<https://www.examdiscuss.com/Amazon/exam/AWS-Solutions-Associate/premium/>

Q  68/218 **Your security team requires each Amazon ECS task to have an IAM policy that limits the task's privileges to only those required for its use of AWS services. How can you achieve this?**

**A.** Use IAM roles for Amazon ECS tasks to associate a specific IAM role with each ECS task definition

**B.** Connect to each running Amazon ECS container instance and add discrete credentials

**C.** Use IAM roles on the Amazon ECS container instances to associate IAM roles with each ECS task on that instance

**D.** Reboot each Amazon ECS task programmatically to generate new instance metadata for each task

**Correct Answer: A**

Q  69/218 **A company is developing a new online gaming application The application will run on Amazon EC2 instances in multiple AWS Regions and will have a high number of globally distributed users A solutions architect must design the application to optimize network latency for the users.  
Which actions should the solutions architect take to meet these requirements? (Select TWO )**

**A.** Create an Amazon Route 53 weighted routing policy Configure the routing policy to give the highest weight to the EC2 instances in the Region that has the largest number of users.

**B.** Integrate AWS Client VPN into the application Instruct users to select which Region is closest to them after they launch the application Establish a VPN connection to that Region

**C.** Configure AWS Global Accelerator Create Regional endpoint groups in each Region where an EC2 fleet is hosted

**D.** Configure an Amazon API Gateway endpoint in each Region where an EC2 fleet is hosted Instruct users to select which Region is closest to them after they launch the application Use the API Gateway endpoint that is closest to them

**E.** Create a content delivery network (CDN) by using Amazon CloudFront Enable caching for static and dynamic content, and specify a high expiration period

**Correct Answer: C,E**

**Q** 70/218

**A company is processing data on a daily basis. The results of the operations are stored in an Amazon S3 bucket, analyzed daily for one week, and then must remain immediately accessible for occasional analysis.  
What is the MOST cost-effective storage solution alternative to the current configuration?**

A. Configure a lifecycle policy to delete the objects after 30 days.

B. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

C. Configure a lifecycle policy to transition the objects to Amazon S3 Glacier after 30 days.

D. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

**Correct Answer: D**

**Q**71/218

**What is the charge for the data transfer incurred in replicating data between your primary and standby?**

A. Half of the standard data transfer charge

B. Same as the standard data transfer charge

C. No charge. It is free

D. Double the standard data transfer charge

**Correct Answer: C**

**Q 72/218**

**What is the maximum number of data points for an HTTP data request that a user can include in PutMetricRequest in the CloudWatch?**

A. 30

B. 50

C. 10

D. 20

**Correct Answer: D**

**The size of a PutMetricData request of CloudWatch is limited to 8KB for the HTTP GET requests and 40KB for the HTTP POST requests. The user can include a maximum of 20 data points in one PutMetricData request.  
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch\_concepts.html**

Q 73/218 **You try to connect via SSH to a newly created Amazon EC2 instance and get one of the error messages:  
"Network error: Connection timed out" or "Error connecting to [instance], reason: -> Connection timed out connect," You have confirmed that the network and security group rules are configured correctly and the instance is passing status checks. What steps should you take to identify the source of the behavior? Choose 2 answers**

**A.** Verify that the Amazon EC2 instance was launched with the proper IAM role

**B.** Verify that your IAM user policy has permission to launch Amazon EC2 instances

**C.** Verify that the private key file corresponds to the Amazon EC2 key pair assigned at launch

**D.** Verify that you are connecting with the appropriate user name for your AMI

**E.** Verify that your federation trust to AWS has been established

**Correct Answer: A,C**

Q 74/218 **WilI I be charged if the DB instance is idle?**

**A.** No

**B.** Yes

**C.** Only is running in GovCloud

**D.** Only if running in VPC

**Correct Answer: B**

Q  75/218 **A company has an AWS account that contains three VPCs (Dev, Test, and Prod) in the same region. Test is peered to both prod and Dev. All VPCs have non-overlapping CIDR blocks. The company wants to push minor code releases from Dev to Prod to speed up time to market. Which of the following options helps the company accomplish this?**

**A.** Attach a security gateway to Dev. Add a new entry in the Prod route table identifying the gateway as the target

**B.** Create a new entry to Prod in the Dev route table using the peering connection as the target

**C.** The VPCs have non-overlapping CIDR blocks in the same account. The route tables contain local routes for all VPCs

**D.** Create a new peering connection between Prod and Dev along with appropriate routes

**Correct Answer: D**

Q 76/218

**A Solutions Architect is designing a system that will store Personally Identifiable Information (PII) in an Amazon S3 bucket. Due to compliance and regulatory requirements, both the master keys and unencrypted data should never be sent to AWS.  
What Amazon S3 encryption technique should the Architect choose?**

**A.** Amazon S3 server-side encryption with a customer-provided key

**B.** Amazon S3 client-side encryption with an AWS KMS-managed customer master key (CMK)

**C.** Amazon S3 client-side encryption with a client-side master key

**D.** Amazon S3 server-side encryption with an AWS KMS-managed key

**Correct Answer: C**

Q 77/218 **One of your AWS Data Pipeline activities has failed consequently and has entered a hard failure state after retrying thrice.  
You want to try it again. Is it possible to increase the number of automatic retries to more than thrice?**

**A.** Yes, you can increase the number of automatic retries to 6.

**B.** Yes, you can increase the number of automatic retries to indefinite number.

**C.** No, you cannot increase the number of automatic retries.

**D.** Yes, you can increase the number of automatic retries to 10.

**Correct Answer: D**

Explanation/Reference:  
Explanation:  
In AWS Data Pipeline, an activity fails if all of its activity attempts return with a failed state. By default, an activity retries three times before entering a hard failure state. You can increase the number of automatic retries to 10. However, the system does not allow indefinite retries.  
https://aws.amazon.com/datapipeline/faqs/

Q 78/218 **You have a video transcoding application running on Amazon EC2. Each instance polls a queue to find out which video should be transcoded, and then runs a transcoding process. If this process is interrupted, the video will be transcoded by another instance based on the queuing system. You have a large backlog of videos which need to be transcoded and would like to reduce this backlog by adding more instances. You will need these instances only until the backlog is reduced. Which type of Amazon EC2 instances should you use to reduce the backlog in the most cost efficient way?**

