**Assignment-19-May-2022**

1. **What is the difference between NAT Gateway and NAT instance?**

| **Attribute** | **NAT gateway** | **NAT instance** |
| --- | --- | --- |
| Availability | Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture. | Use a script to manage failover between instances. |
| Bandwidth | Scale up to 45 Gbps. | Depends on the bandwidth of the instance type. |
| Maintenance | Managed by AWS. You do not need to perform any maintenance. | Managed by you, for example, by installing software updates or operating system patches on the instance. |
| Performance | Software is optimized for handling NAT traffic. | A generic AMI that's configured to perform NAT. |
| Cost | Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways. | Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size. |
| Type and size | Uniform offering; you don’t need to decide on the type or size. | Choose a suitable instance type and size, according to your predicted workload. |
| Public IP addresses | Choose the Elastic IP address to associate with a public NAT gateway at creation. | Use an Elastic IP address or a public IP address with a NAT instance. You can change the public IP address at any time by associating a new Elastic IP address with the instance. |
| Private IP addresses | Automatically selected from the subnet's IP address range when you create the gateway. | Assign a specific private IP address from the subnet's IP address range when you launch the instance. |
| Security groups | You cannot associate security groups with NAT gateways. You can associate them with the resources behind the NAT gateway to control inbound and outbound traffic. | Associate with your NAT instance and the resources behind your NAT instance to control inbound and outbound traffic. |
| Network ACLs | Use a network ACL to control the traffic to and from the subnet in which your NAT gateway resides. | Use a network ACL to control the traffic to and from the subnet in which your NAT instance resides. |
| Flow logs | Use flow logs to capture the traffic. | Use flow logs to capture the traffic. |
| Port forwarding | Not supported. | Manually customize the configuration to support port forwarding. |

1. **What is the difference between Security group and NACLs?**

|  |  |
| --- | --- |
| **Security Group** | **NACL (Network Access Control List)** |
| It supports only ****allow**** rules, and by default, all the rules are denied. You cannot deny the rule for establishing a connection. | It supports both ****allow and deny**** rules, and by default, all the rules are denied. You need to add the rule which you can either allow or deny it. |
| It is a ****stateful**** means that any changes made in the inbound rule will be automatically reflected in the outbound rule. For example, If you are allowing an incoming port 80, then you also have to add the outbound rule explicitly. | It is a ****stateless**** means that any changes made in the inbound rule will not reflect the outbound rule, i.e., you need to add the outbound rule separately. For example, if you add an inbound rule port number 80, then you also have to explicitly add the outbound rule. |
| It is associated with an EC2 instance. | It is associated with a subnet. |
| All the rules are evaluated before deciding whether to allow the traffic. | Rules are evaluated in order, starting from the lowest number. |
| Security Group is applied to an instance only when you specify a security group while launching an instance. | NACL has applied automatically to all the instances which are associated with an instance. |
| It is the first layer of defense. | It is the second layer of defense. |

1. **What is a public IP address?**

A public IP address is an IPv4 address that's reachable from the Internet. You can use public addresses for communication between your instances and the Internet.

When you launch an instance in a default VPC, we assign it a public IP address by default. When you launch an instance into a nondefault VPC, the subnet has an attribute that determines whether instances launched into that subnet receive a public IP address from the public IPv4 address pool. By default, we don't assign a public IP address to instances launched in a nondefault subnet

1. **What is a private IP address?**

A private IPv4 address is an IP address that's not reachable over the Internet. You can use private IPv4 addresses for communication between instances in the same VPC.

