**Q1.** 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.

Q2. 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
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
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

Q3. 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.

Q4. 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

Q5. 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

Q6. 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.

Q7. 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.
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.
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)
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.

Q7. 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.
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.
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.

Q8. 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.

Q9. 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

Q10. 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.

Q11. 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
2. An Internet Gateway to allow a VPN connection.
3. An Elastic IP address on the VPC instance
4. An IP address space that does not conflict with the one on-premises
5. Entries in Amazon Route 53 that allow the Instance to resolve its dependencies’ IP addresses
6. A VM Import of the current virtual machine

Q12. You have a periodic Image analysis application that gets some files In Input analyzes them and tor 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

A. 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

B. 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

C. 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

D. 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 ot hosts depending on the length of the SQS queue.

Q13. 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.
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.
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.
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.

QUESTION 14   
are the new IT architect in a company that operates a mobile sleep tracking application When activated at night, the mobile app is sending collected data points of 1 kilobyte every 5 minutes to your backend   
The backend takes care of authenticating the user and writing the data points into an Amazon DynamoDB table.   
Every morning, you scan the table to extract and aggregate last night's data on a per user basis, and store the results in Amazon S3.   
Users are notified via Amazon SMS mobile push notifications that new data is available, which is parsed and visualized by (The mobile app Currently you have around 100k users who are mostly based out of North America.   
You have been tasked to optimize the architecture of the backend system to lower cost what would you recommend? (Choose 2 answers)

A.    Create a new Amazon DynamoDB (able each day and drop the one for the previous day after its data is on Amazon S3.   
B.    Have the mobile app access Amazon DynamoDB directly instead of JSON files stored on Amazon S3.   
C.    Introduce an Amazon SQS queue to buffer writes to the Amazon DynamoDB table and reduce provisioned write throughput.   
D.    Introduce Amazon Elasticache lo cache reads from the Amazon DynamoDB table and reduce provisioned read throughput.   
E.    Write data directly into an Amazon Redshift cluster replacing both Amazon DynamoDB and Amazon S3.

Q15. 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.

Q16. 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.
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.
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.
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

Q17. 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.
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
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
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.

Q18. 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.

Q19. An AWS customer is deploying an application mat 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 Designed by the customer’s Key management service in order to be  
trusted for authentication.  
Which of the following configurations will support these requirements?

A. Configure an IAM Role that grants access to an Amazon S3 object containing a signed certificate and configure me Auto Scaling group to launch instances with this role Have the instances bootstrap get the certificate from Amazon S3 upon first boot.

B. 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.

C. 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.

D. 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.

**Q20.** 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.

Q21. 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
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
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
4. Backup RDS database to S3 using Oracle RMAN. Backup the EC2 instances using AMIs, and supplement with EBS snapshots for individual volume restore.

Q22. 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

Q23. 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.
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
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.

Q24. 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)
4. EC2 Key Pairs
5. Launch configurations
6. Security Groups

Q25. 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
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.
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.
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.

Q26. 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.

Q27. 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. Sort stale 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.

Q28. 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.
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)

Q29. 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.

Q30. 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.

Q31. 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]

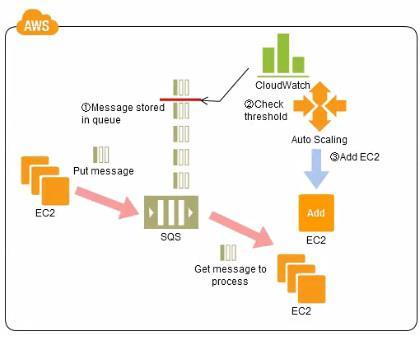
1. Use an EC2 Instance that is launched with an EC2 role providing access to the Score Data DynamoDB table and the GameState S3 bucket that communicates with the mobile app via web services.
2. Use temporary security credentials that assume a role providing access to the Score Data DynamoDB table and 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.

Q32. 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
3. Increase the RDS MySQL Instance size and Implement provisioned IOPS
4. Add an RDS MySQL read replica in each availability zone

Q33. 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.
3. Implement Elastic Load Balancing with SSL listeners In front of the web applications
4. Implement a reverse proxy layer in front of web servers and configure IDS/IPS agents on each reverse proxy server

Q34. 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.

Q35. 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.
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.
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.
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.

Q36. 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.

Q37. 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).
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
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.
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.
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.

Q38. 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.
3. Whitelist the ELB IP addresses and route payment requests from the Application servers through the ELB.
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.

Q39. 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?

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

Q40. 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
2. Enable route propagation to the Virtual Private Gateway (VGW)
3. Enable route propagation to the customer gateway (CGW)
4. Modify the route table of all Instances using the ‘route’ command.
5. Modify the Instances VPC subnet route table by adding a route back to the customer’s on-premises environment.

