Core Infrastructure Requirements for ECS EC2 Launch Type

1. **VPC**
    - A custom VPC to isolate your ECS cluster network.
    - Enable DNS support and hostnames for service discovery.
2. **Subnets**
    - Multiple subnets across different Availability Zones (AZs) for high availability.
    - Both **public subnets** (for NAT gateway, internet gateway) and **private subnets** (where ECS EC2 instances run).
    - ECS EC2 instances should be launched in **private subnets** to improve security.
3. **Internet Gateway**
    - Attach an Internet Gateway (IGW) to the VPC to enable internet access for public subnets.
4. **Route Tables**
    - Public route table that routes 0.0.0.0/0 traffic to the Internet Gateway.
    - Private route table(s) associated with private subnets.
    - Private route table must route outbound internet traffic (0.0.0.0/0) to a **NAT Gateway** (which resides in a public subnet) to allow ECS instances internet access for pulling images, updates, etc.
5. **NAT Gateway** (optional but recommended)
    - Allows ECS EC2 instances in private subnets to reach the internet securely.
6. **Security Groups**
    - Define security group(s) to control inbound/outbound traffic.
    - Open necessary ports (e.g., 22 for SSH, 3000 for container app).
    - Egress open for outbound internet access.
7. **IAM Role and Instance Profile**
    - An IAM role with `AmazonEC2ContainerServiceforEC2Role` policy attached.
    - IAM Instance Profile attached to EC2 instances, enabling ECS to manage containers securely.
8. **ECS Cluster**
    - An ECS cluster resource to logically group your EC2 container instances.
9. **EC2 Instances (ECS Container Instances)**
    - Launch EC2 instances inside private subnets.
    - Use ECS-optimized AMI.
    - Instance type as per your requirement (`t3.medium` in this case).
    - Pass user data to configure ECS agent to join the cluster.