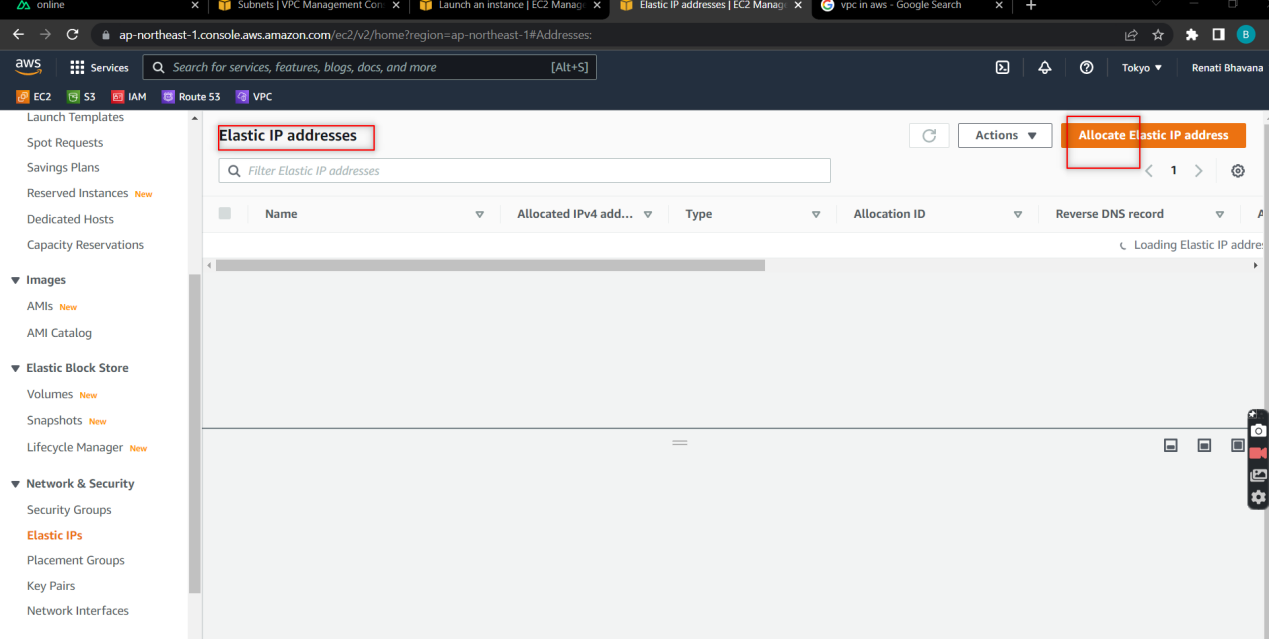
1. **What is an elastic IP address?**

An Elastic IP address is a public IPv4 address that you can allocate to your account. You can associate it to and disassociate it from instances as you require. It's allocated to your account until you choose to release it.

It will be constant even though u stopped and start instance the elastic IP Address will remain same.

1. **Hands on – Allocate an Elastic IP address to an EC2 instance and release it(include steps with screen shots)**

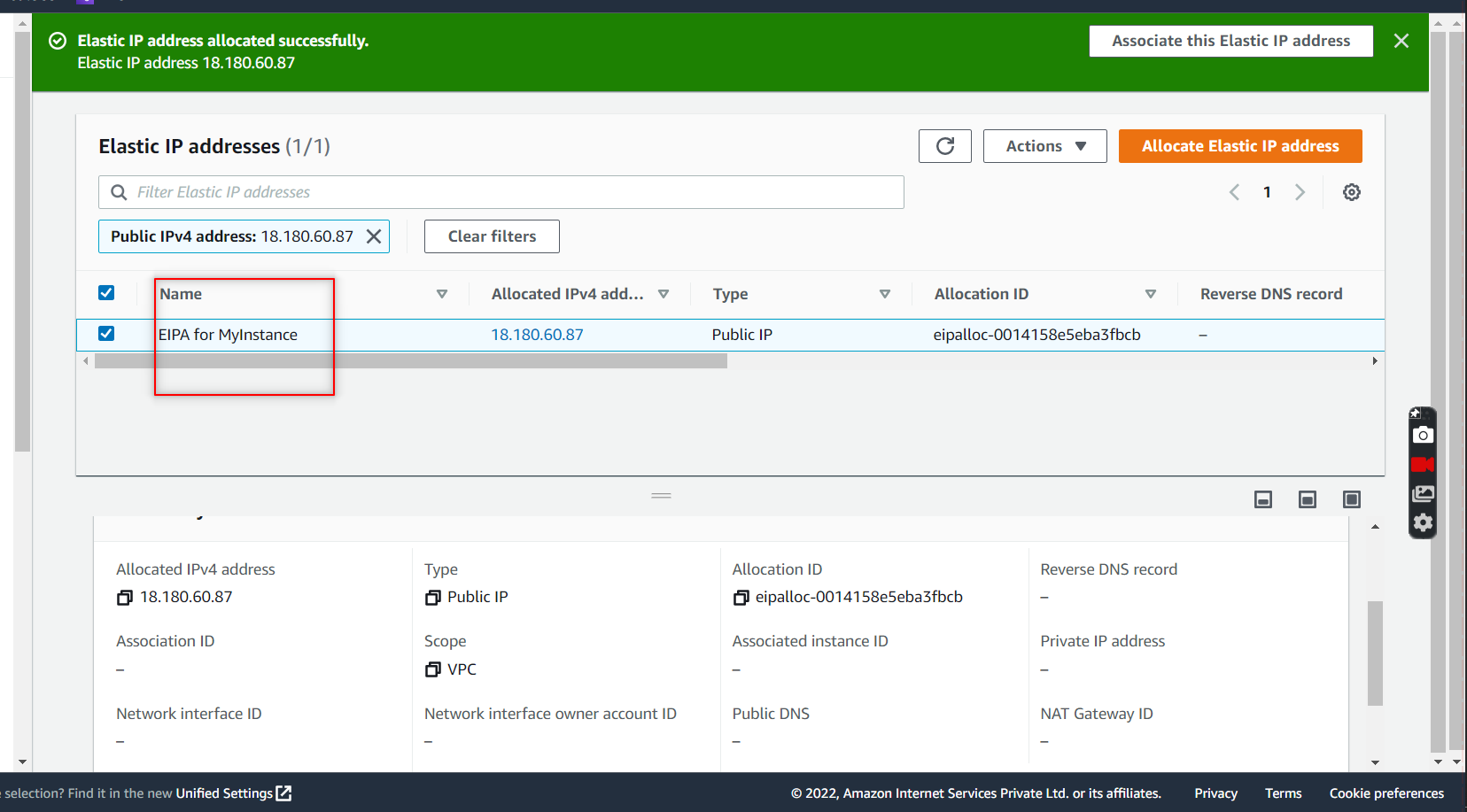
**Go to EC2 ->Click on Elastic IP Address and click on Allocate Elastic IP Address.**