**A.** Reserved instances

**B.** Spot instances

**C.** Dedicated instances

**D.** On-demand instances

**Correct Answer: B** Reference: http://aws.amazon.com/ec2/purchasing-options/spot-instances/

Q  79/218 **A Solutions Architect is building a multi-tier website. The web servers will be in a public subnet, and the database servers will be in a private subnet. Only the web servers can be accessed from the internet.  
The database servers must have Internet access for software updates. Which solution meets these requirements?**

**A.** Allow Internet traffic on the private subnet through the network ACL

**B.** Use an egress-only internet Gateway

**C.** Use a NAT Gateway.

**D.** Assign Elastic IP addresses to the database instances

Q 79/218 **A Solutions Architect is building a multi-tier website. The web servers will be in a public subnet, and the database servers will be in a private subnet. Only the web servers can be accessed from the internet.  
The database servers must have Internet access for software updates. Which solution meets these requirements?**

**A.** Allow Internet traffic on the private subnet through the network ACL

**B.** Use an egress-only internet Gateway

**C.** Use a NAT Gateway.

**D.** Assign Elastic IP addresses to the database instances

**Correct Answer: C**

Q  80/218 **A Solutions Architect needs to deploy an HTTP/HTTPS service on Amazon EC2 instances with support for WebSockets using load balancers.  
How can the Architect meet these requirements?**

**A.** Configure an Application Load Balancer.

**B.** Configure a Network Load Balancer.

**C.** Configure a Classic Load Balancer.

**D.** Configure a Layer-4 Load Balancer.

**Correct Answer: A**

Q  81/218 **A company is storing application data in Amazon S3 bucket across multiple AWS Regions. Company policy requires that encryption keys be generated at the company headquarters, but the encryption keys may be stored in AWS after generation. The Solutions Architect plans to configure cross-region replication.  
Which solution will encrypt the data while requiring the LEAST amount of operational overhead?**

**A.** Configure S3 object encryption **using** AWS CLI **with** Server\_Side Encryption **with** AWS **KMS\_managed** keys (SSE-KMS)

**B.** Configure the application to write to an S3 bucket using client-side encryption.

**C.** Configure S3 buckets to encrypt using AES-256.

**D.** Configure S3 bucket to use Server-Side encryption with AWS KMS-Management Keys (SSE-KMS) with imported key met--- in both region.

**Correct Answer: ~~A~~**

**The key requirements are:**

**Encryption keys generated at company headquarters.** This points towards **using** Customer-Managed Keys (CMKs) **in** AWS KMS, **specifically** those with imported key material, or possibly a custom key store like **AWS CloudHSM** or an **external key store**, **if** the generation process **is outside** KMS entirely.

**Encryption keys may be stored in AWS after generation.** This is perfectly handled by KMS, especially with imported key material.

**Cross-region replication.** This means S3's Replication (**CRR**) feature will be used.

**Encrypt data.**

1. **LEAST amount of operational overhead.** This is critical for the solution choice**.**

**Let's analyze the options:**

* **A. Configure S3 object encryption using AWS CLI with Server-Side Encryption with AWS KMS-managed keys (SSE-KMS)**
  + This specifies using SSE-KMS, which is good for meeting the encryption and storing keys in AWS requirements.
  + Using AWS CLI for configuration is a common way to set this up.
  + However, "AWS KMS-managed keys" often refers to AWS-managed CMKs (aws/s3) or customer-managed CMKs (CMKs where AWS generates the key material). The problem states keys are generated at headquarters. This option doesn't explicitly mention importing key material. Also, relying solely on aws/s3 keys for cross-region replication with a custom key generation policy might be complex to manage for cross-region replication if the source and destination keys are different and custom policies are needed.
* **B. Configure the application to write to an S3 bucket using client-side encryption.**
  + Client-side encryption (CSE) means the application encrypts the data *before* sending it to S3. This directly supports the "keys generated at headquarters" policy, as the application would use those keys.
  + However, CSE significantly increases operational overhead for the application development team. They have to manage the encryption/decryption logic, key rotation, key storage, and ensure secure handling of keys within the application. For cross-region replication, the replicas would also be encrypted with the same client-side key, meaning you'd need the key in the destination region for decryption, adding to the application's complexity in the disaster recovery region. This is explicitly *not* the least operational overhead.
* **C. Configure S3 buckets to encrypt using AES-256.**
  + This refers to SSE-S3 (Server-Side Encryption with S3-managed keys). While it uses AES-256 encryption, the keys are entirely managed by AWS, and the company has no control over their generation or direct management, violating the "keys generated at company headquarters" policy. Also, for cross-region replication of SSE-S3 objects, they remain SSE-S3 unless explicitly configured otherwise for the destination, but the key control requirement is not met.
* **D. Configure S3 bucket to use Server-Side encryption with AWS KMS-Management Keys (SSE-KMS) with imported key material in both regions.**
  + This option directly addresses all requirements while aiming for least operational overhead.
  + SSE-KMS: Provides server-side encryption, handled by S3.
  + Imported Key Material: Directly satisfies the requirement that "encryption keys be generated at the company headquarters, but the encryption keys may be stored in AWS after generation." You generate the key material on-premises and then securely import it into AWS KMS.
  + "in both regions": For cross-region replication with SSE-KMS, it's generally recommended to use separate KMS keys in the source and destination regions. AWS KMS supports Multi-Region Keys, which allows you to have the same key material (imported from HQ) in KMS keys across multiple regions, enabling encryption in one region and decryption in another using the "same" logical key. This significantly reduces operational overhead for replication, as S3 can automatically re-encrypt objects with the destination region's KMS key (which shares the same imported key material) during replication. This is the most efficient and low-overhead way to manage keys and replication under these constraints.

**Conclusion:**

Option D is the best solution because it directly meets all stated requirements with the least operational overhead for the application layer. The combination of SSE-KMS with imported key material and the proper configuration across regions (ideally using Multi-Region Keys for simplicity) automates the encryption and replication process effectively while adhering to the company's key generation policy.

