Vendor: Amazon

Exam Code: SAA-C02

Exam Name: AWS Certified Solutions Architect - Associate (SAA-C02) Exam

Version: 20.101

Important Notice

Product

Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within One year after your purchase.

You can login member center and download the latest product anytime. (Product downloaded from member center is always the latest.)

PS: Ensure you can pass the exam, please check the latest product in 2-3 days before the exam again.

Feedback

We devote to promote the product quality and the grade of service to ensure customers interest.

If you have any questions about our product, please provide Exam Number, Version, Page Number, Question Number, and your Login Account to us, please contact us at support@passleader.com and our technical experts will provide support in 24 hours.

Copyright

Order ID: **********

PayPal Name: **********

PayPal ID: **********

QUESTION 1
A solutions architect is designing a new service behind Amazon API Gateway.
The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second.
The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth Data can be queried using simple key-value requests.
Which combination of AWS services would meet these requirements? (Select TWO)

A. AWS Fargate
B. AWS Lambda
C. Amazon DynamoDB
D. Amazon EC2 Auto Scaling
E. MySQL-compatible Amazon Aurora

Answer: BC
Explanation:
In this case AWS Lambda can perform the computation and store the data in an Amazon DynamoDB table. Lambda can scale concurrent executions to meet demand easily and DynamoDB is built for key-value data storage requirements and is also serverless and easily scalable. This is therefore a cost effective solution for unpredictable workloads.
CORRECT: "AWS Lambda" is a correct answer.
CORRECT: "Amazon DynamoDB" is also a correct answer.
INCORRECT: "AWS Fargate" is incorrect as containers run constantly and therefore incur costs even when no requests are being made.
INCORRECT: "Amazon EC2 Auto Scaling" is incorrect as this uses EC2 instances which will incur costs even when no requests are being made.
INCORRECT: "Amazon RDS" is incorrect as this is a relational database not a No-SQL database. It is therefore not suitable for key-value data storage requirements.
References:
https://aws.amazon.com/lambda/features/
https://aws.amazon.com/dynamodb//

QUESTION 2
A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning.
This application runs on AWS Fargate and the connected storage needs to have concurrent access to files and deliver high performance.
Which storage option should the solutions architect recommend?

A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

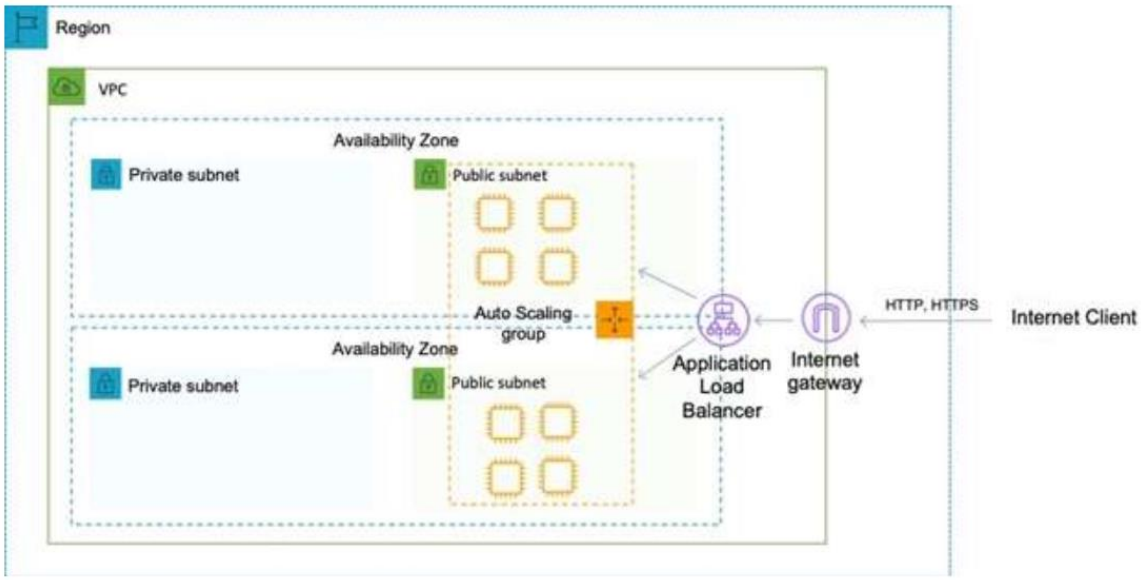
Answer: B
Explanation:
https://aws.amazon.com/efs/
Keyword: Concurrent Access to files + Deliver High Performance
Amazon FSx -

A high-performance file system optimized for fast processing of workloads. Lustre is a popular open-source parallel file system.
Also supports concurrent access to the same file or directory from thousands of compute instances.
Amazon IAM with FSx -
• Amazon FSx is integrated with AWS Identity and Access Management (IAM).
• This integration means that you can control the actions your AWS IAM users and groups can take to manage your file systems (such as creating and deleting file systems).
• You can also tag your Amazon FSx resources and control the actions that your IAM users and groups can take based on those tags.
Fargate Launch Type - So, Answer C & D Ruled-out as per Neal David
- Fargate automatically provisions resources
- Fargate provisions and manages compute
- Charged for running tasks
- No EFS and EBS integration
- Fargate handles cluster optimization
- Limited control, infrastructure is automated

QUESTION 3
A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB).
A solutions architect needs to modify the infrastructure to be highly available without modifying the application.
Which architecture should the solutions architect choose that provides high availability?

A. Create an Auto Scaling group that uses three instances across each of two Regions
B. Modify the Auto Scaling group to use three instances across each of two Availability Zones
C. Create an Auto Scaling template that can be used to quickly create more instances in another Region
D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier

Answer: B
Explanation:
High availability can be enabled for this architecture quite simply by modifying the existing Auto Scaling group to use multiple availability zones. The ASG will automatically balance the load so you don't actually need to specify the instances per AZ.
The architecture for the web tier will look like the one below:



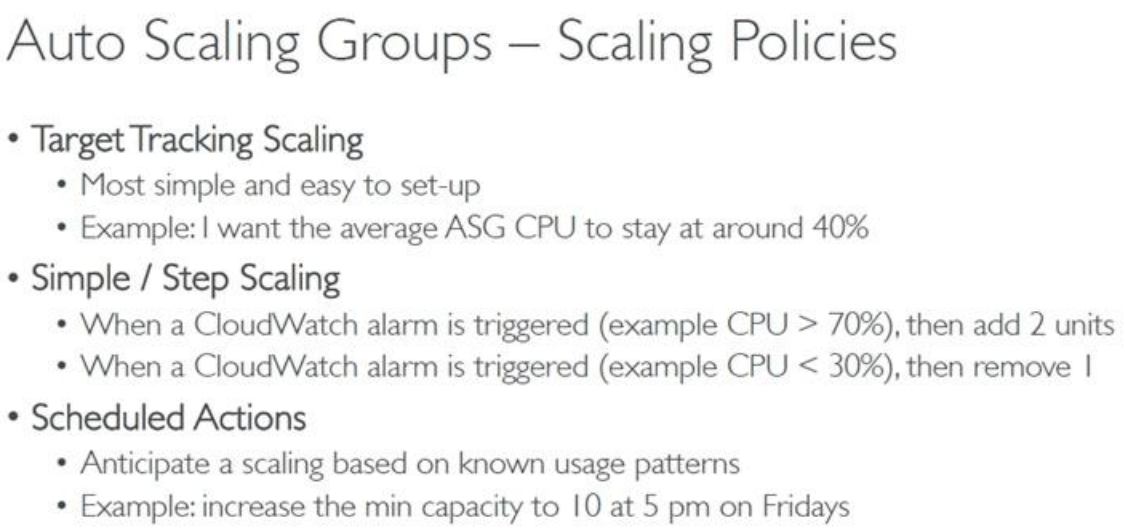
CORRECT: "Modify the Auto Scaling group to use four instances across each of two Availability Zones" is the correct answer.
INCORRECT: "Create an Auto Scaling group that uses four instances across each of two Regions" is incorrect as EC2 Auto Scaling does not support multiple regions.
INCORRECT: "Create an Auto Scaling template that can be used to quickly create more instances in another Region" is incorrect as EC2 Auto Scaling does not support multiple regions.
INCORRECT: "Create an Auto Scaling group that uses four instances across each of two subnets" is incorrect as the subnets could be in the same AZ.
References:
https://aws.amazon.com/ec2/autoscaling/

QUESTION 4
A company runs an internal browser-based application The application runs on Amazon EC2 instances behind an Application Load Balancer.
The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones.
The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.
How should the scaling be changed to address the staff complaints and keep costs to a minimum?

