1. You are working with a customer who is using Chef configuration management in their data center. Which service is designed to let the customer leverage existing Chef recipes in AWS?
   1. Amazon Simple Workflow Service
   2. AWS Elastic Beanstalk
   3. AWS CloudFormation
   4. **AWS OpsWorks**
2. Your mission is to create a lights-out datacenter environment, and you plan to use AWS OpsWorks to accomplish this. First you created a stack and added an App Server layer with an instance running in it. Next you added an application to the instance, and now you need to deploy a MySQL RDS database instance. Which of the following answers accurately describe how to add a backend database server to an OpsWorks stack? Choose 3 answers
   1. **Add a new database layer and then add recipes to the deploy actions of the database and App Server layers.**(Refer [link](http://docs.aws.amazon.com/opsworks/latest/userguide/customizing-rds.html))
   2. Use OpsWorks’ “Clone Stack” feature to create a second RDS stack in another Availability Zone for redundancy in the event of a failure in the Primary AZ. To switch to the secondary RDS instance, set the [:database] attributes to values that are appropriate for your server which you can do by using custom JSON.
   3. **The variables that characterize the RDS database connection—host, user, and so on—are set using the corresponding values from the deploy JSON’s [:deploy][:app\_name][:database] attributes.** (Refer [link](http://docs.aws.amazon.com/opsworks/latest/userguide/customizing-rds.html))
   4. Cookbook attributes are stored in a repository, so OpsWorks requires that the “password”: “your\_password” attribute for the RDS instance must be encrypted using at least a 256-bit key.
   5. **Set up the connection between the app server and the RDS layer by using a custom recipe. The recipe configures the app server as required, typically by creating a configuration file. The recipe gets the connection data such as the host and database name from a set of attributes in the stack configuration and deployment JSON that AWS OpsWorks installs on every instance.** (Refer [link](http://docs.aws.amazon.com/opsworks/latest/userguide/customizing-rds.html))
3. You are tasked with the migration of a highly trafficked node.js application to AWS. In order to comply with organizational standards Chef recipes must be used to configure the application servers that host this application and to support application lifecycle events. Which deployment option meets these requirements while minimizing administrative burden?
   1. **Create a new stack within Opsworks add the appropriate layers to the stack and deploy the application**
   2. Create a new application within Elastic Beanstalk and deploy this application to a new environment (need to comply with chef recipes)
   3. Launch a Node JS server from a community AMI and manually deploy the application to the launched EC2 instance
   4. Launch and configure Chef Server on an EC2 instance and leverage the AWS CLI to launch application servers and configure those instances using Chef.
4. A web-startup runs its very successful social news application on Amazon EC2 with an Elastic Load Balancer, an Auto-Scaling group of Java/Tomcat application-servers, and DynamoDB as data store. The main web application best runs on m2.xlarge instances since it is highly memory- bound. Each new deployment requires semi-automated creation and testing of a new AMI for the application servers which takes quite a while and is therefore only done once per week. Recently, a new chat feature has been implemented in node.js and waits to be integrated in the architecture. First tests show that the new component is CPU bound Because the company has some experience with using Chef, they decided to streamline the deployment process and use AWS OpsWorks as an application life cycle tool to simplify management of the application and reduce the deployment cycles. What configuration in AWS OpsWorks is necessary to integrate the new chat module in the most cost-efficient and flexible way?
   1. Create one AWS Ops Works stack, create one AWS Ops Works layer, create one custom recipe
   2. **Create one AWS Ops Works stack, create two AWS Ops Works layers create one custom recipe** (Single environment stack, two layers for java and node.js application using built-in recipes and custom recipe for DynamoDB connectivity only as other configuration. Refer [link](http://docs.aws.amazon.com/opsworks/latest/userguide/other-services.html))
   3. Create two AWS Ops Works stacks, create two AWS Ops Works layers create one custom recipe
   4. Create two AWS Ops Works stacks, create two AWS Ops Works layers create two custom recipe
5. You company runs a complex customer relations management system that consists of around 10 different software components all backed by the same Amazon Relational Database (RDS) database. You adopted AWS OpsWorks to simplify management and deployment of that application and created an AWS OpsWorks stack with layers for each of the individual components. An internal security policy requires that all instances should run on the latest Amazon Linux AMI and that instances must be replaced within one month after the latest Amazon Linux AMI has been released. AMI replacements should be done without incurring application downtime or capacity problems. You decide to write a script to be run as soon as a new Amazon Linux AMI is released. Which solutions support the security policy and meet your requirements? Choose 2 answers
   1. Assign a custom recipe to each layer, which replaces the underlying AMI. Use AWS OpsWorks life-cycle events to incrementally execute this custom recipe and update the instances with the new AMI.
   2. **Create a new stack and layers with identical configuration, add instances with the latest Amazon Linux AMI specified as a custom AMI to the new layer, switch DNS to the new stack, and tear down the old stack.** (Blue-Green Deployment)
   3. Identify all Amazon Elastic Compute Cloud (EC2) instances of your AWS OpsWorks stack, stop each instance, replace the AMI ID property with the ID of the latest Amazon Linux AMI ID, and restart the instance. To avoid downtime, make sure not more than one instance is stopped at the same time.
   4. Specify the latest Amazon Linux AMI as a custom AMI at the stack level, terminate instances of the stack and let AWS OpsWorks launch new instances with the new AMI. (Will lead to downtime)
   5. **Add new instances with the latest Amazon Linux AMI specified as a custom AMI to all AWS OpsWorks layers of your stack, and terminate the old ones.**
6. When thinking of AWS OpsWorks, which of the following is not an instance type you can allocate in a stack layer?
   1. 24/7 instances (24/7 instances are supported and started manually and run until you stop them)
   2. **Spot instances** (Does not support spot instance directly but can be used with auto scaling Refer [link](https://forums.aws.amazon.com/thread.jspa?threadID=117372))
   3. Time-based instances (Time-based instances are run by AWS OpsWorks on a specified daily and weekly schedule)
   4. Load-based instances (Load-based instances are automatically started and stopped by AWS OpsWorks, based on specified load metrics, such as CPU utilization)
7. Which of the following tools does not directly support AWS OpsWorks, for monitoring your stacks?
   1. **AWS Config** (Refer [link](http://docs.aws.amazon.com/opsworks/latest/userguide/monitoring.html))
   2. Amazon CloudWatch Metrics (AWS OpsWorks uses CloudWatch to provide thirteen custom metrics with detailed monitoring for each instance in the stack)
   3. AWS CloudTrail (AWS OpsWorks integrates with CloudTrail to log every AWS OpsWorks API call and store the data in an S3 bucket)
   4. Amazon CloudWatch Logs (You can use Amazon CloudWatch Logs to monitor your stack’s system, application, and custom logs.)
8. When thinking of AWS OpsWorks, which of the following is true?
   1. **Stacks have many layers, layers have many instances.**
   2. Instances have many stacks, stacks have many layers.
   3. Layers have many stacks, stacks have many instances.
   4. Layers have many instances, instances have many stacks.

 Your company Is moving towards tracking web page users with a small tracking Image loaded on each page Currently you are serving this image out of US-East, but are starting to get concerned about the time It takes to load the image for users on the west coast. What are the two best ways to speed up serving this image? Choose 2 answers

1. **Use Route 53’s Latency Based Routing and serve the image out of US-West-2 as well as US-East-1**
2. **Serve the image out through CloudFront**
3. Serve the image out of S3 so that it isn’t being served oft of your web application tier
4. Use EBS PIOPs to serve the image faster out of your EC2 instances

 You deployed your company website using Elastic Beanstalk and you enabled log file rotation to S3. An Elastic Map Reduce job is periodically analyzing the logs on S3 to build a usage dashboard that you share with your CIO. You recently improved overall performance of the website using Cloud Front for dynamic content delivery and your website as the origin. After this architectural change, the usage dashboard shows that the traffic on your website dropped by an order of magnitude. How do you fix your usage dashboard’? **[PROFESSIONAL]**

1. **Enable CloudFront to deliver access logs to S3 and use them as input of the Elastic Map Reduce job**
2. Turn on Cloud Trail and use trail log tiles on S3 as input of the Elastic Map Reduce job
3. Change your log collection process to use Cloud Watch ELB metrics as input of the Elastic Map Reduce job
4. Use Elastic Beanstalk “Rebuild Environment” option to update log delivery to the Elastic Map Reduce job.
5. Use Elastic Beanstalk ‘Restart App server(s)” option to update log delivery to the Elastic Map Reduce job.

 An AWS customer runs a public blogging website. The site users upload two million blog entries a month. The average blog entry size is 200 KB. The access rate to blog entries drops to negligible 6 months after publication and users rarely access a blog entry 1 year after publication. Additionally, blog entries have a high update rate during the first 3 months following publication; this drops to no updates after 6 months. The customer wants to use CloudFront to improve his user’s load times. Which of the following recommendations would you make to the customer? **[PROFESSIONAL]**

1. Duplicate entries into two different buckets and create two separate CloudFront distributions where S3 access is restricted only to Cloud Front identity
2. Create a CloudFront distribution with “US & Europe” price class for US/Europe users and a different CloudFront distribution with All Edge Locations for the remaining users.
3. **Create a CloudFront distribution with S3 access restricted only to the CloudFront identity and partition the blog entry’s location in S3 according to the month it was uploaded to be used with CloudFront behaviors**
4. Create a CloudFront distribution with Restrict Viewer Access Forward Query string set to true and minimum TTL of 0.

 Your company has on-premises multi-tier PHP web application, which recently experienced downtime due to a large burst in web traffic due to a company announcement. Over the coming days, you are expecting similar announcements to drive similar unpredictable bursts, and are looking to find ways to quickly improve your infrastructures ability to handle unexpected increases in traffic. The application currently consists of 2 tiers a web tier, which consists of a load balancer, and several Linux Apache web servers as well as a database tier which hosts a Linux server hosting a MySQL database. Which scenario below will provide full site functionality, while helping to improve the ability of your application in the short timeframe required? **[PROFESSIONAL]**

1. **Offload traffic from on-premises environment Setup a CloudFront distribution and configure CloudFront to cache objects from a custom origin Choose to customize your object cache behavior, and select a TTL that objects should exist in cache.**
2. Migrate to AWS Use VM Import/Export to quickly convert an on-premises web server to an AMI create an Auto Scaling group, which uses the imported AMI to scale the web tier based on incoming traffic Create an RDS read replica and setup replication between the RDS instance and on-premises MySQL server to migrate the database.
3. Failover environment: Create an S3 bucket and configure it tor website hosting Migrate your DNS to Route53 using zone (lie import and leverage Route53 DNS failover to failover to the S3 hosted website.
4. Hybrid environment Create an AMI which can be used of launch web serfers in EC2 Create an Auto Scaling group which uses the \* AMI to scale the web tier based on incoming traffic Leverage Elastic Load Balancing to balance traffic between on-premises web servers and those hosted in AWS.

 You are building a system to distribute confidential training videos to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publically accessible from S3 directly?

1. **Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.**
2. Add the CloudFront account security group “amazon-cf/amazon-cf-sg” to the appropriate S3 bucket policy.
3. Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
4. Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

 A media production company wants to deliver high-definition raw video for preproduction and dubbing to customer all around the world. They would like to use Amazon CloudFront for their scenario, and they require the ability to limit downloads per customer and video file to a configurable number. A CloudFront download distribution with TTL=0 was already setup to make sure all client HTTP requests hit an authentication backend on Amazon Elastic Compute Cloud (EC2)/Amazon RDS first, which is responsible for restricting the number of downloads. Content is stored in S3 and configured to be accessible only via CloudFront. What else needs to be done to achieve an architecture that meets the requirements? Choose 2 answers **[PROFESSIONAL]**

1. **Enable URL parameter forwarding, let the authentication backend count the number of downloads per customer in RDS, and return the content S3 URL unless the download limit is reached.**
2. Enable CloudFront logging into an S3 bucket, leverage EMR to analyze CloudFront logs to determine the number of downloads per customer, and return the content S3 URL unless the download limit is reached. (CloudFront logs are logged periodically and EMR not being real time, hence not suitable)
3. Enable URL parameter forwarding, let the authentication backend count the number of downloads per customer in RDS, and invalidate the CloudFront distribution as soon as the download limit is reached. (Distribution are not invalidated but Objects)
4. Enable CloudFront logging into the S3 bucket, let the authentication backend determine the number of downloads per customer by parsing those logs, and return the content S3 URL unless the download limit is reached. (CloudFront logs are logged periodically and EMR not being real time, hence not suitable)
5. **Configure a list of trusted signers, let the authentication backend count the number of download requests per customer in RDS, and return a dynamically signed URL unless the download limit is reached.**

 Your customer is implementing a video on-demand streaming platform on AWS. The requirements are to support for multiple devices such as iOS, Android, and PC as client devices, using a standard client player, using streaming technology (not download) and scalable architecture with cost effectiveness **[PROFESSIONAL]**

1. Store the video contents to Amazon Simple Storage Service (S3) as an origin server. Configure the Amazon CloudFront distribution with a streaming option to stream the video contents
2. **Store the video contents to Amazon S3 as an origin server. Configure the Amazon CloudFront distribution with a download option to stream the video contents** (Refer [link](http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web.html))
3. Launch a streaming server on Amazon Elastic Compute Cloud (EC2) (for example, Adobe Media Server), and store the video contents as an origin server. Configure the Amazon CloudFront distribution with a download option to stream the video contents
4. Launch a streaming server on Amazon Elastic Compute Cloud (EC2) (for example, Adobe Media Server), and store the video contents as an origin server. Launch and configure the required amount of streaming servers on Amazon EC2 as an edge server to stream the video contents

 You are an architect for a news -sharing mobile application. Anywhere in the world, your users can see local news on of topics they choose. They can post pictures and videos from inside the application. Since the application is being used on a mobile phone, connection stability is required for uploading content, and delivery should be quick. Content is accessed a lot in the first minutes after it has been posted, but is quickly replaced by new content before disappearing. The local nature of the news means that 90 percent of the uploaded content is then read locally (less than a hundred kilometers from where it was posted). What solution will optimize the user experience when users upload and view content (by minimizing page load times and minimizing upload times)? **[PROFESSIONAL]**

1. Upload and store the content in a central Amazon Simple Storage Service (S3) bucket, and use an Amazon Cloud Front Distribution for content delivery.
2. Upload and store the content in an Amazon Simple Storage Service (S3) bucket in the region closest to the user, and use multiple Amazon Cloud Front distributions for content delivery.
3. Upload the content to an Amazon Elastic Compute Cloud (EC2) instance in the region closest to the user, send the content to a central Amazon Simple Storage Service (S3) bucket, and use an Amazon Cloud Front distribution for content delivery.
4. **Use an Amazon Cloud Front distribution for uploading the content to a central Amazon Simple Storage Service (S3) bucket and for content delivery.**

 To enable end-to-end HTTPS connections from the user‘s browser to the origin via CloudFront, which of the following options are valid? Choose 2 answers **[PROFESSIONAL]**

1. Use self signed certificate in the origin and CloudFront default certificate in CloudFront. (Origin cannot be self signed)
2. Use the CloudFront default certificate in both origin and CloudFront (CloudFront cert cannot be applied to origin)
3. **Use 3rd-party CA certificate in the origin and CloudFront default certificate in CloudFront**
4. **Use 3rd-party CA certificate in both origin and CloudFront**
5. Use a self signed certificate in both the origin and CloudFront (Origin cannot be self signed)

 Your application consists of 10% writes and 90% reads. You currently service all requests through a Route53 Alias Record directed towards an AWS ELB, which sits in front of an EC2 Auto Scaling Group. Your system is getting very expensive when there are large traffic spikes during certain news events, during which many more people request to read similar data all at the same time. What is the simplest and cheapest way to reduce costs and scale with spikes like this? **[PROFESSIONAL]**

1. Create an S3 bucket and asynchronously replicate common requests responses into S3 objects. When a request comes in for a precomputed response, redirect to AWS S3
2. Create another ELB and Auto Scaling Group layer mounted on top of the other system, adding a tier to the system. Serve most read requests out of the top layer
3. **Create a CloudFront Distribution and direct Route53 to the Distribution. Use the ELB as an Origin and specify Cache Behaviors to proxy cache requests, which can be served late.** (CloudFront can server request from cache and multiple cache behavior can be defined based on rules for a given URL pattern based on file extensions, file names, or any portion of a URL. Each cache behavior can include the CloudFront configuration values: origin server name, viewer connection protocol, minimum expiration period, query string parameters, cookies, and trusted signers for private content.)
4. Create a Memcached cluster in AWS ElastiCache. Create cache logic to serve requests, which can be served late from the in-memory cache for increased performance.

 You are designing a service that aggregates clickstream data in batch and delivers reports to subscribers via email only once per week. Data is extremely spikey, geographically distributed, high-scale, and unpredictable. How should you design this system?

1. Use a large RedShift cluster to perform the analysis, and a fleet of Lambdas to perform record inserts into the RedShift tables. Lambda will scale rapidly enough for the traffic spikes.
2. **Use a CloudFront distribution with access log delivery to S3. Clicks should be recorded as query string GETs to the distribution. Reports are built and sent by periodically running EMR jobs over the access logs in S3.** (CloudFront is a Gigabit-Scale HTTP(S) global request distribution service and works fine with peaks higher than 10 Gbps or 15,000 RPS. It can handle scale, geo-spread, spikes, and unpredictability. Access Logs will contain the GET data and work just fine for batch analysis and email using EMR. Other streaming options are expensive as not required as the need is to batch analyze)
3. Use API Gateway invoking Lambdas which PutRecords into Kinesis, and EMR running Spark performing GetRecords on Kinesis to scale with spikes. Spark on EMR outputs the analysis to S3, which are sent out via email.
4. Use AWS Elasticsearch service and EC2 Auto Scaling groups. The Autoscaling groups scale based on click throughput and stream into the Elasticsearch domain, which is also scalable. Use Kibana to generate reports periodically.

 Your website is serving on-demand training videos to your workforce. Videos are uploaded monthly in high resolution MP4 format. Your workforce is distributed globally often on the move and using company-provided tablets that require the HTTP Live Streaming (HLS) protocol to watch a video. Your company has no video transcoding expertise and it required you might need to pay for a consultant. How do you implement the most cost-efficient architecture without compromising high availability and quality of video delivery? **[PROFESSIONAL]**

1. **Elastic Transcoder to transcode original high-resolution MP4 videos to HLS. S3 to host videos with lifecycle Management to archive original flies to Glacier after a few days. CloudFront to serve HLS transcoded videos from S3**
2. A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number or nodes depending on the length of the queue S3 to host videos with Lifecycle Management to archive all files to Glacier after a few days CloudFront to serve HLS transcoding videos from Glacier
3. Elastic Transcoder to transcode original high-resolution MP4 videos to HLS EBS volumes to host videos and EBS snapshots to incrementally backup original rues after a few days. CloudFront to serve HLS transcoded videos from EC2.
4. A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queue. EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few days. CloudFront to serve HLS transcoded videos from EC2
5. You are developing a highly available web application using stateless web servers. Which services are suitable for storing session state data? Choose 3 answers.
   1. Elastic Load Balancing
   2. **Amazon Relational Database Service (RDS)**
   3. Amazon CloudWatch
   4. **Amazon ElastiCache**
   5. **Amazon DynamoDB**
   6. AWS Storage Gateway
6. Your firm has uploaded a large amount of aerial image data to S3. In the past, in your on-premises environment, you used a dedicated group of servers to oaten process this data and used Rabbit MQ, an open source messaging system, to get job information to the servers. Once processed the data would go to tape and be shipped offsite. Your manager told you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost. Which is correct? **[PROFESSIONAL]**
   1. Use SQS for passing job messages, use Cloud Watch alarms to terminate EC2 worker instances when they become idle. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.
   2. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.
   3. **Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS. Once data is processed, change the storage class of the S3 objects to Glacier.**
   4. Use SNS to pass job messages use Cloud Watch alarms to terminate spot worker instances when they become idle. Once data is processed, change the storage class of the S3 object to Glacier.
7. You are developing a new mobile application and are considering storing user preferences in AWS, which would provide a more uniform cross-device experience to users using multiple mobile devices to access the application. The preference data for each user is estimated to be 50KB in size. Additionally 5 million customers are expected to use the application on a regular basis. The solution needs to be cost-effective, highly available, scalable and secure, how would you design a solution to meet the above requirements? **[PROFESSIONAL]**
   1. Setup an RDS MySQL instance in 2 availability zones to store the user preference data. Deploy a public facing application on a server in front of the database to manage security and access credentials
   2. **Setup a DynamoDB table with an item for each user having the necessary attributes to hold the user preferences. The mobile application will query the user preferences directly from the DynamoDB table. Utilize STS. Web Identity Federation, and DynamoDB Fine Grained Access Control to authenticate and authorize access**
   3. Setup an RDS MySQL instance with multiple read replicas in 2 availability zones to store the user preference data .The mobile application will query the user preferences from the read replicas. Leverage the MySQL user management and access privilege system to manage security and access credentials.
   4. Store the user preference data in S3 Setup a DynamoDB table with an item for each user and an item attribute pointing to the user’ S3 object. The mobile application will retrieve the S3 URL from DynamoDB and then access the S3 object directly utilize STS, Web identity Federation, and S3 ACLs to authenticate and authorize access.
8. A company is building a voting system for a popular TV show, viewers would watch the performances then visit the show’s website to vote for their favorite performer. It is expected that in a short period of time after the show has finished the site will receive millions of visitors. The visitors will first login to the site using their Amazon.com credentials and then submit their vote. After the voting is completed the page will display the vote totals. The company needs to build the site such that can handle the rapid influx of traffic while maintaining good performance but also wants to keep costs to a minimum. Which of the design patterns below should they use? **[PROFESSIONAL]**
   1. Use CloudFront and an Elastic Load balancer in front of an auto-scaled set of web servers, the web servers will first can the Login With Amazon service to authenticate the user then process the users vote and store the result into a multi-AZ Relational Database Service instance.
   2. Use CloudFront and the static website hosting feature of S3 with the Javascript SDK to call the Login With Amazon service to authenticate the user, use IAM Roles to gain permissions to a DynamoDB table to store the users vote.
   3. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first call the Login with Amazon service to authenticate the user, the web servers will process the users vote and store the result into a DynamoDB table using IAM Roles for EC2 instances to gain permissions to the DynamoDB table.
   4. **Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first call the Login. With Amazon service to authenticate the user, the web servers would process the users vote and store the result into an SQS queue using IAM Roles for EC2 Instances to gain permissions to the SQS queue. A set of application servers will then retrieve the items from the queue and store the result into a DynamoDB table**
9. A large real-estate brokerage is exploring the option to adding a cost-effective location-based alert to their existing mobile application. The application backend infrastructure currently runs on AWS. Users who opt in to this service will receive alerts on their mobile device regarding real-estate offers in proximity to their location. For the alerts to be relevant delivery time needs to be in the low minute count. The existing mobile app has 5 million users across the US. Which one of the following architectural suggestions would you make to the customer? **[PROFESSIONAL]**
   1. Mobile application will submit its location to a web service endpoint utilizing Elastic Load Balancing and EC2 instances. DynamoDB will be used to store and retrieve relevant offers. EC2 instances will communicate with mobile earners/device providers to push alerts back to mobile application. —
   2. Use AWS Direct Connect or VPN to establish connectivity with mobile carriers EC2 instances will receive the mobile applications location through carrier connection: RDS will be used to store and relevant offers. EC2 instances will communicate with mobile carriers to push alerts back to the mobile application
   3. **Mobile application will send device location using SQS. EC2 instances will retrieve the relevant offers from DynamoDB. AWS Mobile Push will be used to send offers to the mobile application**
   4. Mobile application will send device location using AWS Mobile Push. EC2 instances will retrieve the relevant offers from DynamoDB. EC2 instances will communicate with mobile carriers/device providers to push alerts back to the mobile application.
10. You are running a news website in the eu-west-1 region that updates every 15 minutes. The website has a worldwide audience and it uses an Auto Scaling group behind an Elastic Load Balancer and an Amazon RDS database. Static content resides on Amazon S3, and is distributed through Amazon CloudFront. Your Auto Scaling group is set to trigger a scale up event at 60% CPU utilization; you use an Amazon RDS extra-large DB instance with 10.000 Provisioned IOPS its CPU utilization is around 80%. While freeable memory is in the 2 GB range. Web analytics reports show that the average load time of your web pages is around 1.5 to 2 seconds, but your SEO consultant wants to bring down the average load time to under 0.5 seconds. How would you improve page load times for your users? (Choose 3 answers) **[PROFESSIONAL]**
    1. Lower the scale up trigger of your Auto Scaling group to 30% so it scales more aggressively.
    2. **Add an Amazon ElastiCache caching layer to your application for storing sessions and frequent DB queries**
    3. **Configure Amazon CloudFront dynamic content support to enable caching of re-usable content from your site**
    4. **Switch Amazon RDS database to the high memory extra-large Instance type**
    5. Set up a second installation in another region, and use the Amazon Route 53 latency-based routing feature to select the right region.
11. A read only news reporting site with a combined web and application tier and a database tier that receives large and unpredictable traffic demands must be able to respond to these traffic fluctuations automatically. What AWS services should be used meet these requirements? **[PROFESSIONAL]**
    1. **Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaling group monitored with CloudWatch. And RDS with read replicas.**
    2. Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch and RDS with read replicas
    3. Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch. And multi-AZ RDS
    4. Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaling group monitored with CloudWatch and multi-AZ RDS
12. You have a periodic Image analysis application that gets some files as input, analyzes them and for each file writes some data in output to a ten file. The number of files in input per day is high and concentrated in a few hours of the day. Currently you have a server on EC2 with a large EBS volume that hosts the input data and the results it takes almost 20 hours per day to complete the process. What services could be used to reduce the elaboration time and improve the availability of the solution? **[PROFESSIONAL]**
    1. **S3 to store I/O files. SQS to distribute elaboration commands to a group of hosts working in parallel. Auto scaling to dynamically size the group of hosts depending on the length of the SQS queue**
    2. EBS with Provisioned IOPS (PIOPS) to store I/O files. SNS to distribute elaboration commands to a group of hosts working in parallel Auto Scaling to dynamically size the group of hosts depending on the number of SNS notifications
    3. S3 to store I/O files, SNS to distribute evaporation commands to a group of hosts working in parallel. Auto scaling to dynamically size the group of hosts depending on the number of SNS notifications
    4. EBS with Provisioned IOPS (PIOPS) to store I/O files SOS to distribute elaboration commands to a group of hosts working in parallel Auto Scaling to dynamically size the group to hosts depending on the length of the SQS queue.
13. A 3-tier e-commerce web application is current deployed on-premises and will be migrated to AWS for greater scalability and elasticity. The web server currently shares read-only data using a network distributed file system The app server tier uses a clustering mechanism for discovery and shared session state that depends on IP multicast The database tier uses shared-storage clustering to provide database fail over capability, and uses several read slaves for scaling. Data on all servers and the distributed file system directory is backed up weekly to off-site tapes. Which AWS storage and database architecture meets the requirements of the application? **[PROFESSIONAL]**
    1. Web servers store read-only data in S3, and copy from S3 to root volume at boot time. App servers share state using a combination of DynamoDB and IP unicast. Database use RDS with multi-AZ deployment and one or more Read Replicas. Backup web and app servers backed up weekly via AMIs, database backed up via DB snapshots.
    2. Web servers store read-only data in S3, and copy from S3 to root volume at boot time. App servers share state using a combination of DynamoDB and IP unicast. Database use RDS with multi-AZ deployment and one or more Read replicas. Backup web servers app servers, and database backed up weekly to Glacier using snapshots (Snapshots to Glacier don’t work directly with EBS snapshots)
    3. Web servers store read-only data in S3 and copy from S3 to root volume at boot time. App servers share state using a combination of DynamoDB and IP unicast. Database use RDS with multi-AZ deployment. Backup web and app servers backed up weekly via AMIs. Database backed up via DB snapshots (Need Read replicas for scalability and elasticity)
    4. Web servers, store read-only data in an EC2 NFS server, mount to each web server at boot time App servers share state using a combination of DynamoDB and IP multicast Database use RDS with multi-AZ deployment and one or more Read Replicas Backup web and app servers backed up weekly via AMIs database backed up via DB snapshots (IP multicast not available in AWS)
14. Our company is getting ready to do a major public announcement of a social media site on AWS. The website is running on EC2 instances deployed across multiple Availability Zones with a Multi-AZ RDS MySQL Extra Large DB Instance. The site performs a high number of small reads and writes per second and relies on an eventual consistency model. After comprehensive tests you discover that there is read contention on RDS MySQL. Which are the best approaches to meet these requirements? (Choose 2 answers) **[PROFESSIONAL]**
    1. **Deploy ElasticCache in-memory cache running in each availability zone**
    2. Implement sharding to distribute load to multiple RDS MySQL instances (Would distributed read write both, focus is on read contention)
    3. Increase the RDS MySQL Instance size and Implement provisioned IOPS (Would distributed read write both, focus is on read contention)
    4. **Add an RDS MySQL read replica in each availability zone**
15. Run 2-tier app with the following: an ELB, three web app server on EC2, and 1 MySQL RDS db. With grown load, db queries take longer and longer and slow down the overall response time for user request. What Options could speed up performance? (Choose 3) **[PROFESSIONAL]**
    1. **Create an RDS read-replica and redirect half of the database read request to it**
    2. **Cache database queries in amazon ElastiCache**
    3. Setup RDS in multi-availability zone mode.
    4. **Shard the database and distribute loads between shards.**
    5. Use amazon CloudFront to cache database queries.
16. You have a web application leveraging an Elastic Load Balancer (ELB) In front of the web servers deployed using an Auto Scaling Group Your database is running on Relational Database Service (RDS) The application serves out technical articles and responses to them in general there are more views of an article than there are responses to the article. On occasion, an article on the site becomes extremely popular resulting in significant traffic Increases that causes the site to go down. What could you do to help alleviate the pressure on the infrastructure while maintaining availability during these events? Choose 3 answers **[PROFESSIONAL]**
    1. **Leverage CloudFront for the delivery of the articles.**
    2. **Add RDS read-replicas for the read traffic going to your relational database**
    3. **Leverage Elastic Cache for caching the most frequently used data.**
    4. Use SQS to queue up the requests for the technical posts and deliver them out of the queue (does not process and would not be real time)
    5. Use Route53 health checks to fail over to an S3 bucket for an error page (more of an error handling then availability)
17. Your website is serving on-demand training videos to your workforce. Videos are uploaded monthly in high resolution MP4 format. Your workforce is distributed globally often on the move and using company-provided tablets that require the HTTP Live Streaming (HLS) protocol to watch a video. Your company has no video transcoding expertise and it required you might need to pay for a consultant. How do you implement the most cost-efficient architecture without compromising high availability and quality of video delivery? **[PROFESSIONAL]**
    1. **Elastic Transcoder to transcode original high-resolution MP4 videos to HLS. S3 to host videos with lifecycle Management to archive original flies to Glacier after a few days. CloudFront to serve HLS transcoded videos from S3** (Elastic Transcoder for High quality, S3 to host videos cheaply, Glacier for archives and CloudFront for high availability)
    2. A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number or nodes depending on the length of the queue S3 to host videos with Lifecycle Management to archive all files to Glacier after a few days CloudFront to serve HLS transcoding videos from Glacier
    3. Elastic Transcoder to transcode original high-resolution MP4 videos to HLS EBS volumes to host videos and EBS snapshots to incrementally backup original rues after a few days. CloudFront to serve HLS transcoded videos from EC2.
    4. A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queue. EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few days. CloudFront to serve HLS transcoded videos from EC2
18. To meet regulatory requirements, a pharmaceuticals company needs to archive data after a drug trial test is concluded. Each drug trial test may generate up to several thousands of files, with compressed file sizes ranging from 1 byte to 100MB. Once archived, data rarely needs to be restored, and on the rare occasion when restoration is needed, the company has 24 hours to restore specific files that match certain metadata. Searches must be possible by numeric file ID, drug name, participant names, date ranges, and other metadata. Which is the most cost-effective architectural approach that can meet the requirements? **[PROFESSIONAL]**
    1. Store individual files in Amazon Glacier, using the file ID as the archive name. When restoring data, query the Amazon Glacier vault for files matching the search criteria. (Individual files are expensive and does not allow searching by participant names etc)
    2. Store individual files in Amazon S3, and store search metadata in an Amazon Relational Database Service (RDS) multi-AZ database. Create a lifecycle rule to move the data to Amazon Glacier after a certain number of days. When restoring data, query the Amazon RDS database for files matching the search criteria, and move the files matching the search criteria back to S3 Standard class. (As the data is not needed can be stored to Glacier directly and the data need not be moved back to S3 standard)
    3. Store individual files in Amazon Glacier, and store the search metadata in an Amazon RDS multi-AZ database. When restoring data, query the Amazon RDS database for files matching the search criteria, and retrieve the archive name that matches the file ID returned from the database query. (Individual files and Multi-AZ is expensive)
    4. **First, compress and then concatenate all files for a completed drug trial test into a single Amazon Glacier archive. Store the associated byte ranges for the compressed files along with other search metadata in an Amazon RDS database with regular snapshotting. When restoring data, query the database for files that match the search criteria, and create restored files from the retrieved byte ranges.**
    5. Store individual compressed files and search metadata in Amazon Simple Storage Service (S3). Create a lifecycle rule to move the data to Amazon Glacier, after a certain number of days. When restoring data, query the Amazon S3 bucket for files matching the search criteria, and retrieve the file to S3 reduced redundancy in order to move it back to S3 Standard class. (Once the data is moved from S3 to Glacier the metadata is lost, as Glacier does not have metadata and must be maintained externally)
19. A document storage company is deploying their application to AWS and changing their business model to support both free tier and premium tier users. The premium tier users will be allowed to store up to 200GB of data and free tier customers will be allowed to store only 5GB. The customer expects that billions of files will be stored. All users need to be alerted when approaching 75 percent quota utilization and again at 90 percent quota use. To support the free tier and premium tier users, how should they architect their application? **[PROFESSIONAL]**
    1. **The company should utilize an amazon simple work flow service activity worker that updates the users data counter in amazon dynamo DB. The activity worker will use simple email service to send an email if the counter increases above the appropriate thresholds.**
    2. The company should deploy an amazon relational data base service relational database with a store objects table that has a row for each stored object along with size of each object. The upload server will query the aggregate consumption of the user in questions by first determining the files store by the user, and then querying the stored objects table for respective file sizes) and send an email via amazon simple email service if the thresholds are breached.
    3. The company should write both the content length and the username of the files owner as S3 metadata for the object. They should then create a file watcher to iterate over each object and aggregate the size for each user and send a notification via amazon simple queue service to an emailing service if the storage threshold is exceeded.
    4. The company should create two separated amazon simple storage service buckets one for data storage for free tier users and another for data storage for premium tier users. An amazon simple workflow service activity worker will query all objects for a given user based on the bucket the data is stored
20. Your company has been contracted to develop and operate a website that tracks NBA basketball statistics. Statistical data to derive reports like “best game-winning shots from the regular season” and more frequently built reports like “top shots of the game” need to be stored durably for repeated lookup. Leveraging social media techniques, NBA fans submit and vote on new report types from the existing data set so the system needs to accommodate variability in data queries and new static reports must be generated and posted daily. Initial research in the design phase indicates that there will be over 3 million report queries on game day by end users and other applications that use this application as a data source. It is expected that this system will gain in popularity over time and reach peaks of 10-15 million report queries of the system on game days. Select the answer that will allow your application to best meet these requirements while minimizing costs. **[PROFESSIONAL]**
    1. Launch a multi-AZ MySQL Amazon Relational Database Service (RDS) Read Replica connected to your multi AZ master database and generate reports by querying the Read Replica. Perform a daily table cleanup.
    2. Implement a multi-AZ MySQL RDS deployment and have the application generate reports from Amazon ElastiCache for in-memory performance results. Utilize the default expire parameter for items in the cache.
    3. **Generate reports from a multi-AZ MySQL Amazon RDS deployment and have an offline task put reports in Amazon Simple Storage Service (S3) and use CloudFront to cache the content. Use a TTL to expire objects daily.** (Offline task with S3 storage and CloudFront cache)
    4. Query a multi-AZ MySQL RDS instance and store the results in a DynamoDB table. Generate reports from the DynamoDB table. Remove stale tables daily.
21. Instance A and instance B are running in two different subnets A and B of a VPC. Instance A is not able to ping instance B. What are two possible reasons for this? (Pick 2 correct answers)
    1. The routing table of subnet A has no target route to subnet B
    2. **The security group attached to instance B does not allow inbound ICMP traffic**
    3. The policy linked to the IAM role on instance A is not configured correctly
    4. **The NACL on subnet B does not allow outbound ICMP traffic**
22. An instance is launched into a VPC subnet with the network ACL configured to allow all inbound traffic and deny all outbound traffic. The instance’s security group is configured to allow SSH from any IP address and deny all outbound traffic. What changes need to be made to allow SSH access to the instance?
    1. The outbound security group needs to be modified to allow outbound traffic.
    2. **The outbound network ACL needs to be modified to allow outbound traffic.**
    3. Nothing, it can be accessed from any IP address using SSH.
    4. Both the outbound security group and outbound network ACL need to be modified to allow outbound traffic.
23. From what services I can block incoming/outgoing IPs?
    1. Security Groups
    2. DNS
    3. ELB
    4. VPC subnet
    5. IGW
    6. **NACL**
24. What is the difference between a security group in VPC and a network ACL in VPC (chose 3 correct answers)
    1. Security group restricts access to a Subnet while ACL restricts traffic to EC2
    2. **Security group restricts access to EC2 while ACL restricts traffic to a subnet**
    3. Security group can work outside the VPC also while ACL only works within a VPC
    4. **Network ACL performs stateless filtering and Security group provides stateful filtering**
    5. **Security group can only set Allow rule, while ACL can set Deny rule also**
25. You are currently hosting multiple applications in a VPC and have logged numerous port scans coming in from a specific IP address block. Your security team has requested that all access from the offending IP address block be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP address block?
    1. Create an AD policy to modify Windows Firewall settings on all hosts in the VPC to deny access from the IP address block
    2. **Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP address block**
    3. Add a rule to all of the VPC 5 Security Groups to deny access from the IP address block
    4. Modify the Windows Firewall settings on all Amazon Machine Images (AMIs) that your organization uses in that VPC to deny access from the IP address block
26. You have two Elastic Compute Cloud (EC2) instances inside a Virtual Private Cloud (VPC) in the same Availability Zone (AZ) but in different subnets. One instance is running a database and the other instance an application that will interface with the database. You want to confirm that they can talk to each other for your application to work properly. Which two things do we need to confirm in the VPC settings so that these EC2 instances can communicate inside the VPC? Choose 2 answers
    1. **A network ACL that allows communication between the two subnets.**
    2. Both instances are the same instance class and using the same Key-pair.
    3. That the default route is set to a NAT instance or Internet Gateway (IGW) for them to communicate.
    4. **Security groups are set to allow the application host to talk to the database on the right port/protocol**
27. A benefits enrollment company is hosting a 3-tier web application running in a VPC on AWS, which includes a NAT (Network Address Translation) instance in the public Web tier. There is enough provisioned capacity for the expected workload tor the new fiscal year benefit enrollment period plus some extra overhead Enrollment proceeds nicely for two days and then the web tier becomes unresponsive, upon investigation using CloudWatch and other monitoring tools it is discovered that there is an extremely large and unanticipated amount of inbound traffic coming from a set of 15 specific IP addresses over port 80 from a country where the benefits company has no customers. The web tier instances are so overloaded that benefit enrollment administrators cannot even SSH into them. Which activity would be useful in defending against this attack?
    1. Create a custom route table associated with the web tier and block the attacking IP addresses from the IGW (internet Gateway)
    2. Change the EIP (Elastic IP Address) of the NAT instance in the web tier subnet and update the Main Route Table with the new EIP
    3. Create 15 Security Group rules to block the attacking IP addresses over port 80
    4. **Create an inbound NACL (Network Access control list) associated with the web tier subnet with deny rules to block the attacking IP addresses**
28. Which of the following statements describes network ACLs? (Choose 2 answers)
    1. Responses to allowed inbound traffic are allowed to flow outbound regardless of outbound rules, and vice versa (are stateless)
    2. **Using network ACLs, you can deny access from a specific IP range**
    3. **Keep network ACL rules simple and use a security group to restrict application level access**
    4. NACLs are associated with a single Availability Zone (associated with Subnet)
29. You are designing security inside your VPC. You are considering the options for establishing separate security zones and enforcing network traffic rules across different zone to limit Instances can communications.  How would you accomplish these requirements? Choose 2 answers
    1. Configure a security group for every zone. Configure a default allow all rule. Configure explicit deny rules for the zones that shouldn’t be able to communicate with one another (Security group does not allow deny rules)
    2. **Configure you instances to use pre-set IP addresses with an IP address range every security zone. Configure NACL to explicitly allow or deny communication between the different IP address ranges, as required for interzone communication**
    3. **Configure a security group for every zone. Configure allow rules only between zone that need to be able to communicate with one another. Use implicit deny all rule to block any other traffic**
    4. Configure multiple subnets in your VPC, one for each zone. Configure routing within your VPC in such a way that each subnet only has routes to other subnets with which it needs to communicate, and doesn’t have routes to subnets with which it shouldn’t be able to communicate. (default routes are unmodifiable)
30. Your entire AWS infrastructure lives inside of one Amazon VPC. You have an Infrastructure monitoring application running on an Amazon instance in Availability Zone (AZ) A of the region, and another application instance running in AZ B. The monitoring application needs to make use of ICMP ping to confirm network reachability of the instance hosting the application. Can you configure the security groups for these instances to only allow the ICMP ping to pass from the monitoring instance to the application instance and nothing else” If so how?
    1. No Two instances in two different AZ’s can’t talk directly to each other via ICMP ping as that protocol is not allowed across subnet (i.e. broadcast) boundaries (Can communicate)
    2. Yes Both the monitoring instance and the application instance have to be a part of the same security group, and that security group needs to allow inbound ICMP (Need not have to be part of same security group)
    3. **Yes, The security group for the monitoring instance needs to allow outbound ICMP and the application instance’s security group needs to allow Inbound ICMP** (is stateful, so just allow outbound ICMP from monitoring and inbound ICMP on monitored instance)
    4. Yes, Both the monitoring instance’s security group and the application instance’s security group need to allow both inbound and outbound ICMP ping packets since ICMP is not a connection-oriented protocol (Security groups are stateful)
31. A user has configured a VPC with a new subnet. The user has created a security group. The user wants to configure that instances of the same subnet communicate with each other. How can the user configure this with the security group?
    1. There is no need for a security group modification as all the instances can communicate with each other inside the same subnet
    2. Configure the subnet as the source in the security group and allow traffic on all the protocols and ports
    3. **Configure the security group itself as the source and allow traffic on all the protocols and ports**
    4. The user has to use VPC peering to configure this
32. You are designing a data leak prevention solution for your VPC environment. You want your VPC Instances to be able to access software depots and distributions on the Internet for product updates. The depots and distributions are accessible via third party CDNs by their URLs. You want to explicitly deny any other outbound connections from your VPC instances to hosts on the Internet. Which of the following options would you consider?
    1. **Configure a web proxy server in your VPC and enforce URL-based rules for outbound access Remove default routes.** (Security group and NACL cannot have URLs in the rules nor does the route)
    2. Implement security groups and configure outbound rules to only permit traffic to software depots.
    3. Move all your instances into private VPC subnets remove default routes from all routing tables and add specific routes to the software depots and distributions only.
    4. Implement network access control lists to all specific destinations, with an Implicit deny as a rule.
33. You have an EC2 Security Group with several running EC2 instances. You change the Security Group rules to allow inbound traffic on a new port and protocol, and launch several new instances in the same Security Group. The new rules apply:
    1. **Immediately to all instances in the security group.**
    2. Immediately to the new instances only.
    3. Immediately to the new instances, but old instances must be stopped and restarted before the new rules apply.
    4. To all instances, but it may take several minutes for old instances to see the changes.