**The final answer is D​**

Q 82/218 **A company has a High Performance Computing (HPC) cluster in its on-premises data center, which runs thousands of jobs in parallel for one week every month, processing petabytes of images. The images are stored on a network file server, which is replicated to a disaster recovery site. The on-premises data center has reached capacity and has started to spread the jobs out over the course of the month in order to better utilize the cluster, causing a delay in the job completion.  
The company has asked its Solutions Architect to design a cost-effective solution on AWS to scale beyond the current capacity of 5,000 cores and 10 petabytes of data. The solution must require the least amount of management overhead and maintain the current level of durability.  
Which solution will meet the company's requirements?**

**A.** Submit the list of jobs to be processed to an Amazon SQS to queue the jobs that need to be processed.  
Create a diversified cluster of Amazon EC2 worker instances using Spot Fleet that will automatically scale based on the queue depth. Use Amazon EFS to store all the data sharing it across all instances in the cluster.

**B.** Create an Amazon EMR cluster with a combination of On Demand and Reserved Instance Task Nodes that will use Spark to pull data from Amazon S3. Use Amazon DynamoDB to maintain a list of jobs that need to be processed by the Amazon EMR cluster.

**C.** Create a container in the Amazon Elastic Container Registry with the executable file for the job. Use Amazon ECS with Spot Fleet in Auto Scaling groups. Store the raw data in Amazon EBS SC1 volumes and write the output to Amazon S3.

**D.** Store the raw data in Amazon S3, and use AWS Batch with Managed Compute Environments to create Spot Fleets. Submit jobs to AWS Batch Job Queues to pull down objects from Amazon S3 onto Amazon EBS volumes for temporary storage to be processed, and then write the results back to Amazon S3.

**Correct Answer: B**

Q 83/218 **A Solutions Architect is designing a mobile application that will capture receipt images to track expenses. The Architect wants to store the images on Amazon S3. However, uploading images through the web server will create too much traffic.  
What is the MOST efficient method to store images from a mobile application on Amazon S3?**

**A.** Upload to a second bucket, and have a Lambda event copy the image to the primary bucket.

**B.** Upload to a separate Auto Scaling group of servers behind an ELB Classic Load Balancer, and have them write to the Amazon S3 bucket.

**C.** Expand the web server fleet with Spot Instances to provide the resources to handle the images.

**D.** Upload directly to S3 using a pre-signed URL.

**Correct Answer: D**

Q 84/218 **A company wants to create an application that will transmit protected health information (PHI) to thousands of service consumers in different AWS accounts. The application servers will sit in private VPC subnets. The routing for the application must be fault tolerant.  
What should be done to meet these requirements?**

**A.** Create an internal Application Load Balancer in the service provider VPC and put application servers behind it.

**B.** Create a virtual private gateway connection between each pair of service provider VPCs and service consumer VPCs.

**C.** Create a VPC endpoint service and grant permissions to specific service consumers to create a connection.

**D.** Create a proxy server in the service provider VPC to route requests from service consumers to the application servers.

**Correct Answer: C**

Q  85/218 **A company is hosting multiple websites for several lines of business under its registered parent domain. Users accessing these websites will be routed to appropriate backend Amazon EC2 instances based on the subdomain. The websites host static webpages, images, and server-side scripts like PHP and JavaScript.  
Some of the websites experience peak access during the first two hours of business with constant usage throughout the rest of the day. A solutions architect needs to design a solution that will automatically adjust capacity to these traffic patterns while keeping costs low.  
Which combination of AWS services or features will meet these requirements? (Select TWO.)**

**A.** Application Load Balancer

**B.** Amazon EC2 Auto Scaling

**C.** Amazon S3 website hosting

**D.** Network Load Balancer

**E.** AWS Batch

**Correct Answer: B,C**

Q  86/218 **An organization is setting up a backup and restore system in AWS of their in premise system. The organization needs High Availability(HA) and Disaster Recovery(DR) but is okay to have a longer recovery time to save costs.  
Which of the below mentioned setup options helps achieve the objective of cost saving as well as DR in the most effective way?**

**A.** Setup pre-configured servers and create AMIs. Use EIP and Route 53 to quickly switch over to AWS from in premise.

**B.** Setup the backup data on S3 and transfer data to S3 regularly **using** the storage gateway.

**C.** Setup a small instance with AutoScaling; in case of DR start diverting all the load to AWS from on premise.

**D.** Replicate on premise DB to EC2 at regular intervals and setup a scenario similar to the pilot light.

**Correct Answer: B** AWS has many solutions for Disaster Recovery(DR) and High Availability(HA). When the organization wants to have HA and DR but are okay to have a longer recovery time they should select the option backup and restore with S3. The **data can be sent** to S3 using either **Direct Connect**, **Storage Gateway** or **over the internet.**  
The EC2 instance will pick the data from the S3 bucket when started and setup the environment. This process takes longer but is ***very cost*** effective due to *the low pricing of S3*. In all the other options, the EC2 instance might be running or there will be AMI storage costs. Thus, it will be a costlier option. In this scenario the organization should plan appropriate tools to take a backup, plan the retention policy for data and setup security of the data.  
Reference:  
http://d36cz9buwru1tt.cloudfront.net/AWS\_Disaster\_Recovery.pdf

Q 87/218 **A solutions architect is migrating an existing workload to AWS Fargate. The task can only run in a private subnet within the VPC where there is no direct connectivity from outside the system to the application.  
When the Fargate task is launched, the task fails with the following error:  
CannotPullContainerError: API error (500): Get  
https://111122223333.dkr.ecr.us-east-1.amazonaws.com/v2/: net/http: request cancelled while waiting for connection How should the solutions architect correct this error?**

**A.** Ensure the network mode is set to bridge in the Fargate task definition.

**B.** Ensure the task is set to ENABLED for the auto-assign public IP setting when launching the task.

**C.** Ensure the task is set to DISABLED for the auto-assign public IP setting when launching the task.  
Configure a NAT gateway in the private subnet in the VPC to route requests to the internet.