A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens
B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period
C. Implement a target tracking action triggered at a lower CPU threshold and decrease the cooldown period
D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens

Answer: A
Explanation:
Though this sounds like a good use case for scheduled actions, both answers using scheduled actions will have 20 instances running regardless of actual demand. A better option to be more cost effective is to use a target tracking action that triggers at a lower CPU threshold.

With this solution the scaling will occur before the CPU utilization gets to a point where performance is affected. This will result in resolving the performance issues whilst minimizing costs. Using a reduced cooldown period will also more quickly terminate unneeded instances, further reducing costs.



References:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html

QUESTION 5
A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images.
Image customization parameters will be in any request sent to an AWS API Gateway API.
The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image.
The solution must be highly available for viewing and customizing images
What is the MOST cost-effective solution to meet these requirements?

A. Use Amazon EC2 instances to manipulate the original image into the requested customization.
Store the original and manipulated images in Amazon S3.
Configure an Elastic Load Balancer in front of the EC2 instances.
B. Use AWS Lambda to manipulate the original image to the requested customization.
Store the original and manipulated images in Amazon S3.
Configure an Amazon CloudFront distribution with the S3 bucket as the ongin.
C. Use AWS Lambda to manipulate the original image to the requested customization.
Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB.
Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
D. Use Amazon EC2 instances to manipulate the original image into the requested customization.
Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB.
Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Answer: B
Explanation:
All solutions presented are highly available. The key requirement that must be satisfied is that the solution should be cost-effective and you must choose the most cost-effective option.

Therefore, it's best to eliminate services such as Amazon EC2 and ELB as these require ongoing costs even when they're not used. Instead, a fully serverless solution should be used. AWS Lambda, Amazon S3 and CloudFront are the best services to use for these requirements.
CORRECT: "Use AWS Lambda to manipulate the original images to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin" is the correct answer.
INCORRECT: "Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances" is incorrect. This is not the most cost-effective option as the ELB and EC2 instances will incur costs even when not used.
INCORRECT: "Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances" is incorrect. This is not the most cost-effective option as the ELB will incur costs even when not used. Also, Amazon DynamoDB will incur RCU/WCUs when running and is not the best choice for storing images.
INCORRECT: "Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin" is incorrect. This is not the most cost-effective option as the EC2 instances will incur costs even when not used
References:
https://aws.amazon.com/serverless/

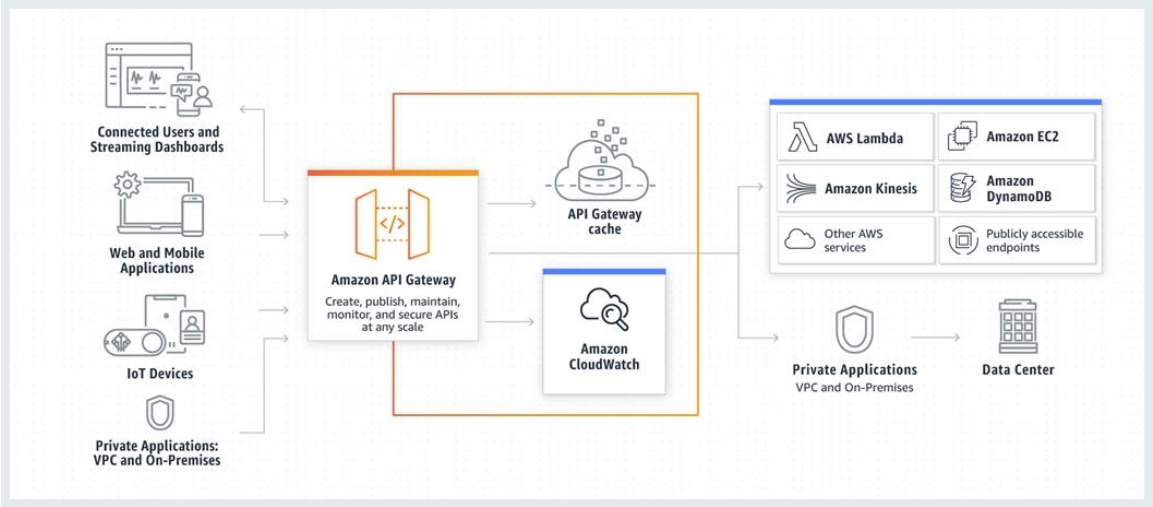
QUESTION 6
A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours.
The company wants to use these data points in its existing analytics platform A solutions architect must determine the most viable multi-tier option to support this architecture.
The data points must be accessible from the REST API.
Which action meets these requirements for storing and retrieving location data?

A. Use Amazon Athena with Amazon S3
B. Use Amazon API Gateway with AWS Lambda
C. Use Amazon QuickSight with Amazon Redshift
D. Use Amazon API Gateway with Amazon Kinesis Data Analytics

Answer: B
Explanation:
Keyword: Data points in its existing analytics platform + Data points must be accessible from the REST API + Track the location of its bicycles during peak operating hours

They already have an analytics platform, A (Athena) and D (Kinesis Data Analytics) are out of the race even tough S3 & APT Gateway Support REST API. Now B and C are in Race. C will not support REST API. So answer should be B as per below details.

Now if we talk about data type, we are talking about GEO location data for their bicycles. API Gateway will be support REST API. So, exact solution should be API Gateway with AWS Lambda along with Amazon Kinesis Data Analytics (Assume its used already).



CORRECT: "Use Amazon API Gateway with AWS Lambda" is the correct answer.
INCORRECT: "Use Amazon Athena with Amazon S3" is incorrect as they already have analytics platform.
INCORRECT: "Use Amazon QuickSight with Amazon Redshift" is incorrect. This is not support REST API.
INCORRECT: "Use Amazon API Gateway with Amazon Kinesis Data Analytics" is incorrect as they already have analytics platform.

References:
https://aws.amazon.com/api-gateway/
https://aws.amazon.com/lambda/
https://aws.amazon.com/kinesis/data-analytics/

QUESTION 7
A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.
Which storage solution should the solutions architect use?

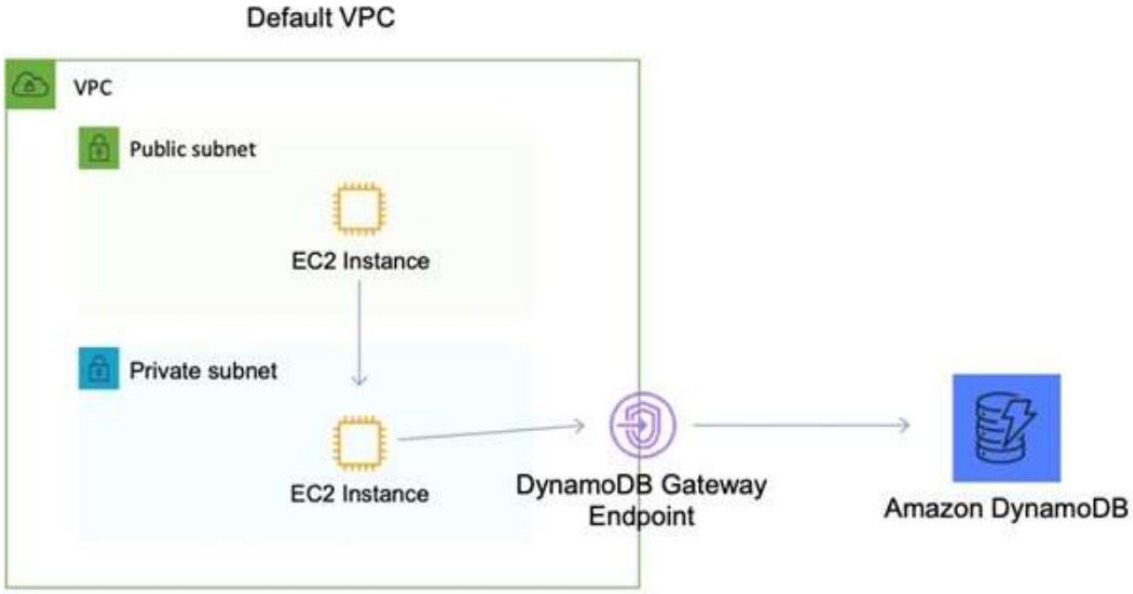
A. Amazon EBS
B. Amazon EC2 instance store
C. Amazon EFS
D. Amazon S3

Answer: B
Explanation:
It is block storage made for high trough put and low latency.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

QUESTION 8
A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet.
What should the solutions architect do to accomplish this? (Select TWO)

A. Create a route table entry for the endpoint
B. Create a gateway endpoint for DynamoDB
C. Create a new DynamoDB table that uses the endpoint
D. Create an ENI for the endpoint in each of the subnets of the VPC
E. Create a security group entry in the default security group to provide access

Answer: AB
Explanation:
Amazon DynamoDB and Amazon S3 support gateway endpoints, not interface endpoints. With a gateway endpoint you create the endpoint in the VPC, attach a policy allowing access to the service, and then specify the route table to create a route table entry in.