****

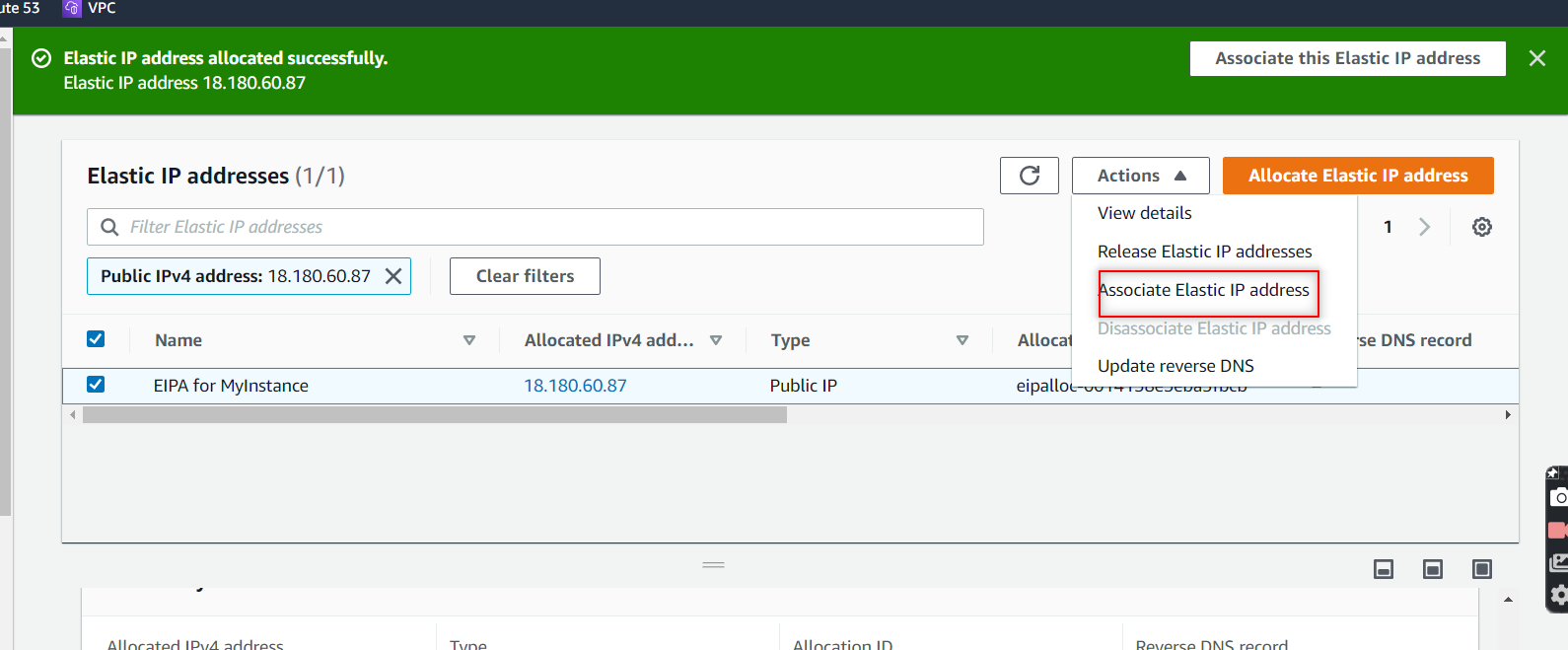
**Do as same below and click on allocate.**

