Cloud Security

1) There are several counter actions to mimimize the risk of port scanning:

- limit security group access to the absolute minimum,
- choose the more secure over the less secure protocols (https instead of http),
- if possible limit the ip address ranges, which are allowed to connect.
(e.g. only your application servers should be able access your database)

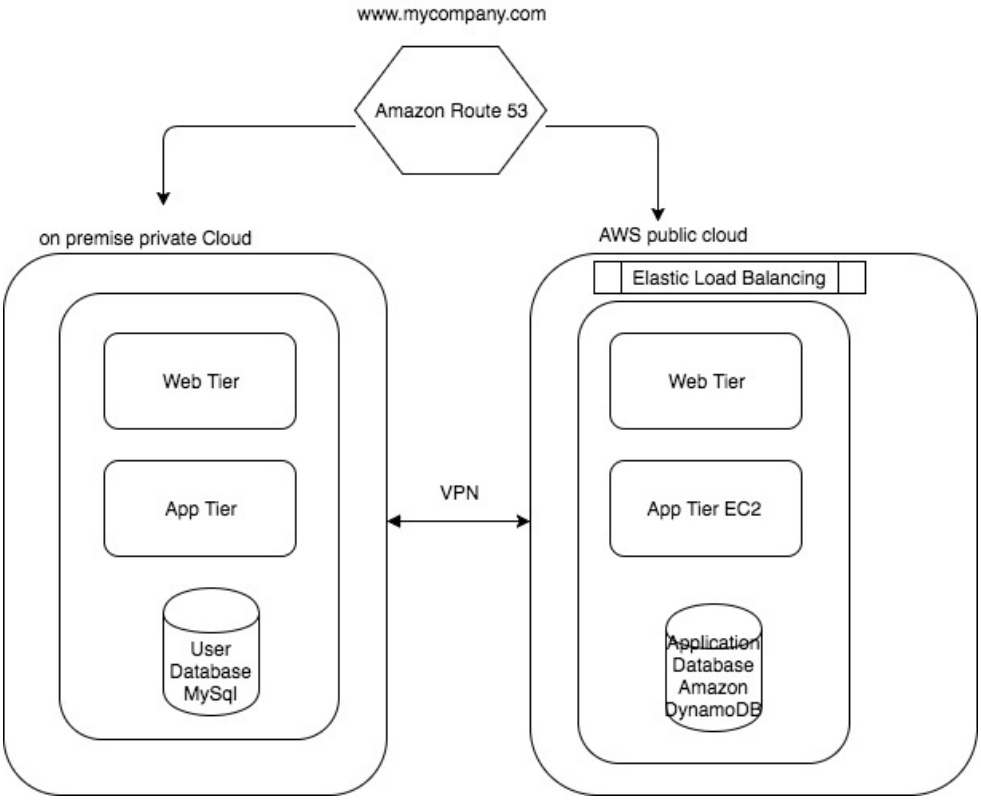
2) 2 mechanisms to improve the EBS' volumes dependability:
- Taking snapshots of the EBS volume
- Configuring multiple EBS volumes using RAID

3) How can you control access to S3 buckets and objects?
- create and manage multiple users under one AWS account with IAM(Identity and Access Management)
- ACL for reading and writing access to buckets and objects
- bucket policies which allow users to access my Amazon S3 ressources

4) To make authenticated email requests, emails can be sent with a DKIM signature, which uses a 1024-bit DKIM Key. SES has a feature called Easy DKIM, which will add DKIM signature automatically for you. Appropriate DNS record settings must be configured first to set this up.

5) -when launching the cluster at default settings , security group for master and slave nodes will be created
- inbound rules: allows inboud traffic from instances in the EMR master security group
- outbound rules: provides outbound access from user specified instances in the EMR security group

Cloud Architecture



A proper Hybrid cloud environment provides a fine balance between the scalable ressources of a public cloud and the ressources of an on-premise infrastructure. In the following text I am going to discuss which components of the IT infrastructure should be migrated to the cloud and how to set up the connection between those two distinct clouds in order to have a seamlessly integrated cloud environment. Furthermore a technology recommendation based on how to best achieve those goals will be given.

Most webapplications today are multitiered and consists of the following layer:
Database layer , application Layer , Web Server Layer.
As our company is hosting several web applications, there is the question: which applications and components should be moved into the cloud and which ones should remain deployed in our on-premise private cloud.
Also The applications have to communicate with each other, so the interrelated connections between them induce their complexity, which needs to be handled. Best would be in an all in one Panel, where the system administrator has an overview about the whole infrastructure, both public and private Cloud Infrastructure. Hereby I recommend the technology rackconnect, which allows you to connect multiple distinct clouds to a common Cloud Environment.

If the Web application needs to be ready for high peak usage and therefore must be scalable on-demand fast and securely, one should think of which layer of the application should be moved to the public cloud and which layer should remain on-premise.

User sensitive data should stay in the local database server such as MySQL. Everything else like application data which has lower significant value in terms of privacy violation can be

moved to a public cloud storage Servers using key-value databases, herefore I recommend Amazon DynamoDB which is highly scalable and very fast. Also an

The Webserver handles request and responses, whereas the application server handles the business logic such as interactions with the database and handling support or business critical operations.
Depending on how much those applications communicate with each other and retrieve and write data to the database, high performance applications will generally have a higher latency when moved entirely to the cloud.
In periods of high peak usage though, additional instances of the application could be deployed on the public cloud, which grant high scalability and Availability on demand.
Elastic Load Balancing will be used to distribute HTTP requests among the webservers, which will be instantiated by Amazon Elastic Compute Cloud instances (EC2). this provides greater stability in times of high incoming web traffic. So as for the application tier in the public cloud, it will be configured with several application server across different availability zones and with alert mechanisms in place to allow vertical and horizontal scaling if needed. Metrics for which those alert mechanism are going to be activated can be CPU-idle, free memory, and system load. Application server will be also deployed on ES2 instances.

As our on premise application servers, our user databases and our public cloud app servers need to exchange data with each other, the communication between these components will happen through a VPN secured connection. Amazon offers a service called AWS Direct Connect which ensures such a secure VPN connection between our public and private cloud applications.