Q41. 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.

Q41. 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.
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.
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.
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.
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.

Q42. 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

Q43. 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.
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.
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.
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.

Q44. 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

Q45. 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 (raffle 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.

Q46. Your company produces customer commissioned one-of-a-kind skiing helmets combining nigh fashion with custom technical enhancements. Customers can show off 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?

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.
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.
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).
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).

Q47. 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.
2. Configure your Web servers with EIPs. Place the Web servers in a Route53 Record Set and configure health checks against all Web servers.
3. Configure ELB with HTTPS listeners, and place the Web servers behind it.
4. Configure your web servers as the origins for a CloudFront distribution. Use custom SSL certificates on your CloudFront distribution

Q48. 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.
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.

Q49. 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.
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.
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.
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

Q50. 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

Q51. 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

Q52. 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.

Q53. Which is a valid Amazon Resource name (ARN) for IAM?

A. aws:iam::123456789012:instance-profile/Webserver

B. arn:aws:iam::123456789012:instance-profile/Webserver

C. 123456789012:aws:iam::instance-profile/Webserver

D. arn:aws:iam::123456789012::instance-profile/Webserver

Q54. Dave is the main administrator in Example Corp., and he decides to use paths to help delineate the users in the company and set up a separate administrator group for each path-based division. Following is a

subset of the full list of paths he plans to use:

• /marketing

• /sales

• /legal

Dave creates an administrator group for the marketing part of the company and calls it

Marketing\_Admin.

He assigns it the /marketing path. The group's ARN is

arn:aws:iam::123456789012:group/marketing/Marketing\_Admin.

Dave assigns the following policy to the Marketing\_Admin group that gives the group permission to use

all IAM actions with all groups and users in the /marketing path. The policy also gives the

Marketing\_Admin group permission to perform any AWS S3 actions on the objects in the portion of the

corporate bucket.

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Deny",

"Action": "iam:\*",

"Resource": [

"arn:aws:iam::123456789012:group/marketing/\*",

"arn:aws:iam::123456789012:user/marketing/\*"

]

},

{

"Effect": "Allow",

"Action": "s3:\*",

"Resource": "arn:aws:s3:::example\_bucket/marketing/\*"

},

{

"Effect": "Allow",

"Action": "s3:ListBucket\*",

"Resource": "arn:aws:s3:::example\_bucket",

"Condition":{"StringLike":{"s3:prefix": "marketing/\*"}}

}

]

}

A. True

B. False

Q55. Your fortune 500 company has under taken a TCO analysis evaluating the use of Amazon S3 versus acquiring more hardware The outcome was that ail 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)

A. Setting up a federation proxy or identity provider

B. Using AWS Security Token Service to generate temporary tokens

C. Tagging each folder in the bucket

D. Configuring IAM role

E. Setting up a matching IAM user for every user in your corporate directory that needs access to a folder in the bucket.

Q56. 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

Q57. 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.

Q58. 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
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.

Q59. 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.
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.

Q60. You have an application running on an EC2 Instance, which will allow users to download files 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?

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.

Q61. 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.
2. Leverage resource based tagging along with an IAM user, which can prevent specific users from terminating production EC2 resources.
3. Leverage EC2 termination protection and multi-factor authentication, which together require users to authenticate before terminating EC2 instances.
4. Create an IAM user and apply an IAM role, which prevents users from terminating production EC2 instances.

Q62. 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
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
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

Q64. 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.

Q66. You need a persistent and durable storage to trace call activity of an IVR (Interactive Voice Response) system. Call duration is mostly in the 2-3 minutes timeframe. Each traced call can be either active or terminated. An external application needs to know each minute the list of currently active calls, which are usually a few calls/second. Put once per month there is a periodic peak up to 1000

calls/second for a few hours The system is open 24/7 and any downtime should be avoided. Historical

data is periodically archived to files. Cost saving is a priority for this project.

What database implementation would better fit this scenario, keeping costs as low as possible?

A. Use RDS Multi-AZ with two tables, one for -Active calls" and one for -Terminated calls". In this way the "Active calls\_ table is always small and effective to access.

B. Use DynamoDB with a "Calls" table and a Global Secondary Index on a "IsActive'" attribute that is present for active calls only In this way the Global Secondary index is sparse and more effective.

C. Use DynamoDB with a 'Calls" table and a Global secondary index on a 'State" attribute that can equal to "active" or "terminated" in this way the Global Secondary index can be used for all Items in

the table.

D. Use RDS Multi-AZ with a "CALLS" table and an Indexed "STATE\* field that can be equal to 'ACTIVE" or -TERMINATED" In this way the SOL query Is optimized by the use of the Index.