****

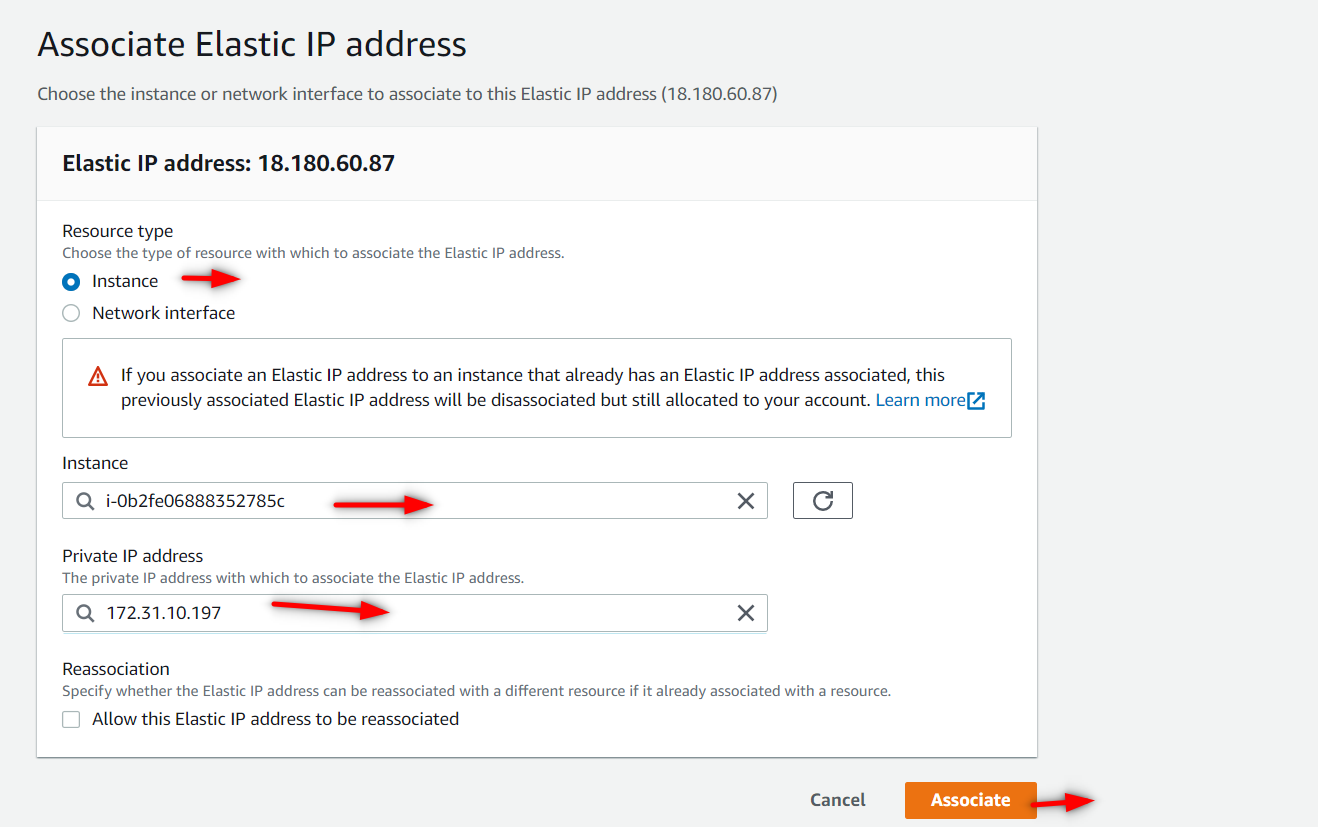
**Here the Elastic IP Address got created.**