**D.** Ensure the task is set to DISABLED for the auto-assign public IP setting when launching the task.  
Configure a NAT gateway in the public subnet in the VPC to route requests to the internet.

**Correct Answer: C**

Q  88/218 **A company hosts a popular web application. The web application connects to a database running in a private VPC subnet. The web servers must be accessible only to customers on an SSL connection. The RDS MySQL database server must be accessible only from the web servers.  
How should the Architect design a solution to meet the requirements without impacting running applications?**

**A.** Create a network ACL on the web server's subnet, and allow HTTPS inbound and MySQL outbound.  
Place both database and web servers on the same subnet.

**B.** Open an HTTPS port on the security group for web servers and set the source to 0.0.0.0/0. Open the MySQL port on the database security group and attach it to the MySQL instance. Set the source to Web Server Security Group.

**C.** Open the MySQL port on the security group for web servers and set the source to 0.0.0.0/0. Open the HTTPS port on the database security group and attach it to the MySQL instance. Set the source to Web Server Security Group

**D.** Create a network ACL on the web server's subnet, and allow HTTPS inbound, and specify the source as  
0.0.0.0/0. Create a network ACL on a database subnet, allow MySQL port inbound for web servers, and deny all outbound traffic.

**Correct Answer: B**

Q  89/218 **A company needs to share an Amazon S3 bucket with an external vendor. The bucket owner must be able to access all objects.  
Which action should be taken to share the S3 bucket?**

**A.** Update the bucket to enable cross-origin resource sharing (CPORS)

**B.** Create a bucket policy to require users to grant bucket-owner-full when uploading objects

**C.** Update the bucket to be a Requester Pays bucket

**D.** Create an IAM policy to require users to grant bucket-owner-full control when uploading objects.

**Correct Answer: A**

Q 90/218 **A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office to Amazon S3 Glacier The solution must avoid saturating the branch office's low-bandwidth internet connection What is the MOST cost-effective solution1?**

**A.** Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier

**B.** Mount the network-attached file system to Amazon S3 and copy the files directly. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier

**C.** Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination Create a bucket policy to enforce a VPC endpoint

**D.** Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly Create a bucket policy to enforce a VPC endpoint

**Correct Answer: A**

Q 91/218 **What is the minimum time Interval for the data that Amazon CloudWatch receives and aggregates?**

**A.** One second

**B.** Five seconds

**C.** One minute

**D.** Three minutes

**E.** Five minutes

**Correct Answer: C**

Many metrics are received and aggregated at 1-minute intervals. Some are at 3-minute or 5-minute intervals.

Q  90/218 **A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office to Amazon S3 Glacier The solution must avoid saturating the branch office's low-bandwidth internet connection What is the MOST cost-effective solution1?**

**A.** Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier

**B.** Mount the network-attached file system to Amazon S3 and copy the files directly. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier

**C.** Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination Create a bucket policy to enforce a VPC endpoint

**D.** Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly Create a bucket policy to enforce a VPC endpoint

**Correct Answer: A**

Q  91/218 **What is the minimum time Interval for the data that Amazon CloudWatch receives and aggregates?**

**A.** One second

**B.** Five seconds

**C.** One minute

**D.** Three minutes

**E.** Five minutes

**Correct Answer: C**

Many metrics are received and aggregated at 1-minute intervals. Some are at 3-minute or 5-minute intervals.

Q 92/218 **A company wants to build an immutable infrastructure for its software applications The company wants to test the software applications before sending traffic to them The company seeks an efficient solution that limits the effects of application bugs Which combination of steps should a solutions architect recommend? {Select TWO)**

**A.** Use AWS Cloud Formation with a parameter set to the staging value in a separate environment other than the production environment

**B.** Apply Amazon Route 53 weighted routing to test the staging environment and gradually increase the traffic as the tests pass

**C.** Use AWS Cloud Formation to update the production infrastructure and roll back the stack if the update fails

**D.** Use AWS Cloud Formation to deploy the staging environment with a snapshot deletion policy and reuse the resources in the production environment if the tests pass

**E.** Apply Amazon Route 53 failover routing to test the staging environment and fail over to the production environment if the tests pass

**Correct Answer: C,D**

Q  93/218 **A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.**

**A screenshot of a computer program

AI-generated content may be incorrect.  
A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?**

**A.** Deleting Amazon EC2 instances

**B.** Deleting IAM users

**C.** Deleting directories

**D.** Deleting logs from Amazon CloudWatch Logs

**Correct Answer: A**

Q 94/218 **Which requirements must be met in order for a Solutions Architect to specify that an Amazon EC2 instance should stop rather than terminate when its Spot Instance is interrupted? (Choose two.)**

**A.** The Spot Instance request type must be persistent.

**B.** The root volume must be an instance store volume.

**C.** The launch configuration is changed.

**D.** The Spot Instance request type must be one-time.

**E.** The root volume must be an Amazon EBS volume.

**Correct Answer: A,E**

Q  95/218 **In AWS IAM, which of the following predefined policy condition keys checks how long ago (in seconds) the MFA-validated security credentials making the request were issued using multi- factor authentication (MFA)?**

**A.** aws:MultiFactorAuthAge

**B.** aws:MultiFactorAuthLast

**C.** aws:MFAAge

**D.** aws:MultiFactorAuthPrevious

**Correct Answer: A** aws:MultiFactorAuthAge is one of the predefined keys provided by AWS that can be included within a Condition element of an IAM policy. The key allows to check how long ago (in seconds) the MFA-validated security credentials making the request were issued using Multi-Factor Authentication (MFA).  
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage\_ElementDescriptions.html

Q 96/218 **An application is running on an Amazon EC2 instance in a private subnet. The application needs to read and write data onto Amazon Kinesis Data Streams, and corporate policy requires that this traffic should not go to the internet.  
How can these requirements be met?**

**A.** Configure a NAT gateway in a public subnet and route all traffic to Amazon Kinesis through the NAT gateway.

**B.** Configure an interface VPC endpoint for Kinesis and route all traffic to Kinesis through the gateway VPC endpoint.

**C.** Configure an AWS Direct Connect private virtual interface for Kinesis and route all traffic to Kinesis through the virtual interface.

