1. Basics & Setup

• EC2 vs Lambda: EC2 gives you full server control; good for long-running workloads. Lambda is serverless, pay-per-execution, ideal for event-driven workloads. Use EC2 if you need OS-level control.

• Choosing Instance Type: Start with t3 or t4g for general workloads, m for balanced compute/memory, c for CPU-intensive, r for memory-heavy. Use AWS Instance Selector tool to decide.

• On-Demand vs Reserved vs Spot: On-Demand = pay-as-you-go. Reserved = 1–3 year commitment, cheaper. Spot = unused capacity, cheapest but can be interrupted anytime.

• SSH / Session Manager: For SSH: ensure inbound port 22 in Security Group is open to your IP. For Session Manager: enable in Systems Manager, attach IAM role with AmazonSSMManagedInstanceCore.

• Public vs Private IP: Public IP = internet-facing, changes if stopped/started (unless Elastic IP). Private IP = internal VPC communication, persistent until termination.

2. Storage

• EBS vs Instance Store: EBS = persistent, survives stop/start. Instance Store = temporary, faster, data lost when stopped.

• Increase EBS Size: Modify volume size in EC2 Console → Volumes, then resize filesystem inside the instance.

• Snapshots: Point-in-time backup of EBS; incremental after first snapshot. Cost is based on GB stored in S3. Can restore into new volumes.

• Multiple EC2 to One EBS: Not directly possible except with multi-attach on certain Nitro instances for clustered apps.

3. Networking

• Assign Elastic IP: Allocate Elastic IP in EC2 → associate with instance. Charges apply if unused.

• Cannot Access from Internet: Check SG rules, NACLs, Public IP, and route table to Internet Gateway.

• Security Groups vs NACLs: SG = stateful, instance-level. NACL = stateless, subnet-level.

• Private Subnet Internet Access: Use NAT Gateway/Instance and update route tables.

4. Security

• SSH Key Management: Generate via AWS Console, rotate periodically, update authorized_keys.

• Secure EC2: Use IAM roles, EBS encryption, MFA, close unused ports, patch regularly.

• EBS Encryption: Enable at creation, or copy snapshot with encryption and restore.

• IAM Roles with EC2: Attach IAM roles at launch or later to allow service access without keys.

5. Scaling & Availability

• Auto Scaling Group: Define Launch Template/Config → Create ASG → Set min/max/desired capacity → Attach to Load Balancer.

• ALB vs NLB vs CLB: ALB = HTTP/HTTPS, path-based. NLB = TCP/UDP low latency. CLB = legacy.

• Multi-AZ Setup: Launch in multiple AZs, use Load Balancer, replicate data.

6. Cost & Billing

• Reduce Costs: Use Spot for flexible workloads, stop unused instances, downsize, buy Reserved Instances.

• Track Costs: Enable Cost Explorer and AWS Budgets. Tag resources for allocation.

• Free Tier Expiry: After 12 months, billed at On-Demand rates. Set budget alerts.

7. Maintenance & Troubleshooting

• High CPU Usage: Monitor via CloudWatch, identify process, scale vertically or horizontally.

• Lost SSH Key: Stop instance, detach root volume, attach to another, update authorized_keys, reattach.

• Unresponsive Instance: Try EC2 Instance Connect or Session Manager, then stop/start or restore from snapshot.

• Update OS/Software: For Linux: sudo yum update / apt update && upgrade. For Windows: use Windows Update or Patch Manager.