Route Table

Destination	Target
pl-6ca54005 (com.amazonaws.ap-southeast-2.s3, 54.231.248.0/22, 54.231.252.0/24, 52.95.128.0/21)	vpce-ID

CORRECT: "Create a route table entry for the endpoint" is a correct answer.
CORRECT: "Create a gateway endpoint for DynamoDB" is also a correct answer.
INCORRECT: "Create a new DynamoDB table that uses the endpoint" is incorrect as it is not necessary to create a new DynamoDB table.
INCORRECT: "Create an ENI for the endpoint in each of the subnets of the VPC" is incorrect as an ENI is used by an interface endpoint, not a gateway endpoint.
INCORRECT: "Create a VPC peering connection between the VPC and DynamoDB" is incorrect as you cannot create a VPC peering connection between a VPC and a public AWS service as public services are outside of VPCs.
References:
https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html

QUESTION 9
A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB).
The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures.

What should the solutions architect recommend?

A. Leverage Amazon CloudFront with the ALB endpoint as the origin
B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB
C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked
D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances

Answer: C
Explanation:
https://aws.amazon.com/waf/
https://aws.amazon.com/shield/
https://aws.amazon.com/shield/features/

QUESTION 10
A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that allows users to access this data using an API.
The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.
Which solution should the solutions architect suggest?

A. Set up an Amazon API Gateway and use Amazon ECS.
B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
C. Set up an Amazon API Gateway and use AWS Lambda functions
D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling

Answer: C
Explanation:
This question is simply asking you to work out the best compute service for the stated requirements. The key requirements are that the compute service should be suitable for a workload that can range quite broadly in demand from no requests to large bursts of traffic. AWS Lambda is an ideal solution as you pay only when requests are made and it can easily scale to accommodate the large bursts in traffic. Lambda works well with both API Gateway and Amazon RDS.
CORRECT: "Set up an Amazon API Gateway and use AWS Lambda functions" is the correct answer.
INCORRECT: "Set up an Amazon API Gateway and use Amazon ECS" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic.
INCORRECT: "Set up an Amazon API Gateway and use AWS Elastic Beanstalk" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic.
INCORRECT: "Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic.
References:
https://docs.aws.amazon.com/lambda/latest/dg/invocation-scaling.html

QUESTION 11
A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes.
The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID).

What should a solutions architect do to meet these requirements?

A. Launch the application on EC2 instances in each Availability Zone.
Attach EBS volumes to each EC2 instance.
B. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones.
Mount an instance store on each EC2 instance.
C. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones.
Store data on Amazon EFS and mount a target on each instance.
D. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones.
Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: C
Explanation:
To increase the resiliency of the application the solutions architect can use Auto Scaling groups to launch and terminate instances across multiple availability zones based on demand. An application load balancer (ALB) can be used to direct traffic to the web application running on the EC2 instances.
Lastly, the Amazon Elastic File System (EFS) can assist with increasing the resilience of the application by providing a shared file system that can be mounted by multiple EC2 instances from multiple availability zones.
CORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance" is the correct answer.
INCORRECT: "Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance" is incorrect as the EBS volumes are single points of failure which are not shared with other instances.
INCORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance" is incorrect as instance stores are ephemeral data stores which means data is lost when powered down. Also, instance stores cannot be shared between instances.
INCORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as there are data retrieval charges associated with this S3 tier. It is not a suitable storage tier for application files.
References:
https://docs.aws.amazon.com/efs/

QUESTION 12
A company has an application that calls AWS Lambda functions.
A recent code review found database credentials stored in the source code.
The database credentials need to be removed from the Lambda source code.
The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.
What should a solutions architect recommend to meet these requirements?

A. Store the password in AWS CloudHSM.
Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID.
B. Store the password in AWS Secrets Manager.
Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.
C. Move the database password to an environment variable associated with the Lambda function.
Retrieve the password from the environment variable upon execution.
D. Store the password in AWS Key Management Service (AWS KMS).

Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID.

Answer: B

QUESTION 13
A solutions architect needs the static website within an Amazon S3 bucket. A solutions architect needs to ensure that data can be recovered in case of accidental deletion.

Which action will accomplish this?

A. Enable Amazon S3 versioning
B. Enable Amazon S3 Intelligent-Tiering.
C. Enable an Amazon S3 lifecycle policy
D. Enable Amazon S3 cross-Region replication.

Answer: A
Explanation:
Object versioning is a means of keeping multiple variants of an object in the same Amazon S3 bucket. Versioning provides the ability to recover from both unintended user actions and application failures. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket.
CORRECT: "Enable Amazon S3 versioning" is the correct answer.
INCORRECT: "Enable Amazon S3 Intelligent-Tiering" is incorrect. This is a storage class that automatically moves data between frequent access and infrequent access classes based on usage patterns.
INCORRECT: "Enable an Amazon S3 lifecycle policy" is incorrect. An S3 lifecycle policy is a set of rules that define actions that apply to groups of S3 objects such as transitioning objects to another storage class.
INCORRECT: "Enable Amazon S3 cross-Region replication" is incorrect as this is used to copy objects to different regions. CRR relies on versioning which is the feature that is required for protecting against accidental deletion.
References:
https://d0.awsstatic.com/whitepapers/protecting-s3-against-object-deletion.pdf

QUESTION 14
A company is managing health records on-premises.
The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels.
The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space.
The CTO has requested a solutions architect design a solution to move existing data and support future records.
Which services can the solutions architect recommend to meet these requirements'?

A. Use AWS DataSync to move existing data to AWS.
Use Amazon S3 to store existing and new data.
Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
B. Use AWS Storage Gateway to move existing data to AWS.
Use Amazon S3 to store existing and new data.
Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
C. Use AWS DataSync to move existing data to AWS.
Use Amazon S3 to store existing and new data.

Enable Amazon S3 object lock and enable AWS CloudTrail with management events.

D. Use AWS Storage Gateway to move existing data to AWS.
Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data.
Enable Amazon S3 object lock and enable Amazon S3 server access logging.

Answer: A
Explanation:
Keyword: Move existing data and support future records + Granular audit access at all levels

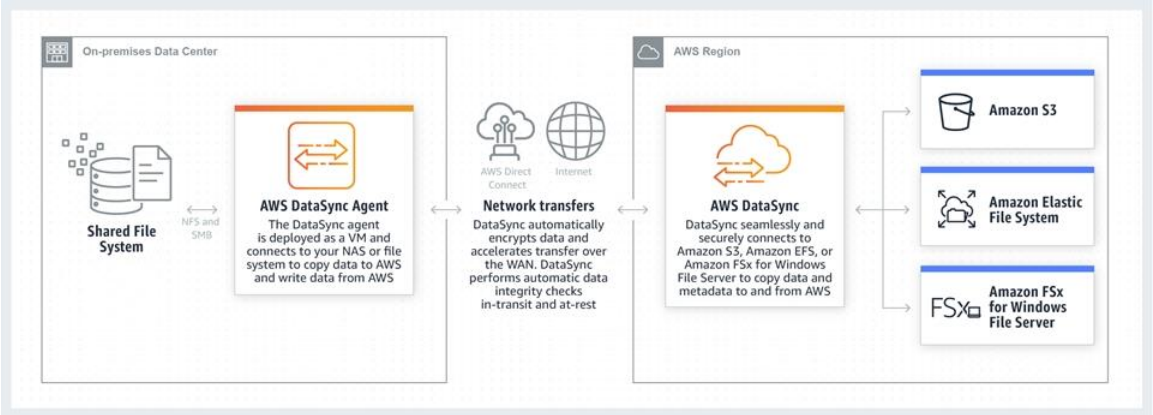
Use AWS DataSync to migrate existing data to Amazon S3, and then use the File Gateway configuration of AWS Storage Gateway to retain access to the migrated data and for ongoing updates from your on-premises file-based applications.

