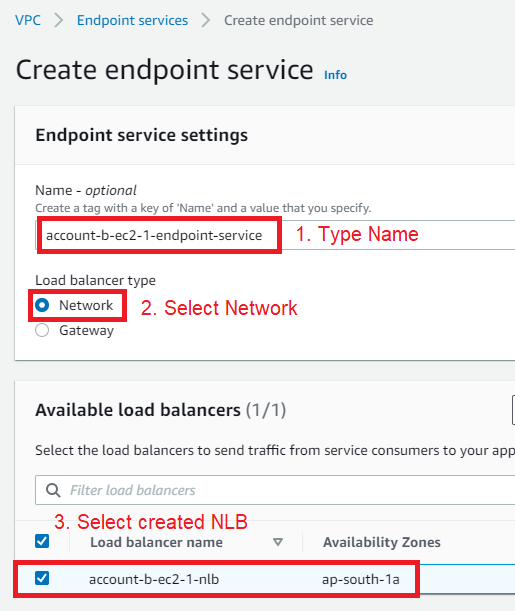
* We need to **endpoint Service** for above instances.
* Type = **endpoint** in search bar 🡪 Click **Endpoint Service**

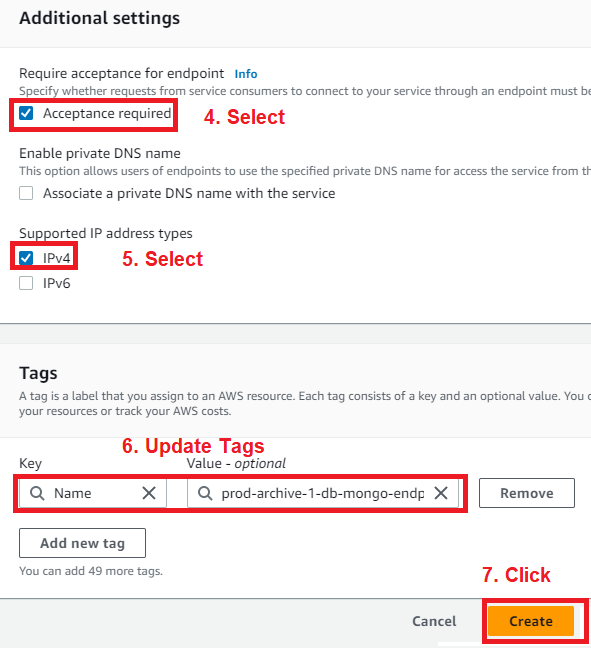


* Click on Create endpoint services.