 A photo-sharing service stores pictures in Amazon Simple Storage Service (S3) and allows application sign-in using an OpenID Connect-compatible identity provider. Which AWS Security Token Service approach to temporary access should you use for the Amazon S3 operations?

1. SAML-based Identity Federation
2. Cross-Account Access
3. AWS IAM users
4. **Web Identity Federation**

 Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?

1. Use an IAM policy that references the LDAP account identifiers and the AWS credentials.
2. Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP
3. **Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials**. (Refer [Link](https://aws.amazon.com/blogs/aws/aws-identity-and-access-management-now-with-identity-federation/))
4. Use IAM roles to automatically rotate the IAM credentials when LDAP credentials are updated.
5. Use the LDAP credentials to restrict a group of users from launching specific EC2 instance types.

 You are designing a photo sharing mobile app the application will store all pictures in a single Amazon S3 bucket. Users will upload pictures from their mobile device directly to Amazon S3 and will be able to view and download their own pictures directly from Amazon S3. You want to configure security to handle potentially millions of users in the most secure manner possible. What should your server-side application do when a new user registers on the photo-sharing mobile application? **[PROFESSIONAL]**

1. Create a set of long-term credentials using AWS Security Token Service with appropriate permissions Store these credentials in the mobile app and use them to access Amazon S3.
2. **Record the user’s Information in Amazon RDS and create a role in IAM with appropriate permissions. When the user uses their mobile app create temporary credentials using the AWS Security Token Service ‘AssumeRole’ function. Store these credentials in the mobile app’s memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.**
3. Record the user’s Information in Amazon DynamoDB. When the user uses their mobile app create temporary credentials using AWS Security Token Service with appropriate permissions. Store these credentials in the mobile app’s memory and use them to access Amazon S3 Generate new credentials the next time the user runs the mobile app.
4. Create IAM user. Assign appropriate permissions to the IAM user Generate an access key and secret key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.
5. Create an IAM user. Update the bucket policy with appropriate permissions for the IAM user Generate an access Key and secret Key for the IAM user, store them In the mobile app and use these credentials to access Amazon S3.

 Your company has recently extended its datacenter into a VPC on AWS to add burst computing capacity as needed Members of your Network Operations Center need to be able to go to the AWS Management Console and administer Amazon EC2 instances as necessary. You don’t want to create new IAM users for each NOC member and make those users sign in again to the AWS Management Console. Which option below will meet the needs for your NOC members? **[PROFESSIONAL]**

1. Use OAuth 2.0 to retrieve temporary AWS security credentials to enable your NOC members to sign in to the AWS Management Console.
2. Use Web Identity Federation to retrieve AWS temporary security credentials to enable your NOC members to sign in to the AWS Management Console.
3. **Use your on-premises SAML 2.O-compliant identity provider (IDP) to grant the NOC members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint.**
4. Use your on-premises SAML 2.0-compliant identity provider (IDP) to retrieve temporary security credentials to enable NOC members to sign in to the AWS Management Console

 A corporate web application is deployed within an Amazon Virtual Private Cloud (VPC) and is connected to the corporate data center via an iPsec VPN. The application must authenticate against the on-premises LDAP server. After authentication, each logged-in user can only access an Amazon Simple Storage Space (S3) keyspace specific to that user. Which two approaches can satisfy these objectives? (Choose 2 answers) **[PROFESSIONAL]**

1. Develop an identity broker that authenticates against IAM security Token service to assume a IAM role in order to get temporary AWS security credentials. The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket. (Needs to authenticate against LDAP and not IAM)
2. **The application authenticates against LDAP and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service to assume that IAM role. The application can use the temporary credentials to access the appropriate S3 bucket.** (Authenticates with LDAP and calls the AssumeRole)
3. **Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service to get IAM federated user credentials The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.** (Custom Identity broker implementation, with authentication with LDAP and using federated token)
4. The application authenticates against LDAP the application then calls the AWS identity and Access Management (IAM) Security Token service to log in to IAM using the LDAP credentials the application can use the IAM temporary credentials to access the appropriate S3 bucket. (Can’t login to IAM using LDAP credentials)
5. The application authenticates against IAM Security Token Service using the LDAP credentials the application uses those temporary AWS security credentials to access the appropriate S3 bucket. (Need to authenticate with LDAP)

 Company B is launching a new game app for mobile devices. Users will log into the game using their existing social media account to streamline data capture. Company B would like to directly save player data and scoring information from the mobile app to a DynamoDB table named Score Data When a user saves their game the progress data will be stored to the Game state S3 bucket. what is the best approach for storing data to DynamoDB and S3? **[PROFESSIONAL]**

1. Use an EC2 Instance that is launched with an EC2 role providing access to the Score Data DynamoDB table and the GameState S3 bucket that communicates with the mobile app via web services.
2. **Use temporary security credentials that assume a role providing access to the Score Data DynamoDB table and the Game State S3 bucket using web identity federation**
3. Use Login with Amazon allowing users to sign in with an Amazon account providing the mobile app with access to the Score Data DynamoDB table and the Game State S3 bucket.
4. Use an IAM user with access credentials assigned a role providing access to the Score Data DynamoDB table and the Game State S3 bucket for distribution with the mobile app.

 A user has created a mobile application which makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK and root account access/secret access key to connect to DynamoDB from mobile. Which of the below mentioned statements is true with respect to the best practice for security in this scenario?

1. User should create a separate IAM user for each mobile application and provide DynamoDB access with it
2. User should create an IAM role with DynamoDB and EC2 access. Attach the role with EC2 and route all calls from the mobile through EC2
3. **The application should use an IAM role with web identity federation which validates calls to DynamoDB with identity providers, such as Google, Amazon, and Facebook**
4. Create an IAM Role with DynamoDB access and attach it with the mobile application

 You are managing the AWS account of a big organization. The organization has more than 1000+ employees and they want to provide access to the various services to most of the employees. Which of the below mentioned options is the best possible solution in this case?

1. The user should create a separate IAM user for each employee and provide access to them as per the policy
2. The user should create an IAM role and attach STS with the role. The user should attach that role to the EC2 instance and setup AWS authentication on that server
3. The user should create IAM groups as per the organization’s departments and add each user to the group for better access control
4. **Attach an IAM role with the organization’s authentication service to authorize each user for various AWS services**

 Your fortune 500 company has under taken a TCO analysis evaluating the use of Amazon S3 versus acquiring more hardware The outcome was that all employees would be granted access to use Amazon S3 for storage of their personal documents. Which of the following will you need to consider so you can set up a solution that incorporates single sign-on from your corporate AD or LDAP directory and restricts access for each user to a designated user folder in a bucket? (Choose 3 Answers) **[PROFESSIONAL]**

1. **Setting up a federation proxy or identity provider**
2. **Using AWS Security Token Service to generate temporary tokens**
3. Tagging each folder in the bucket
4. **Configuring IAM role**
5. Setting up a matching IAM user for every user in your corporate directory that needs access to a folder in the bucket

 An AWS customer is deploying a web application that is composed of a front-end running on Amazon EC2 and of confidential data that is stored on Amazon S3. The customer security policy that all access operations to this sensitive data must be authenticated and authorized by a centralized access management system that is operated by a separate security team. In addition, the web application team that owns and administers the EC2 web front-end instances is prohibited from having any ability to access the data that circumvents this centralized access management system. Which of the following configurations will support these requirements? **[PROFESSIONAL]**

1. Encrypt the data on Amazon S3 using a CloudHSM that is operated by the separate security team. Configure the web application to integrate with the CloudHSM for decrypting approved data access operations for trusted end-users. (S3 doesn’t integrate directly with CloudHSM, also there is no centralized access management system control)
2. **Configure the web application to authenticate end-users against the centralized access management system. Have the web application provision trusted users STS tokens entitling the download of approved data directly from Amazon S3** (Controlled access and admins cannot access the data as it needs authentication)
3. Have the separate security team create and IAM role that is entitled to access the data on Amazon S3. Have the web application team provision their instances with this role while denying their IAM users access to the data on Amazon S3 (Web team would have access to the data)
4. Configure the web application to authenticate end-users against the centralized access management system using SAML. Have the end-users authenticate to IAM using their SAML token and download the approved data directly from S3. (not the way SAML auth works and not sure if the centralized access management system is SAML complaint)

 What is web identity federation?

1. Use of an identity provider like Google or Facebook to become an AWS IAM User.
2. **Use of an identity provider like Google or Facebook to exchange for temporary AWS security credentials.**
3. Use of AWS IAM User tokens to log in as a Google or Facebook user.
4. Use of AWS STS Tokens to log in as a Google or Facebook user.

 Games-R-Us is launching a new game app for mobile devices. Users will log into the game using their existing Facebook account and the game will record player data and scoring information directly to a DynamoDB table. What is the most secure approach for signing requests to the DynamoDB API?

1. Create an IAM user with access credentials that are distributed with the mobile app to sign the requests
2. Distribute the AWS root account access credentials with the mobile app to sign the requests
3. **Request temporary security credentials using web identity federation to sign the requests**
4. Establish cross account access between the mobile app and the DynamoDB table to sign the requests

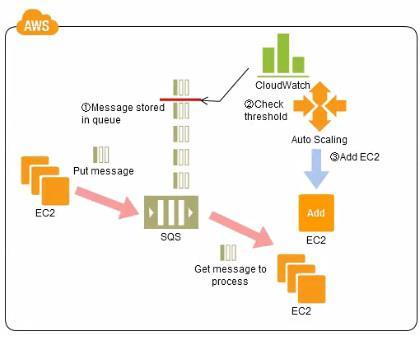
 You are building a mobile app for consumers to post cat pictures online. You will be storing the images in AWS S3. You want to run the system very cheaply and simply. Which one of these options allows you to build a photo sharing application without needing to worry about scaling expensive uploads processes, authentication/authorization and so forth?

1. **Build the application out using AWS Cognito and web identity federation to allow users to log in using Facebook or Google Accounts. Once they are logged in, the secret token passed to that user is used to directly access resources on AWS, like AWS S3.** (Amazon Cognito is a superset of the functionality provided by web identity federation. Refer [link](https://blogs.aws.amazon.com/security/post/Tx3SYCORF5EKRC0/How-Does-Amazon-Cognito-Relate-to-Existing-Web-Identity-Federation))
2. Use JWT or SAML compliant systems to build authorization policies. Users log in with a username and password, and are given a token they can use indefinitely to make calls against the photo infrastructure.
3. Use AWS API Gateway with a constantly rotating API Key to allow access from the client-side. Construct a custom build of the SDK and include S3 access in it.
4. Create an AWS oAuth Service Domain ad grant public signup and access to the domain. During setup, add at least one major social media site as a trusted Identity Provider for users.

 The Marketing Director in your company asked you to create a mobile app that lets users post sightings of good deeds known as random acts of kindness in 80-character summaries. You decided to write the application in JavaScript so that it would run on the broadest range of phones, browsers, and tablets. Your application should provide access to Amazon DynamoDB to store the good deed summaries. Initial testing of a prototype shows that there aren’t large spikes in usage. Which option provides the most cost-effective and scalable architecture for this application? **[PROFESSIONAL]**