**D.** Configure a gateway VPC endpoint for Kinesis and route all traffic to Kinesis through the gateway VPCendpoint.

Q 97/218 **A company is developing several critical long-running applications hosted on Docker.  
How should a Solutions Architect design a solution to meet the scalability and orchestration requirements on AWS?**

**A.** Use Amazon ECS and Service Auto Scaling.

**B.** Use Spot Instances for orchestration and for scaling containers on existing Amazon EC2 instances.

**C.** Use AWS OpsWorks to launch containers in new Amazon EC2 instances.

**D.** Use Auto Scaling groups to launch containers on existing Amazon EC2 instances.

**Correct Answer: A** Explanation https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html

Q 97/218 **A company is developing several critical long-running applications hosted on Docker.  
How should a Solutions Architect design a solution to meet the scalability and orchestration requirements on AWS?**

**A.** Use Amazon ECS and Service Auto Scaling.

**B.** Use Spot Instances for orchestration and for scaling containers on existing Amazon EC2 instances.

**C.** Use AWS OpsWorks to launch containers in new Amazon EC2 instances.

**D.** Use Auto Scaling groups to launch containers on existing Amazon EC2 instances.

**Correct Answer: A E**xplanation https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html

Q 98/218 **A Solutions Architect is developing software on AWS that requires access to multiple AWS services, including an Amazon EC2 instance. This is a security sensitive application, and AWS credentials such as Access Key ID and Secret Access Key need to be protected and cannot be exposed anywhere in the system.  
What security measure would satisfy these requirements?**

**A.** Enable multi-factor authentication for the AWS root account

**B.** Assign an IAM role to the Amazon EC2 instance.

**C.** Store the AWS Access Key ID/Secret Access Key combination in software comments.

**D.** Assign an IAM user to the Amazon EC2 instance.

**Correct Answer: B**

Q 99/218 **A company needs to retain application log files for a critical application for 10 years. The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed. Theapplication generates more than 10 TB of logs per month. Which storage option meets these requirements MOST cost-effectively?**

**A.** Store the logs in Amazon S3. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive

**B.** Store the logs in Amazon CloudWatch Logs. Use Amazon S3 Lifecycle policies to move logs more than  
1 month old to S3 Glacier Deep Archive.

**C.** Store the logs in Amazon S3. Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.

**D.** Store the logs in Amazon CloudWatch Logs. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.

**Correct Answer: C**

Q 100/218 **A company needs to use AWS resources to expand capacity for a website hosted in an on- premises data center. The AWS resources will include load balancers, Auto Scaling, and Amazon EC2 instances that will access an on-premises database. Network connectivity has been established, but no traffic is going to the AWS environment.  
How should Amazon Route 53 be configured to distribute load to the AWS environment? (Select TWO.)**

**A.** Set up a routing policy for failover using the on-premises environment as primary and the load balancer as secondary.

**B.** Create multiple A records for the EC2 instances.

**C.** Set up an A record to point the DNS name to the IP address of the load balancer.

**D.** Set up a weighted routing policy, distributing the workload between the load balancer and the on- premises environment.

**E.** Set up a geolocation routing policy to distribute the workload between the load balancer and the on- premises environment.

**Correct Answer: C,D**

Q 101/218 **An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size. The application owner will make the log file available to the vendor for a limited time.  
What is the MOST secure way to do this?**

**A.** Enable public read on the S3 object and provide the link to the vendor.

**B.** Upload the file to Amazon WorkDocs and share the public link with the vendor.

**C.** Generate a presigned URL and have the vendor download the log file before it expires.

**D.** Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi- factor authentication.

**Correct Answer: C** Share an object with others  
All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a presigned URL, using their own security credentials, to grant time-limited permission to download the objects.  
When you create a presigned URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method (GET to download the object) and expiration date and time. The presigned URLs are valid only for the specified duration.  
Anyone who receives the presigned URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a presigned URL.  
Reference: https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html

Q 102/218 **Your company has an 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?**

**A.** 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.

**B.** 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.

**C.** 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.

**D.** 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.

**Correct Answer: C**

Q 103/218 **You manually launch a NAT AMI in a public subnet. The network is properly configured. Security groups and network access control lists are property configured. Instances in a private subnet can access the NAT. The NAT can access the Internet. However, private instances cannot access the Internet. What additional step is required to allow access from the private instances?**

**A.** Disable Source/Destination Check on the NAT instance.

**B.** Enable Source/Destination Check on the private Instances.

**C.** Disable Source/Destination Check on the private instances.

**D.** Enable Source/Destination Check on the NAT instance.

**Correct Answer: C**

Q 104/218 **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 DynamoOB 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?**

**A.** Add a WAF tier by creating a new ELB and an AutoScalmg 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 thier pass the traffic to the current web tier The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group

**B.** Add previously identified hostile source IPs as an explicit INBOUND DENY NACL to the web tier subnet.

**C.** 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.

**D.** 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.

**Correct Answer: A**

Q 105/218 **An AWS Lambda function requires access to an Amazon RDS for SQL Server instance. It is against company policy to store passwords in Lambda functions.  
How can a Solution Architect enable the Lambda function to retrieve the database password without violating company policy?**

**A.** Store a one-way hash of the password in the Lambda function

**B.** Have the Lambda function use the AWS Systems Manager Parameter Store

**C.** Add an IAM policy for IAM database access to the Lambda execution role

**D.** Connect to the Amazon RDS for SQL Server instance by using a role assigned to the Lambda function

**Correct Answer: A**

Q 106/218 **Which of the following approaches provides the lowest cost for Amazon Elastic Block Store snapshots while giving you the ability to fully restore data?**

**A.** Maintain a single snapshot the latest snapshot is both Incremental and complete.

**B.** Maintain a volume snapshot; subsequent snapshots will overwrite one another

**C.** Maintain two snapshots: the original snapshot and the latest incremental snapshot.

**D.** Maintain the most current snapshot, archive the original and incremental to Amazon Glacier.

**Correct Answer: C**

Q 107/218 **A company is preparing to give AWS Management Console access to developers.  
Company policy mandates identity federation and role based access control. Roles are currently assigned using groups in the corporate Active Directory. What combination of the following will give developers access to the AWS console? Choose 2 answers**