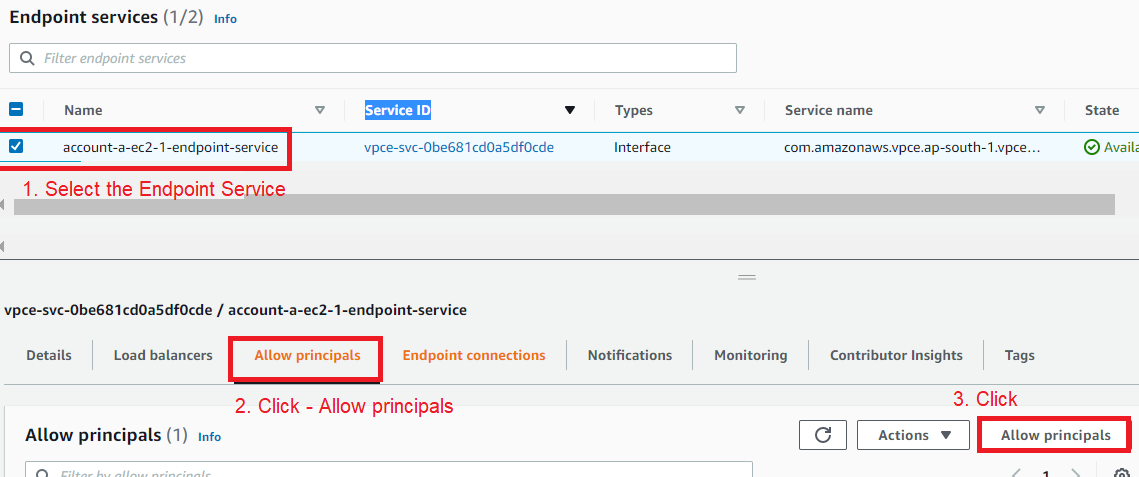
* Select the Following



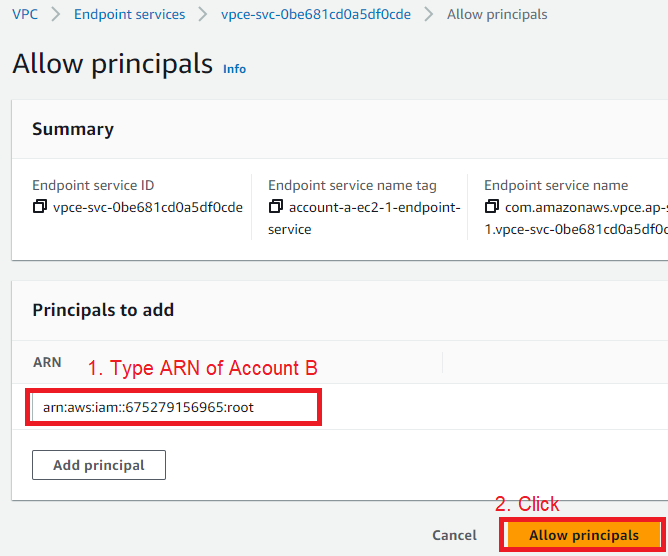


### **Allow Principle for endpoint service**

* Select the Created **Endpoint Servive** 🡪 Click on **Allow principals** 🡪 Click **Allow principals**