1. Provide the JavaScript client with temporary credentials from the Security Token Service using a Token Vending Machine (TVM) on an EC2 instance to provide signed credentials mapped to an Amazon Identity and Access Management (IAM) user allowing DynamoDB puts and S3 gets. You serve your mobile application out of an S3 bucket enabled as a web site. Your client updates DynamoDB. (Single EC2 instance not a scalable architecture)
2. **Register the application with a Web Identity Provider like Amazon, Google, or Facebook, create an IAM role for that provider, and set up permissions for the IAM role to allow S3 gets and DynamoDB puts. You serve your mobile application out of an S3 bucket enabled as a web site. Your client updates DynamoDB.** (Can work with JavaScript SDK, is scalable and cost effective)
3. Provide the JavaScript client with temporary credentials from the Security Token Service using a Token Vending Machine (TVM) to provide signed credentials mapped to an IAM user allowing DynamoDB puts. You serve your mobile application out of Apache EC2 instances that are load-balanced and autoscaled. Your EC2 instances are configured with an IAM role that allows DynamoDB puts. Your server updates DynamoDB. (Is Scalable but Not cost effective)
4. Register the JavaScript application with a Web Identity Provider like Amazon, Google, or Facebook, create an IAM role for that provider, and set up permissions for the IAM role to allow DynamoDB puts. You serve your mobile application out of Apache EC2 instances that are load-balanced and autoscaled. Your EC2 instances are configured with an IAM role that allows DynamoDB puts. Your server updates DynamoDB. (Is Scalable but Not cost effective)
5. A company is building software on AWS that requires access to various AWS services. Which configuration should be used to ensure that AWS credentials (i.e., Access Key ID/Secret Access Key combination) are not compromised?
   1. Enable Multi-Factor Authentication for your AWS root account.
   2. **Assign an IAM role to the Amazon EC2 instance.**
   3. Store the AWS Access Key ID/Secret Access Key combination in software comments.
   4. Assign an IAM user to the Amazon EC2 Instance.
6. A company is preparing to give AWS Management Console access to developers. Company policy mandates identity federation and role-based access control. Roles are currently assigned using groups in the corporate Active Directory. What combination of the following will give developers access to the AWS console? (Select 2) Choose 2 answers
   1. **AWS Directory Service AD Connector**
   2. AWS Directory Service Simple AD
   3. AWS Identity and Access Management groups
   4. **AWS identity and Access Management roles**
   5. AWS identity and Access Management users
7. A customer needs corporate IT governance and cost oversight of all AWS resources consumed by its divisions. The divisions want to maintain administrative control of the discrete AWS resources they consume and keep those resources separate from the resources of other divisions. Which of the following options, when used together will support the autonomy/control of divisions while enabling corporate IT to maintain governance and cost oversight? Choose 2 answers
   1. Use AWS Consolidated Billing and disable AWS root account access for the child accounts.
   2. **Enable IAM cross-account access for all corporate IT administrators in each child account.** (Provides IT governance)
   3. Create separate VPCs for each division within the corporate IT AWS account.
   4. **Use AWS Consolidated Billing to link the divisions’ accounts to a parent corporate account.** (Will provide cost oversight)
   5. Write all child AWS CloudTrail and Amazon CloudWatch logs to each child account’s Amazon S3 ‘Log’ bucket.
8. Which of the following items are required to allow an application deployed on an EC2 instance to write data to a DynamoDB table? Assume that no security keys are allowed to be stored on the EC2 instance. (Choose 2 answers)
   1. **Create an IAM Role that allows write access to the DynamoDB table**
   2. **Add an IAM Role to a running EC2 instance.** (With latest enhancement from AWS, IAM role can be assigned to a running EC2 instance)
   3. Create an IAM User that allows write access to the DynamoDB table.
   4. Add an IAM User to a running EC2 instance.
   5. Launch an EC2 Instance with the IAM Role included in the launch configuration (This was the correct answer before, as AWS did not allow IAM role to be added to an existing instance)
9. You are looking to migrate your Development (Dev) and Test environments to AWS. You have decided to use separate AWS accounts to host each environment. You plan to link each accounts bill to a Master AWS account using Consolidated Billing. To make sure you Keep within budget you would like to implement a way for administrators in the Master account to have access to stop, delete and/or terminate resources in both the Dev and Test accounts. Identify which option will allow you to achieve this goal. **[PROFESSIONAL]**
   1. Create IAM users in the Master account with full Admin permissions. Create cross-account roles in the Dev and Test accounts that grant the Master account access to the resources in the account by inheriting permissions from the Master account.
   2. Create IAM users and a cross-account role in the Master account that grants full Admin permissions to the Dev and Test accounts.
   3. **Create IAM users in the Master account Create cross-account roles in the Dev and Test accounts that have full Admin permissions and grant the Master account access**
   4. Link the accounts using Consolidated Billing. This will give IAM users in the Master account access to resources in the Dev and Test accounts
10. You have an application running on an EC2 Instance which will allow users to download flies from a private S3 bucket using a pre-assigned URL. Before generating the URL the application should verify the existence of the file in S3. How should the application use AWS credentials to access the S3 bucket securely? **[PROFESSIONAL]**
    1. Use the AWS account access Keys the application retrieves the credentials from the source code of the application.
    2. Create a IAM user for the application with permissions that allow list access to the S3 bucket launch the instance as the IAM user and retrieve the IAM user’s credentials from the EC2 instance user data.
    3. **Create an IAM role for EC2 that allows list access to objects in the S3 bucket. Launch the instance with the role, and retrieve the role’s credentials from the EC2 Instance metadata**
    4. Create an IAM user for the application with permissions that allow list access to the S3 bucket. The application retrieves the IAM user credentials from a temporary directory with permissions that allow read access only to the application user.
11. An administrator is using Amazon CloudFormation to deploy a three tier web application that consists of a web tier and application tier that will utilize Amazon DynamoDB for storage when creating the CloudFormation template which of the following would allow the application instance access to the DynamoDB tables without exposing API credentials?  **[PROFESSIONAL]**
    1. Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and associate the Role to the application instances by referencing an instance profile.
    2. Use the Parameter section in the Cloud Formation template to nave the user input Access and Secret Keys from an already created IAM user that has me permissions required to read and write from the required DynamoDB table.
    3. **Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and reference the Role in the instance profile property of the application instance.**
    4. Create an identity and Access Management user in the CloudFormation template that has permissions to read and write from the required DynamoDB table, use the GetAtt function to retrieve the Access and secret keys and pass them to the application instance through user-data.
12. An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise’s account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions? **[PROFESSIONAL]**
    1. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.
    2. Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS application create a new access and secret key for the user and provide these credentials to the SaaS provider.
    3. **Create an IAM role for cross-account access allows the SaaS provider’s account to assume the role and assign it a policy that allows only the actions required by the SaaS application.**
    4. Create an IAM role for EC2 instances, assign it a policy mat allows only the actions required tor the SaaS application to work, provide the role ARM to the SaaS provider to use when launching their application instances.
13. A user has created an application which will be hosted on EC2. The application makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK to connect with from the EC2 instance. Which of the below mentioned statements is true with respect to the best practice for security in this scenario?
    1. **The user should attach an IAM role with DynamoDB access to the EC2 instance**
    2. The user should create an IAM user with DynamoDB access and use its credentials within the application to connect with DynamoDB
    3. The user should create an IAM role, which has EC2 access so that it will allow deploying the application
    4. The user should create an IAM user with DynamoDB and EC2 access. Attach the user with the application so that it does not use the root account credentials
14. A customer is in the process of deploying multiple applications to AWS that are owned and operated by different development teams. Each development team maintains the authorization of its users independently from other teams. The customer’s information security team would like to be able to delegate user authorization to the individual development teams but independently apply restrictions to the users permissions based on factors such as the users device and location. For example, the information security team would like to grant read-only permissions to a user who is defined by the development team as read/write whenever the user is authenticating from outside the corporate network. What steps can the information security team take to implement this capability? **[PROFESSIONAL]**
    1. Operate an authentication service that generates AWS STS tokens with IAM policies from application-defined IAM roles. (no user separation, will just help generate temporary tokens)
    2. **Add additional IAM policies to the application IAM roles that deny user privileges based on information security policy.** (Different policy with deny rules based on location, device and more restrictive wins)
    3. Configure IAM policies that restrict modification of the application IAM roles only to the information security team. (Authorization should still be in developers control)
    4. Enable federation with the internal LDAP directory and grant the application teams permissions to modify users.
15. You are creating an Auto Scaling group whose Instances need to insert a custom metric into CloudWatch. Which method would be the best way to authenticate your CloudWatch PUT request?
    1. **Create an IAM role with the Put MetricData permission and modify the Auto Scaling launch configuration to launch instances in that role**
    2. Create an IAM user with the PutMetricData permission and modify the Auto Scaling launch configuration to inject the users credentials into the instance User Data
    3. Modify the appropriate Cloud Watch metric policies to allow the Put MetricData permission to instances from the Auto Scaling group
    4. Create an IAM user with the PutMetricData permission and put the credentials in a private repository and have applications on the server pull the credentials as needed
16. A user has configured an HTTPS listener on an ELB. The user has not configured any security policy which can help to negotiate SSL between the client and ELB. What will ELB do in this scenario?
    1. By default ELB will select the first version of the security policy
    2. **By default ELB will select the latest version of the policy**
    3. ELB creation will fail without a security policy
    4. It is not required to have a security policy since SSL is already installed
17. A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. The ELB security policy supports various ciphers. Which of the below mentioned options helps identify the matching cipher at the client side to the ELB cipher list when client is requesting ELB DNS over SSL
    1. Cipher Protocol
    2. Client Configuration Preference
    3. **Server Order Preference**
    4. Load Balancer Preference
18. A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. Which of the below mentioned security policies is supported by ELB?
    1. Dynamic Security Policy
    2. All the other options
    3. **Predefined Security Policy**
    4. Default Security Policy
19. A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. Which of the below mentioned SSL protocols is not supported by the security policy?
    1. **TLS 1.3**
    2. TLS 1.2
    3. SSL 2.0
    4. SSL 3.0
20. A user has configured ELB with a TCP listener at ELB as well as on the back-end instances. The user wants to enable a proxy protocol to capture the source and destination IP information in the header. Which of the below mentioned statements helps the user understand a proxy protocol with TCP configuration?
    1. **If the end user is requesting behind a proxy server then the user should not enable a proxy protocol on ELB**
    2. ELB does not support a proxy protocol when it is listening on both the load balancer and the back-end instances
    3. Whether the end user is requesting from a proxy server or directly, it does not make a difference for the proxy protocol
    4. If the end user is requesting behind the proxy then the user should add the “isproxy” flag to the ELB Configuration
21. A user has enabled session stickiness with ELB. The user does not want ELB to manage the cookie; instead he wants the application to manage the cookie. What will happen when the server instance, which is bound to a cookie, crashes?
    1. The response will have a cookie but stickiness will be deleted
    2. **The session will not be sticky until a new cookie is inserted**
    3. ELB will throw an error due to cookie unavailability
    4. The session will be sticky and ELB will route requests to another server as ELB keeps replicating the Cookie
22. A user has created an ELB with Auto Scaling. Which of the below mentioned offerings from ELB helps the user to stop sending new requests traffic from the load balancer to the EC2 instance when the instance is being deregistered while continuing in-flight requests?
    1. ELB sticky session
    2. ELB deregistration check
    3. **ELB connection draining**
    4. ELB auto registration Off
23. When using an Elastic Load Balancer to serve traffic to web servers, which one of the following is true?
    1. Web servers must be publicly accessible
    2. The same security group must be applied to both the ELB and EC2 instances
    3. ELB and EC2 instance must be in the same subnet
    4. **ELB and EC2 instances must be in the same VPC**
24. A user has configured Elastic Load Balancing by enabling a Secure Socket Layer (SSL) negotiation configuration known as a Security Policy. Which of the below mentioned options is not part of this secure policy while negotiating the SSL connection between the user and the client?
    1. SSL Protocols
    2. **Client Order Preference**
    3. SSL Ciphers
    4. Server Order Preference
25. A user has created an ELB with the availability zone us-east-1. The user wants to add more zones to ELB to achieve High Availability. How can the user add more zones to the existing ELB?
    1. It is not possible to add more zones to the existing ELB
    2. Only option is to launch instances in different zones and add to ELB
    3. The user should stop the ELB and add zones and instances as required
    4. **The user can add zones on the fly from the AWS console**
26. A user has launched an ELB which has 5 instances registered with it. The user deletes the ELB by mistake. What will happen to the instances?
    1. ELB will ask the user whether to delete the instances or not
    2. Instances will be terminated
    3. ELB cannot be deleted if it has running instances registered with it
    4. **Instances will keep running**
27. A Sys-admin has created a shopping cart application and hosted it on EC2. The EC2 instances are running behind ELB. The admin wants to ensure that the end user request will always go to the EC2 instance where the user session has been created. How can the admin configure this?
    1. Enable ELB cross zone load balancing
    2. Enable ELB cookie setup
    3. **Enable ELB sticky session**
    4. Enable ELB connection draining
28. A user has setup connection draining with ELB to allow in-flight requests to continue while the instance is being deregistered through Auto Scaling. If the user has not specified the draining time, how long will ELB allow inflight requests traffic to continue?
    1. 600 seconds
    2. 3600 seconds
    3. **300 seconds**
    4. 0 seconds
29. A customer has a web application that uses cookie Based sessions to track logged in users. It is deployed on AWS using ELB and Auto Scaling. The customer observes that when load increases Auto Scaling launches new Instances but the load on the existing Instances does not decrease, causing all existing users to have a sluggish experience. Which two answer choices independently describe a behavior that could be the cause of the sluggish user experience?
    1. ELB’s normal behavior sends requests from the same user to the same backend instance (its not by default)
    2. **ELB’s behavior when sticky sessions are enabled causes ELB to send requests in the same session to the same backend**
    3. A faulty browser is not honoring the TTL of the ELB DNS name (DNS TTL would only impact the ELB instances if scaled and not the EC2 instances to which the traffic is routed)
    4. **The web application uses long polling such as comet or websockets. Thereby keeping a connection open to a web server tor a long time**
30. A customer has an online store that uses the cookie-based sessions to track logged-in customers. It is deployed on AWS using ELB and autoscaling. When the load increases, Auto scaling automatically launches new web servers, but the load on the web servers do not decrease. This causes the customers a poor experience. What could be causing the issue ?
    1. ELB DNS records Time to Live is set too high (DNS TTL would only impact the ELB instances if scaled and not the EC2 instances to which the traffic is routed)
    2. **ELB is configured to send requests with previously established sessions**
    3. Website uses CloudFront which is keeping sessions alive
    4. New Instances are not being added to the ELB during the Auto Scaling cool down period
31. You are designing a multi-platform web application for AWS. The application will run on EC2 instances and will be accessed from PCs, tablets and smart phones. Supported accessing platforms are Windows, MACOS, IOS and Android. Separate sticky session and SSL certificate setups are required for different platform types. Which of the following describes the most cost effective and performance efficient architecture setup?
    1. Setup a hybrid architecture to handle session state and SSL certificates on-prem and separate EC2 Instance groups running web applications for different platform types running in a VPC.
    2. Set up one ELB for all platforms to distribute load among multiple instance under it. Each EC2 instance implements all functionality for a particular platform.
    3. Set up two ELBs. The first ELB handles SSL certificates for all platforms and the second ELB handles session stickiness for all platforms for each ELB run separate EC2 instance groups to handle the web application for each platform.
    4. **Assign multiple ELBs to an EC2 instance or group of EC2 instances running the common components of the web application, one ELB for each platform type. Session stickiness and SSL termination are done at the ELBs.** (Session stickiness requires HTTPS listener with SSL termination on the ELB and ELB does not support multiple SSL certs so one is required for each cert)
32. You are migrating a legacy client-server application to AWS. The application responds to a specific DNS domain (e.g. www.example.com) and has a 2-tier architecture, with multiple application servers and a database server. Remote clients use TCP to connect to the application servers. The application servers need to know the IP address of the clients in order to function properly and are currently taking that information from the TCP socket. A Multi-AZ RDS MySQL instance will be used for the database. During the migration you can change the application code but you have to file a change request. How would you implement the architecture on AWS in order to maximize scalability and high availability?
    1. **File a change request to implement Proxy Protocol support In the application. Use an ELB with a TCP Listener and Proxy Protocol enabled to distribute load on two application servers in different AZs.** (ELB with TCP listener and proxy protocol will allow IP to be passed )
    2. File a change request to Implement Cross-Zone support in the application. Use an ELB with a TCP Listener and Cross-Zone Load Balancing enabled, two application servers in different AZs.
    3. File a change request to implement Latency Based Routing support in the application. Use Route 53 with Latency Based Routing enabled to distribute load on two application servers in different AZs.
    4. File a change request to implement Alias Resource support in the application Use Route 53 Alias Resource Record to distribute load on two application servers in different AZs.
33. A user has created an ELB with three instances. How many security groups will ELB create by default?
    1. 3
    2. 5
    3. **2** (One for ELB to allow inbound and Outbound to listener and health check port of instances and One for the Instances to allow inbound from ELB)
    4. 1
34. You have a web-style application with a stateless but CPU and memory-intensive web tier running on a cc2 8xlarge EC2 instance inside of a VPC The instance when under load is having problems returning requests within the SLA as defined by your business The application maintains its state in a DynamoDB table, but the data tier is properly provisioned and responses are consistently fast. How can you best resolve the issue of the application responses not meeting your SLA?
    1. **Add another cc2 8xlarge application instance, and put both behind an Elastic Load Balancer**
    2. Move the cc2 8xlarge to the same Availability Zone as the DynamoDB table (Does not improve the response time and performance)
    3. Cache the database responses in ElastiCache for more rapid access (Data tier is responding fast)
    4. Move the database from DynamoDB to RDS MySQL in scale-out read-replica configuration (Data tier is responding fast)
35. An organization has configured a VPC with an Internet Gateway (IGW). pairs of public and private subnets (each with one subnet per Availability Zone), and an Elastic Load Balancer (ELB) configured to use the public subnets. The applications web tier leverages the ELB, Auto Scaling and a Multi-AZ RDS database instance. The organization would like to eliminate any potential single points of failure in this design. What step should you take to achieve this organization’s objective?
    1. **Nothing, there are no single points of failure in this architecture.**
    2. Create and attach a second IGW to provide redundant internet connectivity. (VPC can be attached only 1 IGW)
    3. Create and configure a second Elastic Load Balancer to provide a redundant load balancer. (ELB scales by itself with multiple availability zones configured with it)
    4. Create a second multi-AZ RDS instance in another Availability Zone and configure replication to provide a redundant database. (Multi AZ requires 2 different AZ for setup and already has a standby)
36. Your application currently leverages AWS Auto Scaling to grow and shrink as load Increases/ decreases and has been performing well. Your marketing team expects a steady ramp up in traffic to follow an upcoming campaign that will result in a 20x growth in traffic over 4 weeks. Your forecast for the approximate number of Amazon EC2 instances necessary to meet the peak demand is 175. What should you do to avoid potential service disruptions during the ramp up in traffic?
    1. Ensure that you have pre-allocated 175 Elastic IP addresses so that each server will be able to obtain one as it launches (max limit 5 EIP and a service request needs to be submitted)
    2. **Check the service limits in Trusted Advisor and adjust as necessary so the forecasted count remains within limits.**
    3. Change your Auto Scaling configuration to set a desired capacity of 175 prior to the launch of the marketing campaign (Will cause 175 instances to be launched and running but not gradually scale)
    4. Pre-warm your Elastic Load Balancer to match the requests per second anticipated during peak demand (Does not need pre warming as the load is increasing steadily)
37. Which of the following features ensures even distribution of traffic to Amazon EC2 instances in multiple Availability Zones registered with a load balancer?
    1. Elastic Load Balancing request routing
    2. An Amazon Route 53 weighted routing policy (does not control traffic to EC2 instance)
    3. **Elastic Load Balancing cross-zone load balancing**
    4. An Amazon Route 53 latency routing policy (does not control traffic to EC2 instance)
38. Your web application front end consists of multiple EC2 instances behind an Elastic Load Balancer. You configured ELB to perform health checks on these EC2 instances, if an instance fails to pass health checks, which statement will be true?
    1. The instance gets terminated automatically by the ELB (it is done by Autoscaling)
    2. The instance gets quarantined by the ELB for root cause analysis.
    3. The instance is replaced automatically by the ELB. (it is done by Autoscaling)
    4. **The ELB stops sending traffic to the instance that failed its health check**
39. You have a web application running on six Amazon EC2 instances, consuming about 45% of resources on each instance. You are using auto-scaling to make sure that six instances are running at all times. The number of requests this application processes is consistent and does not experience spikes. The application is critical to your business and you want high availability at all times. You want the load to be distributed evenly between all instances. You also want to use the same Amazon Machine Image (AMI) for all instances. Which of the following architectural choices should you make?
    1. Deploy 6 EC2 instances in one availability zone and use Amazon Elastic Load Balancer. (Single AZ will not provide High Availability)
    2. Deploy 3 EC2 instances in one region and 3 in another region and use Amazon Elastic Load Balancer. (Different region, AMI would not be available unless copied)
    3. **Deploy 3 EC2 instances in one availability zone and 3 in another availability zone and use Amazon Elastic Load Balancer.**
    4. Deploy 2 EC2 instances in three regions and use Amazon Elastic Load Balancer. (Different region, AMI would not be available unless copied)
40. You are designing an SSL/TLS solution that requires HTTPS clients to be authenticated by the Web server using client certificate authentication. The solution must be resilient. Which of the following options would you consider for configuring the web server infrastructure? (Choose 2 answers)
    1. **Configure ELB with TCP listeners on TCP/443. And place the Web servers behind it.** (terminate SSL on the instance using client-side certificate)
    2. **Configure your Web servers with EIPs. Place the Web servers in a Route53 Record Set and configure health checks against all Web servers.** (Remove ELB and use Web Servers directly with Route 53)
    3. Configure ELB with HTTPS listeners, and place the Web servers behind it. (ELB with HTTPs does not support Client-Side certificates)
    4. Configure your web servers as the origins for a CloudFront distribution. Use custom SSL certificates on your CloudFront distribution (CloudFront [does not](http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/RequestAndResponseBehaviorCustomOrigin.html#RequestCustomClientSideSslAuth) Client-Side ssl certificates)
41. You are designing an application that contains protected health information. Security and compliance requirements for your application mandate that all protected health information in the application use encryption at rest and in transit. The application uses a three-tier architecture where data flows through the load balancer and is stored on Amazon EBS volumes for processing, and the results are stored in Amazon S3 using the AWS SDK. Which of the following two options satisfy the security requirements? Choose 2 answers
    1. Use SSL termination on the load balancer, Amazon EBS encryption on Amazon EC2 instances, and Amazon S3 with server-side encryption. (connection between ELB and EC2 not encrypted)
    2. Use SSL termination with a SAN SSL certificate on the load balancer, Amazon EC2 with all Amazon EBS volumes using Amazon EBS encryption, and Amazon S3 with server-side encryption with customer-managed keys.
    3. **Use TCP load balancing on the load balancer, SSL termination on the Amazon EC2 instances, OS-level disk encryption on the Amazon EBS volumes, and Amazon S3 with server-side encryption.**
    4. Use TCP load balancing on the load balancer, SSL termination on the Amazon EC2 instances, and Amazon S3 with server-side encryption. (Does not mention EBS encryption)
    5. **Use SSL termination on the load balancer, an SSL listener on the Amazon EC2 instances, Amazon EBS encryption on EBS volumes containing PHI, and Amazon S3 with server-side encryption.**
42. A startup deploys its photo-sharing site in a VPC. An elastic load balancer distributes web traffic across two subnets. The load balancer session stickiness is configured to use the AWS-generated session cookie, with a session TTL of 5 minutes. The web server Auto Scaling group is configured as min-size=4, max-size=4. The startup is preparing for a public launch, by running load-testing software installed on a single Amazon Elastic Compute Cloud (EC2) instance running in us-west-2a. After 60 minutes of load-testing, the web server logs show the following:WEBSERVER LOGS | # of HTTP requests from load-tester | # of HTTP requests from private beta users || webserver #1 (subnet in us-west-2a): | 19,210 | 434 || webserver #2 (subnet in us-west-2a): | 21,790 | 490 || webserver #3 (subnet in us-west-2b): | 0 | 410 || webserver #4 (subnet in us-west-2b): | 0 | 428 |Which recommendations can help ensure that load-testing HTTP requests are evenly distributed across the four web servers? Choose 2 answers
    1. Launch and run the load-tester Amazon EC2 instance from us-east-1 instead.
    2. Configure Elastic Load Balancing session stickiness to use the app-specific session cookie.
    3. **Re-configure the load-testing software to re-resolve DNS for each web request.** (Refer [link](https://aws.amazon.com/articles/1636185810492479))
    4. Configure Elastic Load Balancing and Auto Scaling to distribute across us-west-2a and us-west-2b.
    5. **Use a third-party load-testing service which offers globally distributed test clients.**(Refer [link](https://aws.amazon.com/articles/1636185810492479))
43. To serve Web traffic for a popular product your chief financial officer and IT director have purchased 10 m1.large heavy utilization Reserved Instances (RIs) evenly spread across two availability zones: Route 53 is used to deliver the traffic to an Elastic Load Balancer (ELB). After several months, the product grows even more popular and you need additional capacity As a result, your company purchases two c3.2xlarge medium utilization RIs You register the two c3.2xlarge instances with your ELB and quickly find that the ml large instances are at 100% of capacity and the c3.2xlarge instances have significant capacity that’s unused Which option is the most cost effective and uses EC2 capacity most effectively?
    1. **Use a separate ELB for each instance type and distribute load to ELBs with Route 53 weighted round robin**
    2. Configure Autoscaling group and Launch Configuration with ELB to add up to 10 more on-demand mi large instances when triggered by CloudWatch shut off c3.2xlarge instances (increase cost as you still pay for the RI)
    3. Route traffic to EC2 m1.large and c3.2xlarge instances directly using Route 53 latency based routing and health checks shut off ELB (will not still use the capacity effectively)
    4. Configure ELB with two c3.2xlarge Instances and use on-demand Autoscailng group for up to two additional c3.2xlarge instances Shut on m1.large instances(Increases cost, as you still pay for the 10 m1.large RI)
44. Which header received at the EC2 instance identifies the port used by the client while requesting ELB?
    1. X-Forwarded-Proto
    2. X-Requested-Proto
    3. **X-Forwarded-Port**
    4. X-Requested-Port
45. A user has configured ELB with two instances running in separate AZs of the same region? Which of the below mentioned statements is true?
    1. **Multi AZ instances will provide HA with ELB** (ELB provides HA to route traffic to healthy instances only it does not provide scalability)
    2. Multi AZ instances are not possible with a single ELB
    3. Multi AZ instances will provide scalability with ELB
    4. The user can achieve both HA and scalability with ELB
46. A user is configuring the HTTPS protocol on a front end ELB and the SSL protocol for the back-end listener in ELB. What will ELB do?
    1. It will allow you to create the configuration, but the instance will not pass the health check
    2. Receives requests on HTTPS and sends it to the back end instance on SSL
    3. **It will not allow you to create this configuration** (Will give error “Load Balancer protocol is an application layer protocol, but instance protocol is not. Both the Load Balancer protocol and the instance protocol should be at the same layer. Please fix.”)
    4. It will allow you to create the configuration, but ELB will not work as expected
47. An ELB is diverting traffic across 5 instances. One of the instances was unhealthy only for 20 minutes. What will happen after 20 minutes when the instance becomes healthy?
    1. ELB will never divert traffic back to the same instance
    2. ELB will not automatically send traffic to the same instance. However, the user can configure to start sending traffic to the same instance
    3. **ELB starts sending traffic to the instance once it is healthy**
    4. ELB terminates the instance once it is unhealthy. Thus, the instance cannot be healthy after 10 minutes
48. A user has hosted a website on AWS and uses ELB to load balance the multiple instances. The user application does not have any cookie management. How can the user bind the session of the requestor with a particular instance?
    1. Bind the IP address with a sticky cookie
    2. Create a cookie at the application level to set at ELB
    3. Use session synchronization with ELB
    4. **Let ELB generate a cookie for a specified duration**
49. A user has configured a website and launched it using the Apache web server on port 80. The user is using ELB with the EC2 instances for Load Balancing. What should the user do to ensure that the EC2 instances accept requests only from ELB?
    1. Open the port for an ELB static IP in the EC2 security group
    2. **Configure the security group of EC2, which allows access to the ELB source security group**
    3. Configure the EC2 instance so that it only listens on the ELB port
    4. Configure the security group of EC2, which allows access only to the ELB listener
50. AWS Elastic Load Balancer supports SSL termination.
    1. For specific availability zones only
    2. False
    3. For specific regions only
    4. **For all regions**
51. User has launched five instances with ELB. How can the user add the sixth EC2 instance to ELB?
    1. **The user can add the sixth instance on the fly.**
    2. The user must stop the ELB and add the sixth instance.
    3. The user can add the instance and change the ELB config file.
    4. The ELB can only have a maximum of five instances.
52. A customer is running a multi-tier web application farm in a virtual private cloud (VPC) that is not connected to their corporate network. They are connecting to the VPC over the Internet to manage all of their Amazon EC2 instances running in both the public and private subnets. They have only authorized the bastion-security-group with Microsoft Remote Desktop Protocol (RDP) access to the application instance security groups, but the company wants to further limit administrative access to all of the instances in the VPC. Which of the following Bastion deployment scenarios will meet this requirement?
    1. Deploy a Windows Bastion host on the corporate network that has RDP access to all instances in the VPC.
    2. Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow SSH access to the bastion from anywhere.
    3. Deploy a Windows Bastion host with an Elastic IP address in the private subnet, and restrict RDP access to the bastion from only the corporate public IP addresses.
    4. **Deploy a Windows Bastion host with an auto-assigned Public IP address in the public subnet, and allow RDP access to the bastion from only the corporate public IP addresses.**
53. You are designing a system that has a Bastion host. This component needs to be highly available without human intervention. Which of the following approaches would you select?
    1. Run the bastion on two instances one in each AZ
    2. Run the bastion on an active Instance in one AZ and have an AMI ready to boot up in the event of failure
    3. **Configure the bastion instance in an Auto Scaling group Specify the Auto Scaling group to include multiple AZs but have a min-size of 1 and max-size of 1**
    4. Configure an ELB in front of the bastion instance
54. You’ve been brought in as solutions architect to assist an enterprise customer with their migration of an ecommerce platform to Amazon Virtual Private Cloud (VPC) The previous architect has already deployed a 3- tier VPC. The configuration is as follows: VPC vpc-2f8t>C447  
    IGW ig-2d8bc445  
    NACL acl-2080c448  
    Subnets and Route Tables:  
    Web server’s subnet-258bc44d  
    Application server’s subnet-248DC44c  
    Database server’s subnet-9189c6f9  
    Route Tables:  
    rtb-2i8bc449  
    rtb-238bc44b  
    Associations:  
    Subnet-258bc44d: rtb-2i8bc449  
    Subnet-248DC44c: rtb-238bc44b  
    Subnet-9189c6f9: rtb-238bc44b  
    You are now ready to begin deploying EC2 instances into the VPC. Web servers must have direct access to the internet Application and database servers cannot have direct access to the internet. Which configuration below will allow you the ability to remotely administer your application and database servers, as well as allow these servers to retrieve updates from the Internet?
    1. Create a bastion and NAT Instance in subnet-258bc44d and add a route from rtb-238bc44b to subnet-258bc44d. (Route should point to the NAT)
    2. Add a route from rtb-238bc44b to igw-2d8bc445 and add a bastion and NAT instance within Subnet-248DC44c. (Adding IGW to routertb-238bc44b would expose the Application and Database server to internet. Bastion and NAT should be in public subnet)
    3. Create a Bastion and NAT Instance in subnet-258bc44d. Add a route from rtb-238bc44b to igw-2d8bc445. And a new NACL that allows access between subnet-258bc44d and subnet-248bc44c. (Route should point to NAT and not Internet Gateway else it would be internet accessible.)
    4. **Create a Bastion and NAT instance in subnet-258bc44d and add a route from rtb-238bc44b to the NAT instance.** (Bastion and NAT should be in the public subnet. As Web Server has direct access to Internet, the subnet subnet-258bc44d should be public and Route rtb-2i8bc449 pointing to IGW. Route rtb-238bc44b for private subnets should point to NAT for outgoing internet access)
55. You are tasked with setting up a Linux bastion host for access to Amazon EC2 instances running in your VPC. Only clients connecting from the corporate external public IP address 72.34.51.100 should have SSH access to the host. Which option will meet the customer requirement?
    1. **Security Group Inbound Rule: Protocol – TCP. Port Range – 22, Source 72.34.51.100/32**
    2. Security Group Inbound Rule: Protocol – UDP, Port Range – 22, Source 72.34.51.100/32
    3. Network ACL Inbound Rule: Protocol – UDP, Port Range – 22, Source 72.34.51.100/32
    4. Network ACL Inbound Rule: Protocol – TCP, Port Range-22, Source 72.34.51.100/0
56. Fill in the blanks: \_\_\_\_\_\_\_\_\_ let you categorize your EC2 resources in different ways, for example, by purpose, owner, or environment.
    1. Wildcards
    2. Pointers
    3. **Tags**
    4. Special filters
57. Please select the Amazon EC2 resource, which can be tagged.
    1. Key pairs
    2. Elastic IP addresses
    3. Placement groups
    4. **Amazon EBS snapshots**
58. Can the string value of ‘Key’ be prefixed with aws:?
    1. **No**
    2. Only for EC2 not S3
    3. Yes
    4. Only for S3 not EC
59. What is the maximum key length of a tag?
    1. 512 Unicode characters
    2. 64 Unicode characters
    3. 256 Unicode characters
    4. **128 Unicode characters**
60. An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?
    1. Launch the test and production instances in separate regions and allow region wise access to the group (possible using location constraint condition but not flexible)
    2. Define the IAM policy which allows access based on the instance ID (not flexible as it would change)
    3. Create an IAM policy with a condition which allows access to only small instances (not flexible as it would change)
    4. **Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags** (possible using ResourceTag condition)
61. A user has launched multiple EC2 instances for the purpose of development and testing in the same region. The user wants to find the separate cost for the production and development instances. How can the user find the cost distribution?
    1. The user should download the activity report of the EC2 services as it has the instance ID wise data
    2. It is not possible to get the AWS cost usage data of single region instances separately
    3. User should use Cost Distribution Metadata and AWS detailed billing
    4. **User should use Cost Allocation Tags and AWS billing reports**
62. An organization is using cost allocation tags to find the cost distribution of different departments and projects. One of the instances has two separate tags with the key/value as “InstanceName/HR”, “CostCenter/HR”. What will AWS do in this case?
    1. InstanceName is a reserved tag for AWS. Thus, AWS will not allow this tag
    2. AWS will not allow the tags as the value is the same for different keys
    3. AWS will allow tags but will not show correctly in the cost allocation report due to the same value of the two separate keys
    4. **AWS will allow both the tags and show properly in the cost distribution report**
63. A user is launching an instance. He is on the “Tag the instance” screen. Which of the below mentioned information will not help the user understand the functionality of an AWS tag?
    1. Each tag will have a key and value