**A.** AWS identity and Access Management roles

**B.** AWS identity and Access Management groups

**C.** AWS identity and Access Management users

**D.** AWS Directory Service AD connector

**E.** AWS Directory Service Simple AD

**Correct Answer: A,D**

Q 108/218 **A weather forecasting company needs to process hundreds of gigabytes of data with sub-mill (second latency.  
The company has a high performance computing (HPC) environment in its data center and wants to expand its forecasting capabilities A solutions architect must identify a highly available cloud storage solution that can handle large amounts of sustained throughput Files that are stored in the solution should be accessible to thousands of compute instances that will simultaneously access and process the entire dataset What should the solutions architect do to meet these requirements?**

**A.** Use Amazon FSx for Lustre scratch file systems.

**B.** Use Amazon Elastic File System (Amazon EFS) with Bursting Throughput mode

**C.** Use Amazon FSx for Lustre persistent file systems

**D.** Use Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode

**Correct Answer: C**

Q 109/218 **An Elastic IP address (EIP) is a static IP address designed for dynamic cloud computing. With an EIP, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. Your EIP is associated with your AWS account, not a particular EC2 instance, and it remains associated with your account until you choose to explicitly release it. By default how many EIPs is each AWS account limited to on a per region basis?**

**A.** 1

**B.** 5

**C.** Unlimited

**D.** 10

**Correct Answer: B** By default, all AWS accounts are limited to 5 Elastic IP addresses per region for each AWS account, because public (IPv4) Internet addresses are a scarce public resource. AWS strongly encourages you to use an EIP primarily for load balancing use cases, and use DNS hostnames for all other inter-node communication.  
If you feel your architecture warrants additional EIPs, you would need to complete the Amazon EC2  
Elastic IP Address Request Form and give reasons as to your need for additional addresses.  
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html#using-instance-ad dressing-limit

Q 110/218 **You have been asked to design a fault-tolerant and scalable web application across three availability zones. The presentation logic will reside on web servers behind an ELB classic load balancer, and the application logic will reside on a set of app servers behind a second load balancer. How should you use auto scaling groups?**

**A.** Deploy one auto scaling group that includes al the web and app servers across all availability zones

**B.** Deploy two Auto Scaling groups: one for the web servers in all Availability zones and one for the app servers in all Availability zones

**C.** Deploy six auto scaling groups: a web server group in each Availability zone and an app server group in each availability zone

**D.** Deploy three auto scaling groups: one for each Availability zone that includes both web and app servers

**Correct Answer: D**

Q 111/218 **True or false: A VPC contains multiple subnets, where each subnet can span multiple Availability Zones.**

**A.** This is true only if requested during the set-up of VPC.

**B.** This is true.

**C.** This is false.

**D.** This is true only for US regions.

**Correct Answer: C**

A VPC can span several Availability Zones. In contrast, a subnet must reside within a single Availability Zone.  
Reference: https://aws.amazon.com/vpc/faqs/

Q 112/218 **A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer. The web server is vulnerable to cross-site scripting (XSS) attacks.  
What should a solutions architect do to remediate the vulnerability?**

**A.** Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.

**B.** Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.

**C.** Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.

**D.** Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard.

**Correct Answer: C**

Working with cross-site scripting match conditions  
Attackers sometimes insert scripts into web requests in an effort to exploit vulnerabilities in web applications.  
You can create one or more cross-site scripting match conditions to identify the parts of web requests, such as the URI or the query string, that you want AWS WAF Classic to inspect for possible malicious scripts. Later in the process, when you create a web ACL, you specify whether to allow or block requests that appear to contain malicious scripts.  
Web Application Firewall  
You can now use AWS WAF to protect your web applications on your Application Load Balancers. AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.  
Reference: https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html  
https://aws.amazon.com/elasticloadbalancing/features/

Q  113/218 **A company copies 200 TB of data from a recent ocean survey onto AWS Snowball Edge Storage Optimized devices The company has a high performance computing (HPC) cluster that is hosted on AWS to look for oil and gas deposits A solutions architect must provide the cluster with consistent sub-millisecond latency and high-throughput access to the data on the Snowball Edge Storage Optimized devices The company is sending the devices back to AWS Which solution will meet these requirements'?**

**A.** Create an Amazon S3 bucket and an Amazon Elastic File System (Amazon EFS) file system Import the data into the S3 bucket Copy the data from the S3 bucket to the EFS file system Access the EFS file system from the HPC cluster instances

**B.** Create an Amazon FSx for Lustre file system Import the data directly into the FSx for Lustre file system Access the FSx for Lustre file system from the HPC cluster instances

**C.** Create an Amazon S3 bucket Import the data into the S3 bucket. Configure an AWS Storage Gateway file gateway to use the S3 bucket Access the file gateway from the HPC cluster instances

**D.** Create an Amazon S3 bucket Import the data into the S3 bucket Configure an Amazon FSx for Lustre file system and integrate it with the S3 bucket Access the FSx for Lustre file system from the HPC cluster instances

**Correct Answer: C**

Q 114/218 **An organization hosts an app on EC2 instances which multiple developers need access to in order to perform updates.  
The organization plans to implement some security best practices related to instance access.  
Which one of the following recommendations will NOT help improve its security in this way?**

**A.** Disable the password based login for all the users. All the users should use their own keys to connect with the instance securely.

**B.** Create an IAM policy allowing only IAM users to connect to the EC2 instances with their own SSH key.

**C.** Create a procedure to revoke the access rights of the individual user when they are not required to connect to EC2 instance anymore for the purpose of application configuration.