****

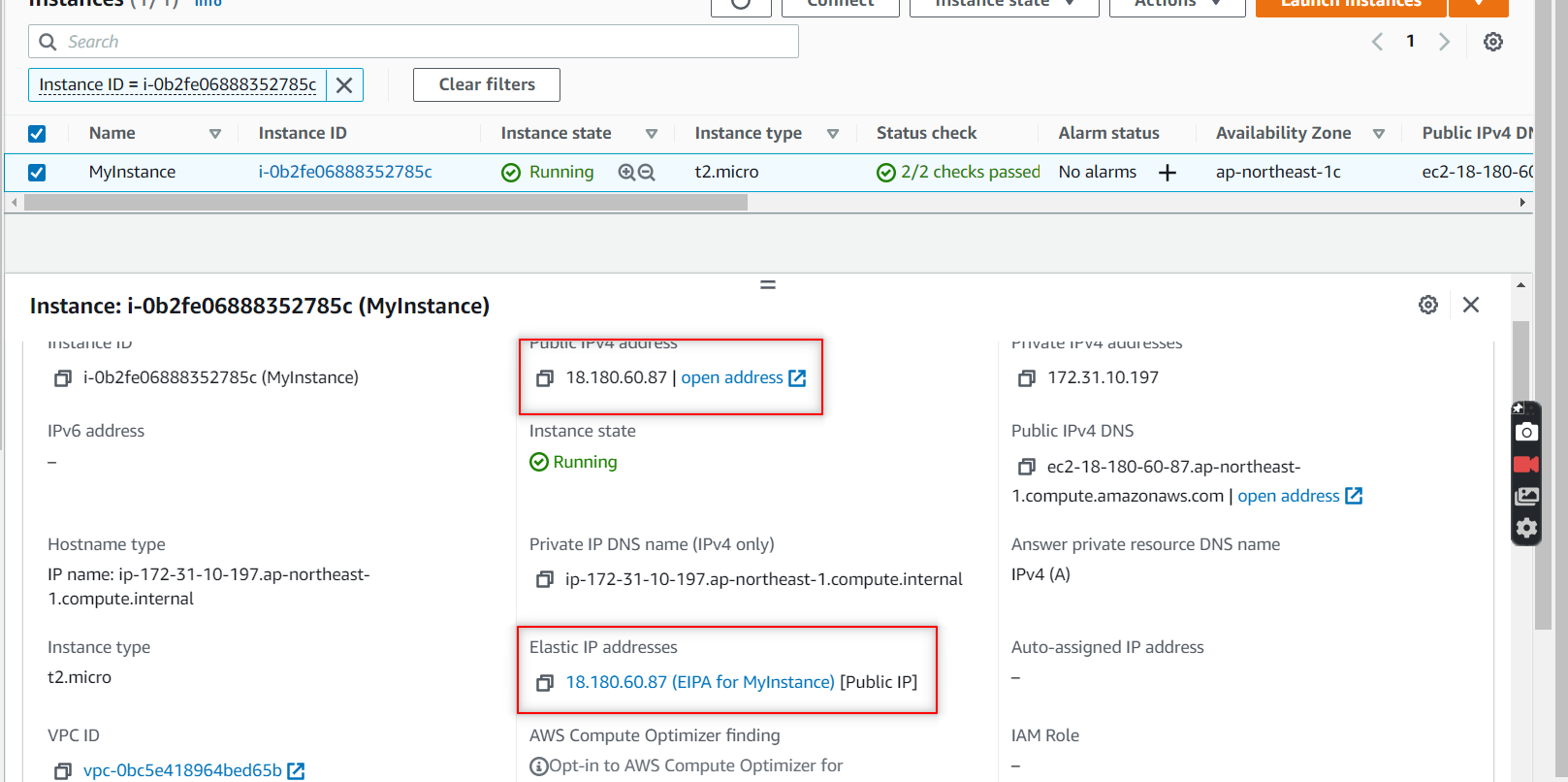
**To assign it to Instance ,Click on created EIA and go to actions and choose Associate Elastic IP Address**