    2. The user can apply tags to the S3 bucket
    3. **The maximum value of the tag key length is 64 unicode characters**
    4. AWS tags are used to find the cost distribution of various resources
64. Your system recently experienced down time during the troubleshooting process. You found that a new administrator mistakenly terminated several production EC2 instances. Which of the following strategies will help prevent a similar situation in the future? The administrator still must be able to:- launch, start stop, and terminate development resources. – launch and start production instances.
    1. Create an IAM user, which is not allowed to terminate instances by leveraging production EC2 termination protection. (EC2 termination protection is enabled on EC2 instance)
    2. **Leverage resource based tagging along with an IAM user, which can prevent specific users from terminating production EC2 resources.** (Identify production resources using tags and add explicit deny)
    3. Leverage EC2 termination protection and multi-factor authentication, which together require users to authenticate before terminating EC2 instances. (Does not still prevent user from terminating instance)
    4. Create an IAM user and apply an IAM role, which prevents users from terminating production EC2 instances. (Role is not applied to User but assumed by the User also need a way to identify production EC2 instances)
65. Your manager has requested you to tag EC2 instances to organize and manage a load balancer. Which of the following statements about tag restrictions is incorrect?
    1. The maximum key length is 127 Unicode characters.
    2. The maximum value length is 255 Unicode characters.
    3. Tag keys and values are case sensitive.
    4. **The maximum number of tags per load balancer is 20.** (50 is the limit)
66. What is the maximum number of tags that a user can assign to an EC2 instance?
    1. **50**
    2. 10
    3. 5
    4. 25
67. You are running a successful multi-tier web application on AWS and your marketing department has asked you to add a reporting tier to the application. The reporting tier will aggregate and publish status reports every 30 minutes from user-generated information that is being stored in your web applications database. You are currently running a Multi-AZ RDS MySQL instance for the database tier. You also have implemented ElastiCache as a database caching layer between the application tier and database tier. Please select the answer that will allow you to successfully implement the reporting tier with as little impact as possible to your database.
    1. Continually send transaction logs from your master database to an S3 bucket and generate the reports off the S3 bucket using S3 byte range requests.
    2. Generate the reports by querying the synchronously replicated standby RDS MySQL instance maintained through Multi-AZ (Standby instance cannot be used as a scaling solution)
    3. **Launch a RDS Read Replica connected to your Multi-AZ master database and generate reports by querying the Read Replica.**
    4. Generate the reports by querying the ElastiCache database caching tier. (ElasticCache does not maintain full data and is simply a caching solution)
68. A company is deploying a new two-tier web application in AWS. The company has limited staff and requires high availability, and the application requires complex queries and table joins. Which configuration provides the solution for the company’s requirements?
    1. MySQL Installed on two Amazon EC2 Instances in a single Availability Zone (does not provide High Availaility out of the box)
    2. **Amazon RDS for MySQL with Multi-AZ**
    3. Amazon ElastiCache (Just a caching solution)
    4. Amazon DynamoDB (Not suitable for complex queries and joins)
69. Your company is getting ready to do a major public announcement of a social media site on AWS. The website is running on EC2 instances deployed across multiple Availability Zones with a Multi-AZ RDS MySQL Extra Large DB Instance. The site performs a high number of small reads and writes per second and relies on an eventual consistency model. After comprehensive tests you discover that there is read contention on RDS MySQL. Which are the best approaches to meet these requirements? (Choose 2 answers)
    1. **Deploy ElastiCache in-memory cache running in each availability zone**
    2. Implement sharding to distribute load to multiple RDS MySQL instances (this is only a read contention, the writes work fine)
    3. Increase the RDS MySQL Instance size and Implement provisioned IOPS (not scalable, this is only a read contention, the writes work fine)
    4. **Add an RDS MySQL read replica in each availability zone**
70. Your company has HQ in Tokyo and branch offices all over the world and is using logistics software with a multi-regional deployment on AWS in Japan, Europe and US. The logistic software has a 3-tier architecture and currently uses MySQL 5.6 for data persistence. Each region has deployed its own database. In the HQ region you run an hourly batch process reading data from every region to compute cross-regional reports that are sent by email to all offices this batch process must be completed as fast as possible to quickly optimize logistics. How do you build the database architecture in order to meet the requirements?
    1. **For each regional deployment, use RDS MySQL with a master in the region and a read replica in the HQ region**
    2. For each regional deployment, use MySQL on EC2 with a master in the region and send hourly EBS snapshots to the HQ region
    3. For each regional deployment, use RDS MySQL with a master in the region and send hourly RDS snapshots to the HQ region
    4. For each regional deployment, use MySQL on EC2 with a master in the region and use S3 to copy data files hourly to the HQ region
    5. Use Direct Connect to connect all regional MySQL deployments to the HQ region and reduce network latency for the batch process
71. What would happen to an RDS (Relational Database Service) multi-Availability Zone deployment if the primary DB instance fails?
    1. IP of the primary DB Instance is switched to the standby DB Instance.
    2. A new DB instance is created in the standby availability zone.
    3. **The canonical name record (CNAME) is changed from primary to standby.**
    4. The RDS (Relational Database Service) DB instance reboots.
72. Your business is building a new application that will store its entire customer database on a RDS MySQL database, and will have various applications and users that will query that data for different purposes. Large analytics jobs on the database are likely to cause other applications to not be able to get the query results they need to, before time out. Also, as your data grows, these analytics jobs will start to take more time, increasing the negative effect on the other applications. How do you solve the contention issues between these different workloads on the same data?
    1. Enable Multi-AZ mode on the RDS instance
    2. Use ElastiCache to offload the analytics job data
    3. **Create RDS Read-Replicas for the analytics work**
    4. Run the RDS instance on the largest size possible
73. Will my standby RDS instance be in the same Availability Zone as my primary?
    1. Only for Oracle RDS types
    2. Yes
    3. Only if configured at launch
    4. **No**
74. Is creating a Read Replica of another Read Replica supported?
    1. Only in certain regions
    2. **Only with MySQL based RDS**
    3. Only for Oracle RDS types
    4. No
75. A user is planning to set up the Multi-AZ feature of RDS. Which of the below mentioned conditions won’t take advantage of the Multi-AZ feature?
    1. Availability zone outage
    2. A manual failover of the DB instance using Reboot with failover option
    3. **Region outage**
    4. When the user changes the DB instance’s server type
76. When you run a DB Instance as a Multi-AZ deployment, the “\_\_\_\_\_” serves database writes and reads
    1. secondary
    2. backup
    3. stand by
    4. **primary**
77. When running my DB Instance as a Multi-AZ deployment, can I use the standby for read or write operations?
    1. Yes
    2. Only with MSSQL based RDS
    3. Only for Oracle RDS instances
    4. **No**
78. Read Replicas require a transactional storage engine and are only supported for the \_\_\_\_\_\_\_\_\_ storage engine
    1. OracleISAM
    2. MSSQLDB
    3. **InnoDB**
    4. MyISAM
79. A user is configuring the Multi-AZ feature of an RDS DB. The user came to know that this RDS DB does not use the AWS technology, but uses server mirroring to achieve replication. Which DB is the user using right now?
    1. MySQL
    2. Oracle
    3. **MS SQL**
    4. PostgreSQL
80. If I have multiple Read Replicas for my master DB Instance and I promote one of them, what happens to the rest of the Read Replicas?
    1. **The remaining Read Replicas will still replicate from the older master DB Instance**
    2. The remaining Read Replicas will be deleted
    3. The remaining Read Replicas will be combined to one read replica
81. If you have chosen Multi-AZ deployment, in the event of a planned or unplanned outage of your primary DB Instance, Amazon RDS automatically switches to the standby replica. The automatic failover mechanism simply changes the \_\_\_\_\_\_ record of the main DB Instance to point to the standby DB Instance.
    1. DNAME
    2. **CNAME**
    3. TXT
    4. MX
82. When automatic failover occurs, Amazon RDS will emit a DB Instance event to inform you that automatic failover occurred. You can use the \_\_\_\_\_ to return information about events related to your DB Instance
    1. FetchFailure
    2. DescriveFailure
    3. **DescribeEvents**
    4. FetchEvents
83. The new DB Instance that is created when you promote a Read Replica retains the backup window period.
    1. **TRUE**
    2. FALSE
84. Will I be alerted when automatic failover occurs?
    1. **Only if SNS configured**
    2. No
    3. Yes
    4. Only if Cloudwatch configured
85. Can I initiate a “forced failover” for my MySQL Multi-AZ DB Instance deployment?
    1. Only in certain regions
    2. Only in VPC
    3. **Yes**
    4. No
86. A user is accessing RDS from an application. The user has enabled the Multi-AZ feature with the MS SQL RDS DB. During a planned outage how will AWS ensure that a switch from DB to a standby replica will not affect access to the application?
    1. RDS will have an internal IP which will redirect all requests to the new DB
    2. **RDS uses DNS to switch over to standby replica for seamless transition**
    3. The switch over changes Hardware so RDS does not need to worry about access
    4. RDS will have both the DBs running independently and the user has to manually switch over
87. Which of the following is part of the failover process for a Multi-AZ Amazon Relational Database Service (RDS) instance?
    1. The failed RDS DB instance reboots.
    2. The IP of the primary DB instance is switched to the standby DB instance.
    3. **The DNS record for the RDS endpoint is changed from primary to standby.**
    4. A new DB instance is created in the standby availability zone.
88. Which of these is not a reason a Multi-AZ RDS instance will failover?
    1. An Availability Zone outage
    2. A manual failover of the DB instance was initiated using Reboot with failover
    3. To autoscale to a higher instance class (Refer [link](https://aws.amazon.com/rds/details/multi-az/))
    4. **Master database corruption occurs**
    5. The primary DB instance fails
89. You need to scale an RDS deployment. You are operating at 10% writes and 90% reads, based on your logging. How best can you scale this in a simple way?
    1. Create a second master RDS instance and peer the RDS groups.
    2. Cache all the database responses on the read side with CloudFront.
    3. **Create read replicas for RDS since the load is mostly reads.**
    4. Create a Multi-AZ RDS installs and route read traffic to standby.
90. How does Amazon RDS multi Availability Zone model work?
    1. **A second, standby database is deployed and maintained in a different availability zone from master, using synchronous replication.** (Refer [link](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html))
    2. A second, standby database is deployed and maintained in a different availability zone from master using asynchronous replication.
    3. A second, standby database is deployed and maintained in a different region from master using asynchronous replication.
    4. A second, standby database is deployed and maintained in a different region from master using synchronous replication.
91. A customer is running an application in US-West (Northern California) region and wants to setup disaster recovery failover to the Asian Pacific (Singapore) region. The customer is interested in achieving a low Recovery Point Objective (RPO) for an Amazon RDS multi-AZ MySQL database instance. Which approach is best suited to this need?
    1. Synchronous replication
    2. **Asynchronous replication**
    3. Route53 health checks
    4. Copying of RDS incremental snapshots
92. A user is using a small MySQL RDS DB. The user is experiencing high latency due to the Multi AZ feature. Which of the below mentioned options may not help the user in this situation?
    1. Schedule the automated back up in non-working hours
    2. Use a large or higher size instance
    3. Use PIOPS
    4. **Take a snapshot from standby Replica**
93. Are Reserved Instances available for Multi-AZ Deployments?
    1. Only for Cluster Compute instances
    2. **Yes for all instance types**
    3. Only for M3 instance types
94. My Read Replica appears “stuck” after a Multi-AZ failover and is unable to obtain or apply updates from the source DB Instance. What do I do?
    1. **You will need to delete the Read Replica and create a new one to replace it.**
    2. You will need to disassociate the DB Engine and re associate it.
    3. The instance should be deployed to Single AZ and then moved to Multi- AZ once again
    4. You will need to delete the DB Instance and create a new one to replace it.
95. What is the charge for the data transfer incurred in replicating data between your primary and standby?
    1. **No charge. It is free.**
    2. Double the standard data transfer charge
    3. Same as the standard data transfer charge
    4. Half of the standard data transfer charge
96. A user has enabled the Multi AZ feature with the MS SQL RDS database server. Which of the below mentioned statements will help the user understand the Multi AZ feature better?
    1. In a Multi AZ, AWS runs two DBs in parallel and copies the data asynchronously to the replica copy
    2. In a Multi AZ, AWS runs two DBs in parallel and copies the data synchronously to the replica copy
    3. **In a Multi AZ, AWS runs just one DB but copies the data synchronously to the standby replica**
    4. AWS MS SQL does not support the Multi AZ feature
97. A company is running a batch analysis every hour on their main transactional DB running on an RDS MySQL instance to populate their central Data Warehouse running on Redshift. During the execution of the batch their transactional applications are very slow. When the batch completes they need to update the top management dashboard with the new data. The dashboard is produced by another system running on-premises that is currently started when a manually-sent email notifies that an update is required The on-premises system cannot be modified because is managed by another team. How would you optimize this scenario to solve performance issues and automate the process as much as possible?
    1. Replace RDS with Redshift for the batch analysis and SNS to notify the on-premises system to update the dashboard
    2. Replace RDS with Redshift for the batch analysis and SQS to send a message to the on-premises system to update the dashboard
    3. **Create an RDS Read Replica for the batch analysis and SNS to notify me on-premises system to update the dashboard**
    4. Create an RDS Read Replica for the batch analysis and SQS to send a message to the on-premises system to update the dashboard.
98. Which of the following notification endpoints or clients does Amazon Simple Notification Service support? Choose 2 answers
    1. **Email**
    2. CloudFront distribution
    3. File Transfer Protocol
    4. **Short Message Service**
    5. Simple Network Management Protocol
99. What happens when you create a topic on Amazon SNS?
    1. The topic is created, and it has the name you specified for it.
    2. **An ARN (Amazon Resource Name) is created**
    3. You can create a topic on Amazon SQS, not on Amazon SNS.
    4. This question doesn’t make sense.
100. A user has deployed an application on his private cloud. The user is using his own monitoring tool. He wants to configure that whenever there is an error, the monitoring tool should notify him via SMS. Which of the below mentioned AWS services will help in this scenario?
     1. None because the user infrastructure is in the private cloud/
     2. **AWS SNS**
     3. AWS SES
     4. AWS SMS
101. A user wants to make so that whenever the CPU utilization of the AWS EC2 instance is above 90%, the redlight of his bedroom turns on. Which of the below mentioned AWS services is helpful for this purpose?
     1. AWS CloudWatch + AWS SES
     2. **AWS CloudWatch + AWS SNS**
     3. It is not possible to configure the light with the AWS infrastructure services
     4. AWS CloudWatch and a dedicated software turning on the light
102. A user is trying to understand AWS SNS. To which of the below mentioned end points is SNS unable to send a notification?
     1. Email JSON
     2. HTTP
     3. AWS SQS
     4. **AWS SES**
103. A user is running a webserver on EC2. The user wants to receive the SMS when the EC2 instance utilization is above the threshold limit. Which AWS services should the user configure in this case?
     1. AWS CloudWatch + AWS SES
     2. **AWS CloudWatch + AWS SNS**
     3. AWS CloudWatch + AWS SQS
     4. AWS EC2 + AWS CloudWatch
104. A user is planning to host a mobile game on EC2 which sends notifications to active users on either high score or the addition of new features. The user should get this notification when he is online on his mobile device. Which of the below mentioned AWS services can help achieve this functionality?
     1. **AWS Simple Notification Service**
     2. AWS Simple Queue Service
     3. AWS Mobile Communication Service
     4. AWS Simple Email Service
105. You are providing AWS consulting service for a company developing a new mobile application that will be leveraging amazon SNS push for push notifications. In order to send direct notification messages to individual devices each device registration identifier or token needs to be registered with SNS, however the developers are not sure of the best way to do this. You advise them to: –
     1. Bulk upload the device tokens contained in a CSV file via the AWS Management Console
     2. Let the push notification service (e.g. Amazon Device messaging) handle the registration
     3. Implement a token vending service to handle the registration
     4. **Call the CreatePlatformEndpoint API function to register multiple device tokens.** (Refer [documentation](http://docs.aws.amazon.com/sns/latest/dg/mobile-push-send-devicetoken.html))
106. A company is running a batch analysis every hour on their main transactional DB running on an RDS MySQL instance to populate their central Data Warehouse running on Redshift. During the execution of the batch their transactional applications are very slow. When the batch completes they need to update the top management dashboard with the new data. The dashboard is produced by another system running on-premises that is currently started when a manually-sent email notifies that an update is required The on-premises system cannot be modified because is managed by another team. How would you optimize this scenario to solve performance issues and automate the process as much as possible?
     1. Replace RDS with Redshift for the batch analysis and SNS to notify the on-premises system to update the dashboard
     2. Replace RDS with Redshift for the batch analysis and SQS to send a message to the on-premises system to update the dashboard
     3. **Create an RDS Read Replica for the batch analysis and SNS to notify me on-premises system to update the dashboard**
     4. Create an RDS Read Replica for the batch analysis and SQS to send a message to the on-premises system to update the dashboard.
107. Which of the following are valid SNS delivery transports? Choose 2 answers.
     1. **HTTP**
     2. UDP
     3. **SMS**
     4. DynamoDB
     5. Named Pipes
108. What is the format of structured notification messages sent by Amazon SNS?
     1. An XML object containing MessageId, UnsubscribeURL, Subject, Message and other values
     2. An JSON object containing MessageId, DuplicateFlag, Message and other values
     3. An XML object containing MessageId, DuplicateFlag, Message and other values
     4. **An JSON object containing MessageId, unsubscribeURL, Subject, Message and other values**
109. Which of the following are valid arguments for an SNS Publish request? Choose 3 answers.
     1. **TopicAm**
     2. **Subject**
     3. Destination
     4. Format
     5. **Message**
     6. Language
110. A company is building a two-tier web application to serve dynamic transaction-based content. The data tier is leveraging an Online Transactional Processing (OLTP) database. What services should you leverage to enable an elastic and scalable web tier?
     1. **Elastic Load Balancing, Amazon EC2, and Auto Scaling**
     2. Elastic Load Balancing, Amazon RDS with Multi-AZ, and Amazon S3
     3. Amazon RDS with Multi-AZ and Auto Scaling
     4. Amazon EC2, Amazon DynamoDB, and Amazon S3
111. You have been given a scope to deploy some AWS infrastructure for a large organization. The requirements are that you will have a lot of EC2 instances but may need to add more when the average utilization of your Amazon EC2 fleet is high and conversely remove them when CPU utilization is low. Which AWS services would be best to use to accomplish this?
     1. Amazon CloudFront, Amazon CloudWatch and Elastic Load Balancing
     2. Auto Scaling, Amazon CloudWatch and AWS CloudTrail
     3. **Auto Scaling, Amazon CloudWatch and Elastic Load Balancing**
     4. Auto Scaling, Amazon CloudWatch and AWS Elastic Beanstalk
112. A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling AddToLoadBalancer, which adds instances to the load balancer. process for a while. What will happen to the instances launched during the suspension period?
     1. **The instances will not be registered with ELB and the user has to manually register when the process is resumed**
     2. The instances will be registered with ELB only once the process has resumed
     3. Auto Scaling will not launch the instance during this period due to process suspension
     4. It is not possible to suspend only the AddToLoadBalancer process
113. You have an Auto Scaling group associated with an Elastic Load Balancer (ELB). You have noticed that instances launched via the Auto Scaling group are being marked unhealthy due to an ELB health check, but these unhealthy instances are not being terminated. What do you need to do to ensure trial instances marked unhealthy by the ELB will be terminated and replaced?
     1. Change the thresholds set on the Auto Scaling group health check
     2. **Add an Elastic Load Balancing health check to your Auto Scaling group**
     3. Increase the value for the Health check interval set on the Elastic Load Balancer
     4. Change the health check set on the Elastic Load Balancer to use TCP rather than HTTP checks
114. You are responsible for a web application that consists of an Elastic Load Balancing (ELB) load balancer in front of an Auto Scaling group of Amazon Elastic Compute Cloud (EC2) instances. For a recent deployment of a new version of the application, a new Amazon Machine Image (AMI) was created, and the Auto Scaling group was updated with a new launch configuration that refers to this new AMI. During the deployment, you received complaints from users that the website was responding with errors. All instances passed the ELB health checks. What should you do in order to avoid errors for future deployments? (Choose 2 answer) **[PROFESSIONAL]**
     1. Add an Elastic Load Balancing health check to the Auto Scaling group. Set a short period for the health checks to operate as soon as possible in order to prevent premature registration of the instance to the load balancer.
     2. Enable EC2 instance CloudWatch alerts to change the launch configuration’s AMI to the previous one. Gradually terminate instances that are using the new AMI.
     3. **Set the Elastic Load Balancing health check configuration to target a part of the application that fully tests application health and returns an error if the tests fail.**
     4. **Create a new launch configuration that refers to the new AMI, and associate it with the group. Double the size of the group, wait for the new instances to become healthy, and reduce back to the original size. If new instances do not become healthy, associate the previous launch configuration.**
     5. Increase the Elastic Load Balancing Unhealthy Threshold to a higher value to prevent an unhealthy instance from going into service behind the load balancer.
115. What is the order of most-to-least rapidly-scaling (fastest to scale first)? A) EC2 + ELB + Auto Scaling B) Lambda C) RDS
     1. **B, A, C** (Lambda is designed to scale instantly. EC2 + ELB + Auto Scaling require single-digit minutes to scale out. RDS will take at least 15 minutes, and will apply OS patches or any other updates when applied.)
     2. C, B, A
     3. C, A, B
     4. A, C, B
116. A user has hosted an application on EC2 instances. The EC2 instances are configured with ELB and Auto Scaling. The application server session time out is 2 hours. The user wants to configure connection draining to ensure that all in-flight requests are supported by ELB even though the instance is being deregistered. What time out period should the user specify for connection draining?
     1. 5 minutes
     2. **1 hour** (max allowed is 3600 secs that is close to 2 hours to keep the in flight requests alive)
     3. 30 minutes
     4. 2 hours
117. You have in total 5 offices, and the entire employee related information is stored under AWS VPC instances. Now all the offices want to connect the instances in VPC using VPN. Which of the below help you to implement this?
     1. you can have redundant customer gateways between your data center and your VPC
     2. you can have multiple locations connected to the AWS VPN CloudHub
     3. You have to define 5 different static IP addresses in route table.
     4. **1 and 2**
     5. 1,2 and 3
118. You have in total 15 offices, and the entire employee related information is stored under AWS VPC instances. Now all the offices want to connect the instances in VPC using VPN. What problem do you see in this scenario?
     1. You can not create more than 1 VPN connections with single VPC (Can be created)
     2. You can not create more than 10 VPN connections with single VPC (soft limit can be extended)
     3. When you create multiple VPN connections, the virtual private gateway can not sends network traffic to the appropriate VPN connection using statically assigned routes. (Can route the traffic to correct connection)
     4. Statically assigned routes cannot be configured in case of more than 1 VPN with virtual private gateway. (can be configured)
     5. **None of above**
119. You have been asked to virtually extend two existing data centers into AWS to support a highly available application that depends on existing, on-premises resources located in multiple data centers and static content that is served from an Amazon Simple Storage Service (S3) bucket. Your design currently includes a dual-tunnel VPN connection between your CGW and VGW. Which component of your architecture represents a potential single point of failure that you should consider changing to make the solution more highly available?
     1. Add another VGW in a different Availability Zone and create another dual-tunnel VPN connection.
     2. **Add another CGW in a different data center and create another dual-tunnel VPN connection.** (Refer [link](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html))
     3. Add a second VGW in a different Availability Zone, and a CGW in a different data center, and create another dual-tunnel.
     4. No changes are necessary: the network architecture is currently highly available.
120. You are designing network connectivity for your fat client application. The application is designed for business travelers who must be able to connect to it from their hotel rooms, cafes, public Wi-Fi hotspots, and elsewhere on the Internet. You do not want to publish the application on the Internet. Which network design meets the above requirements while minimizing deployment and operational costs? **[PROFESSIONAL]**
     1. Implement AWS Direct Connect, and create a private interface to your VPC. Create a public subnet and place your application servers in it. (High Cost and does not minimize deployment)
     2. Implement Elastic Load Balancing with an SSL listener that terminates the back-end connection to the application. (Needs to be published to internet)
     3. Configure an IPsec VPN connection, and provide the users with the configuration details. Create a public subnet in your VPC, and place your application servers in it. (Instances still in public subnet are internet accessible)
     4. **Configure an SSL VPN solution in a public subnet of your VPC, then install and configure SSL VPN client software on all user computers. Create a private subnet in your VPC and place your application servers in it.** (Cost effective and can be in private subnet as well)
121. You are designing a connectivity solution between on-premises infrastructure and Amazon VPC Your server’s on-premises will De communicating with your VPC instances You will De establishing IPSec tunnels over the internet You will be using VPN gateways and terminating the IPsec tunnels on AWS-supported customer gateways. Which of the following objectives would you achieve by implementing an IPSec tunnel as outlined above? (Choose 4 answers) **[PROFESSIONAL]**
     1. End-to-end protection of data in transit
     2. End-to-end Identity authentication
     3. **Data encryption across the Internet**
     4. **Protection of data in transit over the Internet**
     5. **Peer identity authentication between VPN gateway and customer gateway**
     6. **Data integrity protection across the Internet**
122. A development team that is currently doing a nightly six-hour build which is lengthening over time on-premises with a large and mostly under utilized server would like to transition to a continuous integration model of development on AWS with multiple builds triggered within the same day. However, they are concerned about cost, security and how to integrate with existing on-premises applications such as their LDAP and email servers, which cannot move off-premises. The development environment needs a source code repository; a project management system with a MySQL database resources for performing the builds and a storage location for QA to pick up builds from. What AWS services combination would you recommend to meet the development team’s requirements? **[PROFESSIONAL]**
     1. A Bastion host Amazon EC2 instance running a VPN server for access from on-premises, Amazon EC2 for the source code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIP for the source code repository and project management system, Amazon SQL for a build queue, An Amazon Auto Scaling group of Amazon EC2 instances for performing builds and Amazon Simple Email Service for sending the build output. (Bastion is not for VPN connectivity also SES should not be used)
     2. An AWS Storage Gateway for connecting on-premises software applications with cloud-based storage securely, Amazon EC2 for the resource code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIPs for the source code repository and project management system, Amazon Simple Notification Service for a notification initiated build, An Auto Scaling group of Amazon EC2 instances for performing builds and Amazon S3 for the build output. (Storage Gateway does provide secure connectivity but still needs VPN. SNS alone cannot handle builds)
     3. An AWS Storage Gateway for connecting on-premises software applications with cloud-based storage securely, Amazon EC2 for the resource code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIPs for the source code repository and project management system, Amazon SQS for a build queue, An Amazon Elastic Map Reduce (EMR) cluster of Amazon EC2 instances for performing builds and Amazon CloudFront for the build output. (Storage Gateway does not provide secure connectivity, still needs VPN. EMR is not ideal for performing builds as it needs normal EC2 instances)
     4. **A VPC with a VPN Gateway back to their on-premises servers, Amazon EC2 for the source-code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIPs for the source code repository and project management system, SQS for a build queue, An Auto Scaling group of EC2 instances for performing builds and S3 for the build output.** (VPN gateway is required for secure connectivity. SQS for build queue and EC2 for builds)
123. You are designing a personal document-archiving solution for your global enterprise with thousands of employee. Each employee has potentially gigabytes of data to be backed up in this archiving solution. The solution will be exposed to he employees as an application, where they can just drag and drop their files to the archiving system. Employees can retrieve their archives through a web interface. The corporate network has high bandwidth AWS DirectConnect connectivity to AWS. You have regulatory requirements that all data needs to be encrypted before being uploaded to the cloud. How do you implement this in a highly available and cost efficient way?
     1. Manage encryption keys on-premise in an encrypted relational database. Set up an on-premises server with sufficient storage to temporarily store files and then upload them to Amazon S3, providing a client-side master key. (Storing temporary increases cost and not a high availability option)
     2. Manage encryption keys in a Hardware Security Module (HSM) appliance on-premise server with sufficient storage to temporarily store, encrypt, and upload files directly into amazon Glacier. (Not cost effective)
     3. **Manage encryption keys in amazon Key Management Service (KMS), upload to amazon simple storage service (s3) with client-side encryption using a KMS customer master key ID and configure Amazon S3 lifecycle policies to store each object using the amazon glacier storage tier.** (With CSE-KMS the encryption happens at client side before the object is upload to S3 and KMS is cost effective as well)
     4. Manage encryption keys in an AWS CloudHSM appliance. Encrypt files prior to uploading on the employee desktop and then upload directly into amazon glacier (Not cost effective)
124. An AWS customer is deploying an application that is composed of an Auto Scaling group of EC2 Instances. The customers security policy requires that every outbound connection from these instances to any other service within the customers Virtual Private Cloud must be authenticated using a unique x 509 certificate that contains the specific instance-id. In addition an x 509 certificates must be designed by the customer’s Key management service in order to be trusted for authentication.  
     Which of the following configurations will support these requirements?
     1. Configure an IAM Role that grants access to an Amazon S3 object containing a signed certificate and configure the Auto Scaling group to launch instances with this role. Have the instances bootstrap get the certificate from Amazon S3 upon first boot.
     2. Embed a certificate into the Amazon Machine Image that is used by the Auto Scaling group Have the launched instances generate a certificate signature request with the instance’s assigned instance-id to the Key management service for signature.
     3. **Configure the Auto Scaling group to send an SNS notification of the launch of a new instance to the trusted key management service. Have the Key management service generate a signed certificate and send it directly to the newly launched instance.**
     4. Configure the launched instances to generate a new certificate upon first boot. Have the Key management service poll the AutoScaling group for associated instances and send new instances a certificate signature that contains the specific instance-id.
125. What does Amazon SWF stand for?
     1. Simple Web Flow
     2. **Simple Work Flow**
     3. Simple Wireless Forms
     4. Simple Web Form
126. Regarding Amazon SWF, the coordination logic in a workflow is contained in a software program called a \_\_\_\_.
     1. Handler
     2. **Decider**
     3. Coordinator
     4. Worker
127. For which of the following use cases are Simple Workflow Service (SWF) and Amazon EC2 an appropriate solution? Choose 2 answers
     1. Using as an endpoint to collect thousands of data points per hour from a distributed fleet of sensors
     2. **Managing a multi-step and multi-decision checkout process of an e-commerce website**
     3. **Orchestrating the execution of distributed and auditable business processes**
     4. Using as an SNS (Simple Notification Service) endpoint to trigger execution of video transcoding jobs
     5. Using as a distributed session store for your web application
128. Amazon SWF is designed to help users…
     1. … Design graphical user interface interactions
     2. … Manage user identification and authorization
     3. … Store Web content
     4. **… Coordinate synchronous and asynchronous tasks which are distributed and fault tolerant.**
129. What does a “Domain” refer to in Amazon SWF?
     1. A security group in which only tasks inside can communicate with each other
     2. A special type of worker
     3. **A collection of related Workflows**
     4. The DNS record for the Amazon SWF service
130. Your company produces customer commissioned one-of-a-kind skiing helmets combining nigh fashion with custom technical enhancements Customers can show oft their Individuality on the ski slopes and have access to head-up-displays. GPS rear-view cams and any other technical innovation they wish to embed in the helmet. The current manufacturing process is data rich and complex including assessments to ensure that the custom electronics and materials used to assemble the helmets are to the highest standards Assessments are a mixture of human and automated assessments you need to add a new set of assessment to model the failure modes of the custom electronics using GPUs with CUD across a cluster of servers with low latency networking. What architecture would allow you to automate the existing process using a hybrid approach and ensure that the architecture can support the evolution of processes over time? **[PROFESSIONAL]**
     1. Use AWS Data Pipeline to manage movement of data & meta-data and assessments. Use an auto-scaling group of G2 instances in a placement group. (Involves mixture of human assessments)
     2. Use Amazon Simple Workflow (SWF) to manage assessments, movement of data & meta-data. Use an autoscaling group of G2 instances in a placement group. (Human and automated assessments with GPU and low latency networking)
     3. Use Amazon Simple Workflow (SWF) to manage assessments movement of data & meta-data. Use an autoscaling group of C3 instances with SR-IOV (Single Root I/O Virtualization). (C3 and SR-IOV won’t provide GPU as well as Enhanced networking needs to be enabled)
     4. Use AWS data Pipeline to manage movement of data & meta-data and assessments use auto-scaling group of C3 with SR-IOV (Single Root I/O virtualization). (Involves mixture of human assessments)
131. Your startup wants to implement an order fulfillment process for selling a personalized gadget that needs an average of 3-4 days to produce with some orders taking up to 6 months you expect 10 orders per day on your first day. 1000 orders per day after 6 months and 10,000 orders after 12 months. Orders coming in are checked for consistency men dispatched to your manufacturing plant for production quality control packaging shipment and payment processing. If the product does not meet the quality standards at any stage of the process employees may force the process to repeat a step Customers are notified via email about order status and any critical issues with their orders such as payment failure. Your case architecture includes AWS Elastic Beanstalk for your website with an RDS MySQL instance for customer data and orders. How can you implement the order fulfillment process while making sure that the emails are delivered reliably? **[PROFESSIONAL]**
     1. Add a business process management application to your Elastic Beanstalk app servers and re-use the ROS database for tracking order status use one of the Elastic Beanstalk instances to send emails to customers. (Would use a SWF instead of BPM)
     2. Use SWF with an Auto Scaling group of activity workers and a decider instance in another Auto Scaling group with min/max=1. Use the decider instance to send emails to customers. (Decider sending emails might not be reliable)
     3. **Use SWF with an Auto Scaling group of activity workers and a decider instance in another Auto Scaling group with min/max=1. Use SES to send emails to customers.**
     4. Use an SQS queue to manage all process tasks. Use an Auto Scaling group of EC2 Instances that poll the tasks and execute them. Use SES to send emails to customers. (Does not provide an ability to repeat a step)
132. Select appropriate use cases for SWF with Amazon EC2? (Choose 2)
     1. **Video encoding using Amazon S3 and Amazon EC2. In this use case, large videos are uploaded to Amazon S3 in chunks. Application is built as a workflow where each video file is handled as one workflow execution.**
     2. **Processing large product catalogs using Amazon Mechanical Turk. While validating data in large catalogs, the products in the catalog are processed in batches. Different batches can be processed concurrently.**
     3. Order processing system with Amazon EC2, SQS, and SimpleDB. Use SWF notifications to orchestrate an order processing system running on EC2, where notifications sent over HTTP can trigger real-time processing in related components such as an inventory system or a shipping service.
     4. Using as an SQS (Simple Queue Service) endpoint to trigger execution of video transcoding jobs.
133. When you register an activity in Amazon SWF, you provide the following information, except:
     1. a name
     2. timeout values
     3. **a domain**
     4. version
134. Regarding Amazon SWF, at times you might want to record information in the workflow history of a workflow execution that is specific to your use case. \_\_\_\_ enable you to record information in the workflow execution history that you can use for any custom or scenario-specific purpose.
     1. **Markers**
     2. Tags
     3. Hash keys
     4. Events
135. Which of the following statements about SWF are true? Choose 3 answers.
     1. **SWF tasks are assigned once and never duplicated**
     2. SWF requires an S3 bucket for workflow storage
     3. **SWF workflow executions can last up to a year**
     4. SWF triggers SNS notifications on task assignment
     5. **SWF uses deciders and workers to complete tasks**
     6. SWF requires at least 1 EC2 instance per domain