Q67. Your company hosts a social media site supporting users in multiple countries. You have been asked to provide a highly available design tor the application that leverages multiple regions tor the most recently accessed content and latency sensitive portions of the wet) site The most latency sensitive component of the application involves reading user preferences to support web site personalization and ad selection.

In addition to running your application in multiple regions, which option will support this application’s requirements?

A. Serve user content from S3. CloudFront and use Route53 latency-based routing between ELBs in each region Retrieve user preferences from a local DynamoDB table in each region and leverage SQS to capture changes to user preferences with SOS workers for propagating updates to each table.

B. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3. CloudFront with dynamic content and an ELB in each region Retrieve user preferences from an ElasticCache cluster in each region and leverage SNS notifications to propagate user preference changes to a worker node in each region.

user content from S3 CloudFront and Route53 latency-based routing Between ELBs In

each region Retrieve user preferences from a DynamoDB table and leverage SQS to capture changes to user preferences with SOS workers for propagating DynamoDB updates.

D. Serve user content from S3. CloudFront with dynamic content, and an ELB in each region Retrieve user preferences from an ElastiCache cluster in each region and leverage Simple Workflow (SWF) to manage the propagation of user preferences from a centralized OB to each ElastiCache cluster.

Q68. 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.
2. Add a route from rtb-238bc44b to igw-2d8bc445 and add a bastion and NAT instance within Subnet-248DC44c.
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.
4. Create a Bastion and NAT instance in subnet-258bc44d and add a route from rtb-238bc44b to the NAT instance.

Q69. 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.

Q70. 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.

Q71. 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

Q72. You have an application running on an EC2 Instance, which will allow users to download files 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?

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.

Q73. 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

Q74. 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.

Q75. 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.

Q76. 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
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

Q77. Select the correct set of options. These are the initial settings for the default security group:

A. Allow no inbound traffic, Allow all outbound traffic and Allow instances associated with this security group to talk to each other

B. Allow all inbound traffic, Allow no outbound traffic and Allow instances associated with this security

group to talk to each other

C. Allow no inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this

security group to talk to each other

D. Allow all inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other

Q78. How can an EBS volume that is currently attached to an EC2 instance be migrated from one Availability Zone to another?

1. Detach the volume and attach it to another EC2 instance in the other AZ.
2. Simply create a new volume in the other AZ and specify the original volume as the source.
3. Create a snapshot of the volume, and create a new volume from the snapshot in the other AZ
4. Detach the volume, then use the ec2-migrate-volume command to move it to another AZ.

Q79. 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

Q80. 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.

Q81. Which of the following are characteristics of Amazon VPC subnets? Choose 2 answers

A. Each subnet spans at least 2 Availability Zones to provide a high-availability environment.

B. Each subnet maps to a single Availability Zone.

C. CIDR block mask of /25 is the smallest range supported.  
D. By default, all subnets can route between each other, whether they are private or public.

E. Instances in a private subnet can communicate with the Internet only if they have an Elastic IP.

Q82. In AWS, which security aspects are the customer’s responsibility? Choose 4 answers

1. Controlling physical access to compute resources
2. Patch management on the EC2 instances operating system
3. Encryption of EBS (Elastic Block Storage) volumes
4. Life-cycle management of IAM credentials
5. Decommissioning storage devices
6. Security Group and ACL (Access Control List) settings

Q83. When you put objects in Amazon S3, what is the indication that an object was successfully stored?

1. Each S3 account has a special bucket named\_s3\_logs. Success codes are written to this bucket with a timestamp and checksum.
2. A success code is inserted into the S3 object metadata.
3. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful.
4. Amazon S3 is engineered for 99.999999999% durability. Therefore there is no need to confirm that data was inserted.

Q84. 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

Q85. A customer is deploying an SSL enabled web application to AWS and would like to implement a

separation of roles between the EC2 service administrators that are entitled to login to instances as well

as making API calls and the security officers who will maintain and have exclusive access to the

application’s X.509 certificate that contains the private key.

1. Upload the certificate on an S3 bucket owned by the security officers and accessible only by EC2 Role of the web servers.
2. Configure the web servers to retrieve the certificate upon boot from an CloudHSM is managed by the security officers.
3. Configure system permissions on the web servers to restrict access to the certificate only to the authority security officers
4. Configure IAM policies authorizing access to the certificate store only to the security officers and terminate SSL on an ELB.

Q86. 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
2. Ingest data into a DynamoDB table and move old data to a Redshift cluster
3. Replace the RDS instance with a 6 node Redshift cluster with 96TB of storage
4. Keep the current architecture but upgrade RDS storage to 3TB and 10K provisioned IOPS

Q87. 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.
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
4. Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.

