## Question 1 - AWS EC2

Port scanning will be detected by Amazon and they block it. To mitigate any risk of port scanning, all inbound ports are closed by default. If you have to open one, there should be a security group configured.

## Question 2 - AWS EBS

The EBS-volumes are stored redundantly in multiple physical locations, which raises the dependability enormous. To increasing the long-term durability, it is highly recommended to conduct regular snapshots, which can be made publicly available in other AWS Accounts. This snapshot can be copied, to create a new EBS volume, but cannot be deleted.

## Question 3 - AWS S3

1. Identity and Access Management (IAM) policies to create and manage multiple users under a single AWS account
2. Access control lists (ACLs) to give read and write access on buckets or objects to groups of users.
3. Bucket policies to grant users access to your Amazon S3 resources

## Question 4 - AWS SES

Emails sent with DKIM have a DKIM-Signature header field, representing a cryptographically signed message. This message can be decoded by the ISP with a public key to ensure that the message is authentic. These DKIM signatures are optional. Either you set it up, so SES is always adding it, or you add it manually by using the SendRawEmail API

## Question 5 - AWS EMR

EMR automatically sets up security groups for master nodes and for slaves. Both are by default set up not to allow access from external sources