Can you find any issues with the architecture?

- The subnet with Bastion hosts is marked as "Private Subnet."
- The Bastion hosts must be in a public subnet.
- As per the architectural diagram, the NAT Gateways are in Private Subnet. NAT Gateway must reside in a public subnet.

Do you need two NAT Gateways?

- It depends on many factors likes - Project, Architecture, Budget, etc.
- If we had only ONE NAT Gateway and the AZ containing the NAT Gateway goes down, then the EC2 instances (in private subnet) in the other AZ will lose connection to the internet.

How many subnets can you create with the current design?

- Given VPC CIDR: 10.0.0.0/16
- Subnet Bits:
  - 20 - 16 = 4
  - 4 Bits are used for subnetting.
- Number of Subnets:
  - 2^4 = 16
  - 16 Subnets can be created.

What would you recommend if the company wants to have more subnets than the current architecture allows?

- **Option1:** Add one more CIDR block to VPC
- **Option2:** Re-design using more subnet bits (say 5 or 6 or more). Make sure the MAX hosts allowed by subnetting meeting the needs.