An International company has deployed a multi-tier web application that relies on DynamoDB in a single region. For regulatory reasons they need disaster recovery capability in a separate region with a Recovery Time Objective of 2 hours and a Recovery Point Objective of 24 hours. They should synchronize their data on a regular basis and be able to provision the web application rapidly using CloudFormation. The objective is to minimize changes to the existing web application, control the throughput of DynamoDB used for the synchronization of data and synchronize only the modified elements. Which design would you choose to meet these requirements?

1. **Use AWS data Pipeline to schedule a DynamoDB cross region copy once a day. Create a ‘Lastupdated’ attribute in your DynamoDB table that would represent the timestamp of the last update and use it as a filter.** (Refer [Blog Post](https://aws.amazon.com/blogs/aws/copy-dynamodb-data-between-regions-using-the-aws-data-pipeline/))
2. Use EMR and write a custom script to retrieve data from DynamoDB in the current region using a SCAN operation and push it to DynamoDB in the second region. (No Schedule and throughput control)
3. Use AWS data Pipeline to schedule an export of the DynamoDB table to S3 in the current region once a day then schedule another task immediately after it that will import data from S3 to DynamoDB in the other region. (With AWS Data pipeline the data can be copied directly to other DynamoDB table)
4. Send each item into an SQS queue in the second region; use an auto-scaling group behind the SQS queue to replay the write in the second region. (Not Automated to replay the write)
5. You have a business-to-business web application running in a VPC consisting of an Elastic Load Balancer (ELB), web servers, application servers and a database. Your web application should only accept traffic from predefined customer IP addresses. Which two options meet this security requirement? Choose 2 answers
   1. Configure web server VPC security groups to allow traffic from your customers’ IPs (Web server is behind the ELB and customer IPs will never reach web servers)
   2. **Configure your web servers to filter traffic based on the ELB’s “X-forwarded-for” header** (get the customer IPs and create a custom filter to restrict access. Refer [link](https://aws.amazon.com/premiumsupport/knowledge-center/log-client-ip-load-balancer-apache/))
   3. **Configure ELB security groups to allow traffic from your customers’ IPs and deny all outbound traffic** (ELB will see the customer IPs so can restrict access, deny all is basically have no rules in outbound traffic, implicit, and its stateful so would work)
   4. Configure a VPC NACL to allow web traffic from your customers’ IPs and deny all outbound traffic (NACL is stateless, deny all will not work)
6. A user has created a VPC with public and private subnets using the VPC Wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24. Which of the below mentioned entries are required in the main route table to allow the instances in VPC to communicate with each other?
   1. Destination : 20.0.0.0/24 and Target : VPC
   2. Destination : 20.0.0.0/16 and Target : ALL
   3. Destination : 20.0.0.0/0 and Target : ALL
   4. **Destination : 20.0.0.0/16 and Target : Local**
7. A user has created a VPC with two subnets: one public and one private. The user is planning to run the patch update for the instances in the private subnet. How can the instances in the private subnet connect to the internet?
   1. Use the internet gateway with a private IP
   2. Allow outbound traffic in the security group for port 80 to allow internet updates
   3. The private subnet can never connect to the internet
   4. **Use NAT with an elastic IP**
8. A user has launched an EC2 instance and installed a website with the Apache webserver. The webserver is running but the user is not able to access the website from the Internet. What can be the possible reason for this failure?
   1. **The security group of the instance is not configured properly.**
   2. The instance is not configured with the proper key-pairs.
   3. The Apache website cannot be accessed from the Internet.
   4. Instance is not configured with an elastic IP.
9. A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is true in this scenario?
   1. AWS VPC will automatically create a NAT instance with the micro size
   2. **VPC bounds the main route table with a private subnet and a custom route table with a public subnet**
   3. User has to manually create a NAT instance
   4. VPC bounds the main route table with a public subnet and a custom route table with a private subnet
10. A user has created a VPC with public and private subnets. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.1.0/24 and the public subnet uses CIDR 20.0.0.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group of the NAT instance. Which of the below mentioned entries is not required for the NAT security group?
    1. For Inbound allow Source: 20.0.1.0/24 on port 80
    2. For Outbound allow Destination: 0.0.0.0/0 on port 80
    3. **For Inbound allow Source: 20.0.0.0/24 on port 80**
    4. For Outbound allow Destination: 0.0.0.0/0 on port 443
11. A user has created a VPC with CIDR 20.0.0.0/24. The user has used all the IPs of CIDR and wants to increase the size of the VPC. The user has two subnets: public (20.0.0.0/25) and private (20.0.0.128/25). How can the user change the size of the VPC?
    1. The user can delete all the instances of the subnet. Change the size of the subnets to 20.0.0.0/32 and 20.0.1.0/32, respectively. Then the user can increase the size of the VPC using CLI
    2. **It is not possible to change the size of the VPC once it has been created (NOTE – You can now increase the VPC size. Read** [**Post**](https://aws.amazon.com/about-aws/whats-new/2017/08/amazon-virtual-private-cloud-vpc-now-allows-customers-to-expand-their-existing-vpcs/)**)**
    3. User can add a subnet with a higher range so that it will automatically increase the size of the VPC
    4. User can delete the subnets first and then modify the size of the VPC
12. A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). Which of the below mentioned entries is required in the web server security group (WebSecGrp)?
    1. **Configure Destination as DB Security group ID (DbSecGrp) for port 3306 Outbound**
    2. Configure port 80 for Destination 0.0.0.0/0 Outbound
    3. Configure port 3306 for source 20.0.0.0/24 InBound
    4. Configure port 80 InBound for source 20.0.0.0/16
13. A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 by mistake. The user is trying to create another subnet of CIDR 20.0.0.1/24. How can the user create the second subnet?
    1. There is no need to update the subnet as VPC automatically adjusts the CIDR of the first subnet based on the second subnet’s CIDR
    2. The user can modify the first subnet CIDR from the console
    3. **It is not possible to create a second subnet as one subnet with the same CIDR as the VPC has been created**
    4. The user can modify the first subnet CIDR with AWS CLI
14. A user has setup a VPC with CIDR 20.0.0.0/16. The VPC has a private subnet (20.0.1.0/24) and a public subnet (20.0.0.0/24). The user’s data centre has CIDR of 20.0.54.0/24 and 20.1.0.0/24. If the private subnet wants to communicate with the data centre, what will happen?
    1. It will allow traffic communication on both the CIDRs of the data centre
    2. It will not allow traffic with data centre on CIDR 20.1.0.0/24 but allows traffic communication on 20.0.54.0/24
    3. It will not allow traffic communication on any of the data centre CIDRs
    4. **It will allow traffic with data centre on CIDR 20.1.0.0/24 but does not allow on 20.0.54.0/24** (as the CIDR block would be overlapping)
15. A user has created a VPC with public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24 . The NAT instance ID is i-a12345. Which of the below mentioned entries are required in the main route table attached with the private subnet to allow instances to connect with the internet?
    1. **Destination: 0.0.0.0/0 and Target: i-a12345**
    2. Destination: 20.0.0.0/0 and Target: 80
    3. Destination: 20.0.0.0/0 and Target: i-a12345
    4. Destination: 20.0.0.0/24 and Target: i-a12345
16. A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user’s data centre. The user’s data centre has CIDR 172.28.0.0/12. The user has also setup a NAT instance (i-123456) to allow traffic to the internet from the VPN subnet. Which of the below mentioned options is not a valid entry for the main route table in this scenario?
    1. **Destination: 20.0.1.0/24 and Target: i-12345**
    2. Destination: 0.0.0.0/0 and Target: i-12345
    3. Destination: 172.28.0.0/12 and Target: vgw-12345
    4. Destination: 20.0.0.0/16 and Target: local
17. A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC. The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24. What will happen in this scenario?
    1. The VPC will modify the first subnet CIDR automatically to allow the second subnet IP range
    2. It is not possible to create a subnet with the same CIDR as VPC
    3. The second subnet will be created
    4. **It will throw a CIDR overlaps error**
18. A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created both Public and VPN-Only subnets along with hardware VPN access to connect to the user’s data centre. The user has not yet launched any instance as well as modified or deleted any setup. He wants to delete this VPC from the console. Will the console allow the user to delete the VPC?
    1. Yes, the console will delete all the setups and also delete the virtual private gateway
    2. No, the console will ask the user to manually detach the virtual private gateway first and then allow deleting the VPC
    3. **Yes, the console will delete all the setups and detach the virtual private gateway**
    4. No, since the NAT instance is running
19. A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). Which of the below mentioned entries is required in the private subnet database security group (DBSecGrp)?
    1. **Allow Inbound on port 3306 for Source Web Server Security Group (WebSecGrp)**
    2. Allow Inbound on port 3306 from source 20.0.0.0/16
    3. Allow Outbound on port 3306 for Destination Web Server Security Group (WebSecGrp.
    4. Allow Outbound on port 80 for Destination NAT Instance IP
20. A user has created a VPC with a subnet and a security group. The user has launched an instance in that subnet and attached a public IP. The user is still unable to connect to the instance. The internet gateway has also been created. What can be the reason for the error?
    1. **The internet gateway is not configured with the route table**
    2. The private IP is not present
    3. The outbound traffic on the security group is disabled
    4. The internet gateway is not configured with the security group
21. A user has created a subnet in VPC and launched an EC2 instance within it. The user has not selected the option to assign the IP address while launching the instance. Which of the below mentioned statements is true with respect to the Instance requiring access to the Internet?
    1. The instance will always have a public DNS attached to the instance by default
    2. The user can directly attach an elastic IP to the instance
    3. The instance will never launch if the public IP is not assigned
    4. **The user would need to create an internet gateway and then attach an elastic IP to the instance to connect from internet**
22. A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is not true in this scenario?
    1. **VPC will create a routing instance and attach it with a public subnet**
    2. VPC will create two subnets
    3. VPC will create one internet gateway and attach it to VPC
    4. VPC will launch one NAT instance with an elastic IP
23. A user has created a VPC with the public subnet. The user has created a security group for that VPC. Which of the below mentioned statements is true when a security group is created?
    1. It can connect to the AWS services, such as S3 and RDS by default
    2. It will have all the inbound traffic by default
    3. **It will have all the outbound traffic by default**
    4. It will by default allow traffic to the internet gateway
24. A user has created a VPC with CIDR 20.0.0.0/16 using VPC Wizard. The user has created a public CIDR (20.0.0.0/24) and a VPN only subnet CIDR (20.0.1.0/24) along with the hardware VPN access to connect to the user’s data centre. Which of the below mentioned components is not present when the VPC is setup with the wizard?
    1. Main route table attached with a VPN only subnet
    2. **A NAT instance configured to allow the VPN subnet instances to connect with the internet**
    3. Custom route table attached with a public subnet
    4. An internet gateway for a public subnet
25. A user has created a VPC with public and private subnets using the VPC wizard. The user has not launched any instance manually and is trying to delete the VPC. What will happen in this scenario?
    1. It will not allow to delete the VPC as it has subnets with route tables
    2. It will not allow to delete the VPC since it has a running route instance
    3. It will terminate the VPC along with all the instances launched by the wizard
    4. **It will not allow to delete the VPC since it has a running NAT instance**
26. A user has created a public subnet with VPC and launched an EC2 instance within it. The user is trying to delete the subnet. What will happen in this scenario?
    1. It will delete the subnet and make the EC2 instance as a part of the default subnet
    2. **It will not allow the user to delete the subnet until the instances are terminated**
    3. It will delete the subnet as well as terminate the instances
    4. Subnet can never be deleted independently, but the user has to delete the VPC first
27. A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25 and a private subnet with CIDR 20.0.0.128/25. The user has launched one instance each in the private and public subnets. Which of the below mentioned options cannot be the correct IP address (private IP) assigned to an instance in the public or private subnet?
    1. **20.0.0.255**
    2. 20.0.0.132
    3. 20.0.0.122
    4. 20.0.0.55
28. A user has created a VPC with CIDR 20.0.0.0/16. The user has created public and VPN only subnets along with hardware VPN access to connect to the user’s datacenter. The user wants to make so that all traffic coming to the public subnet follows the organization’s proxy policy. How can the user make this happen?
    1. Setting up a NAT with the proxy protocol and configure that the public subnet receives traffic from NAT
    2. Setting up a proxy policy in the internet gateway connected with the public subnet
    3. It is not possible to setup the proxy policy for a public subnet
    4. **Setting the route table and security group of the public subnet which receives traffic from a virtual private gateway**
29. A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user’s data centre. Which of the below mentioned options is a valid entry for the main route table in this scenario?
    1. Destination: 20.0.0.0/24 and Target: vgw-12345
    2. Destination: 20.0.0.0/16 and Target: ALL
    3. Destination: 20.0.1.0/16 and Target: vgw-12345
    4. **Destination: 0.0.0.0/0 and Target: vgw-12345**
30. Which two components provide connectivity with external networks? When attached to an Amazon VPC which two components provide connectivity with external networks? Choose 2 answers
    1. Elastic IPs (EIP) (Does not provide connectivity, public IP address will do as well)
    2. NAT Gateway (NAT) (Not Attached to VPC and still needs IGW)
    3. **Internet Gateway (IGW)**
    4. **Virtual Private Gateway (VGW)**
31. You are attempting to connect to an instance in Amazon VPC without success You have already verified that the VPC has an Internet Gateway (IGW) the instance has an associated Elastic IP (EIP) and correct security group rules are in place. Which VPC component should you evaluate next?
    1. The configuration of a NAT instance
    2. **The configuration of the Routing Table**
    3. The configuration of the internet Gateway (IGW)
    4. The configuration of SRC/DST checking
32. If you want to launch Amazon Elastic Compute Cloud (EC2) Instances and assign each Instance a predetermined private IP address you should:
    1. Assign a group or sequential Elastic IP address to the instances
    2. Launch the instances in a Placement Group
    3. **Launch the instances in the Amazon virtual Private Cloud (VPC)**
    4. Use standard EC2 instances since each instance gets a private Domain Name Service (DNS) already
    5. Launch the Instance from a private Amazon Machine image (AMI)
33. A user has recently started using EC2. The user launched one EC2 instance in the default subnet in EC2-VPC Which of the below mentioned options is not attached or available with the EC2 instance when it is launched?
    1. Public IP address
    2. Internet gateway
    3. **Elastic IP**
    4. Private IP address
34. A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25. The user is trying to create the private subnet with CIDR 20.0.0.128/25. Which of the below mentioned statements is true in this scenario?
    1. It will not allow the user to create the private subnet due to a CIDR overlap
    2. **It will allow the user to create a private subnet with CIDR as 20.0.0.128/25**
    3. This statement is wrong as AWS does not allow CIDR 20.0.0.0/25
    4. It will not allow the user to create a private subnet due to a wrong CIDR range
35. A user has created a VPC with CIDR 20.0.0.0/16 with only a private subnet and VPN connection using the VPC wizard. The user wants to connect to the instance in a private subnet over SSH. How should the user define the security rule for SSH?
    1. **Allow Inbound traffic on port 22 from the user’s network**
    2. The user has to create an instance in EC2 Classic with an elastic IP and configure the security group of a private subnet to allow SSH from that elastic IP
    3. The user can connect to a instance in a private subnet using the NAT instance
    4. Allow Inbound traffic on port 80 and 22 to allow the user to connect to a private subnet over the Internet
36. A company wants to implement their website in a virtual private cloud (VPC). The web tier will use an Auto Scaling group across multiple Availability Zones (AZs). The database will use Multi-AZ RDS MySQL and should not be publicly accessible. What is the minimum number of subnets that need to be configured in the VPC?
    1. 1
    2. 2
    3. 3
    4. **4** (2 public subnets for web instances in multiple AZs and 2 private subnets for RDS Multi-AZ)
37. Which of the following are characteristics of Amazon VPC subnets? Choose 2 answers
    1. **Each subnet maps to a single Availability Zone**
    2. A CIDR block mask of /25 is the smallest range supported
    3. Instances in a private subnet can communicate with the Internet only if they have an Elastic IP.
    4. **By default, all subnets can route between each other, whether they are private or public**
    5. Each subnet spans at least 2 Availability zones to provide a high-availability environment
38. You need to design a VPC for a web-application consisting of an Elastic Load Balancer (ELB). a fleet of web/application servers, and an RDS database The entire Infrastructure must be distributed over 2 availability zones. Which VPC configuration works while assuring the database is not available from the Internet?
    1. One public subnet for ELB one public subnet for the web-servers, and one private subnet for the database
    2. One public subnet for ELB two private subnets for the web-servers, two private subnets for RDS
    3. **Two public subnets for ELB two private subnets for the web-servers and two private subnets for RDS**
    4. Two public subnets for ELB two public subnets for the web-servers, and two public subnets for RDS
39. You have deployed a three-tier web application in a VPC with a CIDR block of 10.0.0.0/28. You initially deploy two web servers, two application servers, two database servers and one NAT instance tor a total of seven EC2 instances. The web, application and database servers are deployed across two availability zones (AZs). You also deploy an ELB in front of the two web servers, and use Route53 for DNS Web traffic gradually increases in the first few days following the deployment, so you attempt to double the number of instances in each tier of the application to handle the new load unfortunately some of these new instances fail to launch. Which of the following could the root caused? (Choose 2 answers) **[PROFESSIONAL]**
    1. The Internet Gateway (IGW) of your VPC has scaled-up adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches.
    2. AWS reserves one IP address in each subnet’s CIDR block for Route53 so you do not have enough addresses left to launch all of the new EC2 instances.
    3. AWS reserves the first and the last private IP address in each subnet’s CIDR block so you do not have enough addresses left to launch all of the new EC2 instances.
    4. **The ELB has scaled-up. Adding more instances to handle the traffic reducing the number of available private IP addresses for new instance launches**
    5. **AWS reserves the first four and the last IP address in each subnet’s CIDR block so you do not have enough addresses left to launch all of the new EC2 instances.**
40. A user wants to access RDS from an EC2 instance using IP addresses. Both RDS and EC2 are in the same region, but different AZs. Which of the below mentioned options help configure that the instance is accessed faster?
    1. **Configure the Private IP of the Instance in RDS security group** (Recommended as the data is transferred within the the Amazon network and not through internet – Refer [link](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithSecurityGroups.html#USER_WorkingWithSecurityGroups.Authorizing\))
    2. Security group of EC2 allowed in the RDS security group
    3. Configuring the elastic IP of the instance in RDS security group
    4. Configure the Public IP of the instance in RDS security group
41. In regards to VPC, select the correct statement:
    1. **You can associate multiple subnets with the same Route Table.**
    2. You can associate multiple subnets with the same Route Table, but you can’t associate a subnet with only one Route Table.
    3. You can’t associate multiple subnets with the same Route Table.
    4. None of these.
42. You need to design a VPC for a web-application consisting of an ELB a fleet of web application servers, and an RDS DB. The entire infrastructure must be distributed over 2 AZ. Which VPC configuration works while assuring the DB is not available from the Internet?
    1. One Public Subnet for ELB, one Public Subnet for the web-servers, and one private subnet for the DB
    2. One Public Subnet for ELB, two Private Subnets for the web-servers, and two private subnets for the RDS
    3. **Two Public Subnets for ELB, two private Subnet for the web-servers, and two private subnet for the RDS**
    4. Two Public Subnets for ELB, two Public Subnet for the web-servers, and two public subnets for the RDS
43. You have an Amazon VPC with one private subnet and one public subnet with a Network Address Translator (NAT) server. You are creating a group of Amazon Elastic Cloud Compute (EC2) instances that configure themselves at startup via downloading a bootstrapping script from Amazon Simple Storage Service (S3) that deploys an application via GIT. Which setup provides the highest level of security?
    1. **Amazon EC2 instances in private subnet, no EIPs, route outgoing traffic via the NAT**
    2. Amazon EC2 instances in public subnet, no EIPs, route outgoing traffic via the Internet Gateway (IGW)
    3. Amazon EC2 instances in private subnet, assign EIPs, route outgoing traffic via the Internet Gateway (IGW)
    4. Amazon EC2 instances in public subnet, assign EIPs, route outgoing traffic via the NAT
44. You have launched an Amazon Elastic Compute Cloud (EC2) instance into a public subnet with a primary private IP address assigned, an internet gateway is attached to the VPC, and the public route table is configured to send all Internet-based traffic to the Internet gateway. The instance security group is set to allow all outbound traffic but cannot access the Internet. Why is the Internet unreachable from this instance?
    1. **The instance does not have a public IP address**
    2. The Internet gateway security group must allow all outbound traffic.
    3. The instance security group must allow all inbound traffic.
    4. The instance “Source/Destination check” property must be enabled.
45. You have an environment that consists of a public subnet using Amazon VPC and 3 instances that are running in this subnet. These three instances can successfully communicate with other hosts on the Internet. You launch a fourth instance in the same subnet, using the same AMI and security group configuration you used for the others, but find that this instance cannot be accessed from the internet. What should you do to enable Internet access?
    1. Deploy a NAT instance into the public subnet.
    2. **Assign an Elastic IP address to the fourth instance**
    3. Configure a publically routable IP Address in the host OS of the fourth instance.
    4. Modify the routing table for the public subnet.
46. You have a load balancer configured for VPC, and all back-end Amazon EC2 instances are in service. However, your web browser times out when connecting to the load balancer’s DNS name. Which options are probable causes of this behavior? Choose 2 answers
    1. **The load balancer was not configured to use a public subnet with an Internet gateway configured**
    2. The Amazon EC2 instances do not have a dynamically allocated private IP address
    3. **The security groups or network ACLs are not property configured for web traffic.**
    4. The load balancer is not configured in a private subnet with a NAT instance.
    5. The VPC does not have a VGW configured.
47. When will you incur costs with an Elastic IP address (EIP)?
    1. When an EIP is allocated.
    2. When it is allocated and associated with a running instance.
    3. **When it is allocated and associated with a stopped instance.**
    4. Costs are incurred regardless of whether the EIP is associated with a running instance.
48. You are deploying an application to track GPS coordinates of delivery trucks in the United States. Coordinates are transmitted from each delivery truck once every three seconds. You need to design an architecture that will enable real-time processing of these coordinates from multiple consumers. Which service should you use to implement data ingestion?
    1. **Amazon Kinesis**
    2. AWS Data Pipeline
    3. Amazon AppStream
    4. Amazon Simple Queue Service
49. You are deploying an application to collect votes for a very popular television show. Millions of users will submit votes using mobile devices. The votes must be collected into a durable, scalable, and highly available data store for real-time public tabulation. Which service should you use?
    1. **Amazon DynamoDB**
    2. Amazon Redshift
    3. Amazon Kinesis
    4. Amazon Simple Queue Service
50. Your company is in the process of developing a next generation pet collar that collects biometric information to assist families with promoting healthy lifestyles for their pets. Each collar will push 30kb of biometric data In JSON format every 2 seconds to a collection platform that will process and analyze the data providing health trending information back to the pet owners and veterinarians via a web portal Management has tasked you to architect the collection platform ensuring the following requirements are met. Provide the ability for real-time analytics of the inbound biometric data Ensure processing of the biometric data is highly durable, elastic and parallel. The results of the analytic processing should be persisted for data mining. Which architecture outlined below will meet the initial requirements for the collection platform?
    1. Utilize S3 to collect the inbound sensor data analyze the data from S3 with a daily scheduled Data Pipeline and save the results to a Redshift Cluster.
    2. **Utilize Amazon Kinesis to collect the inbound sensor data, analyze the data with Kinesis clients and save the results to a Redshift cluster using EMR. (**refer [**link**](https://aws.amazon.com/about-aws/whats-new/2014/02/20/analyze-streaming-data-from-amazon-kinesis-with-amazon-elastic-mapreduce/)**)**
    3. Utilize SQS to collect the inbound sensor data analyze the data from SQS with Amazon Kinesis and save the results to a Microsoft SQL Server RDS instance.
    4. Utilize EMR to collect the inbound sensor data, analyze the data from EUR with Amazon Kinesis and save me results to DynamoDB.
51. Your customer is willing to consolidate their log streams (access logs, application logs, security logs etc.) in one single system. Once consolidated, the customer wants to analyze these logs in real time based on heuristics. From time to time, the customer needs to validate heuristics, which requires going back to data samples extracted from the last 12 hours? What is the best approach to meet your customer’s requirements?
    1. Send all the log events to Amazon SQS. Setup an Auto Scaling group of EC2 servers to consume the logs and apply the heuristics.
    2. **Send all the log events to Amazon Kinesis develop a client process to apply heuristics on the logs** (Can perform real time analysis and stores data for 24 hours which can be extended to 7 days)
    3. Configure Amazon CloudTrail to receive custom logs, use EMR to apply heuristics the logs (CloudTrail is only for auditing)
    4. Setup an Auto Scaling group of EC2 syslogd servers, store the logs on S3 use EMR to apply heuristics on the logs (EMR is for batch analysis)
52. You require the ability to analyze a customer’s clickstream data on a website so they can do behavioral analysis. Your customer needs to know what sequence of pages and ads their customer clicked on. This data will be used in real time to modify the page layouts as customers click through the site to increase stickiness and advertising click-through. Which option meets the requirements for captioning and analyzing this data?
    1. Log clicks in weblogs by URL store to Amazon S3, and then analyze with Elastic MapReduce
    2. **Push web clicks by session to Amazon Kinesis and analyze behavior using Kinesis workers**
    3. Write click events directly to Amazon Redshift and then analyze with SQL
    4. Publish web clicks by session to an Amazon SQS queue men periodically drain these events to Amazon RDS and analyze with SQL
53. Your social media monitoring application uses a Python app running on AWS Elastic Beanstalk to inject tweets, Facebook updates and RSS feeds into an Amazon Kinesis stream. A second AWS Elastic Beanstalk app generates key performance indicators into an Amazon DynamoDB table and powers a dashboard application. What is the most efficient option to prevent any data loss for this application?
    1. Use AWS Data Pipeline to replicate your DynamoDB tables into another region.
    2. Use the second AWS Elastic Beanstalk app to store a backup of Kinesis data onto Amazon Elastic Block Store (EBS), and then create snapshots from your Amazon EBS volumes.
    3. Add a second Amazon Kinesis stream in another Availability Zone and use AWS data pipeline to replicate data across Kinesis streams.
    4. **Add a third AWS Elastic Beanstalk app that uses the Amazon Kinesis S3 connector to archive data from Amazon Kinesis into Amazon S3.**
54. You need to replicate API calls across two systems in real time. What tool should you use as a buffer and transport mechanism for API call events?
    1. AWS SQS
    2. AWS Lambda
    3. **AWS Kinesis** (AWS Kinesis is an event stream service. Streams can act as buffers and transport across systems for in-order programmatic events, making it ideal for replicating API calls across systems)
    4. AWS SNS
55. You need to perform ad-hoc business analytics queries on well-structured data. Data comes in constantly at a high velocity. Your business intelligence team can understand SQL. What AWS service(s) should you look to first?
    1. Kinesis Firehose + RDS
    2. **Kinesis Firehose + RedShift** (Kinesis Firehose provides a managed service for aggregating streaming data and inserting it into RedShift. RedShift also supports ad-hoc queries over well-structured data using a SQL-compliant wire protocol, so the business team should be able to adopt this system easily. Refer [link](https://aws.amazon.com/kinesis/firehose/details/))
    3. EMR using Hive
    4. EMR running Apache Spark
56. A media company produces new video files on-premises every day with a total size of around 100GB after compression. All files have a size of 1-2 GB and need to be uploaded to Amazon S3 every night in a fixed time window between 3am and 5am. Current upload takes almost 3 hours, although less than half of the available bandwidth is used. What step(s) would ensure that the file uploads are able to complete in the allotted time window?
    1. Increase your network bandwidth to provide faster throughput to S3
    2. **Upload the files in parallel to S3 using multipart upload**
    3. Pack all files into a single archive, upload it to S3, then extract the files in AWS
    4. Use AWS Import/Export to transfer the video files
57. You are designing a web application that stores static assets in an Amazon Simple Storage Service (S3) bucket. You expect this bucket to immediately receive over 150 PUT requests per second. What should you do to ensure optimal performance?
    1. Use multi-part upload.
    2. **Add a random prefix to the key names.**
    3. Amazon S3 will automatically manage performance at this scale.
    4. Use a predictable naming scheme, such as sequential numbers or date time sequences, in the key names
58. You have an application running on an Amazon Elastic Compute Cloud instance, that uploads 5 GB video objects to Amazon Simple Storage Service (S3). Video uploads are taking longer than expected, resulting in poor application performance. Which method will help improve performance of your application?
    1. Enable enhanced networking
    2. **Use Amazon S3 multipart upload**
    3. Leveraging Amazon CloudFront, use the HTTP POST method to reduce latency.
    4. Use Amazon Elastic Block Store Provisioned IOPs and use an Amazon EBS-optimized instance
59. Which of the following methods gives you protection against accidental loss of data stored in Amazon S3? (Choose 2)
    1. **Set bucket policies to restrict deletes, and also enable versioning**
    2. By default, versioning is enabled on a new bucket so you don’t have to worry about it (Not enabled by default)
    3. Build a secondary index of your keys to protect the data (improves performance only)
    4. **Back up your bucket to a bucket owned by another AWS account for redundancy**
60. A startup company hired you to help them build a mobile application that will ultimately store billions of image and videos in Amazon S3. The company is lean on funding, and wants to minimize operational costs, however, they have an aggressive marketing plan, and expect to double their current installation base every six months. Due to the nature of their business, they are expecting sudden and large increases to traffic to and from S3, and need to ensure that it can handle the performance needs of their application. What other information must you gather from this customer in order to determine whether S3 is the right option?
    1. You must know how many customers that company has today, because this is critical in understanding what their customer base will be in two years. (No. of customers do not matter)
    2. **You must find out total number of requests per second at peak usage.**
    3. You must know the size of the individual objects being written to S3 in order to properly design the key namespace. (Size does not relate to the key namespace design but the count does)
    4. In order to build the key namespace correctly, you must understand the total amount of storage needs for each S3 bucket. (S3 provided unlimited storage the key namespace design would depend on the number)
61. A document storage company is deploying their application to AWS and changing their business model to support both free tier and premium tier users. The premium tier users will be allowed to store up to 200GB of data and free tier customers will be allowed to store only 5GB. The customer expects that billions of files will be stored. All users need to be alerted when approaching 75 percent quota utilization and again at 90 percent quota use. To support the free tier and premium tier users, how should they architect their application?
    1. **The company should utilize an amazon simple workflow service activity worker that updates the users data counter in amazon dynamo DB. The activity worker will use simple email service to send an email if the counter increases above the appropriate thresholds.**
    2. The company should deploy an amazon relational data base service relational database with a store objects table that has a row for each stored object along with size of each object. The upload server will query the aggregate consumption of the user in questions (by first determining the files store by the user, and then querying the stored objects table for respective file sizes) and send an email via Amazon Simple Email Service if the thresholds are breached. (Good Approach to use RDS but with so many objects might not be a good option)
    3. The company should write both the content length and the username of the files owner as S3 metadata for the object. They should then create a file watcher to iterate over each object and aggregate the size for each user and send a notification via Amazon Simple Queue Service to an emailing service if the storage threshold is exceeded. (List operations on S3 not feasible)
    4. The company should create two separated amazon simple storage service buckets one for data storage for free tier users and another for data storage for premium tier users. An amazon simple workflow service activity worker will query all objects for a given user based on the bucket the data is stored in and aggregate storage. The activity worker will notify the user via Amazon Simple Notification Service when necessary (List operations on S3 not feasible as well as SNS does not address email requirement)
62. Your company host a social media website for storing and sharing documents. the web application allow users to upload large files while resuming and pausing the upload as needed. Currently, files are uploaded to your php front end backed by Elastic Load Balancing and an autoscaling fleet of amazon elastic compute cloud (EC2) instances that scale upon average of bytes received (NetworkIn) After a file has been uploaded. it is copied to amazon simple storage service(S3). Amazon Ec2 instances use an AWS Identity and Access Management (AMI) role that allows Amazon s3 uploads. Over the last six months, your user base and scale have increased significantly, forcing you to increase the auto scaling groups Max parameter a few times. Your CFO is concerned about the rising costs and has asked you to adjust the architecture where needed to better optimize costs. Which architecture change could you introduce to reduce cost and still keep your web application secure and scalable?
    1. Replace the Autoscaling launch Configuration to include c3.8xlarge instances; those instances can potentially yield a network throughput of 10gbps. (no info of current size and might increase cost)
    2. Re-architect your ingest pattern, have the app authenticate against your identity provider as a broker fetching temporary AWS credentials from AWS Secure token service (GetFederation Token). Securely pass the credentials and s3 endpoint/prefix to your app. Implement client-side logic to directly upload the file to amazon s3 using the given credentials and S3 Prefix. (will not provide the ability to handle pause and restarts)
    3. Re-architect your ingest pattern, and move your web application instances into a VPC public subnet. Attach a public IP address for each EC2 instance (using the auto scaling launch configuration settings). Use Amazon Route 53 round robin records set and http health check to DNS load balance the app request this approach will significantly reduce the cost by bypassing elastic load balancing. (ELB is not the bottleneck)
    4. **Re-architect your ingest pattern, have the app authenticate against your identity provider as a broker fetching temporary AWS credentials from AWS Secure token service (GetFederation Token). Securely pass the credentials and s3 endpoint/prefix to your app. Implement client-side logic that used the S3 multipart upload API to directly upload the file to Amazon s3 using the given credentials and s3 Prefix.** (multipart allows one to start uploading directly to S3 before the actual size is known or complete data is downloaded)
63. If an application is storing hourly log files from thousands of instances from a high traffic web site, which naming scheme would give optimal performance on S3?
    1. Sequential
    2. instanceID\_log-HH-DD-MM-YYYY
    3. instanceID\_log-YYYY-MM-DD-HH
    4. **HH-DD-MM-YYYY-log\_instanceID** (HH will give some randomness to start with instead of instaneId where the first characters would be i-)
    5. YYYY-MM-DD-HH-log\_instanceID
64. You are building a solution for a customer to extend their on-premises data center to AWS. The customer requires a 50-Mbps dedicated and private connection to their VPC. Which AWS product or feature satisfies this requirement?
    1. Amazon VPC peering
    2. Elastic IP Addresses
    3. **AWS Direct Connect**
    4. Amazon VPC virtual private gateway
65. Is there any way to own a direct connection to Amazon Web Services?
    1. You can create an encrypted tunnel to VPC, but you don’t own the connection.
    2. Yes, it’s called Amazon Dedicated Connection.
    3. No, AWS only allows access from the public Internet.
    4. **Yes, it’s called Direct Connect**
66. An organization has established an Internet-based VPN connection between their on-premises data center and AWS. They are considering migrating from VPN to AWS Direct Connect. Which operational concern should drive an organization to consider switching from an Internet-based VPN connection to AWS Direct Connect?
    1. AWS Direct Connect provides greater redundancy than an Internet-based VPN connection.
    2. AWS Direct Connect provides greater resiliency than an Internet-based VPN connection.
    3. **AWS Direct Connect provides greater bandwidth than an Internet-based VPN connection.**
    4. AWS Direct Connect provides greater control of network provider selection than an Internet-based VPN connection.
67. Does AWS Direct Connect allow you access to all Availabilities Zones within a Region?
    1. Depends on the type of connection
    2. No
    3. **Yes**
    4. Only when there’s just one availability zone in a region. If there are more than one, only one availability zone can be accessed directly.
68. A customer has established an AWS Direct Connect connection to AWS. The link is up and routes are being advertised from the customer’s end, however the customer is unable to connect from EC2 instances inside its VPC to servers residing in its datacenter. Which of the following options provide a viable solution to remedy this situation? (Choose 2 answers)
    1. Add a route to the route table with an IPSec VPN connection as the target (deals with VPN)
    2. **Enable route propagation to the Virtual Private Gateway (VGW)**
    3. Enable route propagation to the customer gateway (CGW) (route propagation is enabled on VGW)
    4. Modify the route table of all Instances using the ‘route’ command. (no route command available)
    5. **Modify the Instances VPC subnet route table by adding a route back to the customer’s on-premises environment.**
69. A company has configured and peered two VPCs: VPC-1 and VPC-2. VPC-1 contains only private subnets, and VPC-2 contains only public subnets. The company uses a single AWS Direct Connect connection and private virtual interface to connect their on-premises network with VPC-1. Which two methods increase the fault tolerance of the connection to VPC-1? Choose 2 answers
    1. Establish a hardware VPN over the internet between VPC-2 and the on-premises network. (Peered VPC does not support Edge to Edge Routing)
    2. **Establish a hardware VPN over the internet between VPC-1 and the on-premises network**
    3. Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2 (Peered VPC does not support Edge to Edge Routing)
    4. Establish a new AWS Direct Connect connection and private virtual interface in a different AWS region than VPC-1 (need to be in the same region as VPC-1)
    5. **Establish a new AWS Direct Connect connection and private virtual interface in the same AWS region as VPC-1**
70. Your company previously configured a heavily used, dynamically routed VPN connection between your on premises data center and AWS. You recently provisioned a Direct Connect connection and would like to start using the new connection. After configuring Direct Connect settings in the AWS Console, which of the following options will provide the most seamless transition for your users?
    1. Delete your existing VPN connection to avoid routing loops configure your Direct Connect router with the appropriate settings and verity network traffic is leveraging Direct Connect.
    2. Configure your Direct Connect router with a higher BGP priority than your VPN router, verify network traffic is leveraging Direct Connect and then delete your existing VPN connection.
    3. **Update your VPC route tables to point to the Direct Connect connection configure your Direct Connect router with the appropriate settings verify network traffic is leveraging Direct Connect and then delete the VPN connection.**
    4. Configure your Direct Connect router, update your VPC route tables to point to the Direct Connect connection, configure your VPN connection with a higher BGP priority. And verify network traffic is leveraging the Direct Connect connection
71. You are designing the network infrastructure for an application server in Amazon VPC. Users will access all the application instances from the Internet as well as from an on-premises network The on-premises network is connected to your VPC over an AWS Direct Connect link. How would you design routing to meet the above requirements?
    1. Configure a single routing Table with a default route via the Internet gateway. Propagate a default route via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnets (propagating default route would cause conflict)
    2. **Configure a single routing table with a default route via the internet gateway. Propagate specific routes for the on-premises networks via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnets.**
    3. Configure a single routing table with two default routes: one to the internet via an Internet gateway the other to the on-premises network via the VPN gateway use this routing table across all subnets in your VPC. (there cannot be 2 default routes)
    4. Configure two routing tables one that has a default route via the Internet gateway and another that has a default route via the VPN gateway Associate both routing tables with each VPC subnet. (as the instances has to be in public subnet and should have a single routing table associated with them)
72. You are implementing AWS Direct Connect. You intend to use AWS public service end points such as Amazon S3, across the AWS Direct Connect link. You want other Internet traffic to use your existing link to an Internet Service Provider. What is the correct way to configure AWS Direct Connect for access to services such as Amazon S3?
    1. Configure a public Interface on your AWS Direct Connect link. Configure a static route via your AWS Direct Connect link that points to Amazon S3. Advertise a default route to AWS using BGP.
    2. Create a private interface on your AWS Direct Connect link. Configure a static route via your AWS Direct connect link that points to Amazon S3 Configure specific routes to your network in your VPC.
    3. **Create a public interface on your AWS Direct Connect link. Redistribute BGP routes into your existing routing infrastructure advertise specific routes for your network to AWS**
    4. Create a private interface on your AWS Direct connect link. Redistribute BGP routes into your existing routing infrastructure and advertise a default route to AWS.
73. You have been asked to design network connectivity between your existing data centers and AWS. Your application’s EC2 instances must be able to connect to existing backend resources located in your data center. Network traffic between AWS and your data centers will start small, but ramp up to 10s of GB per second over the course of several months. The success of your application is dependent upon getting to market quickly. Which of the following design options will allow you to meet your objectives?
    1. Quickly create an internal ELB for your backend applications, submit a DirectConnect request to provision a 1 Gbps cross connect between your data center and VPC, then increase the number or size of your DirectConnect connections as needed.
    2. Allocate EIPs and an Internet Gateway for your VPC instances to use for quick, temporary access to your backend applications, then provision a VPN connection between a VPC and existing on -premises equipment.
    3. **Provision a VPN connection between a VPC and existing on -premises equipment, submit a DirectConnect partner request to provision cross connects between your data center and the DirectConnect location, then cut over from the VPN connection to one or more DirectConnect connections as needed.**
    4. Quickly submit a DirectConnect request to provision a 1 Gbps cross connect between your data center and VPC, then increase the number or size of your DirectConnect connections as needed.