* Type the **ARN of Account B** 🡪 Click **Allow principals**

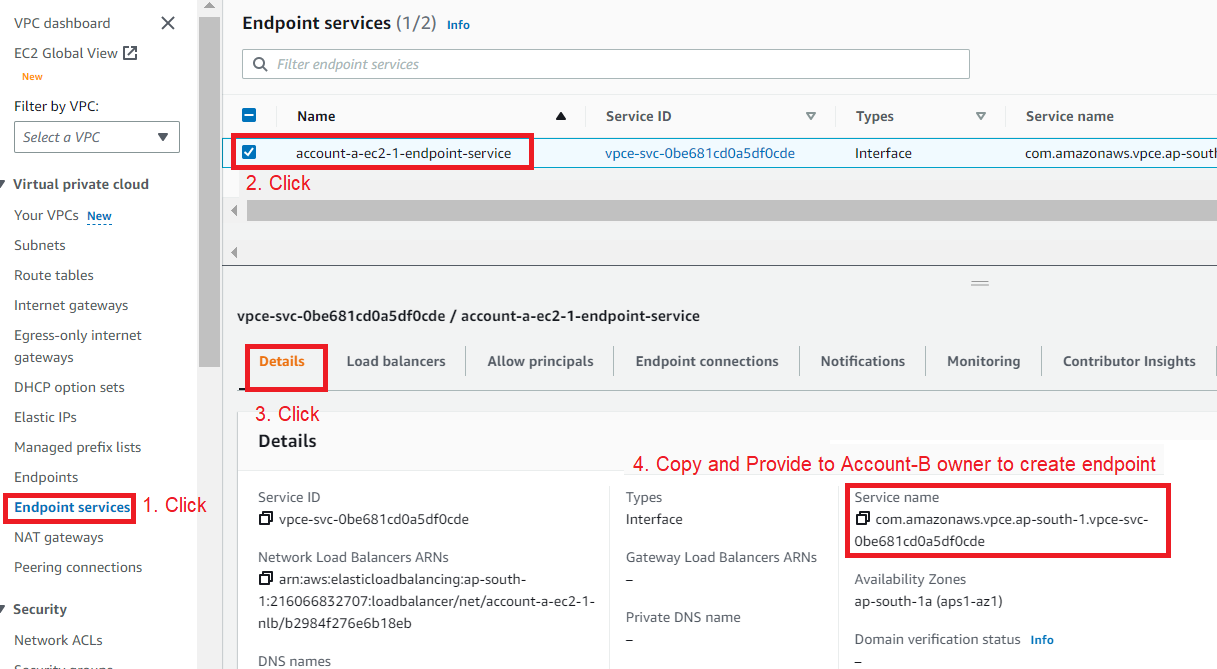


# **Create Endpoint**

* **Endpoint Service Name** of cross Account is required to create endpoint

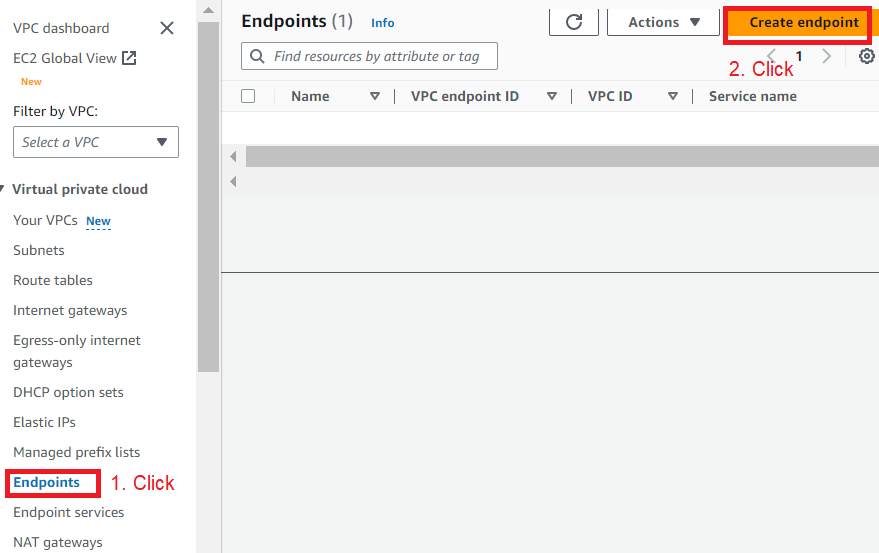
## **How to get endpoint service name.**

* Open **VPC Dashboard** 🡪 Click on **Endpoint Service** 🡪 Select the Created Endpoint Service 🡪 Copy and Provide the **Service Name** to Cross Account Owner