****

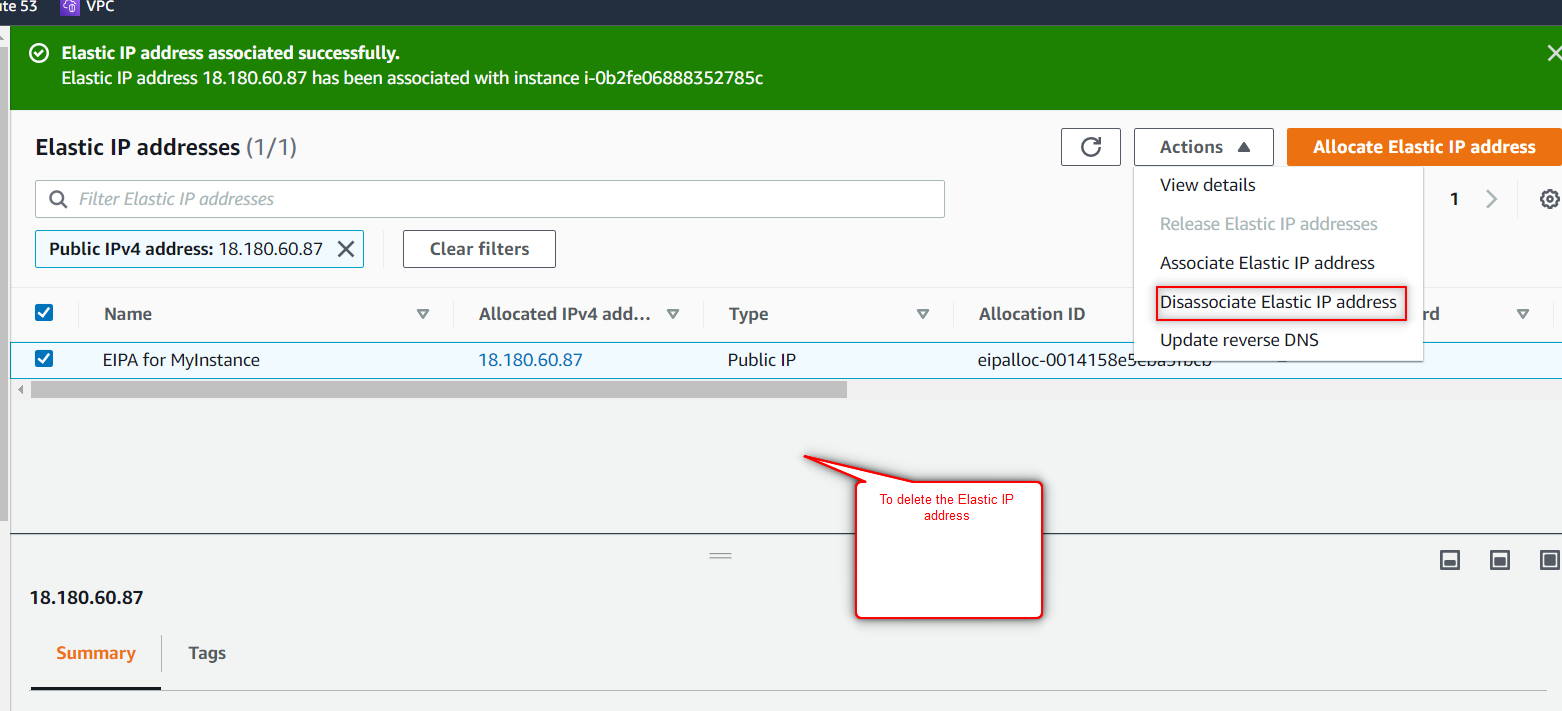
**Here provide the details as mentioned below instance id and private IP Address of which u want to attach the Elastic IP address and click on associate.**

****

**Here u can see the Elastic IP address got attached.**

****

**If you want to delete the Elastic IP Address , just Click on Disassociate Elastic IP Address.**

****

**8.What is Direct connect?**

* AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network solution from your premises to AWS.
* Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office environment, which can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
* Direct Connect is a direct connection which is available on a dedicated line.

**9. What is VPN? And its different types?(Site to site and Cloud hub)**

**Remote access VPNs:**

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.

**Site-to-site VPNs:**

A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

**Cloud-Hub:**

Cloud-Hub is an integration platform as a service (iPaaS) where you can deploy sophisticated cross-cloud integration applications in the cloud, create new APIs on top of existing data sources, integrate on-premises applications with cloud services, and much more.

1. **What is AWS transit Gateway?**

AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once.