74. You are tasked with moving a legacy application from a virtual machine running inside your datacenter to an Amazon VPC. Unfortunately this app requires access to a number of on-premises services and no one who configured the app still works for your company. Even worse there’s no documentation for it. What will allow the application running inside the VPC to reach back and access its internal dependencies without being reconfigured? (Choose 3 answers)
    1. **An AWS Direct Connect link between the VPC and the network housing the internal services** (VPN or a DX for communication)
    2. An Internet Gateway to allow a VPN connection. (Virtual and Customer gateway is needed)
    3. An Elastic IP address on the VPC instance (Don’t need a EIP as private subnets can also interact with on-premises network)
    4. **An IP address space that does not conflict with the one on-premises** (IP address cannot conflict)
    5. Entries in Amazon Route 53 that allow the Instance to resolve its dependencies’ IP addresses (Route 53 is not required)
    6. **A VM Import of the current virtual machine** (VM Import to copy the VM to AWS as there is no documentation it can’t be configured from scratch)
75. After launching an instance that you intend to serve as a NAT (Network Address Translation) device in a public subnet you modify your route tables to have the NAT device be the target of internet bound traffic of your private subnet. When you try and make an outbound connection to the Internet from an instance in the private subnet, you are not successful. Which of the following steps could resolve the issue?
    1. Attaching a second Elastic Network interface (ENI) to the NAT instance, and placing it in the private subnet
    2. Attaching an Elastic IP address to the instance in the private subnet
    3. Attaching a second Elastic Network Interface (ENI) to the instance in the private subnet, and placing it in the public subnet
    4. **Disabling the Source/Destination Check attribute on the NAT instance**
76. You manually launch a NAT AMI in a public subnet. The network is properly configured. Security groups and network access control lists are property configured. Instances in a private subnet can access the NAT. The NAT can access the Internet. However, private instances cannot access the Internet. What additional step is required to allow access from the private instances?
    1. Enable Source/Destination Check on the private Instances.
    2. Enable Source/Destination Check on the NAT instance.
    3. Disable Source/Destination Check on the private instances
    4. **Disable Source/Destination Check on the NAT instance**
77. A user has created a VPC with public and private subnets. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.1.0/24 and the public subnet uses CIDR 20.0.0.0/24. The user is planning to host a web server in the public subnet (port 80. and a DB server in the private subnet (port 3306.. The user is configuring a security group of the NAT instance. Which of the below mentioned entries is **not** required for the NAT security group?
    1. For Inbound allow Source: 20.0.1.0/24 on port 80
    2. For Outbound allow Destination: 0.0.0.0/0 on port 80
    3. **For Inbound allow Source: 20.0.0.0/24 on port 80**(Refer [NATSG](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html#NATSG))
    4. For Outbound allow Destination: 0.0.0.0/0 on port 443
78. A web company is looking to implement an external payment service into their highly available application deployed in a VPC. Their application EC2 instances are behind a public facing ELB. Auto scaling is used to add additional instances as traffic increases. Under normal load the application runs 2 instances in the Auto Scaling group but at peak it can scale 3x in size. The application instances need to communicate with the payment service over the Internet, which requires whitelisting of all public IP addresses used to communicate with it. A maximum of 4 whitelisting IP addresses are allowed at a time and can be added through an API. How should they architect their solution?
    1. **Route payment requests through two NAT instances setup for High Availability and whitelist the Elastic IP addresses attached to the NAT instances**
    2. Whitelist the VPC Internet Gateway Public IP and route payment requests through the Internet Gateway. (Internet gateway is only to route traffic)
    3. Whitelist the ELB IP addresses and route payment requests from the Application servers through the ELB. (ELB does not have a fixed IP address)
    4. Automatically assign public IP addresses to the application instances in the Auto Scaling group and run a script on boot that adds each instances public IP address to the payment validation whitelist API. (would exceed the allowed 4 IP addresses)
79. An organization is planning to use AWS for their production roll out. The organization wants to implement automation for deployment such that it will automatically create a LAMP stack, download the latest PHP installable from S3 and setup the ELB. Which of the below mentioned AWS services meets the requirement for making an orderly deployment of the software?
    1. **AWS Elastic Beanstalk**
    2. AWS CloudFront
    3. AWS CloudFormation
    4. AWS DevOps
80. What does Amazon Elastic Beanstalk provide?
    1. A scalable storage appliance on top of Amazon Web Services.
    2. **An application container on top of Amazon Web Services**
    3. A service by this name doesn’t exist.
    4. A scalable cluster of EC2 instances
81. You want to have multiple versions of your application running at the same time, with all versions launched via AWS Elastic Beanstalk. Is this possible?
    1. However if you have 2 AWS accounts this can be done
    2. AWS Elastic Beanstalk is not designed to support multiple running environments
    3. **AWS Elastic Beanstalk is designed to support a number of multiple running environments**
    4. However AWS Elastic Beanstalk is designed to support only 2 multiple running environments
82. A .NET application that you manage is running in Elastic Beanstalk. Your developers tell you they will need access to application log files to debug issues that arise. The infrastructure will scale up and down. How can you ensure the developers will be able to access only the log files?
    1. Access the log files directly from Elastic Beanstalk
    2. **Enable log file rotation to S3 within the Elastic Beanstalk configuration**
    3. Ask your developers to enable log file rotation in the applications web.config file
    4. Connect to each Instance launched by Elastic Beanstalk and create a Windows Scheduled task to rotate the log files to S3
83. Your team has a tomcat-based Java application you need to deploy into development, test and production environments. After some research, you opt to use Elastic Beanstalk due to its tight integration with your developer tools and RDS due to its ease of management. Your QA team lead points out that you need to roll a sanitized set of production data into your environment on a nightly basis. Similarly, other software teams in your org want access to that same restored data via their EC2 instances in your VPC .The optimal setup for persistence and security that meets the above requirements would be the following. **[PROFESSIONAL]**
    1. Create your RDS instance as part of your Elastic Beanstalk definition and alter its security group to allow access to it from hosts in your application subnets. (Not optimal for persistence as the RDS is associated with the Elastic Beanstalk lifecycle and would not live independently)
    2. Create your RDS instance separately and add its IP address to your application’s DB connection strings in your code. Alter its security group to allow access to it from hosts within your VPC’s IP address block. (RDS is connected using DNS endpoint only)
    3. **Create your RDS instance separately and pass its DNS name to your app’s DB connection string as an environment variable. Create a security group for client machines and add it as a valid source for DB traffic to the security group of the RDS instance itself.** (Security group allows instances to access the RDS with new instances launched without any changes)
    4. Create your RDS instance separately and pass its DNS name to your DB connection string as an environment variable. Alter its security group to allow access to it from hosts in your application subnets. (Not optimal for security adding individual hosts)
84. Your must architect the migration of a web application to AWS. The application consists of Linux web servers running a custom web server. You are required to save the logs generated from the application to a durable location. What options could you select to migrate the application to AWS? (Choose 2) **[PROFESSIONAL]**
    1. Create an AWS Elastic Beanstalk application using the custom web server platform. Specify the web server executable and the application project and source files. Enable log file rotation to Amazon Simple Storage Service (S3). (EB does not work with Custom server executable)
    2. Create Dockerfile for the application. Create an AWS OpsWorks stack consisting of a custom layer. Create custom recipes to install Docker and to deploy your Docker container using the Dockerfile. Create custom recipes to install and configure the application to publish the logs to Amazon CloudWatch Logs (although this is one of the option, the last sentence mentions configure the application to push the logs to S3, which would need changes to application as it needs to use SDK or CLI)
    3. Create Dockerfile for the application. Create an AWS OpsWorks stack consisting of a Docker layer that uses the Dockerfile. Create custom recipes to install and configure Amazon Kinesis to publish the logs into Amazon CloudWatch. (Kinesis not needed)
    4. **Create a Dockerfile for the application. Create an AWS Elastic Beanstalk application using the Docker platform and the Dockerfile. Enable logging the Docker configuration to automatically publish the application logs. Enable log file rotation to Amazon S3.** (Use Docker configuration with awslogs and EB with Docker)
    5. **Use VM import/Export to import a virtual machine image of the server into AWS as an AMI. Create an Amazon Elastic Compute Cloud (EC2) instance from AMI, and install and configure the Amazon CloudWatch Logs agent. Create a new AMI from the instance. Create an AWS Elastic Beanstalk application using the AMI platform and the new AMI.** (Use VM Import/Export to create AMI and CloudWatch logs agent to log)
85. Which of the following groups is AWS Elastic Beanstalk best suited for?
    1. **Those who want to deploy and manage their applications within minutes in the AWS cloud.**
    2. Those who want to privately store and manage Git repositories in the AWS cloud.
    3. Those who want to automate the deployment of applications to instances and to update the applications as required.
    4. Those who want to model, visualize, and automate the steps required to release software.
86. When thinking of AWS Elastic Beanstalk’s model, which is true?
    1. Applications have many deployments, deployments have many environments.
    2. Environments have many applications, applications have many deployments.
    3. **Applications have many environments, environments have many deployments.** (Applications group logical services. Environments belong to Applications, and typically represent different deployment levels (dev, stage, prod, forth). Deployments belong to environments, and are pushes of bundles of code for the environments to run.)
    4. Deployments have many environments, environments have many applications.
87. If you’re trying to configure an AWS Elastic Beanstalk worker tier for easy debugging if there are problems finishing queue jobs, what should you configure?
    1. Configure Rolling Deployments.
    2. Configure Enhanced Health Reporting
    3. Configure Blue-Green Deployments.
    4. **Configure a Dead Letter Queue** (Elastic Beanstalk worker environments support SQS dead letter queues, where worker can send messages that for some reason could not be successfully processed. Dead letter queue provides the ability to sideline, isolate and analyze the unsuccessfully processed messages. Refer [link](http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-tiers.html#worker-deadletter))
88. When thinking of AWS Elastic Beanstalk, which statement is true?
    1. Worker tiers pull jobs from SNS.
    2. Worker tiers pull jobs from HTTP.
    3. Worker tiers pull jobs from JSON.
    4. **Worker tiers pull jobs from SQS.** (Elastic Beanstalk installs a daemon on each EC2 instance in the Auto Scaling group to process SQS messages in the worker environment. Refer [link](http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-tiers.html))
89. You are building a Ruby on Rails application for internal, non-production use, which uses MySQL as a database. You want developers without very much AWS experience to be able to deploy new code with a single command line push. You also want to set this up as simply as possible. Which tool is ideal for this setup?
    1. AWS CloudFormation
    2. AWS OpsWorks
    3. AWS ELB + EC2 with CLI Push
    4. **AWS Elastic Beanstalk**
90. What AWS products and features can be deployed by Elastic Beanstalk? Choose 3 answers.
    1. **Auto scaling groups**
    2. Route 53 hosted zones
    3. **Elastic Load Balancers**
    4. **RDS Instances**
    5. Elastic IP addresses
    6. SQS Queues
91. AWS Elastic Beanstalk stores your application files and optionally server log files in \_\_\_\_.
    1. Amazon Storage Gateway
    2. Amazon Glacier
    3. Amazon EC2
    4. **Amazon S3**
92. When you use the AWS Elastic Beanstalk console to deploy a new application \_\_\_\_.
    1. Need to upload each file separately
    2. Need to create each file and path
    3. **Need to upload a source bundle**
    4. Need to create each file
93. You are designing a social media site and are considering how to mitigate distributed denial-of-service (DDoS) attacks. Which of the below are viable mitigation techniques? (Choose 3 answers)
    1. Add multiple elastic network interfaces (ENIs) to each EC2 instance to increase the network bandwidth.
    2. Use dedicated instances to ensure that each instance has the maximum performance possible.
    3. **Use an Amazon CloudFront distribution for both static and dynamic content.**
    4. **Use an Elastic Load Balancer with auto scaling groups at the web app and Amazon Relational Database Service (RDS) tiers**
    5. **Add alert Amazon CloudWatch to look for high Network in and CPU utilization.**
    6. Create processes and capabilities to quickly add and remove rules to the instance OS firewall.
94. You’ve been hired to enhance the overall security posture for a very large e-commerce site. They have a well architected multi-tier application running in a VPC that uses ELBs in front of both the web and the app tier with static assets served directly from S3. They are using a combination of RDS and DynamoDB for their dynamic data and then archiving nightly into S3 for further processing with EMR. They are concerned because they found questionable log entries and suspect someone is attempting to gain unauthorized access. Which approach provides a cost effective scalable mitigation to this kind of attack?
    1. Recommend that they lease space at a DirectConnect partner location and establish a 1G DirectConnect connection to their VPC they would then establish Internet connectivity into their space, filter the traffic in hardware Web Application Firewall (WAF). And then pass the traffic through the DirectConnect connection into their application running in their VPC. (Not cost effective)
    2. Add previously identified hostile source IPs as an explicit INBOUND DENY NACL to the web tier subnet. (does not protect against new source)
    3. **Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would their pass the traffic to the current web tier The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group**
    4. Remove all but TLS 1.2 from the web tier ELB and enable Advanced Protocol Filtering This will enable the ELB itself to perform WAF functionality. (No advanced protocol filtering in ELB)
95. Which AWS service can help design architecture to persist in-flight transactions?
    1. Elastic IP Address
    2. **SQS**
    3. Amazon CloudWatch
    4. Amazon ElastiCache
96. A company has a workflow that sends video files from their on-premise system to AWS for transcoding. They use EC2 worker instances that pull transcoding jobs from SQS. Why is SQS an appropriate service for this scenario?
    1. SQS guarantees the order of the messages.
    2. SQS synchronously provides transcoding output.
    3. SQS checks the health of the worker instances.
    4. **SQS helps to facilitate horizontal scaling of encoding tasks**
97. Which statement best describes an Amazon SQS use case?
    1. Automate the process of sending an email notification to administrators when the CPU utilization reaches 70% on production servers (Amazon EC2 instances) (CloudWatch + SNS + SES)
    2. **Create a video transcoding website where multiple components need to communicate with each other, but can’t all process the same amount of work simultaneously** (SQS provides loose coupling)
    3. Coordinate work across distributed web services to process employee’s expense reports (SWF – Steps in order and might need manual steps)
    4. Distribute static web content to end users with low latency across multiple countries (CloudFront + S3)
98. Your application provides data transformation services. Files containing data to be transformed are first uploaded to Amazon S3 and then transformed by a fleet of spot EC2 instances. Files submitted by your premium customers must be transformed with the highest priority. How should you implement such a system?
    1. Use a DynamoDB table with an attribute defining the priority level. Transformation instances will scan the table for tasks, sorting the results by priority level.
    2. Use Route 53 latency based-routing to send high priority tasks to the closest transformation instances.
    3. **Use two SQS queues, one for high priority messages, and the other for default priority. Transformation instances first poll the high priority queue; if there is no message, they poll the default priority queue**
    4. Use a single SQS queue. Each message contains the priority level. Transformation instances poll high-priority messages first.
99. Your company plans to host a large donation website on Amazon Web Services (AWS). You anticipate a large and undetermined amount of traffic that will create many database writes. To be certain that you do not drop any writes to a database hosted on AWS. Which service should you use?
    1. Amazon RDS with provisioned IOPS up to the anticipated peak write throughput.
    2. **Amazon Simple Queue Service (SQS) for capturing the writes and draining the queue to write to the database**
    3. Amazon ElastiCache to store the writes until the writes are committed to the database.
    4. Amazon DynamoDB with provisioned write throughput up to the anticipated peak write throughput.
100. A customer has a 10 GB AWS Direct Connect connection to an AWS region where they have a web application hosted on Amazon Elastic Computer Cloud (EC2). The application has dependencies on an on-premises mainframe database that uses a BASE (Basic Available, Soft state, Eventual consistency) rather than an ACID (Atomicity, Consistency, Isolation, Durability) consistency model. The application is exhibiting undesirable behavior because the database is not able to handle the volume of writes. How can you reduce the load on your on-premises database resources in the most cost-effective way?
     1. Use an Amazon Elastic Map Reduce (EMR) S3DistCp as a synchronization mechanism between the onpremises database and a Hadoop cluster on AWS.
     2. **Modify the application to write to an Amazon SQS queue and develop a worker process to flush the queue to the on-premises database**
     3. Modify the application to use DynamoDB to feed an EMR cluster which uses a map function to write to the on-premises database.
     4. Provision an RDS read-replica database on AWS to handle the writes and synchronize the two databases using Data Pipeline.
101. An organization has created a Queue named “modularqueue” with SQS. The organization is not performing any operations such as SendMessage, ReceiveMessage, DeleteMessage, GetQueueAttributes, SetQueueAttributes, AddPermission, and RemovePermission on the queue. What can happen in this scenario?
     1. AWS SQS sends notification after 15 days for inactivity on queue
     2. **AWS SQS can delete queue after 30 days without notification**
     3. AWS SQS marks queue inactive after 30 days
     4. AWS SQS notifies the user after 2 weeks and deletes the queue after 3 weeks.
102. A user is using the AWS SQS to decouple the services. Which of the below mentioned operations is not supported by SQS?
     1. SendMessageBatch
     2. DeleteMessageBatch
     3. CreateQueue
     4. **DeleteMessageQueue**
103. A user has created a queue named “awsmodule” with SQS. One of the consumers of queue is down for 3 days and then becomes available. Will that component receive message from queue?
     1. **Yes, since SQS by default stores message for 4 days**
     2. No, since SQS by default stores message for 1 day only
     3. No, since SQS sends message to consumers who are available that time
     4. Yes, since SQS will not delete message until it is delivered to all consumers
104. A user has created a queue named “queue2” in US-East region with AWS SQS. The user’s AWS account ID is 123456789012. If the user wants to perform some action on this queue, which of the below Queue URL should he use?
     1. **http://sqs.us-east-1.amazonaws.com/123456789012/queue2**
     2. http://sqs.amazonaws.com/123456789012/queue2
     3. http://sqs. 123456789012.us-east-1.amazonaws.com/queue2
     4. http://123456789012.sqs.us-east-1.amazonaws.com/queue2
105. A user has created a queue named “myqueue” with SQS. There are four messages published to queue, which are not received by the consumer yet. If the user tries to delete the queue, what will happen?
     1. A user can never delete a queue manually. AWS deletes it after 30 days of inactivity on queue
     2. **It will delete the queue**
     3. It will initiate the delete but wait for four days before deleting until all messages are deleted automatically.
     4. I t will ask user to delete the messages first
106. A user has developed an application, which is required to send the data to a NoSQL database. The user wants to decouple the data sending such that the application keeps processing and sending data but does not wait for an acknowledgement of DB. Which of the below mentioned applications helps in this scenario?
     1. AWS Simple Notification Service
     2. AWS Simple Workflow
     3. **AWS Simple Queue Service**
     4. AWS Simple Query Service
107. You are building an online store on AWS that uses SQS to process your customer orders. Your backend system needs those messages in the same sequence the customer orders have been put in. How can you achieve that?
     1. It is not possible to do this with SQS
     2. **You can use sequencing information on each message**
     3. You can do this with SQS but you also need to use SWF
     4. Messages will arrive in the same order by default
108. A user has created a photo editing software and hosted it on EC2. The software accepts requests from the user about the photo format and resolution and sends a message to S3 to enhance the picture accordingly. Which of the below mentioned AWS services will help make a scalable software with the AWS infrastructure in this scenario?
     1. AWS Glacier
     2. AWS Elastic Transcoder
     3. AWS Simple Notification Service
     4. **AWS Simple Queue Service**
109. Refer to the architecture diagram of a batch processing solution using Simple Queue Service (SQS) to set up a message queue between EC2 instances, which are used as batch processors. Cloud Watch monitors the number of Job requests (queued messages) and an Auto Scaling group adds or deletes batch servers automatically based on parameters set in Cloud Watch alarms. You can use this architecture to implement which of the following features in a cost effective and efficient manner? 
     1. Reduce the overall time for executing jobs through parallel processing by allowing a busy EC2 instance that receives a message to pass it to the next instance in a daisy-chain setup.
     2. Implement fault tolerance against EC2 instance failure since messages would remain in SQS and worn can continue with recovery of EC2 instances implement fault tolerance against SQS failure by backing up messages to S3.
     3. Implement message passing between EC2 instances within a batch by exchanging messages through SOS.
     4. **Coordinate number of EC2 instances with number of job requests automatically thus Improving cost effectiveness**
     5. Handle high priority jobs before lower priority jobs by assigning a priority metadata field to SQS messages.
110. How does Amazon SQS allow multiple readers to access the same message queue without losing messages or processing them many times?
     1. By identifying a user by his unique id
     2. By using unique cryptography
     3. **Amazon SQS queue has a configurable visibility timeout**
     4. Multiple readers can’t access the same message queue
111. A user has created photo editing software and hosted it on EC2. The software accepts requests from the user about the photo format and resolution and sends a message to S3 to enhance the picture accordingly. Which of the below mentioned AWS services will help make a scalable software with the AWS infrastructure in this scenario?
     1. AWS Elastic Transcoder
     2. AWS Simple Notification Service
     3. **AWS Simple Queue Service**
     4. AWS Glacier
112. How do you configure SQS to support longer message retention?
     1. **Set the MessageRetentionPeriod attribute using the SetQueueAttributes method**
     2. Using a Lambda function
     3. You can’t. It is set to 14 days and cannot be changed
     4. You need to request it from AWS
113. A user has developed an application, which is required to send the data to a NoSQL database. The user wants to decouple the data sending such that the application keeps processing and sending data but does not wait for an acknowledgement of DB. Which of the below mentioned applications helps in this scenario?
     1. AWS Simple Notification Service
     2. AWS Simple Workflow
     3. AWS Simple Query Service
     4. **AWS Simple Queue Service**
114. If a message is retrieved from a queue in Amazon SQS, how long is the message inaccessible to other users by default?
     1. 0 seconds
     2. 1 hour
     3. 1 day
     4. forever
     5. **30 seconds**
115. Which of the following statements about SQS is true?
     1. Messages will be delivered exactly once and messages will be delivered in First in, First out order
     2. Messages will be delivered exactly once and message delivery order is indeterminate
     3. Messages will be delivered one or more times and messages will be delivered in First in, First out order
     4. **Messages will be delivered one or more times and message delivery order is indeterminate** (Before the introduction of FIFO queues)
116. How long can you keep your Amazon SQS messages in Amazon SQS queues?
     1. From 120 secs up to 4 weeks
     2. From 10 secs up to 7 days
     3. **From 60 secs up to 2 weeks**
     4. From 30 secs up to 1 week
117. When a Simple Queue Service message triggers a task that takes 5 minutes to complete, which process below will result in successful processing of the message and remove it from the queue while minimizing the chances of duplicate processing?
     1. **Retrieve the message with an increased visibility timeout, process the message, delete the message from the queue**
     2. Retrieve the message with an increased visibility timeout, delete the message from the queue, process the message
     3. Retrieve the message with increased DelaySeconds, process the message, delete the message from the queue
     4. Retrieve the message with increased DelaySeconds, delete the message from the queue, process the message
118. You need to process long-running jobs once and only once. How might you do this?
     1. Use an SNS queue and set the visibility timeout to long enough for jobs to process.
     2. Use an SQS queue and set the reprocessing timeout to long enough for jobs to process.
     3. **Use an SQS queue and set the visibility timeout to long enough for jobs to process.**
     4. Use an SNS queue and set the reprocessing timeout to long enough for jobs to process.
119. You are getting a lot of empty receive requests when using Amazon SQS. This is making a lot of unnecessary network load on your instances. What can you do to reduce this load?
     1. Subscribe your queue to an SNS topic instead.
     2. **Use as long of a poll as possible, instead of short polls.** (Refer [link](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-long-polling.html))
     3. Alter your visibility timeout to be shorter.
     4. Use <code>sqsd</code> on your EC2 instances.
120. You have an asynchronous processing application using an Auto Scaling Group and an SQS Queue. The Auto Scaling Group scales according to the depth of the job queue. The completion velocity of the jobs has gone down, the Auto Scaling Group size has maxed out, but the inbound job velocity did not increase. What is a possible issue?
     1. **Some of the new jobs coming in are malformed and unprocessable.** (As other options would cause the job to stop processing completely, the only reasonable option seems that some of the recent messages must be malformed and unprocessable)
     2. The routing tables changed and none of the workers can process events anymore. (If changed, none of the jobs would be processed)
     3. Someone changed the IAM Role Policy on the instances in the worker group and broke permissions to access the queue. (If IAM role changed no jobs would be processed)
     4. The scaling metric is not functioning correctly. (scaling metric did work fine as the autoscaling caused the instances to increase)
121. Company B provides an online image recognition service and utilizes SQS to decouple system components for scalability. The SQS consumers poll the imaging queue as often as possible to keep end-to-end throughput as high as possible. However, Company B is realizing that polling in tight loops is burning CPU cycles and increasing costs with empty responses. How can Company B reduce the number of empty responses?
     1. Set the imaging queue visibility Timeout attribute to 20 seconds
     2. **Set the Imaging queue ReceiveMessageWaitTimeSeconds attribute to 20 seconds** (Long polling. Refer [link](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-long-polling.html))
     3. Set the imaging queue MessageRetentionPeriod attribute to 20 seconds
     4. Set the DelaySeconds parameter of a message to 20 seconds
122. A web company is looking to implement an intrusion detection and prevention system into their deployed VPC. This platform should have the ability to scale to thousands of instances running inside of the VPC. How should they architect their solution to achieve these goals?
     1. Configure an instance with monitoring software and the elastic network interface (ENI) set to promiscuous mode packet sniffing to see an traffic across the VPC. (virtual instance running in promiscuous mode to receive or“sniff” traffic)
     2. Create a second VPC and route all traffic from the primary application VPC through the second VPC where the scalable virtualized IDS/IPS platform resides.
     3. Configure servers running in the VPC using the host-based ‘route’ commands to send all traffic through the platform to a scalable virtualized IDS/IPS (host based routing is not allowed)
     4. **Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.**
123. You are designing an intrusion detection prevention (IDS/IPS) solution for a customer web application in a single VPC. You are considering the options for implementing IDS/IPS protection for traffic coming from the Internet. Which of the following options would you consider? (Choose 2 answers)
     1. **Implement IDS/IPS agents on each Instance running In VPC**
     2. Configure an instance in each subnet to switch its network interface card to promiscuous mode and analyze network traffic. (virtual instance running in promiscuous mode to receive or“sniff” traffic)
     3. Implement Elastic Load Balancing with SSL listeners In front of the web applications (ELB with SSL does not serve as IDS/IPS)
     4. **Implement a reverse proxy layer in front of web servers and configure IDS/IPS agents on each reverse proxy server**
124. Which of the following instance types are available as Amazon EBS-backed only? Choose 2 answers
     1. **General purpose T2**
     2. General purpose M3
     3. **Compute-optimized C4**
     4. Compute-optimized C3
     5. Storage-optimized 12
125. A t2.medium EC2 instance type must be launched with what type of Amazon Machine Image (AMI)?
     1. An Instance store Hardware Virtual Machine AMI
     2. An Instance store Paravirtual AMI
     3. **An Amazon EBS-backed Hardware Virtual Machine AMI**
     4. An Amazon EBS-backed Paravirtual AMI
126. You have identified network throughput as a bottleneck on your m1.small EC2 instance when uploading data Into Amazon S3 In the same region. How do you remedy this situation? Add an additional ENI
     1. **Change to a larger Instance**
     2. Use DirectConnect between EC2 and S3
     3. Use EBS PIOPS on the local volume
127. You are using an m1.small EC2 Instance with one 300 GB EBS volume to host a relational database. You determined that write throughput to the database needs to be increased. Which of the following approaches can help achieve this? Choose 2 answers
     1. **Use an array of EBS volumes** (Striping to increase throughput)
     2. Enable Multi-AZ mode.
     3. Place the instance in an Auto Scaling Groups
     4. Add an EBS volume and place into RAID 5 (RAID 5 is not recommended as it provides parity and EBS volumes are already replicated across multiple servers in an Availability Zone for availability and durability, so AWS recommends striping for performance rather than durability)
     5. **Increase the size of the EC2 Instance.**
     6. Put the database behind an Elastic Load Balancer.
128. You are tasked with setting up a cluster of EC2 Instances for a NoSQL database. The database requires random read IO disk performance up to a 100,000 IOPS at 4KB block side per node. Which of the following EC2 instances will perform the best for this workload?
     1. A High-Memory Quadruple Extra Large (m2.4xlarge) with EBS-Optimized set to true and a PIOPs EBS volume
     2. A Cluster Compute Eight Extra Large (cc2.8xlarge) using instance storage
     3. **High I/O Quadruple Extra Large (hi1.4xlarge) using instance storage**
     4. A Cluster GPU Quadruple Extra Large (cg1.4xlarge) using four separate 4000 PIOPS EBS volumes in a RAID 0 configuration
129. You are implementing a URL whitelisting system for a company that wants to restrict outbound HTTP’S connections to specific domains from their EC2-hosted applications you deploy a single EC2 instance running proxy software and configure It to accept traffic from all subnets and EC2 instances in the VPC. You configure the proxy to only pass through traffic to domains that you define in its whitelist configuration You have a nightly maintenance window or 10 minutes where ail instances fetch new software updates. Each update Is about 200MB In size and there are 500 instances In the VPC that routinely fetch updates After a few days you notice that some machines are failing to successfully download some, but not all of their updates within the maintenance window The download URLs used for these updates are correctly listed in the proxy’s whitelist configuration and you are able to access them manually using a web browser on the instances What might be happening? (Choose 2 answers) **[PROFESSIONAL]**
     1. **You are running the proxy on an undersized EC2 instance type so network throughput is not sufficient for all instances to download their updates in time.**
     2. You have not allocated enough storage to the EC2 instance running me proxy so the network buffer is filling up causing some requests to fall
     3. You are running the proxy in a public subnet but have not allocated enough EIPs to support the needed network throughput through the Internet Gateway (IGW)
     4. **You are running the proxy on a affluently-sized EC2 instance in a private subnet and its network throughput is being throttled by a NAT running on an undersized EC2 instance**
     5. The route table for the subnets containing the affected EC2 instances is not configured to direct network traffic for the software update locations to the proxy.
130. You have been asked to design the storage layer for an application. The application requires disk performance of at least 100,000 IOPS in addition; the storage layer must be able to survive the loss of an individual disk, EC2 instance, or Availability Zone without any data loss. The volume you provide must have a capacity of at least 3TB. Which of the following designs will meet these objectives? **[PROFESSIONAL]**
     1. Instantiate an i2.8xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance. Provision 3×1 TB EBS volumes attach them to the instance and configure them as a second RAID 0 volume. Configure synchronous, block-level replication from the ephemeral backed volume to the EBS-backed volume. (Same AZ will not survive the AZ loss)
     2. **Instantiate an i2.8xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the Instance Configure synchronous block-level replication to an identically configured Instance in us-east-1b.**
     3. Instantiate a c3.8xlarge Instance in us-east-1. Provision an AWS Storage Gateway and configure it for 3 TB of storage and 100,000 IOPS. Attach the volume to the instance. (Need synchronous replication to prevent any data loss)
     4. Instantiate a c3.8xlarge instance in us-east-1 provision 4x1TB EBS volumes, attach them to the instance, and configure them as a single RAID 5 volume Ensure that EBS snapshots are performed every 15 minutes. (RAID 5 not recommended by AWS and Need synchronous replication to prevent any data loss)
     5. Instantiate a c3 8xlarge Instance in us-east-1 Provision 3x1TB EBS volumes attach them to the instance, and configure them as a single RAID 0 volume Ensure that EBS snapshots are performed every 15 minutes. (Need synchronous replication to prevent any data loss)
131. You are responsible for a legacy web application whose server environment is approaching end of life. You would like to migrate this application to AWS as quickly as possible, since the application environment currently has the following limitations: The VM’s single 10GB VMDK is almost full. The virtual network interface still uses the 10Mbps driver, which leaves your 100Mbps WAN connection completely underutilized. It is currently running on a highly customized Windows VM within a VMware environment: You do not have the installation media. This is a mission critical application with an RTO (Recovery Time Objective) of 8 hours. RPO (Recovery Point Objective) of 1 hour. How could you best migrate this application to AWS while meeting your business continuity requirements?
     1. **Use the EC2 VM Import Connector for vCenter to import the VM into EC2**
     2. Use Import/Export to import the VM as an EBS snapshot and attach to EC2. (Import/Export is used to transfer large amount of data)
     3. Use S3 to create a backup of the VM and restore the data into EC2.
     4. Use the ec2-bundle-instance API to Import an Image of the VM into EC2 (only bundles an windows instance store instance)
132. You are tasked with moving a legacy application from a virtual machine running inside your datacenter to an Amazon VPC. Unfortunately this app requires access to a number of on-premises services and no one who configured the app still works for your company. Even worse there’s no documentation for it. What will allow the application running inside the VPC to reach back and access its internal dependencies without being reconfigured? (Choose 3 answers)
     1. **An AWS Direct Connect link between the VPC and the network housing the internal services** (VPN or a DX for communication)
     2. An Internet Gateway to allow a VPN connection. (Virtual and Customer gateway is needed)
     3. An Elastic IP address on the VPC instance (Don’t need a EIP as private subnets can also interact with on-premises network)
     4. **An IP address space that does not conflict with the one on-premises** (IP address cannot conflict)
     5. Entries in Amazon Route 53 that allow the Instance to resolve its dependencies’ IP addresses (Route 53 is not required)
     6. **A VM Import of the current virtual machine** (VM Import to copy the VM to AWS as there is no documentation it can’t be configured from scratch)
133. Which of these Disaster Recovery options costs the least?
     1. **Pilot Light** (most systems are down and brought up only after disaster)
     2. Fully Working Low capacity Warm standby
     3. Multi site Active-Active
134. Your company currently has a 2-tier web application running in an on-premises data center. You have experienced several infrastructure failures in the past two months resulting in significant financial losses. Your CIO is strongly agreeing to move the application to AWS. While working on achieving buy-in from the other company executives, he asks you to develop a disaster recovery plan to help improve Business continuity in the short term. He specifies a target Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 1 hour or less. He also asks you to implement the solution within 2 weeks. Your database is 200GB in size and you have a 20Mbps Internet connection. How would you do this while minimizing costs?
     1. Create an EBS backed private AMI which includes a fresh install or your application. Setup a script in your data center to backup the local database every 1 hour and to encrypt and copy the resulting file to an S3 bucket using multi-part upload (while AMI is a right approach to keep cost down, Upload to S3 very Slow)
     2. Install your application on a compute-optimized EC2 instance capable of supporting the application’s average load synchronously replicate transactions from your on-premises database to a database instance in AWS across a secure Direct Connect connection. (EC2 running in Compute Optimized as well as Direct Connect is expensive to start with also Direct Connect cannot be implemented in 2 weeks)
     3. Deploy your application on EC2 instances within an Auto Scaling group across multiple availability zones asynchronously replicate transactions from your on-premises database to a database instance in AWS across a secure VPN connection. (While VPN can be setup quickly asynchronous replication using VPN would work, running instances in DR is expensive)
     4. **Create an EBS backed private AMI that includes a fresh install of your application. Develop a Cloud Formation template which includes your AMI and the required EC2. Auto-Scaling and ELB resources to support deploying the application across Multiple Availability Zones. Asynchronously replicate transactions from your on-premises database to a database instance in AWS across a secure VPN connection. (**Pilot Light approach with only DB running and replicate while you have preconfigured AMI and autoscaling config**)**
135. You are designing an architecture that can recover from a disaster very quickly with minimum down time to the end users. Which of the following approaches is best?
     1. Leverage Route 53 health checks to automatically fail over to backup site when the primary site becomes unreachable
     2. Implement the Pilot Light DR architecture so that traffic can be processed seamlessly in case the primary site becomes unreachable
     3. **Implement either Fully Working Low Capacity Standby or Multi-site Active-Active architecture so that the end users will not experience any delay even if the primary site becomes unreachable**
     4. Implement multi-region architecture to ensure high availability
136. Your customer wishes to deploy an enterprise application to AWS that will consist of several web servers, several application servers and a small (50GB) Oracle database. Information is stored, both in the database and the file systems of the various servers. The backup system must support database recovery, whole server and whole disk restores, and individual file restores with a recovery time of no more than two hours. They have chosen to use RDS Oracle as the database. Which backup architecture will meet these requirements?
     1. Backup RDS using automated daily DB backups. Backup the EC2 instances using AMIs and supplement with file-level backup to S3 using traditional enterprise backup software to provide file level restore (RDS automated backups with file-level backups can be used)
     2. Backup RDS using a Multi-AZ Deployment Backup the EC2 instances using AMIs, and supplement by copying file system data to S3 to provide file level restore (Multi-AZ is more of an Disaster recovery solution)
     3. Backup RDS using automated daily DB backups. Backup the EC2 instances using EBS snapshots and supplement with file-level backups to Amazon Glacier using traditional enterprise backup software to provide file level restore (Glacier not an option with the 2 hours RTO)
     4. Backup RDS database to S3 using Oracle RMAN. Backup the EC2 instances using AMIs, and supplement with EBS snapshots for individual volume restore. (Will use RMAN only if Database hosted on EC2 and not when using RDS)
137. Which statements are true about the Pilot Light Disaster recovery architecture pattern?
     1. Pilot Light is a hot standby (Cold Standby)
     2. **Enables replication of all critical data to AWS**
     3. **Very cost-effective DR pattern**
     4. **Can scale the system as needed to handle current production load**
138. An ERP application is deployed across multiple AZs in a single region. In the event of failure, the Recovery Time Objective (RTO) must be less than 3 hours, and the Recovery Point Objective (RPO) must be 15 minutes. The customer realizes that data corruption occurred roughly 1.5 hours ago. What DR strategy could be used to achieve this RTO and RPO in the event of this kind of failure?
     1. **Take hourly DB backups to S3, with transaction logs stored in S3 every 5 minutes**
     2. Use synchronous database master-slave replication between two availability zones. (Replication won’t help to backtrack and would be sync always)
     3. Take hourly DB backups to EC2 Instance store volumes with transaction logs stored In S3 every 5 minutes. (Instance store not a preferred storage)
     4. Take 15 minute DB backups stored in Glacier with transaction logs stored in S3 every 5 minutes. (Glacier does not meet the RTO)
139. Your company’s on-premises content management system has the following architecture:  
     – Application Tier – Java code on a JBoss application server  
     – Database Tier – Oracle database regularly backed up to Amazon Simple Storage Service (S3) using the Oracle RMAN backup utility  
     – Static Content – stored on a 512GB gateway stored Storage Gateway volume attached to the application server via the iSCSI interfaceWhich AWS based disaster recovery strategy will give you the best RTO?
     1. **Deploy the Oracle database and the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon S3. Generate an EBS volume of static content from the Storage Gateway and attach it to the JBoss EC2 server.**
     2. Deploy the Oracle database on RDS. Deploy the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon Glacier. Generate an EBS volume of static content from the Storage Gateway and attach it to the JBoss EC2 server. (Glacier does help to give best RTO)
     3. Deploy the Oracle database and the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon S3. Restore the static content by attaching an AWS Storage Gateway running on Amazon EC2 as an iSCSI volume to the JBoss EC2 server. (No need to attach the Storage Gateway as an iSCSI volume can just create a EBS volume)
     4. Deploy the Oracle database and the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon S3. Restore the static content from an AWS Storage Gateway-VTL running on Amazon EC2 (VTL is Virtual Tape library and doesn’t fit the RTO)
140. You would like to create a mirror image of your production environment in another region for disaster recovery purposes. Which of the following AWS resources do not need to be recreated in the second region? (Choose 2 answers)
     1. **Route 53 Record Sets**
     2. **IAM Roles**
     3. Elastic IP Addresses (EIP) (are specific to a region)
     4. EC2 Key Pairs (are specific to a region)
     5. Launch configurations
     6. Security Groups (are specific to a region)
141. When using the following AWS services, which should be implemented in multiple Availability Zones for high availability solutions? Choose 2 answers
     1. Amazon DynamoDB (already replicates across AZs)
     2. **Amazon Elastic Compute Cloud (EC2)**
     3. **Amazon Elastic Load Balancing**
     4. Amazon Simple Notification Service (SNS) (Global Managed Service)
     5. Amazon Simple Storage Service (S3) (Global Managed Service)
142. What is the scope of an EBS volume?
     1. VPC
     2. Region
     3. Placement Group
     4. **Availability Zone**
143. What is the scope of AWS IAM?
     1. **Global** (IAM resources are all global; there is not regional constraint)
     2. Availability Zone
     3. Region
     4. Placement Group
144. What is the scope of an EC2 EIP?
     1. Placement Group
     2. Availability Zone
     3. **Region** (An Elastic IP address is tied to a region and can be associated only with an instance in the same region. Refer [link](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resources.html))
     4. VPC
145. What is the scope of an EC2 security group?
     1. Availability Zone
     2. Placement Group
     3. **Region** (A security group is tied to a region and can be assigned only to instances in the same region)
     4. VPC