Need a solution to move existing data and support future records = AWS DataSync should be used for migration.
Need granular audit access at all levels = Data Events should be used in CloudTrail, Management Events is enabled by default.

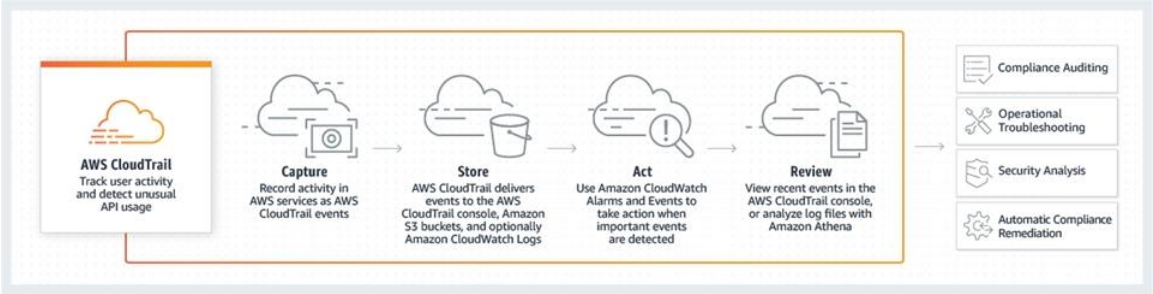
CORRECT: "Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events" is the correct answer.

INCORRECT: "Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events" is incorrect as "current infrastructure is running out of space"
INCORRECT: "Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events." is incorrect as "Management Events is enabled by default"
INCORRECT: "Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging." is incorrect as "current infrastructure is running out of space"

How AWS DataSync Works



How AWS CloudTrail works



References:
https://aws.amazon.com/datasync/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc
https://aws.amazon.com/cloudtrail/
https://aws.amazon.com/storagegateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

QUESTION 15
A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted.
A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed.
The company will make at least one encrypted backup before destroying the old backups
What should be done to enable encryption for future backups?

A. Enable default encryption for the Amazon S3 bucket where backups are stored
B. Modify the backup section of the database configuration to toggle the Enable encryption check box.
C. Create a snapshot of the database.
Copy it to an encrypted snapshot.
Restore the database from the encrypted snapshot.
D. Enable an encrypted read replica on RDS for MySQL.
Promote the encrypted read replica to primary.
Remove the original database instance.

Answer: C
Explanation:
Amazon RDS uses snapshots for backup. Snapshots are encrypted when created only if the database is encrypted and you can only select encryption for the database when you first create it. In this case the database, and hence the snapshots, ad unencrypted.
However, you can create an encrypted copy of a snapshot. You can restore using that snapshot which creates a new DB instance that has encryption enabled. From that point on encryption will be enabled for all snapshots.
CORRECT: "Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot" is the correct answer. INCORRECT: "Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance" is incorrect as you cannot create an encrypted read replica from an unencrypted master.
INCORRECT: "Modify the backup section of the database configuration to toggle the Enable encryption check box" is incorrect as you cannot add encryption for an existing database.
INCORRECT: "Enable default encryption for the Amazon S3 bucket where backups are stored" is incorrect because you do not have access to the S3 bucket in which snapshots are stored.
References:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

QUESTION 16
A client reports that they want see an audit log of any changes made to AWS resources in their account.

What can the client do to achieve this?

A. Set up Amazon CloudWatch monitors on services they own
B. Enable AWS CloudTrail logs to be delivered to an Amazon S3 bucket
C. Use Amazon CloudWatch Events to parse logs
D. Use AWS OpsWorks to manage their resources

Answer: B
Explanation:
A CloudTrail trail can be created which delivers log files to an Amazon S3 bucket.

QUESTION 17
An application running in a private subnet accesses an Amazon DynamoDB table. There is a security requirement that the data never leave the AWS network.

How should this requirement be met?

A. Configure a network ACL on DynamoDB to limit traffic to the private subnet
B. Enable DynamoDB encryption at rest using an AWS KMS key
C. Add a NAT gateway and configure the route table on the private subnet
D. Create a VPC endpoint for DynamoDB and configure the endpoint policy

Answer: D
Explanation:
Hint: Private Subnet = VPC Endpoint

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

QUESTION 18
A three-tier application is being created to host small news articles. The application is expected to serve millions of users. When breaking news occurs, the site must handle very large spikes in traffic without significantly impacting database performance.

Which design meets these requirements while minimizing costs?

A. Use Auto Scaling groups to increase the number of Amazon EC2 instances delivering the web application
B. Use Auto Scaling groups to increase the size of the Amazon RDS instances delivering the database
C. Use Amazon DynamoDB strongly consistent reads to adjust for the increase in traffic
D. Use Amazon DynamoDB Accelerator (DAX) to cache read operations to the database

Answer: D
Explanation:
DAX has in memory cache. If breaking news happens, majority of the users searching will look for the exact same thing. That being said, requests will query the Memory Cache first and will not need to fetch the data from the DB directly.

QUESTION 19
During a review of business applications, a Solutions Architect identifies a critical application with a relational database that was built by a business user and is running on the user's desktop. To reduce the risk of a business interruption, the Solutions Architect wants to migrate the application to a highly available, multi-tiered solution in AWS.
What should the Solutions Architect do to accomplish this with the LEAST amount of disruption to the business?

A. Create an import package of the application code for upload to AWS Lambda, and include a function to create another Lambda function to migrate data into an Amazon RDS database
B. Create an image of the user's desktop, migrate it to Amazon EC2 using VM Import, and place the EC2 instance in an Auto Scaling group
C. Pre-stage new Amazon EC2 instances running the application code on AWS behind an Application Load Balancer and an Amazon RDS Multi-AZ DB instance
D. Use AWS DMS to migrate the backend database to an Amazon RDS Multi-AZ DB instance. Migrate the application code to AWS Elastic Beanstalk

Answer: D

QUESTION 20
A company has thousands of files stored in an Amazon S3 bucket that has a well-defined access pattern. The files are accessed by an application multiple times a day for the first 30 days. Files are rarely accessed within the next 90 days. After that, the files are never accessed again. During the first 120 days, accessing these files should never take more than a few seconds.

Which lifecycle policy should be used for the S3 objects to minimize costs based on the access pattern?

A. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage for the first 30 days. Then move the files to the GLACIER storage class for the next 90 days. Allow the data to expire after that.
B. Use Amazon S3 Standard storage for the first 30 days. Then move the files to Amazon S3 Standard- Infrequent Access (S3 Standard-IA) for the next 90 days. Allow the data to expire after that.
C. Use Amazon S3 Standard storage for first 30 days. Then move the files to the GLACIER storage class for the next 90 days. Allow the data to expire after that.
D. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the first 30 days. After that, move the data to the GLACIER storage class, where is will be deleted automatically.

Answer: B
Explanation:
It is mentioned that they need to access data in few seconds during the 120 days.

QUESTION 21
A company creates business-critical 3D images every night. The images are batch-processed every Friday and require an uninterrupted 48 hours to complete.

What is the MOST cost-effective Amazon EC2 pricing model for this scenario?

A. On-Demand Instances
B. Scheduled Reserved Instances
C. Reserved Instances
D. Spot Instances

Answer: B
Explanation:
Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.
Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week.
CORRECT: "Scheduled Reserved Instances" is the correct answer.
INCORRECT: "Standard Reserved Instances" is incorrect as the workload only runs for 4 hours a day this would be more expensive.
INCORRECT: "On-Demand Instances" is incorrect as this would be much more expensive as there is no discount applied.
INCORRECT: "Spot Instances" is incorrect as the workload cannot be interrupted once started. With Spot instances workloads can be terminated if the Spot price changes or capacity is required.
References:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html

QUESTION 22
An application generates audit logs of operational activities. Compliance requirements mandate that the application retain the logs for 5 years.

