## 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

# Cloud Architecture

#### Web Application:

The DNS service is provided by AWS Route 53, so we don’t have to have another 3rd party involved. The first part in our Web Tier in the AWS region is an elastic load balancer. This distributes the traffic to Web Server Autoscaling groups, consisting of multiple EC2 Instances. The Web Applications are deployed on the EC2 instances by using Elastic Beanstalk.  
The Application Tier also has an ELB fetching the request from the Web Tier and distributing them on the autoscaled ECS instances. The App Tier is requesting the data from the different Databases via the AWS Storage Gateway.  
S3 Buckets are storing Backups, and static objects, such as media and other contents, like HTML, CSS, PHP, etc. Cloudfront is providing the user with this static and dynamic high-volume content in an accelerated fashion.

#### Security:

The AWS Region doesn’t need an exterior firewall with standard open ports (80,433) to the internet. These ports give the user access to the Web Tier. For Application and Database Tier the staff and 3rd parties can have ssh access.

The private On-Premise region has an exterior firewall. The only connection between the both regions is a VPN connection with AWS Direct Connect. On the private region is a Customer gateway and in the AWS region is a virtual private gateway installed. The connection is encrypted and is getting validated from both sides.

#### Monitoring:

CloudWatch is monitoring our AWS region. This gives us the ability to record metrics, collect logfiles and set alarms, to notify us, if the workload is unbalanced. This guarantees, coupled with the ELBs, the ability to react as quick as possible and guarantee a high availability.

#### Messaging:

Simple Queue Service (SQS) is an asynchronous messaging system, which enables the different components to communicate with each other within the cloud. This queue is highly scalable and decouples the services from each other.

#### Data Storage:

The User data is stored in Databases in our private region. These databases are MySQL servers where the user data is saved.  
In our AWS Region, we have a DynamoDB database for the key-value data and a Relational Database Service (RDS) to store the application data.   
The connection and data retrieval between the two regions is done by the AWS Storage Gateway, which has access to the AWS Direct Connect.  
ElastiCache is installed to provide caching services for the applications, which removes load from the databases