 IAM’s Policy Evaluation Logic always starts with a default \_\_\_\_\_\_\_\_\_\_\_\_ for every request, except for those that use the AWS account’s root security credentials b

1. Permit
2. **Deny**
3. Cancel

 An organization has created 10 IAM users. The organization wants each of the IAM users to have access to a separate DynamoDB table. All the users are added to the same group and the organization wants to setup a group level policy for this. How can the organization achieve this?

1. Define the group policy and add a condition which allows the access based on the IAM name
2. **Create a DynamoDB table with the same name as the IAM user name and define the policy rule which grants access based on the DynamoDB ARN using a variable**
3. Create a separate DynamoDB database for each user and configure a policy in the group based on the DB variable
4. It is not possible to have a group level policy which allows different IAM users to different DynamoDB Tables

 An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

1. Create an IAM policy with the security group and use that security group for AWS console login
2. **Create an IAM policy with a condition which denies access when the IP address range is not from the organization**
3. Configure the EC2 instance security group which allows traffic only from the organization’s IP range
4. Create an IAM policy with VPC and allow a secure gateway between the organization and AWS Console

 Can I attach more than one policy to a particular entity?

1. **Yes always**
2. Only if within GovCloud
3. No
4. Only if within VPC

 A \_\_\_\_\_\_\_\_\_\_ is a document that provides a formal statement of one or more permissions.

1. **policy**
2. permission
3. Role
4. resource

 A \_\_\_\_\_\_\_\_\_\_ is the concept of allowing (or disallowing) an entity such as a user, group, or role some type of access to one or more resources.

1. user
2. AWS Account
3. resource
4. **permission**

 True or False: When using IAM to control access to your RDS resources, the key names that can be used are case sensitive. For example, aws:CurrentTime is NOT equivalent to AWS:currenttime.

1. TRUE
2. **FALSE** (Refer [link](http://docs.aws.amazon.com/directconnect/latest/UserGuide/using_iam.html#keys))

 A user has set an IAM policy where it allows all requests if a request from IP 10.10.10.1/32. Another policy allows all the requests between 5 PM to 7 PM. What will happen when a user is requesting access from IP 10.10.10.1/32 at 6 PM?

1. IAM will throw an error for policy conflict
2. It is not possible to set a policy based on the time or IP
3. It will deny access
4. **It will allow access**

 Which of the following are correct statements with policy evaluation logic in AWS Identity and Access Management? Choose 2 answers.

1. **By default, all requests are denied**
2. An explicit allow overrides an explicit deny
3. **An explicit allow overrides default deny**
4. An explicit deny does not override an explicit allow
5. By default, all request are allowed

 A web design company currently runs several FTP servers that their 250 customers use to upload and download large graphic files. They wish to move this system to AWS to make it more scalable, but they wish to maintain customer privacy and keep costs to a minimum. What AWS architecture would you recommend? **[PROFESSIONAL]**

1. **Ask their customers to use an S3 client instead of an FTP client. Create a single S3 bucket. Create an IAM user for each customer. Put the IAM Users in a Group that has an IAM policy that permits access to subdirectories within the bucket via use of the ‘username’ Policy variable.**
2. Create a single S3 bucket with Reduced Redundancy Storage turned on and ask their customers to use an S3 client instead of an FTP client. Create a bucket for each customer with a Bucket Policy that permits access only to that one customer. (Creating bucket for each user is not a scalable model, also 100 buckets are a limit earlier without extending which has since changed [link](https://aws.amazon.com/about-aws/whats-new/2015/08/amazon-s3-introduces-new-usability-enhancements/))
3. Create an auto-scaling group of FTP servers with a scaling policy to automatically scale-in when minimum network traffic on the auto-scaling group is below a given threshold. Load a central list of ftp users from S3 as part of the user Data startup script on each Instance (Expensive)
4. Create a single S3 bucket with Requester Pays turned on and ask their customers to use an S3 client instead of an FTP client. Create a bucket tor each customer with a Bucket Policy that permits access only to that one customer. (Creating bucket for each user is not a scalable model, also 100 buckets are a limit earlier without extending which has since changed [link](https://aws.amazon.com/about-aws/whats-new/2015/08/amazon-s3-introduces-new-usability-enhancements/))

 You are moving an existing traditional system to AWS, and during the migration discover that there is a master server which is a single point of failure. Having examined the implementation of the master server you realize there is not enough time during migration to re-engineer it to be highly available, though you do discover that it stores its state in a local MySQL database. In order to minimize down-time you select RDS to replace the local database and configure master to use it, what steps would best allow you to create a self-healing architecture**[PROFESSIONAL]**

1. **Migrate the local database into multi-AWS RDS database. Place master node into a multi-AZ auto-scaling group with a minimum of one and maximum of one with health checks.**
2. Replicate the local database into a RDS read replica. Place master node into a Cross-Zone ELB with a minimum of one and maximum of one with health checks. (Read Replica does not provide HA and write capability and ELB does not have feature for Min and Max 1 and Cross Zone allows just the equal distribution of load across instances)
3. Migrate the local database into multi-AWS RDS database. Place master node into a Cross-Zone ELB with a minimum of one and maximum of one with health checks. (ELB does not have feature for Min and Max 1 and Cross Zone allows just the equal distribution of load across instances)
4. Replicate the local database into a RDS read replica. Place master node into a multi-AZ auto-scaling group with a minimum of one and maximum of one with health checks. (Read Replica does not provide HA and write capability)

 You are designing Internet connectivity for your VPC. The Web servers must be available on the Internet. The application must have a highly available architecture. Which alternatives should you consider? (Choose 2 answers)

1. Configure a NAT instance in your VPC. Create a default route via the NAT instance and associate it with all subnets. Configure a DNS A record that points to the NAT instance public IP address (NAT is for internet connectivity for instances in private subnet)
2. Configure a CloudFront distribution and configure the origin to point to the private IP addresses of your Web servers. Configure a Route53 CNAME record to your CloudFront distribution.
3. **Place all your web servers behind ELB. Configure a Route53 CNAME to point to the ELB DNS name.**
4. **Assign EIPs to all web servers. Configure a Route53 record set with all EIPs. With health checks and DNS failover.**

 When deploying a highly available 2-tier web application on AWS, which combination of AWS services meets the requirements? 1. AWS Direct Connect 2. Amazon Route 53 3. AWS Storage Gateway 4. Elastic Load Balancing 4. Amazon EC2 5. Auto scaling 6. Amazon VPC 7. AWS Cloud Trail **[PROFESSIONAL]**

1. **2,4,5 and 6**
2. 3,4,5 and 8
3. 1 through 8
4. 1,3,5 and 7
5. 1,2,5 and 6

 Company A has hired you to assist with the migration of an interactive website that allows registered users to rate local restaurants. Updates to the ratings are displayed on the home page, and ratings are updated in real time. Although the website is not very popular today, the company anticipates that It will grow rapidly over the next few weeks. They want the site to be highly available. The current architecture consists of a single Windows Server 2008 R2 web server and a MySQL database running on Linux. Both reside inside an on -premises hypervisor. What would be the most efficient way to transfer the application to AWS, ensuring performance and high-availability? **[PROFESSIONAL]**

1. Export web files to an Amazon S3 bucket in us-west-1. Run the website directly out of Amazon S3. Launch a multi-AZ MySQL Amazon RDS instance in us-west-1a. Import the data into Amazon RDS from the latest MySQL backup. Use Route 53 and create an alias record pointing to the elastic load balancer. (Its an Interactive website, although it can be implemented using Javascript SDK, its a migration and the application would need changes. Also no use of ELB if hosted on S3)
2. **Launch two Windows Server 2008 R2 instances in us-west-1b and two in us-west-1a. Copy the web files from on premises web server to each Amazon EC2 web server, using Amazon S3 as the repository. Launch a multi-AZ MySQL Amazon RDS instance in us-west-2a. Import the data into Amazon RDS from the latest MySQL backup. Create an elastic load balancer to front your web servers. Use Route 53 and create an alias record pointing to the elastic load balancer.** (Although RDS instance is in a different region which will impact performance, this is the only option that works.)
3. Use AWS VM Import/Export to create an Amazon Elastic Compute Cloud (EC2) Amazon Machine Image (AMI) of the web server. Configure Auto Scaling to launch two web servers in us-west-1a and two in us-west-1b. Launch a Multi-AZ MySQL Amazon Relational Database Service (RDS) instance in us-west-1b. Import the data into Amazon RDS from the latest MySQL backup. Use Amazon Route 53 to create a hosted zone and point an A record to the elastic load balancer. (does not create a load balancer)
4. Use AWS VM Import/Export to create an Amazon EC2 AMI of the web server. Configure auto-scaling to launch two web servers in us-west-1a and two in us-west-1b. Launch a multi-AZ MySQL Amazon RDS instance in us-west-1a. Import the data into Amazon RDS from the latest MySQL backup. Create an elastic load balancer to front your web servers. Use Amazon Route 53 and create an A record pointing to the elastic load balancer. (Need to create a aliased record without which the Route 53 pointing to ELB would not work)

 Your company runs a customer facing event registration site. This site is built with a 3-tier architecture with web and application tier servers and a MySQL database. The application requires 6 web tier servers and 6 application tier servers for normal operation, but can run on a minimum of 65% server capacity and a single MySQL database. When deploying this application in a region with three availability zones (AZs) which architecture provides high availability? **[PROFESSIONAL]**

1. A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 2 AZs with 3 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB. and one RDS (Relational Database Service) instance deployed with read replicas in the other AZ.
2. A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer) and an application tier deployed across 3 AZs with 2 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB and one RDS (Relational Database Service) Instance deployed with read replicas in the two other AZs.
3. A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer) and an application tier deployed across 2 AZs with 3 EC2 instances m each AZ inside an Auto Scaling Group behind an ELS and a Multi-AZ RDS (Relational Database Service) deployment.
4. **A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ Inside an Auto Scaling Group behind an ELB (elastic load balancer). And an application tier deployed across 3 AZs with 2 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB. And a Multi-AZ RDS (Relational Database services) deployment.**

 For a 3-tier, customer facing, inclement weather site utilizing a MySQL database running in a Region which has two AZs which architecture provides fault tolerance within the region for the application that minimally requires 6 web tier servers and 6 application tier servers running in the web and application tiers and one MySQL database? **[PROFESSIONAL]**

1. **A web tier deployed across 2 AZs with 6 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 2 AZs with 6 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB. and a Multi-AZ RDS (Relational Database Service) deployment.** (As it needs Fault Tolerance with minimal 6 servers always available)
2. A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each A2 inside an Auto Scaling Group behind an ELB (elastic load balancer) and an application tier deployed across 2 AZs with 3 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB and a Multi-AZ RDS (Relational Database Service) deployment.
3. A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer) and an application tier deployed across 2 AZs with 6 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB and one RDS (Relational Database Service) Instance deployed with read replicas in the other AZs.
4. A web tier deployed across 1 AZs with 6 EC2 (Elastic Compute Cloud) instances in each AZ Inside an Auto Scaling Group behind an ELB (elastic load balancer). And an application tier deployed in the same AZs with 6 EC2 instances inside an Auto scaling group behind an ELB and a Multi-AZ RDS (Relational Database services) deployment, with 6 stopped web tier EC2 instances and 6 stopped application tier EC2 instances all in the other AZ ready to be started if any of the running instances in the first AZ fails.

 You are designing a system which needs, at minimum, 8 m4.large instances operating to service traffic. When designing a system for high availability in the us-east-1 region, which has 6 Availability Zones, you company needs to be able to handle death of a full availability zone. How should you distribute the servers, to save as much cost as possible, assuming all of the EC2 nodes are properly linked to an ELB? Your VPC account can utilize us-east-1’s AZ’s a through f, inclusive.

1. 3 servers in each of AZ’s a through d, inclusive.
2. 8 servers in each of AZ’s a and b.
3. **2 servers in each of AZ’s a through e, inclusive.** (You need to design for N+1 redundancy on Availability Zones. ZONE\_COUNT = (REQUIRED\_INSTANCES / INSTANCE\_COUNT\_PER\_ZONE) + 1. To minimize cost, spread the instances across as many possible zones as you can. By using a though e, you are allocating 5 zones. Using 2 instances, you have 10 total instances. If a single zone fails, you have 4 zones left, with 2 instances each, for a total of 8 instances. By spreading out as much as possible, you have increased cost by only 25% and significantly de-risked an availability zone failure. Refer [link](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-regionsavailability- zones))
4. 4 servers in each of AZ’s a through c, inclusive.

 You need your API backed by DynamoDB to stay online during a total regional AWS failure. You can tolerate a couple minutes of lag or slowness during a large failure event, but the system should recover with normal operation after those few minutes. What is a good approach? **[PROFESSIONAL]**

1. **Set up DynamoDB cross-region replication in a master-standby configuration, with a single standby in another region. Create an Auto Scaling Group behind an ELB in each of the two regions DynamoDB is running in. Add a Route53 Latency DNS Record with DNS Failover, using the ELBs in the two regions as the resource records.** (Use DynamoDB cross-regional replication version with two ELBs and ASGs with Route53 Failover and Latency DNS. Refer [link](http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.CrossRegionRepl.html))
2. Set up a DynamoDB Multi-Region table. Create an Auto Scaling Group behind an ELB in each of the two regions DynamoDB is running in. Add a Route53 Latency DNS Record with DNS Failover, using the ELBs in the two regions as the resource records. (No such thing as DynamoDB Multi-Region table before. However, global tables have been now introduced.)
3. Set up a DynamoDB Multi-Region table. Create a cross-region ELB pointing to a cross-region Auto Scaling Group, and direct a Route53 Latency DNS Record with DNS Failover to the cross-region ELB. (No such thing as Cross Region ELB or cross-region ASG)
4. Set up DynamoDB cross-region replication in a master-standby configuration, with a single standby in another region. Create a cross-region ELB pointing to a cross-region Auto Scaling Group, and direct a Route53 Latency DNS Record with DNS Failover to the cross-region ELB. (No such thing as DynamoDB cross-region table or cross-region ELB)

 You are putting together a WordPress site for a local charity and you are using a combination of Route53, Elastic Load Balancers, EC2 & RDS. You launch your EC2 instance, download WordPress and setup the configuration files connection string so that it can communicate to RDS. When you browse to your URL however, nothing happens. Which of the following could NOT be the cause of this.

1. You have forgotten to open port 80/443 on your security group in which the EC2 instance is placed.
2. Your elastic load balancer has a health check, which is checking a webpage that does not exist; therefore your EC2 instance is not in service.
3. You have not configured an ALIAS for your A record to point to your elastic load balancer
4. **You have locked port 22 down to your specific IP address therefore users cannot access your site using HTTP/HTTPS**

 A development team that is currently doing a nightly six-hour build which is lengthening over time on-premises with a large and mostly under utilized server would like to transition to a continuous integration model of development on AWS with multiple builds triggered within the same day. However, they are concerned about cost, security and how to integrate with existing on-premises applications such as their LDAP and email servers, which cannot move off-premises. The development environment needs a source code repository; a project management system with a MySQL database resources for performing the builds and a storage location for QA to pick up builds from. What AWS services combination would you recommend to meet the development team’s requirements? **[PROFESSIONAL]**