How can these requirements be met?

A. Save the logs in an Amazon S3 bucket and enable Multi-Factor Authentication Delete (MFA Delete) on the bucket.
B. Save the logs in an Amazon EFS volume and use Network File System version 4 (NFSv4) locking with the volume.
C. Save the logs in an Amazon Glacier vault and use the Vault Lock feature.
D. Save the logs in an Amazon EBS volume and take monthly snapshots.

Answer: C
Explanation:
Amazon Glacier, which enables long-term storage of mission-critical data, has added Vault Lock. This new feature allows you to lock your vault with a variety of compliance controls that are

designed to support such long-term records retention.

QUESTION 23
A Solutions Architect is creating an application running in an Amazon VPC that needs to access AWS Systems Manager Parameter Store. Network security rules prohibit any route table entry with a 0.0.0.0/0 destination.

What infrastructure addition will allow access to the AWS service while meeting the requirements?

A. VPC peering
B. NAT instance
C. NAT gateway
D. AWS PrivateLink

Answer: D
Explanation:
To publish messages to Amazon SNS topics from an Amazon VPC, create an interface VPC endpoint. Then, you can publish messages to SNS topics while keeping the traffic within the network that you manage with the VPC. This is the most secure option as traffic does not need to traverse the Internet.
CORRECT: "Use AWS PrivateLink" is the correct answer.
INCORRECT: "Use an Internet Gateway" is incorrect. Internet Gateways are used by instances in public subnets to access the Internet and this is less secure than an VPC endpoint.
INCORRECT: "Use a proxy instance" is incorrect. A proxy instance will also use the public Internet and so is less secure than a VPC endpoint.
INCORRECT: "Use a NAT gateway" is incorrect. A NAT Gateway is used by instances in private subnets to access the Internet and this is less secure than an VPC endpoint.
References:
https://docs.aws.amazon.com/sns/latest/dg/sns-vpc-endpoint.html

QUESTION 24
A photo-sharing website running on AWS allows users to generate thumbnail images of photos stored in Amazon S3. An Amazon DynamoDB table maintains the locations of photos, and thumbnails are easily re- created from the originals if they are accidentally deleted.

How should the thumbnail images be stored to ensure the LOWEST cost?

A. Amazon S3 Standard-Infrequent Access (S3 Standard-IA) with cross-region replication
B. Amazon S3
C. Amazon Glacier
D. Amazon S3 with cross-region replication

Answer: B

QUESTION 25
A company is implementing a data lake solution on Amazon S3. Its security policy mandates that the data stored in Amazon S3 should be encrypted at rest.

Which options can achieve this? (Select TWO.)

A. Use S3 server-side encryption with an Amazon EC2 key pair.
B. Use S3 server-side encryption with customer-provided keys (SSE-C).
C. Use S3 bucket policies to restrict access to the data at rest.
D. Use client-side encryption before ingesting the data to Amazon S3 using encryption keys.
E. Use SSL to encrypt the data while in transit to Amazon S3.

Answer: BD

QUESTION 26
A solutions architect has created a new AWS account and must secure AWS account root user access.
Which combination of actions will accomplish this? (Select TWO.)

A. Ensure the root user uses a strong password
B. Enable multi-factor authentication to the root user
C. Store root user access keys in an encrypted Amazon S3 bucket
D. Add the root user to a group containing administrative permissions.
E. Apply the required permissions to the root user with an inline policy document

Answer: AB
Explanation:
"Enable MFA"
The AWS Account Root User - https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html
"Choose a strong password"
Changing the AWS Account Root User Password - https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_change-root.html

QUESTION 27
A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB).
The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones.
On the first day of every month at midnight the application becomes much slower when the month-end financial calculation batch executes.
This causes the CPU utilization of the EC2 instances to immediately peak to 100% which disrupts the application.
What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

A. Configure an Amazon CloudFront distribution in front of the ALB
B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization
C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances

Answer: C
Explanation:
Scheduled scaling allows you to set your own scaling schedule. In this case the scaling action can be scheduled to occur just prior to the time that the reports will be run each month. Scaling actions are performed automatically as a function of time and date. This will ensure that there are enough EC2 instances to serve the demand and prevent the application from slowing down.
CORRECT: "Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule" is the correct answer.

INCORRECT: "Configure an Amazon CloudFront distribution in front of the ALB" is incorrect as this would be more suitable for providing access to global users by caching content.
INCORRECT: "Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization" is incorrect as this would not prevent the slow-down from occurring as there would be a delay between when the CPU hits 100% and the metric being reported and additional instances being launched.
INCORRECT: "Configure Amazon ElastiCache to remove some of the workload from the EC2 instances" is incorrect as ElastiCache is a database cache, it cannot replace the compute functions of an EC2 instance.
References:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

QUESTION 28
A company is migrating from an on-premises infrastructure to the AWS Cloud.
One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync.
A solutions architect needs to replace the file server farm.
Which service should the solutions architect use?

A. Amazon EFS
B. Amazon FSx
C. Amazon S3
D. AWS Storage Gateway

Answer: B
Explanation:
Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.
Amazon FSx is built on Windows Server and provides a rich set of administrative features that include end-user file restore, user quotas, and Access Control Lists (ACLs).
Additionally, Amazon FSX for Windows File Server supports Distributed File System Replication (DFSR) in both Single-AZ and Multi-AZ deployments as can be seen in the feature comparison table below.

Deployment type	SSD storage	HDD storage	DFS namespaces	DFS replication	Custom DNS name	CA shares
Single-AZ 1	✓		✓	✓	✓	
Single-AZ 2	✓	✓	✓		Coming soon	✓*
Multi-AZ	✓	✓	✓		Coming soon	✓*

CORRECT: "Amazon FSx" is the correct answer.
INCORRECT: "Amazon EFS" is incorrect as EFS only supports Linux systems.
INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.
INCORRECT: "AWS Storage Gateway" is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on-premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company need to replace the file server farm and Amazon FSx is the best choice for this job.
References:
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html

QUESTION 29

A company's website is used to sell products to the public.
The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB).
There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks.
The ALB is the origin for the CloudFront distribution.
A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.
What should a solutions architect do to protect the application?

A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address
B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address
C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address
D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

Answer: B
Explanation:
A new version of the AWS Web Application Firewall was released in November 2019. With AWS WAF classic you create "IP match conditions", whereas with AWS WAF (new version) you create "IP set match statements". Look out for wording on the exam.
The IP match condition / IP set match statement inspects the IP address of a web request's origin against a set of IP addresses and address ranges.
Use this to allow or block web requests based on the IP addresses that the requests originate from.
AWS WAF supports all IPv4 and IPv6 address ranges. An IP set can hold up to 10,000 IP addresses or IP address ranges to check.
CORRECT: "Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address" is the correct answer.
INCORRECT: "Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address" is incorrect as CloudFront does not sit within a subnet so network ACLs do not apply to it.
INCORRECT: "Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address" is incorrect as the source IP addresses of the data in the EC2 instances' subnets will be the ELB IP addresses.
INCORRECT: "Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address." is incorrect as you cannot create deny rules with security groups.
References:
https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-ipset-match.html

QUESTION 30
A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis.
An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket.
Which action will MOST securely grant the EC2 instance access to the S3 bucket?

A. Attach a resource-based policy to the S3 bucket
B. Create an IAM user for the application with specific permissions to the S3 bucket
C. Associate an IAM role with least privilege permissions to the EC2 instance profile

D. Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls

Answer: C
Explanation:
Keyword: Privilege Permission + IAM Role

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

IAM is a feature of your AWS account offered at no additional charge. You will be charged only for use of other AWS services by your users.