**D.** Apply the latest patch of OS and always keep it updated.

**Correct Answer: B** Since AWS is a public cloud any application hosted on EC2 is prone to hacker attacks. It becomes extremely important for a user to setup a proper security mechanism on the EC2 instances. A few of the security measures are listed below:  
\* Always keep the OS updated with the latest patch  
\* Always create separate users with in OS if they need to connect with the EC2 instances, create their keys and disable their password  
\* Create a procedure using which the admin can revoke the access of the user when the business work on the EC2 instance is completed. . Lock down unnecessary ports  
\* Audit any proprietary applications that the user may be running on the EC2 instance. Provide temporary escalated privileges, such as sudo for users who need to perform occasional

Privileged tasks IAM **is useful** when users are required to work with AWS resources and actions, such as launching an instance. **It is not** useful **in this** case because it does not manage who can connect via RDP or SSH with an instance.  
http://aws.amazon.com/articles/1233/

Q 115/218 **How does AWS Data Pipeline execute activities on on-premise resources or AWS resources that you manage?**

**A.** By supplying a Task Runner package that can be installed on your on-premise hosts

**B.** None of these

**C.** By supplying a Task Runner file that the resources can access for execution

**D.** By supplying a Task Runner json script that can be installed on your on-premise hosts

**Correct Answer: A** To enable running activities using on-premise resources, AWS Data Pipeline does the following: It supply a Task Runner package that can be installed on your on-premise hosts. This package continuously polls the AWS Data Pipeline service for work to perform. When it's time to run a particular activity on your on-premise resources, it will issue the appropriate command to the Task Runner.  
https://aws.amazon.com/datapipeline/faqs/

Q 116/218 **You are tasked with setting up a Linux bastion host for access to Amazon EC2 instances running in your VPC. Only clients connecting from the corporate external public IP address 72.34.51.100 should have SSH access to the host. Which option will meet the customer requirement?**

**A.** Security Group Inbound Rule: Protocol - UDP, Port Range - 22, Source 72.34.51.100/32

**B.** Security Group Inbound Rule: Protocol - TCP. Port Range - 22, Source 72.34.51.100/32

**C.** Network ACL Inbound Rule: Protocol - TCP, Port Range-22, Source 72.34.51.100/0

**D.** Network ACL Inbound Rule: Protocol - UDP, Port Range - 22, Source 72.34.51.100/32

**Correct Answer: B**

Q 117/218

**You are playing around with setting up stacks using JSON templates in CloudFormation to try and understand them a little better. You have set up about 5 or 6 but now start to wonder if you are being charged for these stacks.  
What is AWS's billing policy regarding stack resources?**

**A.** You are not charged for the stack resources if they are not taking any traffic.

**B.** You are charged for the stack resources for the time they were operating (but not if you deleted the stack within 30 minutes)

**C.** You are charged for the stack resources for the time they were operating (but not if you deleted the stack within 60 minutes)

**D.** You are charged for the stack resources for the time they were operating (even if you deleted the stack right away)

**Correct Answer: D**

Explanation/Reference:  
Explanation:  
A stack is a collection of AWS resources that you can manage as a single unit. In other words, you can create, update, or delete a collection of resources by creating, updating, or deleting stacks. All the resources in a stack are defined by the stack's AWS CloudFormation template. A stack, for instance, can include all the resources required to run a web application, such as a web server, a database, and networking rules. If you no longer require that web application, you can simply delete the stack, and all of its related resources are deleted. You are charged for the stack resources for the time they were operating (even if you deleted the stack right away).  
<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacks.html>

Q 118/218

**A solutions architect needs to migrate 50 TB of NFS data to Amazon S3. The files are on several NFS file servers on corporate network. These are dense file systems containing tens of millions of small files. The system operators have configured the file interface on an AWS Snowball Edge device and are using a shell script to copy data.  
Developers report that copying the data to the Snowball Edge device is very slow. The solutions architect suspects this may be related to the overhead of encrypting all the small files and transporting them over the network.  
Which changes can be made to speed up the data transfer?**

**A.** Cluster two Snowball Edge devices together to increase the throughput of the devices.

**B.** Connect directly to the USB interface on the Snowball Edge device and copy the files locally.

**C.** Increase the number of parallel copy jobs to increase the throughput of the Snowball Edge device.

**D.** Change the solution to use the S3 Adapter instead of the file interface on the Snowball Edge device.

**Correct Answer: D**

Q 119/218

**In Route 53, what does a Hosted Zone refer to?**

**A.** A hosted zone is a collection of geographical load balancing rules for Route 53.

**B.** A hosted zone is a collection of resource record sets hosted by Route 53.

**C.** A hosted zone is a selection of specific resource record sets hosted by CloudFront for distribution to Route 53.

**D.** A hosted zone is the Edge Location that hosts the Route 53 records for a user.

**Correct Answer: B**

A Hosted Zone refers to a selection of resource record sets hosted by Route 53.  
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/AboutHostedZones.html

Q  120/218

**A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week. What should the company do to guarantee the EC2 capacity?**

**A.** Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

**B.** Purchase Reserved Instances that specify the Region needed.

**C.** Purchase Reserved Instances that specify the Region and three Availability Zones needed.

**D.** Create an On-Demand Capacity Reservation that specifies the Region needed.

**Correct Answer: A**

Q 121/218

**Your supervisor has asked you to build a simple file synchronization service for your department. He doesn't want to spend too much money and he wants to be notified of any changes to files by email. What do you think would be the best Amazon service to use for the email solution?**

**A.** Amazon SES

**B.** Amazon CloudSearch

**C.** Amazon SWF

**D.** Amazon AppStream

**Correct Answer: A**

File change notifications can be sent via email to users following the resource with Amazon Simple Email  
Service (Amazon SES), an easy-to-use, cost-effective email solution.  
Reference: http://media.amazonwebservices.com/architecturecenter/AWS\_ac\_ra\_filesync\_08.pdf

Q 122/218

**A media company asked a Solutions Architect to design a highly available storage solution to serve as a centralized document store for their Amazon EC2 instances. The storage solution needs to be POSIX-compliant, scale dynamically, and be able to serve up to  
100 concurrent EC2 instances.  
Which solution meets these requirements?**

**A.** Create an Amazon S3 bucket and store all of the documents in this bucket.

**B.** Create an Amazon EBS volume and allow multiple users to mount that volume to their EC2 instance(s).

**C.** Use Amazon Glacier to store all of the documents.

**D.** Create an Amazon Elastic File System (Amazon EFS) to store and share the documents.

**Correct Answer: D**

Explanation  
https://docs.aws.amazon.com/efs/latest/ug/creating-using.html  
Creating Resources for Amazon EFS Amazon EFS provides elastic, shared file storage that is POSIX-compliant. The file system you create supports concurrent read and write access from multiple Amazon EC2 instances and is accessible from all of the Availability Zones in the AWS Region where it is created.