1. A Bastion host Amazon EC2 instance running a VPN server for access from on-premises, Amazon EC2 for the source code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIP for the source code repository and project management system, Amazon SQL for a build queue, An Amazon Auto Scaling group of Amazon EC2 instances for performing builds and Amazon Simple Email Service for sending the build output. (Bastion is not for VPN connectivity also SES should not be used)
2. An AWS Storage Gateway for connecting on-premises software applications with cloud-based storage securely, Amazon EC2 for the resource code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIPs for the source code repository and project management system, Amazon Simple Notification Service for a notification initiated build, An Auto Scaling group of Amazon EC2 instances for performing builds and Amazon S3 for the build output. (Storage Gateway does not provide secure connectivity, still needs VPN. SNS alone cannot handle builds)
3. An AWS Storage Gateway for connecting on-premises software applications with cloud-based storage securely, Amazon EC2 for the resource code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIPs for the source code repository and project management system, Amazon SQS for a build queue, An Amazon Elastic Map Reduce (EMR) cluster of Amazon EC2 instances for performing builds and Amazon CloudFront for the build output. (Storage Gateway does not provide secure connectivity, still needs VPN. EMR is not ideal for performing builds as it needs normal EC2 instances)
4. **A VPC with a VPN Gateway back to their on-premises servers, Amazon EC2 for the source-code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIPs for the source code repository and project management system, SQS for a build queue, An Auto Scaling group of EC2 instances for performing builds and S3 for the build output.** (VPN gateway is required for secure connectivity. SQS for build queue and EC2 for builds)
5. Which service enables AWS customers to manage users and permissions in AWS?
   1. AWS Access Control Service (ACS)
   2. **AWS Identity and Access Management (IAM)**
   3. AWS Identity Manager (AIM)
6. IAM provides several policy templates you can use to automatically assign permissions to the groups you create. The \_\_\_\_\_ policy template gives the Admins group permission to access all account resources, except your AWS account information
   1. Read Only Access
   2. Power User Access
   3. AWS Cloud Formation Read Only Access
   4. **Administrator Access**
7. Every user you create in the IAM system starts with \_\_\_\_\_\_\_\_\_.
   1. Partial permissions
   2. Full permissions
   3. **No permissions**
8. Groups can’t \_\_\_\_\_.
   1. be nested more than 3 levels
   2. **be nested at all**
   3. be nested more than 4 levels
   4. be nested more than 2 levels
9. The \_\_\_\_\_ service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console.
   1. Amazon RDS
   2. AWS Integrity Management
   3. **AWS Identity and Access Management**
   4. Amazon EMR
10. An AWS customer is deploying an application that is composed of an AutoScaling group of EC2 Instances. The customers security policy requires that every outbound connection from these instances to any other service within the customers Virtual Private Cloud must be authenticated using a unique x.509 certificate that contains the specific instanceid. In addition an x.509 certificates must be designed by the customer’s Key management service in order to be trusted for authentication. Which of the following configurations will support these requirements?
    1. Configure an IAM Role that grants access to an Amazon S3 object containing a signed certificate and configure the Auto Scaling group to launch instances with this role. Have the instances bootstrap get the certificate from Amazon S3 upon first boot.
    2. Embed a certificate into the Amazon Machine Image that is used by the Auto Scaling group. Have the launched instances generate a certificate signature request with the instance’s assigned instance-id to the Key management service for signature.
    3. **Configure the Auto Scaling group to send an SNS notification of the launch of a new instance to the trusted key management service. Have the Key management service generate a signed certificate and send it directly to the newly launched instance.**
    4. Configure the launched instances to generate a new certificate upon first boot. Have the Key management service poll the AutoScaling group for associated instances and send new instances a certificate signature that contains the specific instance-id.
11. When assessing an organization AWS use of AWS API access credentials which of the following three credentials should be evaluated? Choose 3 answers
    1. Key pairs
    2. **Console passwords**
    3. **Access keys**
    4. **Signing certificates**
    5. Security Group memberships (required for EC2 instance access)
12. An organization has created 50 IAM users. The organization wants that each user can change their password but cannot change their access keys. How can the organization achieve this?
    1. The organization has to create a special password policy and attach it to each user
    2. The root account owner has to use CLI which forces each IAM user to change their password on first login
    3. By default each IAM user can modify their passwords
    4. **Root account owner can set the policy from the IAM console under the password policy screen**
13. An organization has created 50 IAM users. The organization has introduced a new policy which will change the access of an IAM user. How can the organization implement this effectively so that there is no need to apply the policy at the individual user level?
    1. **Use the IAM groups and add users as per their role to different groups and apply policy to group**
    2. The user can create a policy and apply it to multiple users in a single go with the AWS CLI
    3. Add each user to the IAM role as per their organization role to achieve effective policy setup
    4. Use the IAM role and implement access at the role level
14. Your organization’s security policy requires that all privileged users either use frequently rotated passwords or one-time access credentials in addition to username/password. Which two of the following options would allow an organization to enforce this policy for AWS users? Choose 2 answers
    1. **Configure multi-factor authentication for privileged IAM users**
    2. **Create IAM users for privileged accounts (**can set password policy**)**
    3. Implement identity federation between your organization’s Identity provider leveraging the IAM Security Token Service
    4. Enable the IAM single-use password policy option for privileged users (no such option the password expiration can be set from 1 to 1095 days)
15. Your organization is preparing for a security assessment of your use of AWS. In preparation for this assessment, which two IAM best practices should you consider implementing? Choose 2 answers
    1. Create individual IAM users for everyone in your organization
    2. **Configure MFA on the root account and for privileged IAM users**
    3. **Assign IAM users and groups configured with policies granting least privilege access**
    4. Ensure all users have been assigned and are frequently rotating a password, access ID/secret key, and X.509 certificate
16. A company needs to deploy services to an AWS region which they have not previously used. The company currently has an AWS identity and Access Management (IAM) role for the Amazon EC2 instances, which permits the instance to have access to Amazon DynamoDB. The company wants their EC2 instances in the new region to have the same privileges. How should the company achieve this?
    1. Create a new IAM role and associated policies within the new region
    2. **Assign the existing IAM role to the Amazon EC2 instances in the new region**
    3. Copy the IAM role and associated policies to the new region and attach it to the instances
    4. Create an Amazon Machine Image (AMI) of the instance and copy it to the desired region using the AMI Copy feature
17. After creating a new IAM user which of the following must be done before they can successfully make API calls?
    1. Add a password to the user.
    2. Enable Multi-Factor Authentication for the user.
    3. Assign a Password Policy to the user.
    4. **Create a set of Access Keys for the user**
18. An organization is planning to create a user with IAM. They are trying to understand the limitations of IAM so that they can plan accordingly. Which of the below mentioned statements is not true with respect to the limitations of IAM?
    1. **One IAM user can be a part of a maximum of 5 groups** (Refer [link](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_iam-limits.html))
    2. Organization can create 100 groups per AWS account
    3. One AWS account can have a maximum of 5000 IAM users
    4. One AWS account can have 250 roles
19. Within the IAM service a GROUP is regarded as a:
    1. A collection of AWS accounts
    2. It’s the group of EC2 machines that gain the permissions specified in the GROUP.
    3. There’s no GROUP in IAM, but only USERS and RESOURCES.
    4. **A collection of users.**
20. Is there a limit to the number of groups you can have?
    1. Yes for all users except root
    2. No
    3. Yes unless special permission granted
    4. **Yes for all users**
21. What is the default maximum number of MFA devices in use per AWS account (at the root account level)?
    1. **1**
    2. 5
    3. 15
    4. 10
22. When you use the AWS Management Console to delete an IAM user, IAM also deletes any signing certificates and any access keys belonging to the user.
    1. FALSE
    2. This is configurable
    3. **TRUE**
23. You are setting up a blog on AWS. In which of the following scenarios will you need AWS credentials? (Choose 3)
    1. **Sign in to the AWS management console to launch an Amazon EC2 instance**
    2. Sign in to the running instance to instance some software (needs ssh keys)
    3. **Launch an Amazon RDS instance**
    4. Log into your blog’s content management system to write a blog post (need to authenticate using blog authentication)
    5. **Post pictures to your blog on Amazon S3**
24. An organization has 500 employees. The organization wants to set up AWS access for each department. Which of the below mentioned options is a possible solution?
    1. Create IAM roles based on the permission and assign users to each role
    2. Create IAM users and provide individual permission to each
    3. **Create IAM groups based on the permission and assign IAM users to the groups**
    4. It is not possible to manage more than 100 IAM users with AWS
25. An organization has hosted an application on the EC2 instances. There will be multiple users connecting to the instance for setup and configuration of application. The organization is planning to implement certain security best practices. Which of the below mentioned pointers will not help the organization achieve better security arrangement?
    1. Apply the latest patch of OS and always keep it updated.
    2. **Allow only IAM users to connect with the EC2 instances with their own secret access key**. (Refer [link](http://aws.amazon.com/articles/1233/))
    3. Disable the password-based login for all the users. All the users should use their own keys to connect with the instance securely.
    4. Create a procedure to revoke the access rights of the individual user when they are not required to connect to EC2 instance anymore for the purpose of application configuration.
26. You require the ability to analyze a large amount of data, which is stored on Amazon S3 using Amazon Elastic Map Reduce. You are using the cc2.8xlarge instance type, who’s CPUs are mostly idle during processing. Which of the below would be the most cost efficient way to reduce the runtime of the job? **[PROFESSIONAL]**
    1. Create smaller files on Amazon S3.
    2. Add additional cc2.8xlarge instances by introducing a task group.
    3. **Use smaller instances that have higher aggregate I/O performance.**
    4. Create fewer, larger files on Amazon S3.
27. A customer’s nightly EMR job processes a single 2-TB data file stored on Amazon Simple Storage Service (S3). The Amazon Elastic Map Reduce (EMR) job runs on two On-Demand core nodes and three On-Demand task nodes. Which of the following may help reduce the EMR job completion time? Choose 2 answers
    1. Use three Spot Instances rather than three On-Demand instances for the task nodes.
    2. **Change the input split size in the MapReduce job configuration.**
    3. Use a bootstrap action to present the S3 bucket as a local filesystem.
    4. Launch the core nodes and task nodes within an Amazon Virtual Cloud.
    5. **Adjust the number of simultaneous mapper tasks.**
    6. Enable termination protection for the job flow.
28. Your department creates regular analytics reports from your company’s log files. All log data is collected in Amazon S3 and processed by daily Amazon Elastic Map Reduce (EMR) jobs that generate daily PDF reports and aggregated tables in CSV format for an Amazon Redshift data warehouse. Your CFO requests that you optimize the cost structure for this system. Which of the following alternatives will lower costs without compromising average performance of the system or data integrity for the raw data? **[PROFESSIONAL]**
    1. Use reduced redundancy storage (RRS) for PDF and CSV data in Amazon S3. Add Spot instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift. (Only Spot instances impacts performance)
    2. **Use reduced redundancy storage (RRS) for all data in S3. Use a combination of Spot instances and Reserved Instances for Amazon EMR jobs. Use Reserved instances for Amazon Redshift** (Combination of the Spot and reserved with guarantee performance and help reduce cost. Also, RRS would reduce cost and guarantee data integrity, which is different from data durability)
    3. Use reduced redundancy storage (RRS) for all data in Amazon S3. Add Spot Instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift (Only Spot instances impacts performance)
    4. Use reduced redundancy storage (RRS) for PDF and CSV data in S3. Add Spot Instances to EMR jobs. Use Spot Instances for Amazon Redshift. (Spot instances impacts performance and Spot instance not available for Redshift)
29. A research scientist is planning for the one-time launch of an Elastic MapReduce cluster and is encouraged by her manager to minimize the costs. The cluster is designed to ingest 200TB of genomics data with a total of 100 Amazon EC2 instances and is expected to run for around four hours. The resulting data set must be stored temporarily until archived into an Amazon RDS Oracle instance. Which option will help save the most money while meeting requirements? **[PROFESSIONAL]**
    1. **Store ingest and output files in Amazon S3. Deploy on-demand for the master and core nodes and spot for the task nodes.**
    2. Optimize by deploying a combination of on-demand, RI and spot-pricing models for the master, core and task nodes. Store ingest and output files in Amazon S3 with a lifecycle policy that archives them to Amazon Glacier. (Master and Core must be RI or On Demand. Cannot be Spot)
    3. Store the ingest files in Amazon S3 RRS and store the output files in S3. Deploy Reserved Instances for the master and core nodes and on-demand for the task nodes. (Need better durability for ingest file. Spot instances can be used for task nodes for cost saving. RI will not provide cost saving in this case)
    4. Deploy on-demand master, core and task nodes and store ingest and output files in Amazon S3 RRS (Input should be in S3 standard, as re-ingesting the input data might end up being more costly then holding the data for limited time in standard S3)
30. Your company sells consumer devices and needs to record the first activation of all sold devices. Devices are not activated until the information is written on a persistent database. Activation data is very important for your company and must be analyzed daily with a MapReduce job. The execution time of the data analysis process must be less than three hours per day. Devices are usually sold evenly during the year, but when a new device model is out, there is a predictable peak in activation’s, that is, for a few days there are 10 times or even 100 times more activation’s than in average day. Which of the following databases and analysis framework would you implement to better optimize costs and performance for this workload? **[PROFESSIONAL]**
    1. Amazon RDS and Amazon Elastic MapReduce with Spot instances.
    2. **Amazon DynamoDB and Amazon Elastic MapReduce with Spot instances.**
    3. Amazon RDS and Amazon Elastic MapReduce with Reserved instances.
    4. Amazon DynamoDB and Amazon Elastic MapReduce with Reserved instances
31. What does RRS stand for when talking about S3?
    1. Redundancy Removal System
    2. Relational Rights Storage
    3. Regional Rights Standard
    4. **Reduced Redundancy Storage**
32. What is the durability of S3 RRS?
    1. **99.99%**
    2. 99.95%
    3. 99.995%
    4. 99.999999999%
33. What is the Reduced Redundancy option in Amazon S3?
    1. **Less redundancy for a lower cost**
    2. It doesn’t exist in Amazon S3, but in Amazon EBS.
    3. It allows you to destroy any copy of your files outside a specific jurisdiction.
    4. It doesn’t exist at all
34. An application is generating a log file every 5 minutes. The log file is not critical but may be required only for verification in case of some major issue. The file should be accessible over the internet whenever required. Which of the below mentioned options is a best possible storage solution for it?
    1. AWS S3
    2. AWS Glacier
    3. AWS RDS
    4. **AWS S3 RRS** (Reduced Redundancy Storage (RRS) is an Amazon S3 storage option that enables customers to store noncritical, reproducible data at lower levels of redundancy than Amazon S3’s standard storage. RRS is designed to sustain the loss of data in a single facility.)
35. A user has moved an object to Glacier using the life cycle rules. The user requests to restore the archive after 6 months. When the restore request is completed the user accesses that archive. Which of the below mentioned statements is not true in this condition?
    1. The archive will be available as an object for the duration specified by the user during the restoration request
    2. **The restored object’s storage class will be RRS** (After the object is restored the storage class still remains GLACIER. [Read more](http://docs.aws.amazon.com/AmazonS3/latest/dev/restoring-objects.html))
    3. The user can modify the restoration period only by issuing a new restore request with the updated period
    4. The user needs to pay storage for both RRS (restored) and Glacier (Archive) Rates
36. Your department creates regular analytics reports from your company’s log files. All log data is collected in Amazon S3 and processed by daily Amazon Elastic Map Reduce (EMR) jobs that generate daily PDF reports and aggregated tables in CSV format for an Amazon Redshift data warehouse. Your CFO requests that you optimize the cost structure for this system. Which of the following alternatives will lower costs without compromising average performance of the system or data integrity for the raw data? **[PROFESSIONAL]**
    1. Use reduced redundancy storage (RRS) for PDF and CSV data in Amazon S3. Add Spot instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift. (Spot instances impacts performance)
    2. **Use reduced redundancy storage (RRS) for all data in S3. Use a combination of Spot instances and Reserved Instances for Amazon EMR jobs. Use Reserved instances for Amazon Redshift** (Combination of the Spot and reserved with guarantee performance and help reduce cost. Also, RRS would reduce cost and guarantee data integrity, which is different from data durability )
    3. Use reduced redundancy storage (RRS) for all data in Amazon S3. Add Spot Instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift (Spot instances impacts performance)
    4. Use reduced redundancy storage (RRS) for PDF and CSV data in S3. Add Spot Instances to EMR jobs. Use Spot Instances for Amazon Redshift. (Spot instances impacts performance)
37. Which of the below mentioned options can be a good use case for storing content in AWS RRS?
    1. Storing mission critical data Files
    2. Storing infrequently used log files
    3. Storing a video file which is not reproducible
    4. **Storing image thumbnails**
38. A newspaper organization has an on-premises application which allows the public to search its back catalogue and retrieve individual newspaper pages via a website written in Java. They have scanned the old newspapers into JPEGs (approx. 17TB) and used Optical Character Recognition (OCR) to populate a commercial search product. The hosting platform and software is now end of life and the organization wants to migrate its archive to AWS and produce a cost efficient architecture and still be designed for availability and durability. Which is the most appropriate? **[PROFESSIONAL]**
    1. Use S3 with reduced redundancy to store and serve the scanned files, install the commercial search application on EC2 Instances and configure with auto-scaling and an Elastic Load Balancer. (RRS impacts durability and commercial search would add to cost)
    2. Model the environment using CloudFormation. Use an EC2 instance running Apache webserver and an open source search application, stripe multiple standard EBS volumes together to store the JPEGs and search index. (Using EBS is not cost effective for storing files)
    3. **Use S3 with standard redundancy to store and serve the scanned files, use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones.** (Standard S3 and Elastic Beanstalk provides availability and durability, Standard S3 and CloudSearch provides cost effective storage and search)
    4. Use a single-AZ RDS MySQL instance to store the search index and the JPEG images use an EC2 instance to serve the website and translate user queries into SQL. (RDS is not ideal and cost effective to store files, Single AZ impacts availability)
    5. Use a CloudFront download distribution to serve the JPEGs to the end users and Install the current commercial search product, along with a Java Container for the website on EC2 instances and use Route53 with DNS round-robin. (CloudFront needs a source and using commercial search product is not cost effective)
39. A research scientist is planning for the one-time launch of an Elastic MapReduce cluster and is encouraged by her manager to minimize the costs. The cluster is designed to ingest 200TB of genomics data with a total of 100 Amazon EC2 instances and is expected to run for around four hours. The resulting data set must be stored temporarily until archived into an Amazon RDS Oracle instance. Which option will help save the most money while meeting requirements? **[PROFESSIONAL]**
    1. **Store ingest and output files in Amazon S3. Deploy on-demand for the master and core nodes and spot for the task nodes.**
    2. Optimize by deploying a combination of on-demand, RI and spot-pricing models for the master, core and task nodes. Store ingest and output files in Amazon S3 with a lifecycle policy that archives them to Amazon Glacier. (Master and Core must be RI or On Demand. Cannot be Spot)
    3. Store the ingest files in Amazon S3 RRS and store the output files in S3. Deploy Reserved Instances for the master and core nodes and on-demand for the task nodes. (Need better durability for ingest file. Spot instances can be used for task nodes for cost saving.)
    4. Deploy on-demand master, core and task nodes and store ingest and output files in Amazon S3 RRS (Input must be in S3 standard)
40. You currently operate a web application in the AWS US-East region. The application runs on an auto-scaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your EC2, IAM and RDS resources. The solution must ensure the integrity and confidentiality of your log data. Which of these solutions would you recommend?
    1. **Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles, S3 bucket policies and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs. (**Single New bucket with global services option for IAM and MFA delete for confidentiality**)**
    2. Create a new CloudTrail with one new S3 bucket to store the logs. Configure SNS to send log file delivery notifications to your management system. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs. (Missing Global Services for IAM)
    3. Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected Use S3 ACLs and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs. (Existing bucket prevents confidentiality)
    4. Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tools. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs (3 buckets not needed, Missing Global services options)
41. Which of the following are true regarding AWS CloudTrail? Choose 3 answers
    1. **CloudTrail is enabled globally** (it can be enabled for all regions and also per region basis)
    2. CloudTrail is enabled by default (**was not enabled by default, however, it is enabled by default as per the latest** [**AWS enhancements**](https://aws.amazon.com/blogs/aws/new-amazon-web-services-extends-cloudtrail-to-all-aws-customers/))
    3. **CloudTrail is enabled on a per-region basis** (it can be enabled for all regions and also per region basis)
    4. CloudTrail is enabled on a per-service basis (once enabled it is applicable for all the supported services, service can’t be selected)
    5. **Logs can be delivered to a single Amazon S3 bucket for aggregation**
    6. CloudTrail is enabled for all available services within a region. (is enabled only for CloudTrail supported services)
    7. Logs can only be processed and delivered to the region in which they are generated. (can be logged to bucket in any region)
42. An organization has configured the custom metric upload with CloudWatch. The organization has given permission to its employees to upload data using CLI as well SDK. How can the user track the calls made to CloudWatch?
    1. The user can enable logging with CloudWatch which logs all the activities
    2. **Use CloudTrail to monitor the API calls**
    3. Create an IAM user and allow each user to log the data using the S3 bucket
    4. Enable detailed monitoring with CloudWatch
43. A user is trying to understand the CloudWatch metrics for the AWS services. It is required that the user should first understand the namespace for the AWS services. Which of the below mentioned is not a valid namespace for the AWS services?
    1. AWS/StorageGateway
    2. **AWS/CloudTrail (**[CloudWatch supported namespaces](http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/aws-namespaces.html)**)**
    3. AWS/ElastiCache
    4. AWS/SWF
44. Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?
    1. **Use CloudTrail Log File Integrity Validation**. (Refer [link](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html))
    2. Use AWS Config SNS Subscriptions and process events in real time.
    3. Use CloudTrail backed up to AWS S3 and Glacier.
    4. Use AWS Config Timeline forensics.
45. Your CTO has asked you to make sure that you know what all users of your AWS account are doing to change resources at all times. She wants a report of who is doing what over time, reported to her once per week, for as broad a resource type group as possible. How should you do this?
    1. **Create a global AWS CloudTrail Trail. Configure a script to aggregate the log data delivered to S3 once per week and deliver this to the CTO.**
    2. Use CloudWatch Events Rules with an SNS topic subscribed to all AWS API calls. Subscribe the CTO to an email type delivery on this SNS Topic.
    3. Use AWS IAM credential reports to deliver a CSV of all uses of IAM User Tokens over time to the CTO.
    4. Use AWS Config with an SNS subscription on a Lambda, and insert these changes over time into a DynamoDB table. Generate reports based on the contents of this table.
46. You have deployed a web application targeting a global audience across multiple AWS Regions under the domain name example.com. You decide to use Route 53 Latency-Based Routing to serve web requests to users from the region closest to the user. To provide business continuity in the event of server downtime you configure weighted record sets associated with two web servers in separate Availability Zones per region. During a DR test you notice that when you disable all web servers in one of the regions Route 53 does not automatically direct all users to the other region. What could be happening? (Choose 2 answers)
    1. Latency resource record sets cannot be used in combination with weighted resource record sets.
    2. **You did not setup an http health check for one or more of the weighted resource record sets associated with the disabled web servers**
    3. The value of the weight associated with the latency alias resource record set in the region with the disabled servers is higher than the weight for the other region.
    4. One of the two working web servers in the other region did not pass its HTTP health check
    5. **You did not set “Evaluate Target Health” to “Yes” on the latency alias resource record set associated with example.com in the region where you disabled the servers.**
47. The compliance department within your multi-national organization requires that all data for your customers that reside in the European Union (EU) must not leave the EU and also data for customers that reside in the US must not leave the US without explicit authorization. What must you do to comply with this requirement for a web based profile management application running on EC2?
    1. Run EC2 instances in multiple AWS Availability Zones in single Region and leverage an Elastic Load Balancer with session stickiness to route traffic to the appropriate zone to create their profile (should be in 2 different regions – US and Europe)
    2. Run EC2 instances in multiple Regions and leverage Route 53’s Latency Based Routing capabilities to route traffic to the appropriate region to create their profile (Latency based routing policy would not guarantee the compliance requirement)
    3. **Run EC2 instances in multiple Regions and leverage a third party data provider to determine if a user needs to be redirect to the appropriate region to create their profile**
    4. Run EC2 instances in multiple AWS Availability Zones in a single Region and leverage a third party data provider to determine if a user needs to be redirect to the appropriate zone to create their profile(should be in 2 different regions – US and Europe)
48. A US-based company is expanding their web presence into Europe. The company wants to extend their AWS infrastructure from Northern Virginia (us-east-1) into the Dublin (eu-west-1) region. Which of the following options would enable an equivalent experience for users on both continents?
    1. Use a public-facing load balancer per region to load-balance web traffic, and enable HTTP health checks.
    2. Use a public-facing load balancer per region to load-balance web traffic, and enable sticky sessions.
    3. **Use Amazon Route 53, and apply a geolocation routing policy to distribute traffic across both regions**
    4. Use Amazon Route 53, and apply a weighted routing policy to distribute traffic across both regions.
49. You have been asked to propose a multi-region deployment of a web-facing application where a controlled portion of your traffic is being processed by an alternate region. Which configuration would achieve that goal?
    1. **Route 53 record sets with weighted routing policy**
    2. Route 53 record sets with latency based routing policy
    3. Auto Scaling with scheduled scaling actions set
    4. Elastic Load Balancing with health checks enabled
50. Your company is moving towards tracking web page users with a small tracking image loaded on each page. Currently you are serving this image out of us-east, but are starting to get concerned about the time it takes to load the image for users on the west coast. What are the two best ways to speed up serving this image? Choose 2 answers
    1. **Use Route 53’s Latency Based Routing and serve the image out of us-west-2 as well as us-east-1**
    2. **Serve the image out through CloudFront**
    3. Serve the image out of S3 so that it isn’t being served of your web application tier
    4. Use EBS PIOPs to serve the image faster out of your EC2 instances
51. Your API requires the ability to stay online during AWS regional failures. Your API does not store any state, it only aggregates data from other sources – you do not have a database. What is a simple but effective way to achieve this uptime goal?
    1. Use a CloudFront distribution to serve up your API. Even if the region your API is in goes down, the edge locations CloudFront uses will be fine.
    2. Use an ELB and a cross-zone ELB deployment to create redundancy across datacenters. Even if a region fails, the other AZ will stay online.
    3. Create a Route53 Weighted Round Robin record, and if one region goes down, have that region redirect to the other region.
    4. **Create a Route53 Latency Based Routing Record with Failover and point it to two identical deployments of your stateless API in two different regions. Make sure both regions use Auto Scaling Groups behind ELBs.** (Refer [link](http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html))
52. Which of the following services natively encrypts data at rest within an AWS region?Choose 2 answers
    1. **AWS Storage Gateway**
    2. Amazon DynamoDB
    3. Amazon CloudFront
    4. **Amazon Glacier**
    5. Amazon Simple Queue Service
53. What does the AWS Storage Gateway provide?
    1. **It allows to integrate on-premises IT environments with Cloud Storage**
    2. A direct encrypted connection to Amazon S3.
    3. It’s a backup solution that provides an on-premises Cloud storage.
    4. It provides an encrypted SSL endpoint for backups in the Cloud.
54. You’re running an application on-premises due to its dependency on non-x86 hardware and want to use AWS for data backup. Your backup application is only able to write to POSIX-compatible block-based storage. You have 140TB of data and would like to mount it as a single folder on your file server. Users must be able to access portions of this data while the backups are taking place. What backup solution would be most appropriate for this use case?
    1. Use Storage Gateway and configure it to use Gateway Cached volumes.
    2. Configure your backup software to use S3 as the target for your data backups.
    3. Configure your backup software to use Glacier as the target for your data backups
    4. **Use Storage Gateway and configure it to use Gateway Stored volumes** (Data is hosted on the On-premise server as well. The requirement for 140TB is for file server On-Premise more to confuse and not in AWS. Just need a backup solution hence stored instead of cached volumes)
55. A customer has a single 3-TB volume on-premises that is used to hold a large repository of images and print layout files. This repository is growing at 500 GB a year and must be presented as a single logical volume. The customer is becoming increasingly constrained with their local storage capacity and wants an off-site backup of this data, while maintaining low-latency access to their frequently accessed data. Which AWS Storage Gateway configuration meets the customer requirements?
    1. **Gateway-Cached volumes with snapshots scheduled to Amazon S3**
    2. Gateway-Stored volumes with snapshots scheduled to Amazon S3
    3. Gateway-Virtual Tape Library with snapshots to Amazon S3
    4. Gateway-Virtual Tape Library with snapshots to Amazon Glacier
56. You have a proprietary data store on-premises that must be backed up daily by dumping the data store contents to a single compressed 50GB file and sending the file to AWS. Your SLAs state that any dump file backed up within the past 7 days can be retrieved within 2 hours. Your compliance department has stated that all data must be held indefinitely. The time required to restore the data store from a backup is approximately 1 hour. Your on-premise network connection is capable of sustaining 1gbps to AWS. Which backup methods to AWS would be most cost-effective while still meeting all of your requirements?
    1. Send the daily backup files to Glacier immediately after being generated (will not meet the RTO)
    2. Transfer the daily backup files to an EBS volume in AWS and take daily snapshots of the volume (Not cost effective)
    3. Transfer the daily backup files to S3 and use appropriate bucket lifecycle policies to send to Glacier (Store in S3 for seven days and then archive to Glacier)
    4. Host the backup files on a Storage Gateway with Gateway-Cached Volumes and take daily snapshots (Not Cost effective as local storage as well as S3 storage)
57. A customer implemented AWS Storage Gateway with a gateway-cached volume at their main office. An event takes the link between the main and branch office offline. Which methods will enable the branch office to access their data? Choose 3 answers
    1. Use a HTTPS GET to the Amazon S3 bucket where the files are located (gateway volumes are only accessible from the AWS Storage Gateway and cannot be directly accessed using Amazon S3 APIs)
    2. Restore by implementing a lifecycle policy on the Amazon S3 bucket.
    3. Make an Amazon Glacier Restore API call to load the files into another Amazon S3 bucket within four to six hours.
    4. **Launch a new AWS Storage Gateway instance AMI in Amazon EC2, and restore from a gateway snapshot**
    5. **Create an Amazon EBS volume from a gateway snapshot, and mount it to an Amazon EC2 instance.**
    6. **Launch an AWS Storage Gateway virtual iSCSI device at the branch office, and restore from a gateway snapshot**
58. A user is trying to pre-warm a blank EBS volume attached to a Linux instance. Which of the below mentioned steps should be performed by the user?
    1. There is no need to pre-warm an EBS volume (with latest update no pre-warming is needed)
    2. **Contact AWS support to pre-warm** (This used to be the case before, but pre warming is not necessary now)
    3. Unmount the volume before pre-warming
    4. Format the device
59. A user has created an EBS volume of 10 GB and attached it to a running instance. The user is trying to access EBS for first time. Which of the below mentioned options is the correct statement with respect to a first time EBS access?
    1. The volume will show a size of 8 GB
    2. **The volume will show a loss of the IOPS performance the first time** (the volume needed to be wiped cleaned before for new volumes, however pre warming is not needed any more)
    3. The volume will be blank
    4. If the EBS is mounted it will ask the user to create a file system
60. You are running a database on an EC2 instance, with the data stored on Elastic Block Store (EBS) for persistence At times throughout the day, you are seeing large variance in the response times of the database queries Looking into the instance with the isolate command you see a lot of wait time on the disk volume that the database’s data is stored on. What two ways can you improve the performance of the database’s storage while maintaining the current persistence of the data? Choose 2 answers
    1. Move to an SSD backed instance
    2. **Move the database to an EBS-Optimized Instance**
    3. **Use Provisioned IOPs EBS**
    4. Use the ephemeral storage on an m2.4xLarge Instance Instead
61. You have launched an EC2 instance with four (4) 500 GB EBS Provisioned IOPS volumes attached. The EC2 Instance is EBS-Optimized and supports 500 Mbps throughput between EC2 and EBS. The two EBS volumes are configured as a single RAID 0 device, and each Provisioned IOPS volume is provisioned with 4,000 IOPS (4000 16KB reads or writes) for a total of 16,000 random IOPS on the instance. The EC2 Instance initially delivers the expected 16,000 IOPS random read and write performance. Sometime later in order to increase the total random I/O performance of the instance, you add an additional two 500 GB EBS Provisioned IOPS volumes to the RAID. Each volume is provisioned to 4,000 IOPS like the original four for a total of 24,000 IOPS on the EC2 instance Monitoring shows that the EC2 instance CPU utilization increased from 50% to 70%, but the total random IOPS measured at the instance level does not increase at all. What is the problem and a valid solution?
    1. Larger storage volumes support higher Provisioned IOPS rates: increase the provisioned volume storage of each of the 6 EBS volumes to 1TB.
    2. **EBS-Optimized throughput limits the total IOPS that can be utilized use an EBS-Optimized instance that provides larger throughput. (**[EC2 Instance types](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-ec2-config.html) have limit on max throughput and would require larger instance types to provide 24000 IOPS**)**
    3. Small block sizes cause performance degradation, limiting the I’O throughput, configure the instance device driver and file system to use 64KB blocks to increase throughput.
    4. RAID 0 only scales linearly to about 4 devices, use RAID 0 with 4 EBS Provisioned IOPS volumes but increase each Provisioned IOPS EBS volume to 6.000 IOPS.
    5. The standard EBS instance root volume limits the total IOPS rate, change the instant root volume to also be a 500GB 4,000 Provisioned IOPS volume
62. A user has deployed an application on an EBS backed EC2 instance. For a better performance of application, it requires dedicated EC2 to EBS traffic. How can the user achieve this?
    1. Launch the EC2 instance as EBS provisioned with PIOPS EBS
    2. Launch the EC2 instance as EBS enhanced with PIOPS EBS
    3. Launch the EC2 instance as EBS dedicated with PIOPS EBS
    4. **Launch the EC2 instance as EBS optimized with PIOPS EBS**
63. What does Amazon ElastiCache provide?
    1. A service by this name doesn’t exist. Perhaps you mean Amazon CloudCache.
    2. A virtual server with a huge amount of memory.
    3. **A managed In-memory cache service**
    4. An Amazon EC2 instance with the Memcached software already pre-installed.
64. You are developing a highly available web application using stateless web servers. Which services are suitable for storing session state data? Choose 3 answers.
    1. Elastic Load Balancing
    2. **Amazon Relational Database Service (RDS)**
    3. Amazon CloudWatch
    4. **Amazon ElastiCache**
    5. **Amazon DynamoDB**
    6. AWS Storage Gateway
65. Which statement best describes ElastiCache?
    1. Reduces the latency by splitting the workload across multiple AZs
    2. A simple web services interface to create and store multiple data sets, query your data easily, and return the results
    3. **Offload the read traffic from your database in order to reduce latency caused by read-heavy workload**
    4. Managed service that makes it easy to set up, operate and scale a relational database in the cloud
66. Our company is getting ready to do a major public announcement of a social media site on AWS. The website is running on EC2 instances deployed across multiple Availability Zones with a Multi-AZ RDS MySQL Extra Large DB Instance. The site performs a high number of small reads and writes per second and relies on an eventual consistency model. After comprehensive tests you discover that there is read contention on RDS MySQL. Which are the best approaches to meet these requirements? (Choose 2 answers)
    1. **Deploy ElastiCache in-memory cache running in each availability zone**
    2. Implement sharding to distribute load to multiple RDS MySQL instances
    3. Increase the RDS MySQL Instance size and Implement provisioned IOPS
    4. **Add an RDS MySQL read replica in each availability zone**
67. You are using ElastiCache Memcached to store session state and cache database queries in your infrastructure. You notice in CloudWatch that Evictions and Get Misses are both very high. What two actions could you take to rectify this? Choose 2 answers
    1. **Increase the number of nodes in your cluster**
    2. Tweak the max\_item\_size parameter
    3. Shrink the number of nodes in your cluster
    4. **Increase the size of the nodes in the cluster**
68. You have been tasked with moving an ecommerce web application from a customer’s datacenter into a VPC. The application must be fault tolerant and well as highly scalable. Moreover, the customer is adamant that service interruptions not affect the user experience. As you near launch, you discover that the application currently uses multicast to share session state between web servers, In order to handle session state within the VPC, you choose to:
    1. **Store session state in Amazon ElastiCache for Redis** (scalable and makes the web applications stateless)
    2. Create a mesh VPN between instances and allow multicast on it
    3. Store session state in Amazon Relational Database Service (RDS solution not highly scalable)
    4. Enable session stickiness via Elastic Load Balancing (affects user experience if the instance goes down)
69. When you are designing to support a 24-hour flash sale, which one of the following methods best describes a strategy to lower the latency while keeping up with unusually heavy traffic?
    1. Launch enhanced networking instances in a placement group to support the heavy traffic (only improves internal communication)
    2. Apply Service Oriented Architecture (SOA) principles instead of a 3-tier architecture (just simplifies architecture)
    3. Use Elastic Beanstalk to enable blue-green deployment (only minimizes download for applications and ease of rollback)
    4. **Use ElastiCache as in-memory storage on top of DynamoDB to store user sessions** (scalable, faster read/writes and in memory storage)
70. You are configuring your company’s application to use Auto Scaling and need to move user state information. Which of the following AWS services provides a shared data store with durability and low latency?
    1. AWS ElastiCache Memcached (does not provide durability as if the node is gone the data is gone)
    2. Amazon Simple Storage Service
    3. Amazon EC2 instance storage
    4. **Amazon DynamoDB**
71. Your application is using an ELB in front of an Auto Scaling group of web/application servers deployed across two AZs and a Multi-AZ RDS Instance for data persistence. The database CPU is often above 80% usage and 90% of I/O operations on the database are reads. To improve performance you recently added a single-node Memcached ElastiCache Cluster to cache frequent DB query results. In the next weeks the overall workload is expected to grow by 30%. Do you need to change anything in the architecture to maintain the high availability for the application with the anticipated additional load and Why?
    1. **You should deploy two Memcached ElastiCache Clusters in different AZs because the RDS Instance will not be able to handle the load if the cache node fails.**
    2. If the cache node fails the automated ElastiCache node recovery feature will prevent any availability impact. (does not provide high availability, as data is lost if the node is lost)
    3. Yes you should deploy the Memcached ElastiCache Cluster with two nodes in the same AZ as the RDS DB master instance to handle the load if one cache node fails. (Single AZ affects availability as DB is Multi AZ and would be overloaded is the AZ goes down)
    4. No if the cache node fails you can always get the same data from the DB without having any availability impact. (Will overload the database affecting availability)
72. A read only news reporting site with a combined web and application tier and a database tier that receives large and unpredictable traffic demands must be able to respond to these traffic fluctuations automatically. What AWS services should be used meet these requirements?
    1. **Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaling group monitored with CloudWatch and RDS with read replicas.**
    2. Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch and RDS with read replicas (Stateful instances will not allow for scaling)
    3. Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch and multi-AZ RDS (Stateful instances will allow not for scaling & multi-AZ is for high availability and not scaling)
    4. Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaling group monitored with CloudWatch and multi-AZ RDS (multi-AZ is for high availability and not scaling)
73. You have written an application that uses the Elastic Load Balancing service to spread traffic to several web servers. Your users complain that they are sometimes forced to login again in the middle of using your application, after they have already logged in. This is not behavior you have designed. What is a possible solution to prevent this happening?
    1. Use instance memory to save session state.
    2. Use instance storage to save session state.
    3. Use EBS to save session state.
    4. **Use ElastiCache to save session state.**
    5. Use Glacier to save session slate.
74. With which AWS services CloudHSM can be used (select 2)
    1. S3
    2. DynamoDB
    3. **RDS**
    4. ElastiCache
    5. **Amazon Redshift**
75. You have recently joined a startup company building sensors to measure street noise and air quality in urban areas. The company has been running a pilot deployment of around 100 sensors for 3 months. Each sensor uploads 1KB of sensor data every minute to a backend hosted on AWS. During the pilot, you measured a peak of 10 IOPS on the database, and you stored an average of 3GB of sensor data per month in the database. The current deployment consists of a load-balanced auto scaled Ingestion layer using EC2 instances and a PostgreSQL RDS database with 500GB standard storage. The pilot is considered a success and your CEO has managed to get the attention or some potential investors. The business plan requires a deployment of at least 100K sensors, which needs to be supported by the backend. You also need to store sensor data for at least two years to be able to compare year over year Improvements. To secure funding, you have to make sure that the platform meets these requirements and leaves room for further scaling. Which setup will meet the requirements?
    1. Add an SQS queue to the ingestion layer to buffer writes to the RDS instance (RDS instance will not support data for 2 years)
    2. **Ingest data into a DynamoDB table and move old data to a Redshift cluster** (Handle 10K IOPS ingestion and store data into Redshift for analysis)
    3. Replace the RDS instance with a 6 node Redshift cluster with 96TB of storage (Does not handle the ingestion issue)
    4. Keep the current architecture but upgrade RDS storage to 3TB and 10K provisioned IOPS (RDS instance will not support data for 2 years)
76. Which two AWS services provide out-of-the-box user configurable automatic backup-as-a-service and backup rotation options? Choose 2 answers
    1. Amazon S3
    2. **Amazon RDS**
    3. Amazon EBS
    4. **Amazon Redshift**
77. Your department creates regular analytics reports from your company’s log files. All log data is collected in Amazon S3 and processed by daily Amazon Elastic Map Reduce (EMR) jobs that generate daily PDF reports and aggregated tables in CSV format for an Amazon Redshift data warehouse. Your CFO requests that you optimize the cost structure for this system. Which of the following alternatives will lower costs without compromising average performance of the system or data integrity for the raw data?
    1. Use reduced redundancy storage (RRS) for PDF and CSV data in Amazon S3. Add Spot instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift. (Spot instances impacts performance)
    2. **Use reduced redundancy storage (RRS) for all data in S3. Use a combination of Spot instances and Reserved Instances for Amazon EMR jobs. Use Reserved instances for Amazon Redshift** (Combination of the Spot and reserved with guarantee performance and help reduce cost. Also, RRS would reduce cost and guarantee data integrity, which is different from data durability)
    3. Use reduced redundancy storage (RRS) for all data in Amazon S3. Add Spot Instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift (Spot instances impacts performance)
    4. Use reduced redundancy storage (RRS) for PDF and CSV data in S3. Add Spot Instances to EMR jobs. Use Spot Instances for Amazon Redshift. (Spot instances impacts performance and Spot instance not available for Redshift)
78. How can you secure data at rest on an EBS volume?
    1. Encrypt the volume using the S3 server-side encryption service
    2. Attach the volume to an instance using EC2’s SSL interface.
    3. Create an IAM policy that restricts read and write access to the volume.
    4. Write the data randomly instead of sequentially.
    5. **Use an encrypted file system on top of the EBS volume**
79. Your company policies require encryption of sensitive data at rest. You are considering the possible options for protecting data while storing it at rest on an EBS data volume, attached to an EC2 instance. Which of these options would allow you to encrypt your data at rest? (Choose 3 answers)
    1. **Implement third party volume encryption tools** —
    2. Do nothing as EBS volumes are encrypted by default
    3. **Encrypt data inside your applications before storing it on EBS**
    4. **Encrypt data using native data encryption drivers at the file system level**
    5. Implement SSL/TLS for all services running on the server
80. A company is storing data on Amazon Simple Storage Service (S3). The company’s security policy mandates that data is encrypted at rest. Which of the following methods can achieve this? Choose 3 answers
    1. **Use Amazon S3 server-side encryption with AWS Key Management Service managed keys**
    2. **Use Amazon S3 server-side encryption with customer-provided keys**
    3. Use Amazon S3 server-side encryption with EC2 key pair.
    4. Use Amazon S3 bucket policies to restrict access to the data at rest.
    5. **Encrypt the data on the client-side before ingesting to Amazon S3 using their own master key**
    6. Use SSL to encrypt the data while in transit to Amazon S3.
81. Which 2 services provide native encryption
    1. Amazon EBS
    2. **Amazon Glacier**
    3. Amazon Redshift (is optional)
    4. Amazon RDS (is optional)
    5. **Amazon Storage Gateway**
82. With which AWS services CloudHSM can be used (select 2)
    1. S3
    2. DynamoDb
    3. **RDS**
    4. ElastiCache
    5. **Amazon Redshift**