IAM roles for Amazon EC2

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

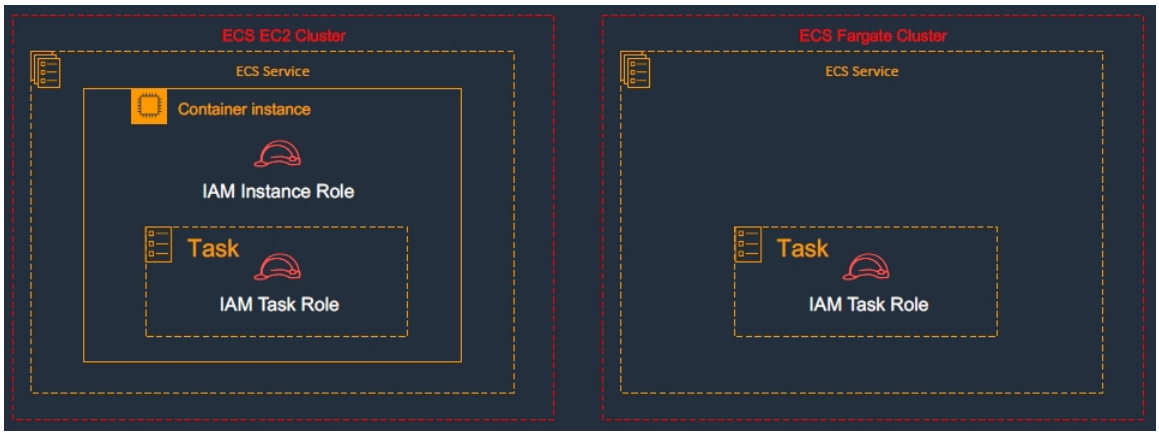
We designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.

Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles as follows:
- Create an IAM role.
- Define which accounts or AWS services can assume the role.
- Define which API actions and resources the application can use after assuming the role.
- Specify the role when you launch your instance, or attach the role to an existing instance.
- Have the application retrieve a set of temporary credentials and use them.

For example, you can use IAM roles to grant permissions to applications running on your instances that need to use a bucket in Amazon S3. You can specify permissions for IAM roles by creating a policy in JSON format. These are similar to the policies that you create for IAM users. If you change a role, the change is propagated to all instances.

When creating IAM roles, associate least privilege IAM policies that restrict access to the specific API calls the application requires.

IAM Roles



References:
https://aws.amazon.com/iam/faqs/
https://youtu.be/YQsK4MtsELU
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

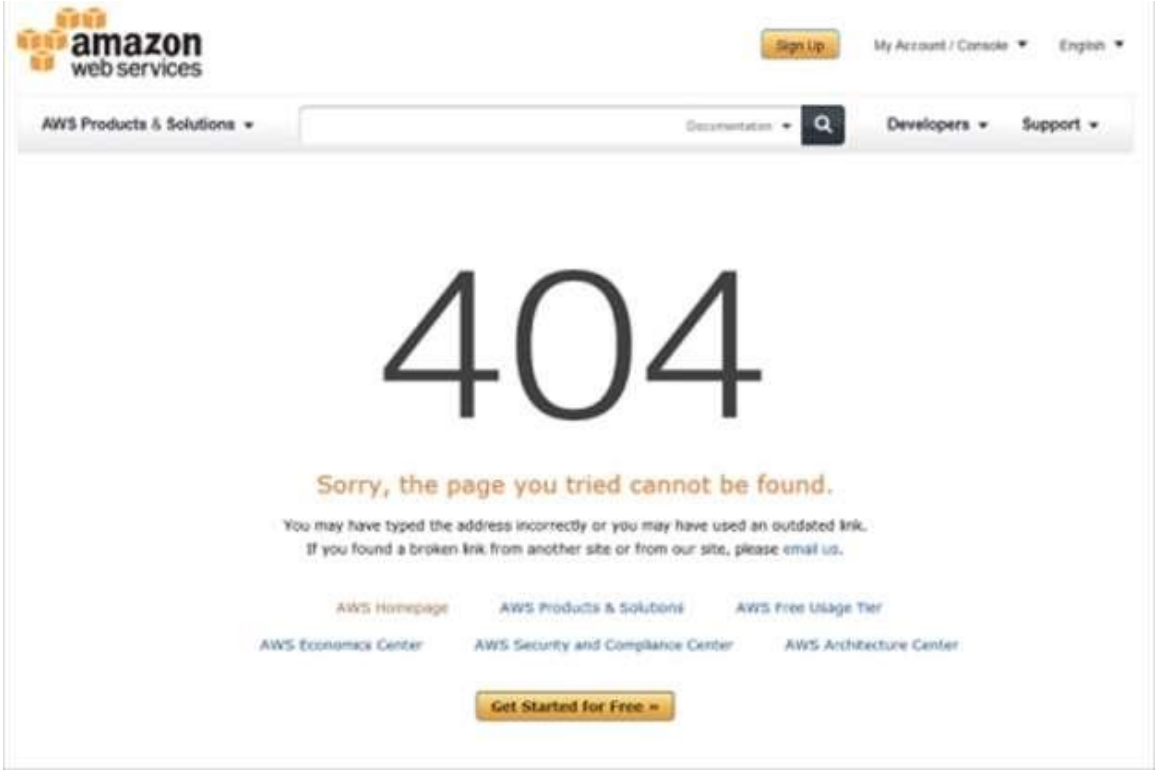
QUESTION 31
A solutions architect is designing a solution where users will De directed to a backup static error page it the primary website is unavailable.
The primary website's DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).
Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins.
Then, create custom error pages for the distribution.
B. Set up a Route 53 active-passive failover configuration.
Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
C. Update the Route 53 record to use a latency-based routing policy.
Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is

sent to the most responsive endpoints.

D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints.
Route 53 will only send requests to the instance if the health checks fail for the ALB.

Answer: B
Explanation:
Using Amazon CloudFront as the front-end provides the option to specify a custom message instead of the default message. To specify the specific file that you want to return and the errors for which the file should be returned, you update your CloudFront distribution to specify those values.
For example, the following is a customized error message:



The CloudFront distribution can use the ALB as the origin, which will cause the website content to be cached on the CloudFront edge caches.
This solution represents the most operationally efficient choice as no action is required in the event of an issue, other than troubleshooting the root cause.

References:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/custom-error-pages.html

QUESTION 32
A solutions architect is designing the cloud architecture for a new application being deployed on AWS.
The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed.
The processor application is stateless.

The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.
Which design should the solutions architect use?

A. Create an Amazon SNS topic to send the jobs that need to be processed.
Create an Amazon Machine Image (AMI) that consists of the processor application.
Create a launch configuration that uses the AMI.
Create an Auto Scaling group using the launch configuration.
Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage
B. Create an Amazon SQS queue to hold the jobs that need to be processed.
Create an Amazon Machine Image (AMI) that consists of the processor application.
Create a launch configuration that uses the AMI.
Create an Auto Scaling group using the launch configuration.
Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage
C. Create an Amazon SQS queue to hold the jobs that needs to be processed.
Create an Amazon Machine Image (AMI) that consists of the processor application.
Create a launch template that uses the AMI.
Create an Auto Scaling group using the launch template.
Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue
D. Create an Amazon SNS topic to send the jobs that need to be processed.
Create an Amazon Machine Image (AMI) that consists of the processor application.
Create a launch template that uses the AMI.
Create an Auto Scaling group using the launch template.
Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Answer: C
Explanation:
In this case we need to find a durable and loosely coupled solution for storing jobs. Amazon SQS is ideal for this use case and can be configured to use dynamic scaling based on the number of jobs waiting in the queue.
To configure this scaling you can use the backlog per instance metric with the target value being the acceptable backlog per instance to maintain. You can calculate these numbers as follows:
Backlog per instance: To calculate your backlog per instance, start with the ApproximateNumberOfMessages queue attribute to determine the length of the SQS queue (number of messages available for retrieval from the queue). Divide that number by the fleet's running capacity, which for an Auto Scaling group is the number of instances in the InService state, to get the backlog per instance.
Acceptable backlog per instance: To calculate your target value, first determine what your application can accept in terms of latency. Then, take the acceptable latency value and divide it by the average time that an EC2 instance takes to process a message.
This solution will scale EC2 instances using Auto Scaling based on the number of jobs waiting in the SQS queue.
CORRECT: "Create an Amazon SQS queue to hold the jobs that needs to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue" is the correct answer.
INCORRECT: "Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage" is incorrect as scaling on network usage does not relate to the number of jobs waiting to be processed.
INCORRECT: "Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the

Auto Scaling group to add and remove nodes based on CPU usage" is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on CPU usage is not the best solution as it does not relate to the number of jobs waiting to be processed.
INCORRECT: "Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic" is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on the number of notifications in SNS is not possible.
References:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html

QUESTION 33
A company has a legacy application that processes data in two parts.
The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently.
How should a solutions architect integrate the microservices?