Q  123/218

**A company wants to run a hybrid workload for data processing. The data needs to be accessed by on-premises applications for local data processing using an NFS protocol, and must also be accessible from the AWS Cloud for further analytics and batch processing.  
Which solution will meet these requirements?**

**A.** Use an AWS storage Gateway tape gateway to copy the backup of the local data to AWS, then perform analytics on this data in the AWS cloud.

**B.** Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all the local storage in the AWS cloud, then perform analytics on this data in the cloud.

**C.** Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly take snapshots of the local data, then copy the data to AWS.

**D.** Use an AWS Storage Gateway file gateway to provide file storage to AWS, then perform analytics on this data in the AWS Cloud.

**Correct Answer: C**

Q 124/218

**After an Amazon VPC instance is launched, can I change the VPC security groups it belongs to?**

**A.** No. You cannot.

**B.** Yes. You can.

**C.** Only if the tag "VPC Change Group" is true

**D.** Only if the tag "VPC\_Change\_Group" is true

**Correct Answer: B**

Q 125/218

**A company collects temperature, humidity, and atmospheric pressure data in cities across multiple continents.  
The average volume of data collected per site each day is 500 GB. Each site has a high-speed internet connection. The company's weather forecasting applications are based in a single Region and analyze the data daily.  
What is the FASTEST way to aggregate data for all of these global sites?**

**A.** Enable Amazon S3 Transfer Acceleration on the destination bucket. Use multipart uploads to directly upload site data to the destination bucket.

**B.** Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.

**C.** Upload the data to an Amazon EC2 instance in the closes Region. Store the data in an Amazon EBS volume. One a day take an EBS snapshot and copy it to the centralize Region. Restore the EBS volume in the centralized Region and run an analysis on the data daily.

**D.** Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.

**Correct Answer: C**

Q 126/218

**A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large, important documents within the application with the following requirements:  
\* The data must be highly durable and available.  
\* The data must always be encrypted at rest and in transit.  
\* The encryption key must be managed by the company and rotated periodically.  
Which of the following solutions should the Solutions Architect recommend?**

**A.** Deploy the storage gateway to AWS in file gateway mode. Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes.

**B.** Use Amazon DynamoDB with SSL to connect to DynamoDB. Use an AWS KMS key to encrypt DynamoDB objects at rest.

**C.** Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.

**D.** Deploy instances with Amazon EBS volumes attached to store this data. Use EBS volume encryption using an AWS KMS key to encrypt the data.

**Correct Answer: A**

Q  127/218

**Which of the following statements is NOT correct when working with your AWS Direct Connect connection after it is set up completely?**

**A.** You can manage your AWS Direct Connect connections and view the connection details.

**B.** You can delete a connection as long as there are no virtual interfaces attached to it.

**C.** You cannot view the current connection ID and verify if it matches the connection ID on the Letter of Authorization (LOA).

**D.** You can accept a host connection by purchasing a hosted connection from the partner (APN).

**Correct Answer: C**

You can manage your AWS Direct Connect connections and view connection details, accept hosted connections, and delete connections. You can view the current status of your connection. You can also view your connection ID, which looks similar to this example dxcon-xxxx, and verify that it matches the connection ID on the Letter of Authorization (LOA) that you received from Amazon.  
http://docs.aws.amazon.com/directconnect/latest/UserGuide/viewdetails.html

Q 128/218

**Fill in the blanks: \_\_ is a durable, block-level storage volume that you can attach to a single, running Amazon EC2 instance.**

**A.** None of these

**B.** Amazon EBS

**C.** All of these

**D.** Amazon 53

**Correct Answer: B**

Q 129/218

**A company is deploying a two-tier, highly available web application to AWS. Which service provides durable storage for static content while utilizing lower Overall CPU resources for the web tier?**

**A.** Amazon 53

**B.** Amazon EBS volume

**C.** Amazon RD5 instance

**D.** Amazon EC2 instance store

**Correct Answer: A**

Q 130/218

**A company has a Microsoft NET application that runs on an on-premises Windows Server. The application stores data by using an Oracle Database Standard Edition server. The company is planning a migration to AWS and wants to minimize development changes while moving the application. The AWS application environment should be highly available.  
Which combination of actions should the company take to meet these requirements? (**Select TWO.**)**

**A.** Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.

**B.** Replatform the application to run on Amazon EC2 with the Amazon Linus Amazon Machine Image (AMI).

**C.** Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

**D.** Refactor the application as serverless with AWS Lambda functions running NET Core.

**E.** Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment.

**Correct Answer: D,E**

Q  131/218

**A workload in an Amazon VPC consists of a single web server launched from a custom AMI.  
Session state is stored in a database.  
How should the Solutions Architect modify this workload to be both highly available and scalable?**

**A.** Create a launch configuration with a desired capacity of two web servers across multiple Availability Zones. Create an Auto Scaling group with the AMI ID of the web server image. Use Amazon Route 53 latency-based routing to balance traffic across the Auto Scaling group.

**B.** Create a launch configuration with the AMI ID of the web server image. Create an Auto Scaling group using the newly-created launch configuration, and a desired capacity of two web servers across multiple Availability Zones. Use Amazon Route 53 weighted routing to balance traffic across the Auto Scaling group.

**C.** Create a launch configuration with the AMI ID of the web server image. Create an Auto Scaling group using the newly-created launch configuration, and a desired capacity of two web servers across multiple Availability Zones. Use an ALB to balance traffic across the Auto Scaling group.

**D.** Create a launch configuration with the AMI ID of the web server image. Create an Auto Scaling group using the newly-created launch configuration, and a desired capacity of two web servers across multiple regions. Use an Application Load Balancer (ALB) to balance traffic across the Auto Scaling group.

**Correct Answer: C**

Q 132/218

**Amazon RDS automated backups and DB Snapshots are currently supported for only the \_\_\_ \_ storage engine**

**A.** lnnoDB

**B.** MyISAM

**Correct Answer: A**