**What is a Region?**

A region in AWS is a geographical area where AWS has its data centers. These regions are spread across different parts of the world, and each one has a specific name like us-east-1 (North Virginia) or eu-west-1 (Ireland). When choosing a region, you are deciding where your AWS resources will be physically located.  
  
For example, if most of your users are in Europe, choosing a region like eu-west-1 (Ireland) can provide faster access compared to selecting us-west-1 (California).

**What is an Availability Zone?**

An availability zone (AZ) is a separate data center within a region. AWS designs availability zones to be independent of each other so that if one goes down due to power failure or other issues, the others in the same region remain operational. This setup ensures that applications stay available even during infrastructure failures.  
  
For example, the us-east-1 region has multiple availability zones labeled us-east-1a, us-east-1b, us-east-1c, and so on.

**What is a Public Subnet?**

A public subnet is a network segment within your Virtual Private Cloud (VPC) that is connected to the internet. This means any resources placed in a public subnet can be accessed from outside AWS.  
  
For a subnet to be public, it must have:  
- An Internet Gateway (IGW) attached to the VPC  
- A route in the route table pointing to the Internet Gateway  
- An instance in the subnet with a public IP address  
  
Public subnets are useful for hosting web servers, API endpoints, or any services that need to be accessible over the internet.

**What is a Private Subnet?**

A private subnet is not directly accessible from the internet. Resources placed in a private subnet cannot be accessed from outside AWS unless you use a NAT Gateway or a VPN.  
  
Private subnets are typically used for databases, application servers, or any other services that should not be publicly accessible.

**How Many Subnets Can Exist in One Region?**

Each VPC in AWS can have up to 200 subnets. Since a region can contain multiple VPCs, the total number of subnets in a region can be much higher.

**How to Launch EC2 Instances in Public or Private Subnets?**

- Public Subnet:  
 - Attach an Internet Gateway to the VPC.  
 - Assign the EC2 instance a public IP address.  
 - Modify the security group to allow necessary inbound traffic.  
- Private Subnet:  
 - Do not attach an Internet Gateway.  
 - Use a NAT Gateway if the instance needs internet access for updates.  
 - Access the instance using a bastion host in the public subnet.

**What are AMIs?**

Amazon Machine Images (AMIs) are pre-configured operating system images used to launch EC2 instances. An AMI includes:  
- An operating system (such as Linux or Windows)  
- Pre-installed applications or configurations  
- Any necessary permissions and settings  
  
AWS provides default AMIs, but you can also create custom AMIs with your own configurations.

**What are Security Groups?**

A security group acts as a virtual firewall that controls incoming and outgoing traffic for EC2 instances. Every EC2 instance must be associated with at least one security group.  
  
Security groups are stateful, meaning:  
- If an incoming request is allowed, the corresponding response is automatically allowed.  
- If outbound traffic is allowed, return traffic is also permitted.

**What are Inbound and Outbound Rules?**

- Inbound rules define which types of traffic are allowed to enter an EC2 instance.  
- Outbound rules define which types of traffic are allowed to leave an EC2 instance.  
  
By default, all outbound traffic is allowed, but inbound traffic is blocked unless explicitly permitted.

**What is the 'Deny by Default' Rule in Security Groups?**

By default, AWS blocks all inbound traffic to an EC2 instance unless you modify the security group rules. This is a security measure to prevent unauthorized access.  
  
For example, if you launch an EC2 instance without changing the security group, you will not be able to connect to it via SSH. You must manually allow inbound traffic on port 22 for SSH access.

**How to Allow Access to EC2 from Security Groups?**

To enable access, you need to modify the security group's inbound rules. Common configurations include:  
- Allowing SSH (port 22) access for remote login (restricted to your IP for security).  
- Allowing HTTP (port 80) for a web server.  
- Allowing HTTPS (port 443) for secure web traffic.

**How to Connect to an EC2 Instance from Your Machine?**

To connect to an EC2 instance via SSH, use the following command:  
  
ssh -i MyKeyPair.pem ec2-user@PUBLIC\_IP  
  
If you get a 'Permission Denied' error, make sure your key file has the correct permissions:  
  
chmod 400 MyKeyPair.pem  
  
If you still have issues, run:  
  
sudo chown $(whoami):$(whoami) MyKeyPair.pem

**How to Set Up a Simple Static Website with EC2?**

To host a basic website on EC2:  
  
1. Connect to the EC2 instance  
  
ssh -i MyKeyPair.pem ec2-user@PUBLIC\_IP  
  
2. Update system packages  
  
sudo yum update -y  
  
3. Install Apache Web Server  
  
sudo yum install -y httpd  
  
4. Start Apache and enable it to run on boot  
  
sudo systemctl start httpd  
sudo systemctl enable httpd  
  
5. Create a simple webpage  
  
echo '<h1>Welcome to My AWS Website</h1>' | sudo tee /var/www/html/index.html  
  
6. Modify the security group to allow HTTP traffic  
- Go to EC2 → Security Groups → Inbound Rules  
- Add a rule allowing HTTP (port 80) from 0.0.0.0/0  
  
7. Access your website  
Open a browser and go to http://PUBLIC\_IP. You should see the webpage you created.  
  
This setup is a basic example of hosting a static website on an EC2 instance.