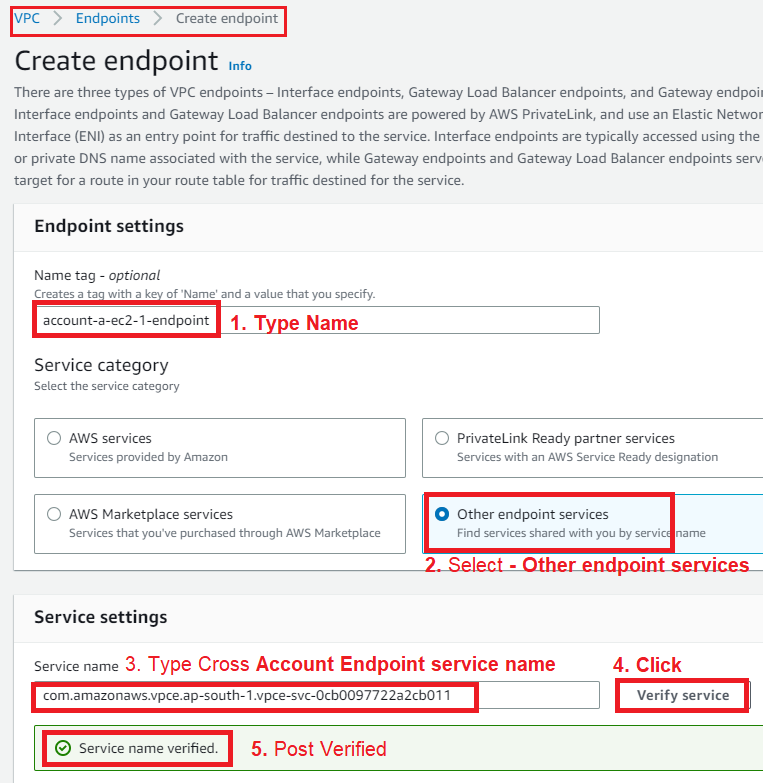


## **Create Endpoint – Account-A**

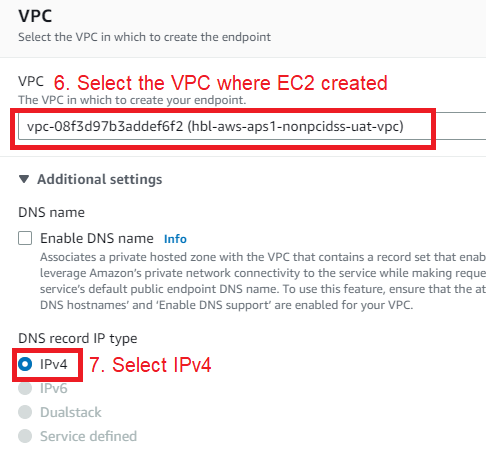
* **Endpoint Service Name** of **Account B** = com.amazonaws.vpce.ap-south-1.vpce-svc-0cb0097722a2cb011
* Open **VPC Dashboard** 🡪 Click on **Endpoint** 🡪 Click **Create endpoint**



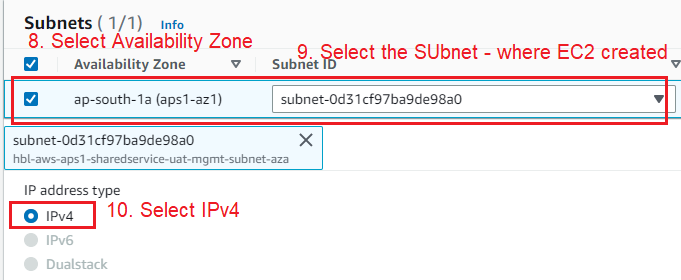
* Type **Name** 🡪 Select **Other endpoint services** 🡪 Type the **Other Account endpoint service name** in service name 🡪 Click **Verify**



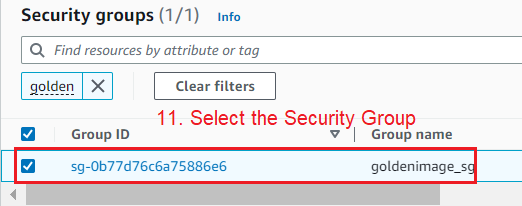
* Select the VPC 🡪 Select IPv4



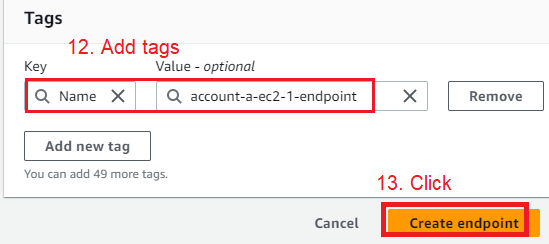
* Select the **Availability Zone** in Subnet Section 🡪 Select the **Subnet ID** (Where EC2 created)