A. Implement code in microservice 1 to send data to an Amazon S3 bucket.
Use S3 event notifications to invoke microservice 2.
B. Implement code in microservice 1 to publish data to an Amazon SNS topic.
Implement code in microservice 2 to subscribe to this topic.
C. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose.
Implement code in microservice 2 to read from Kinesis Data Firehose.
D. Implement code in microservice 1 to send data to an Amazon SQS queue.
Implement code in microservice 2 to process messages from the queue.

Answer: D
Explanation:
This is a good use case for Amazon SQS. The microservices must be decoupled so they can scale independently. An Amazon SQS queue will enable microservice 1 to add messages to the queue. Microservice 2 can then pick up the messages and process them. This ensures that if there's a spike in traffic on the frontend, messages do not get lost due to the backend process not being ready to process them.
CORRECT: "Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue" is the correct answer.
INCORRECT: "Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2" is incorrect as a message queue would be preferable to an S3 bucket.
INCORRECT: "Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic" is incorrect as notifications to topics are pushed to subscribers. In this case we want the second microservice to pickup the messages when ready (pull them).
INCORRECT: "Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose" is incorrect as this is not how Firehose works. Firehose sends data directly to destinations, it is not a message queue.
References:
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html

QUESTION 34
A solutions architect at an ecommerce company wants to back up application log data to Amazon

S3.
The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most.
The company wants to keep costs as low as possible by using the appropriate S3 storage class.
Which S3 storage class should be implemented to meet these requirements?

A. S3 Glacier
B. S3 Intelligent-Tiering
C. S3 Standard-Infrequent Access (S3 Standard-IA)
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B
Explanation:
The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. This is an ideal use case for intelligent-tiering as the access patterns for the log files are not known.
CORRECT: "S3 Intelligent-Tiering" is the correct answer.
INCORRECT: "S3 Standard-Infrequent Access (S3 Standard-IA)" is incorrect as if the data is accessed often retrieval fees could become expensive.
INCORRECT: "S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as if the data is accessed often retrieval fees could become expensive.
INCORRECT: "S3 Glacier" is incorrect as if the data is accessed often retrieval fees could become expensive. Glacier also requires more work in retrieving the data from the archive and quick access requirements can add further costs.
References:
https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access

QUESTION 35
A security team wants to limit access to specific services or actions in all of the team's AWS accounts.
All accounts belong to a large organization in AWS Organizations.
The solution must be scalable and there must be a single point where permissions can be maintained.
What should a solutions architect do to accomplish this?

A. Create an ACL to provide access to the services or actions.
B. Create a security group to allow accounts and attach it to user groups
C. Create cross-account roles in each account to deny access to the services or actions.
D. Create a service control policy in the root organizational unit to deny access to the services or actions

Answer: D
Explanation:
Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines.

SCPs alone are not sufficient for allowing access in the accounts in your organization. Attaching an SCP to an AWS Organizations entity (root, OU, or account) defines a guardrail for what actions the principals can perform. You still need to attach identity-based or resource-based policies to principals or resources in your organization's accounts to actually grant permissions to them.
CORRECT: "Create a service control policy in the root organizational unit to deny access to the services or actions" is the correct answer.
INCORRECT: "Create an ACL to provide access to the services or actions" is incorrect as access control lists are not used for permissions associated with IAM. Permissions policies are used with IAM.
INCORRECT: "Create a security group to allow accounts and attach it to user groups" is incorrect as security groups are instance level firewalls. They do not limit service actions.
INCORRECT: "Create cross-account roles in each account to deny access to the services or actions" is incorrect as this is a complex solution and does not provide centralized control
References:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

QUESTION 36
You are trying to launch an EC2 instance, however the instance seems to go into a terminated status immediately. What would probably not be a reason that this is happening?

A. The AMI is missing a required part.
B. The snapshot is corrupt.
C. You need to create storage in EBS first.
D. You've reached your volume limit.

Answer: C
Explanation:
Amazon EC2 provides a virtual computing environments, known as an instance. After you launch an instance, AWS recommends that you check its status to confirm that it goes from the pending status to the running status, the not terminated status. The following are a few reasons why an Amazon EBS-backed instance might immediately terminate:
You've reached your volume limit.
The AMI is missing a required part.
The snapshot is corrupt.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_InstanceStraightToTerminated.html

QUESTION 37

You have set up an Auto Scaling group. The cool down period for the Auto Scaling group is 7 minutes. The first instance is launched after 3 minutes, while the second instance is launched after 4 minutes. How many minutes after the first instance is launched will Auto Scaling accept another scaling activity request?

A. 11 minutes
B. 7 minutes
C. 10 minutes
D. 14 minutes

Answer: A
Explanation:
If an Auto Scaling group is launching more than one instance, the cool down period for each instance starts after that instance is launched. The group remains locked until the last instance that was launched has completed its cool down period. In this case the cool down period for the first instance starts after 3 minutes and finishes at the 10th minute (3+7 cool down), while for the second instance it starts at the 4th minute and finishes at the 11th minute (4+7 cool down). Thus, the Auto Scaling group will receive another request only after 11 minutes.
Reference: http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html

QUESTION 38
In Amazon EC2 Container Service components, what is the name of a logical grouping of container instances on which you can place tasks?

A. A cluster
B. A container instance
C. A container
D. A task definition

Answer: A
Explanation:
Amazon ECS contains the following components:
A Cluster is a logical grouping of container instances that you can place tasks on. A Container instance is an Amazon EC2 instance that is running the Amazon ECS agent and has been registered into a cluster.
A Task definition is a description of an application that contains one or more container definitions.
A Scheduler is the method used for placing tasks on container instances. A Service is an Amazon ECS service that allows you to run and maintain a specified number of instances of a task definition simultaneously.
A Task is an instantiation of a task definition that is running on a container instance. A Container is a Linux container that was created as part of a task.
Reference: http://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html

QUESTION 39
In the context of AWS support, why must an EC2 instance be unreachable for 20 minutes rather than allowing customers to open tickets immediately?

A. Because most reachability issues are resolved by automated processes in less than 20 minutes
B. Because all EC2 instances are unreachable for 20 minutes every day when AWS does routine maintenance
C. Because all EC2 instances are unreachable for 20 minutes when first launched
D. Because of all the reasons listed here

Answer: A
Explanation:
An EC2 instance must be unreachable for 20 minutes before opening a ticket, because most reachability issues are resolved by automated processes in less than 20 minutes and will not require any action on the part of the customer. If the instance is still unreachable after this time frame has passed, then you should open a case with support.
Reference: https://aws.amazon.com/premiumsupport/faqs/

QUESTION 40
Can a user get a notification of each instance start / terminate configured with Auto Scaling?

A. Yes, if configured with the Launch Config
B. Yes, always
C. Yes, if configured with the Auto Scaling group
D. No

Answer: C
Explanation:
The user can get notifications using SNS if he has configured the notifications while creating the Auto Scaling group.
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html

QUESTION 41
Amazon EBS provides the ability to create backups of any Amazon EC2 volume into what is known as _____.

A. snapshots
B. images
C. instance backups
D. mirrors

Answer: A
Explanation:
Amazon allows you to make backups of the data stored in your EBS volumes through snapshots that can later be used to create a new EBS volume.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION 42
To specify a resource in a policy statement, in Amazon EC2, can you use its Amazon Resource Name (ARN)?

A. Yes, you can.
B. No, you can't because EC2 is not related to ARN.
C. No, you can't because you can't specify a particular Amazon EC2 resource in an IAM policy.
D. Yes, you can but only for the resources that are not affected by the action.

Answer: A
Explanation:
Some Amazon EC2 API actions allow you to include specific resources in your policy that can be

created or modified by the action. To specify a resource in the statement, you need to use its Amazon Resource Name (ARN).
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pdf

QUESTION 43
After you recommend Amazon Redshift to a client as an alternative solution to paying data warehouses to analyze his data, your client asks you to explain why you are recommending Redshift. Which of the following would be a reasonable response to his request?

