PART 1 Q&A

1. If a website is down, as a LAMP stack engineer you can go through the following process to troubleshoot and pinpoint where the problem might be. Hence its good practice to check the following:

   a. Once of the first thing is to ping the website on a Linux terminal for a response.

      I. Check the Apache server. It could be a part or whole server issue. There may have been a configuration change or the whole server may have crashed. Check the server logs to investigate.
      II. A follow through step if the servers are fine is to troubleshoot the application/check for bugs in code. This could be as a result of code changes made by another developer may have caused the website to go down. Code changes could also be related to the database as that is linked with the application.
      III. Check if there is a DNS problem, or an expired domain, a networking problem.

   b. Check the default website

      Check the IIS server and windows configuration as below and authenticate SQL.

      I. Browse the website if website is down, IIS version error will show

      II. Ensure features under application development features e.g. ASP.NET, ISAPI filter and extensions.

      III. Check off HTTP features e.g. static content, HTTP errors

      IV. Restart service on server

      V. Check the ASP.NET for the site is allowed under ISAPI and CGI restrictions.

      VI. Check to see your ASP.NET is started under application pool.

      VII. Check authentication with SQL server in program files to analyse your web.config file (check your serve name and user login)

      VIII. Check windows and SQL authentication is checked

   c. The firewall ensure secure access to a website, hence if a firewall is down or having issues, website access could be affected. Check the firewall configuration for any breach and rectify.
      For load balancers (LB), this is could be that the servers behind LB are fully trafficked hence access to the website is down because all the servers are taking in more than

their configured capacity. Troubleshoot the LB configuration for connectivity or performance related problems.

d. If a website is back up and running, you can run the following:

Run a perform test check to check speed, network, responsiveness and the workload of both the servers and application.

Monitor the traffic and to see how increase influx can be managed and configured better.

2. Changing permissions for '/bin/chmod' returns an 'operation not permitted' result. This is because chmod is the command and system call which is used to change the access permissions of files system objects. Therefore, changing/removing execute permission would render the chmod command non-functional if such operation was permitted hence it's not.

3. AWS security group when configured instantly affects all instances within it.

PART 2: SCENARIOS

4. The best practice to allow your EC2 instances to talk to, say S3 or RDS is to create a Role.

5. If the ELB times out, it is because the security group (SG) is not configured to allow traffic from the ELB to the Instances behind the SG.

6. Problems with lack of connectivity includes:
   I. Configurations with the following:
   II. Internet gateway
   III. Virtual private gateway
   IV. AWS site-to- Client site connections
   V. NAT gateway and NAT instance
   VI. VPC peering connection
   VII. End points

   Further AWS services that could affect connectivity include configurations changes to security groups, NACLs.

7. Loss of connection to a server. The following can be checked to ensure re-connection:
   I. The amount of EBS volume on the server
   II. The security group configurations
   III. Check if port for access e.g. SSH is open
   IV. Incorrect SSH user, some AMI use different user for the CentOS AMI is *centos*.

8. On your AWS management console or using the CLI, you can add additional EBS volume while your instance is running to improve performance, or you can scale up the instance which is more difficult as it will requires you to stop the instance to upgrade.

9. Setting up Cloud watch to monitor instance performance is a way to avoid unawareness of EC2 overload in the future.

10. Configure your server, to PUT out an error application page in the event of website failover.