* Select the Security Group

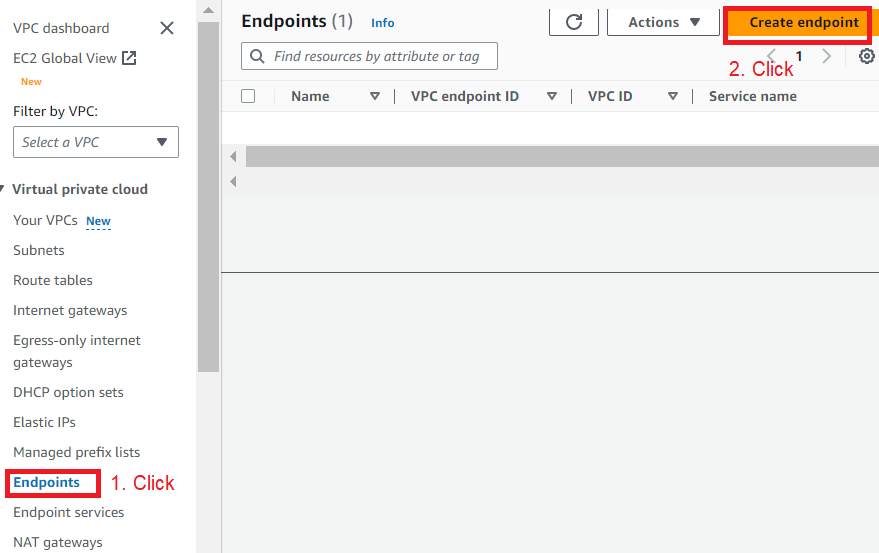


* Add Tags 🡪 Click **Create endpoint**

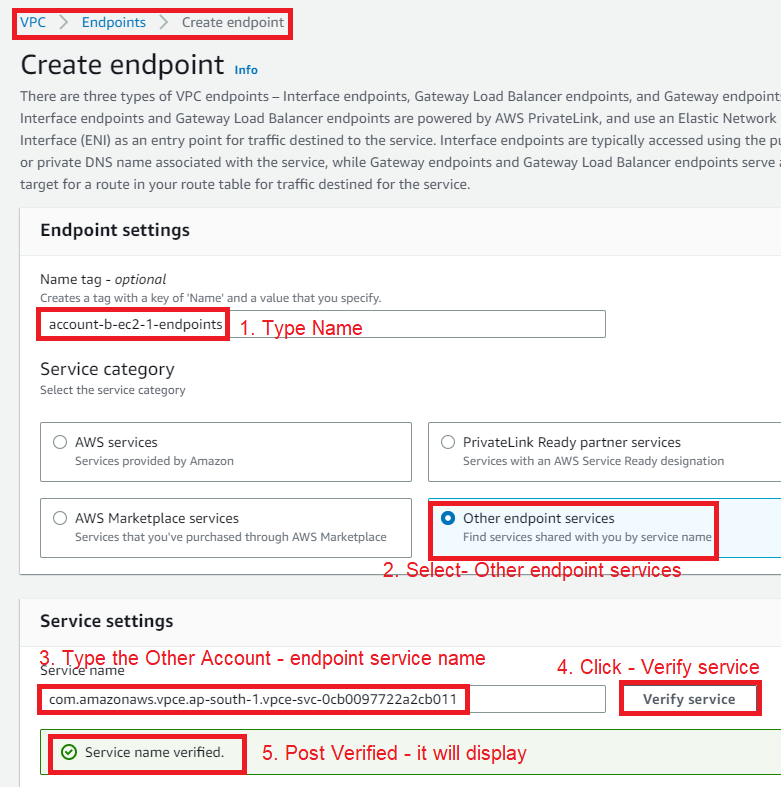


## **Create Endpoint – Account-B**

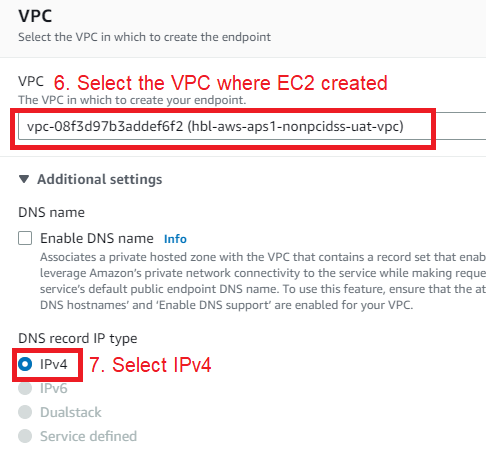
* Endpoint Service Name of Account A = com.amazonaws.vpce.ap-south-1.vpce-svc-0be681cd0a5df0cde
* Open **VPC Dashboard** 🡪 Click on **Endpoint** 🡪 Click **Create endpoint**



