1. AWS의 각 서비스에 접근하기 위해서는 Access key를 사용할 수 있지만, 유출될 위험이 존재하므로 IAM Role을 부여하여 보다 안전하게 접근하는 것이 좋음
 즉 IAM은 EC2 내 애플리케이션에게 접근 권한을 부여하므로 EC2에 Access key를 저장하는 일이 없어 안전함

2. DynamoDB와 Elasticache는 대표적인 Storage Service이며 Key-Value 쌍을 저장하기 용이하여 Session data를 저장하는데 적합함.

3. S3는 AWS의 대표적인 Storage Service이며, Versioning 기능은 우발적인 삭제로부터 데이터를 보호하기에 매우 용이함.
 delete marker 기능을 이용하여 실수로 삭제하였다 하더라도, 다시 복구하는 것이 가능

4. '관계형 데이터'를 저장하는 Storage를 찾고 있으므로 Aurora가 가장 적합하며, Aurora는 autoscaling 기능을 보유하고 있기 때문에 확장이 용이함

5. AWS 설명서에 따르면 16000 IOPS 또는 250MiB/s 이상의 볼륨당 처리량을 필요로 하는 서비스의 경우, EBS Provisioned IOPS SSD을 사용할 것을 권장함

6. 문제에서는 scaling을 지원하지 않는 서비스, 사용자가 직접 scaling을 신경써야할 서비스를 찾고 있으므로 EC2가 정답
 Lambda, SQS, DynamoDB 모두 Autoscaling을 통해 자동으로 확장하지만 EC2의 경우 Autosclaing을 별도로 설정해주어야 함

7. S3는 수명주기관리를 통해 S3내 저장된 Object들의 Storage Class를 지정할 수 있으며, 사용 패턴에 따라 일정기간이 지난 후에 다른 Class로 지정하여 비용을 절감할 수 있음

8. VPN의 경우, 암호화된 터널이 존재한다 하더라도 결국은 외부 인터넷을 통하게 되므로 보다 더 강한 보안을 원한다면 아마존 백본 네트워크(AZ - S3)만을 통하는 S3 endpoint를 사용할 수 있음

9. Redshfit는 Enhanced Routing을 통해 VPC 내에서만 통신이 가능하도록 보안조치를 취할 수 있으며, Cluster Security group을 사용해 Cluster에 접근할 수 있는 대상을 제어할 수 있음

10. Public, Private Subnet을 나누어 외부에 노출되어야할 Public Subnet에 있는 인스턴스에만 공인 IP를 제공하고, 그밖의 서비스들은 Private Subnet 내에서 사설 IP만을 할당하여 보안 강도을 높임
 또한 사설 IP만을 갖는 Private Subnet이 외부 인터넷에 접속해야 할 때를 대비하여 Public Subnet에 NAT Gateway를 생성하고 Private Subnet에서 Routing 설정을 NAT Gateway로 연결하여 외부에서 접근하지 못하는 인터넷 통로를 생성함