Q88. 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

Q89. 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.

Q90. 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?

A. 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.

B. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in

SOS Once data is processed,

C. Change the storage class of the S3 objects to Reduced Redundancy Storage. 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.

D. 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.

Q91. 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 mat they lease space at a DirectConnect partner location and establish a 1G DirectConnect connection to tneirvPC 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.
2. Add previously identified hostile source IPs as an explicit INBOUND DENY NACL to the web tier subnet.
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 then pass the traffic to the current web tier. 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.

Q92. 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.
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.

Q93. 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
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.

Q94. 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.
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.
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.
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.

Q95. 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.

Q96. 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.

Q97. 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.
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.
4. No if the cache node fails you can always get the same data from the DB without having any availability impact.

Q98. 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.
3. Take hourly DB backups to EC2 Instance store volumes with transaction logs stored In S3 every 5 minutes.
4. Take 15 minute DB backups stored in Glacier with transaction logs stored in S3 every 5 minutes.

Q99. 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
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.
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.

Q100. You control access to S3 buckets and objects with:

A. Identity and Access Management (IAM) Policies.

B. Access Control Lists (ACLs).

C. Bucket Policies.

D. All of the above

Q101. The AWS IT infrastructure that AWS provides, complies with the following IT security standards,  
including:

A. SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), SOC 2 and SOC 3

B. FISMA, DIACAP, and FedRAMP

C. PCI DSS Level 1, ISO 27001, ITAR and FIPS 140-2

D. HIPAA, Cloud Security Alliance (CSA) and Motion Picture Association of America (MPAA)

E. All of the above

Q102. Auto Scaling requests are signed with a \_\_\_\_\_\_\_\_\_ signature calculated from the request and the user’s

private key.

A. SSL

B. AES-256

C. HMAC-SHA1

D. X.509

The following policy can be attached to an IAM group. It lets an IAM user in that group access a "home

directory" in AWS S3 that matches their user name using the console.

{

"Version": "2012-10-17",

"Statement": [

{

"Action": ["s3:\*"],

"Effect": "Allow",

"Resource": ["arn:aws:s3:::bucket-name"],

"Condition":{"StringLike":{"s3:prefix":["home/${aws:username}/\*"]}}

},

{

"Action":["s3:\*"],

"Effect":"Allow",

"Resource": ["arn:aws:s3:::bucket-name/home/${aws:username}/\*"]

}

]

}

A. True

B. False

Q103. What does elasticity mean to AWS?

A. The ability to scale computing resources up easily, with minimal friction and down with latency.

B. The ability to scale computing resources up and down easily, with minimal friction.

C. The ability to provision cloud computing resources in expectation of future demand.

D. The ability to recover from business continuity events with minimal friction.

Q104. The following are AWS Storage services? Choose 2 Answers

A. AWS Relational Database Service (AWS RDS)

B. AWS ElastiCache

C. AWS Glacier

D. AWS Import/Export

Q105. How is AWS readily distinguished from other vendors in the traditional IT computing landscape?

A. Experienced. Scalable and elastic. Secure. Cost-effective. Reliable

B. Secure. Flexible. Cost-effective. Scalable and elastic. Global

C. Secure. Flexible. Cost-effective. Scalable and elastic. Experienced

D. Flexible. Cost-effective. Dynamic. Secure. Experienced

Q106. 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.
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

Q107. Your company is storing millions of sensitive transactions across thousands of 100-GB files that must be

encrypted in transit and at rest. Analysts concurrently depend on subsets of files, which can consume up

to 5 TB of space, to generate simulations that can be used to steer business decisions. You are required

to design an AWS solution that can cost effectively accommodate the long-term storage and in-flight

subsets of data.

A. Use Amazon Simple Storage Service (S3) with server-side encryption, and run simulations on subsets

in ephemeral drives on Amazon EC2.

B. Use Amazon S3 with server-side encryption, and run simulations on subsets in-memory on Amazon

EC2.

C. Use HDFS on Amazon EMR, and run simulations on subsets in ephemeral drives on Amazon EC2.

D. Use HDFS on Amazon Elastic MapReduce (EMR), and run simulations on subsets in-memory on

Amazon Elastic Compute Cloud (EC2).

E. Store the full data set in encrypted Amazon Elastic Block Store (EBS) volumes, and regularly capture

snapshots that can be cloned to EC2 workstations.

Q108. 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
3. Configure Amazon CloudTrail to receive custom logs, use EMR to apply heuristics the logs
4. Setup an Auto Scaling group of EC2 syslogd servers, store the logs on S3 use EMR to apply heuristics on the logs

Q109. 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?

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.
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.
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.
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.
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.