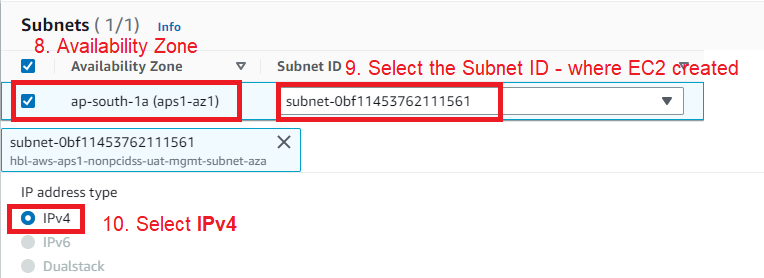
* Type **Name** 🡪 Select **Other endpoint services** 🡪 Type the **Other Account endpoint service name** in service name 🡪 Click **Verify**



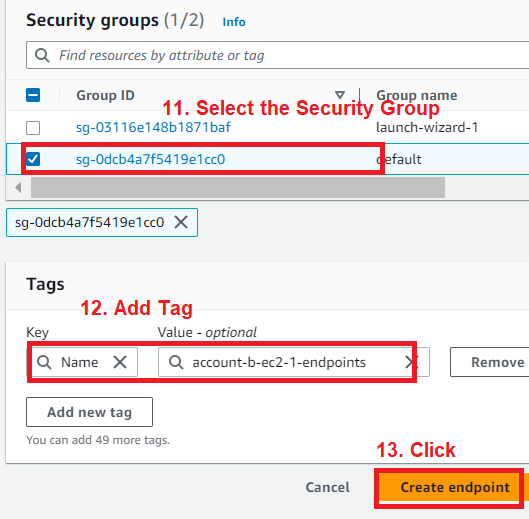
* Select the **VPC** (where EC2 created) 🡪 Select **IPv4**



* Select the Availability Zone in Subnet Section 🡪 Select the Subnet ID (Where EC2 created)



* Select the **Security Group** 🡪 Add Tag 🡪 Click **create endpoint**

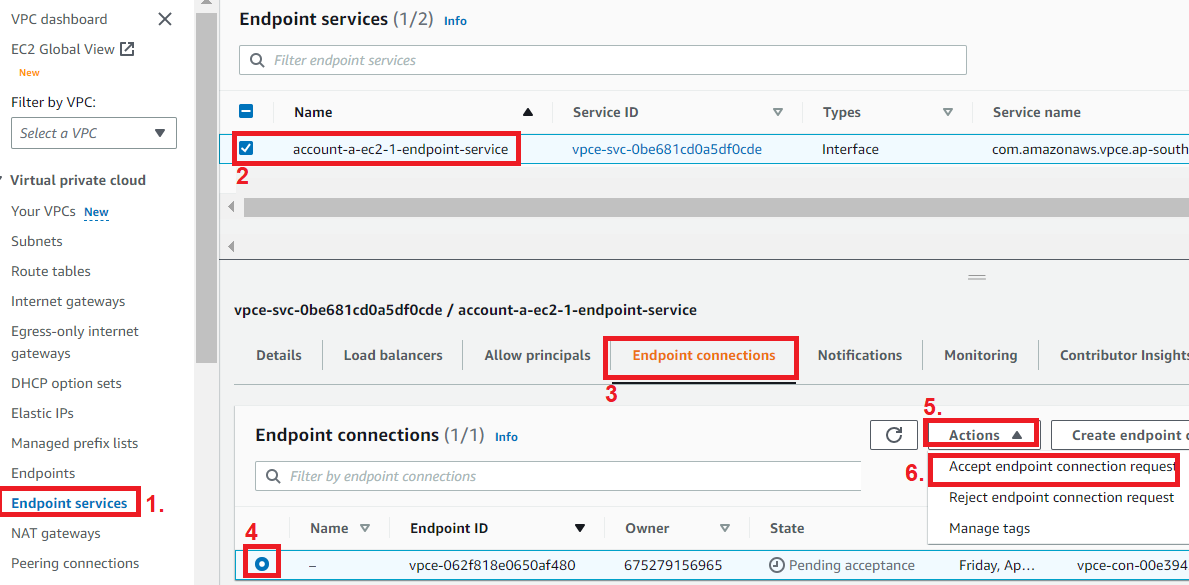


# **Accept the Endpoint Request**

* To establish Connection **Cross Account Admin** must **accept** the Endpoint Creation request.

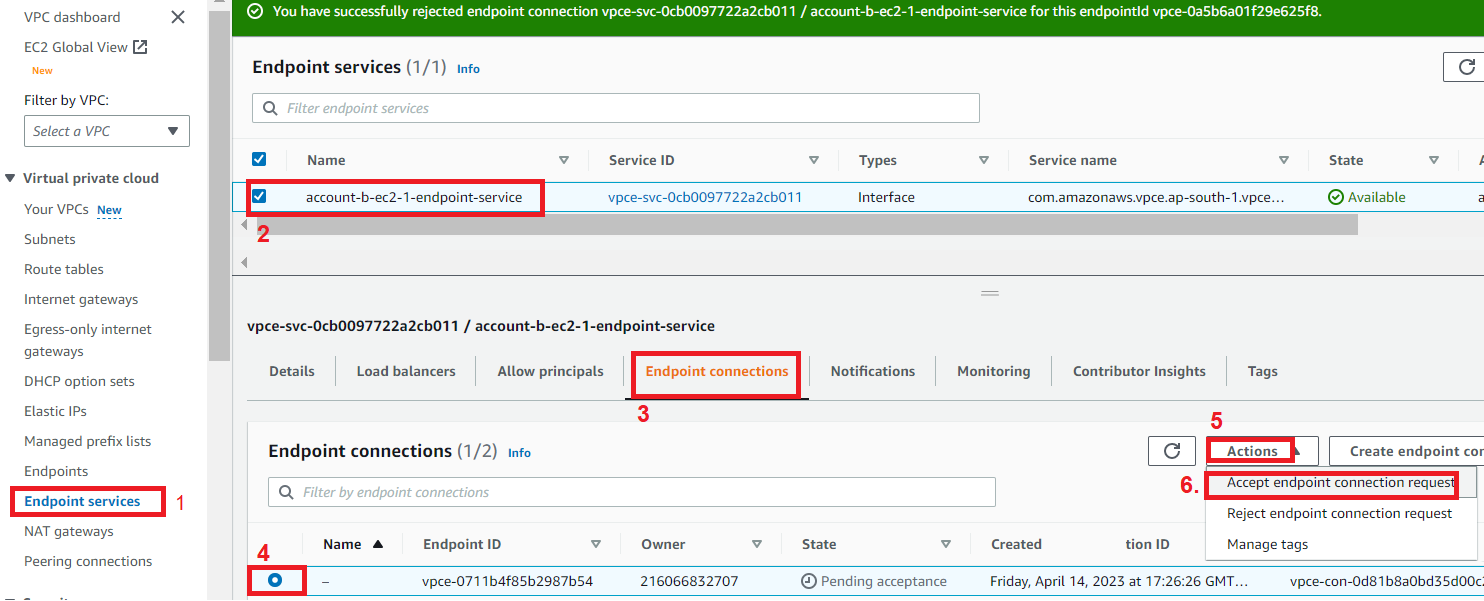
## **Accept Request – Account-A**

* Click **VPC Dashboard** 🡪 Click **Endpoint Service** 🡪 Select Created Endpoint Service 🡪 Click Endpoint Connect 🡪 Select the Request 🡪 Click **Action** 🡪 Click **Accept endpoint connection request**



## **Accept Request – Account-B**

* Click **VPC Dashboard** 🡪 Click **Endpoint Service** 🡪 Select Created Endpoint Service 🡪 Click Endpoint Connect 🡪 Select the Request 🡪 Click **Action** 🡪 Click **Accept endpoint connection request**



# **Update the Security Group of EC2**

* Update the Security Group of EC2 which accept the Request.

# **How to Connect to Cross Account EC2.**

* Open **VPC Dashboard** 🡪 Click **Endpoints** 🡪 Select Created endpoint 🡪 Click **Subnet** 🡪Ip address reflected in IPv4 address – This Can use to access Cross Account EC2.