A. It has high performance at scale as data and query complexity grows.
B. It prevents reporting and analytic processing from interfering with the performance of OLTP workloads.
C. You don't have the administrative burden of running your own data warehouse and dealing with setup, durability, monitoring, scaling, and patching.
D. All answers listed are a reasonable response to his question

Answer: D
Explanation:
Amazon Redshift delivers fast query performance by using columnar storage technology to improve I/O efficiency and parallelizing queries across multiple nodes. Redshift uses standard PostgreSQL JDBC and ODBC drivers, allowing you to use a wide range of familiar SQL clients. Data load speed scales linearly with cluster size, with integrations to Amazon S3, Amazon DynamoDB, Amazon Elastic MapReduce, Amazon Kinesis or any SSH-enabled host. AWS recommends Amazon Redshift for customers who have a combination of needs, such as:
High performance at scale as data and query complexity grows Desire to prevent reporting and analytic processing from interfering with the performance of OLTP workloads Large volumes of structured data to persist and query using standard SQL and existing BI tools Desire to the administrative burden of running one's own data warehouse and dealing with setup, durability, monitoring, scaling and patching
Reference: https://aws.amazon.com/running_databases/#redshift_anchor

QUESTION 44
One of the criteria for a new deployment is that the customer wants to use AWS Storage Gateway. However you are not sure whether you should use gateway-cached volumes or gateway-stored volumes or even what the differences are. Which statement below best describes those differences?

A. Gateway-cached lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally.
Gateway-stored enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.
B. Gateway-cached is free whilst gateway-stored is not.
C. Gateway-cached is up to 10 times faster than gateway-stored.
D. Gateway-stored lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally.
Gateway-cached enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.

Answer: A
Explanation:
Volume gateways provide cloud-backed storage volumes that you can mount as Internet Small Computer System Interface (iSCSI) devices from your on-premises application servers. The gateway supports the following volume configurations:

Gateway-cached volumes ?You store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Gateway-cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data. Gateway-stored volumes ?If you need low-latency access to your entire data set, you can configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3. This configuration provides durable and inexpensive off-site backups that you can recover to your local data center or Amazon EC2. For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2.
Reference: http://docs.aws.amazon.com/storagegateway/latest/userguide/volume-gateway.html

QUESTION 45
A user is launching an EC2 instance in the US East region. Which of the below mentioned options is recommended by AWS with respect to the selection of the availability zone?

A. Always select the AZ while launching an instance
B. Always select the US-East-1-a zone for HA
C. Do not select the AZ; instead let AWS select the AZ
D. The user can never select the availability zone while launching an instance

Answer: C
Explanation:
When launching an instance with EC2, AWS recommends not to select the availability zone (AZ). AWS specifies that the default Availability Zone should be accepted. This is because it enables AWS to select the best Availability Zone based on the system health and available capacity. If the user launches additional instances, only then an Availability Zone should be specified. This is to specify the same or different AZ from the running instances.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

QUESTION 46
A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB).
The website has a mix of dynamic and static content Users around the globe are reporting that the website is slow.
Which set of actions will improve website performance for users worldwide?

A. Create an Amazon CloudFront distribution and configure the ALB as an origin.
Then update the Amazon Route 53 record to point to the CloudFront distribution.
B. Create a latency-based Amazon Route 53 record for the ALB.
Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
C. Launch nev. EC2 instances hosting the same web application in different Regions closer to the users.
Then register the instances with the same ALB using cross-Region VPC peering.
D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances.
Then update an Amazon Route 53 record to point to the S3 buckets.

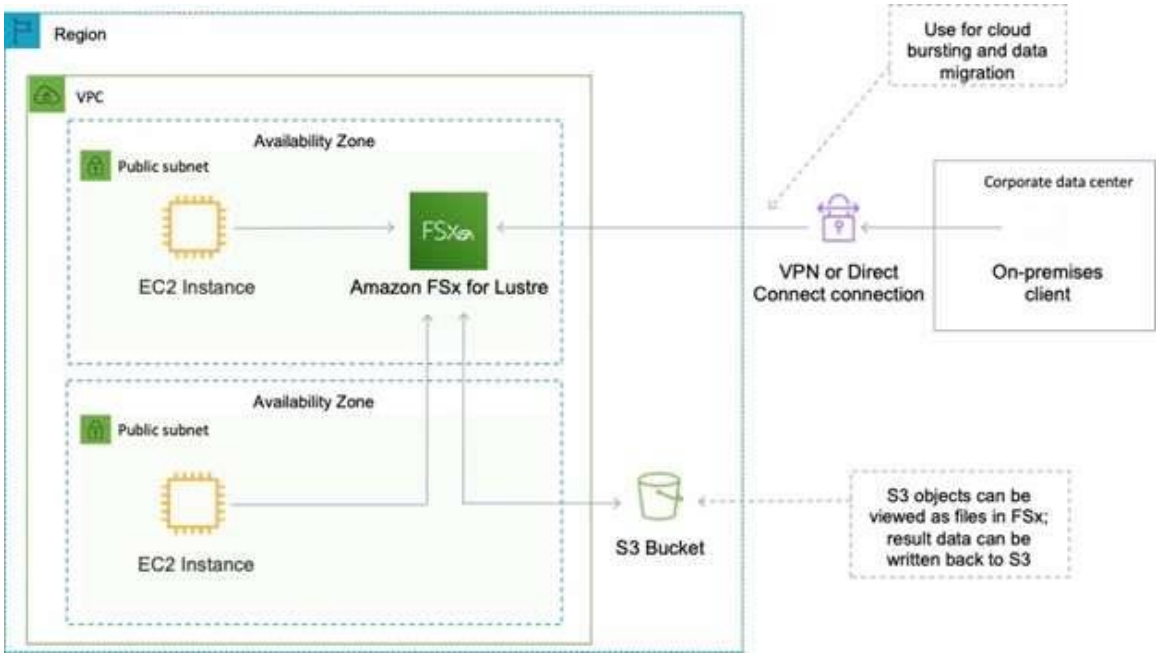
Answer: A
Explanation:
Amazon CloudFront is a content delivery network (CDN) that improves website performance by caching content at edge locations around the world. It can serve both dynamic and static content.

This is the best solution for improving the performance of the website.
CORRECT: "Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution" is the correct answer.
INCORRECT: "Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB" is incorrect. Latency routing routes based on the latency between the client and AWS. There is no mention in the answer about creating the new instances in another region therefore the only advantage is in using larger instance sizes. For a dynamic site this adds complexity in keeping the instances in sync.
INCORRECT: "Launch new EC2 instances hosting the same web application in different Regions closer to the users. Use an AWS Transit Gateway to connect customers to the closest region" is incorrect as Transit Gateway is a service for connecting on-premises networks and VPCs to a single gateway.
INCORRECT: "Migrate the website to an Amazon S3 bucket in the Regions closest to the users. Then create an Amazon Route 53 geolocation record to point to the S3 buckets" is incorrect as with S3 you can only host static websites, not dynamic websites.
References:
https://aws.amazon.com/cloudfront/dynamic-content/

QUESTION 47
A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud.
The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application and more economical cold storage to hold the data when the application is not actively running.
Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO)

A. Amazon S3 for cold data storage
B. Amazon EFS for cold data storage
C. Amazon S3 for high-performance parallel storage
D. Amazon FSx for Lustre for high-performance parallel storage
E. Amazon FSx for Windows for high-performance parallel storage

Answer: AD
Explanation:
Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high-performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA).
These workloads commonly require data to be presented via a fast and scalable file system interface, and typically have data sets stored on long-term data stores like Amazon S3.



Amazon FSx works natively with Amazon S3, making it easy to access your S3 data to run data processing workloads. Your S3 objects are presented as files in your file system, and you can write your results back to S3. This lets you run data processing workloads on FSx for Lustre and store your long- term data on S3 or on-premises data stores.
Therefore, the best combination for this scenario is to use S3 for cold data and FSx for Lustre for the parallel HPC job.
CORRECT: "Amazon S3 for cold data storage" is the correct answer.
CORRECT: "Amazon FSx for Lustre for high-performance parallel storage" is the correct answer.
INCORRECT: "Amazon EFS for cold data storage" is incorrect as FSx works natively with S3 which is also more economical.
INCORRECT: "Amazon S3 for high-performance parallel storage" is incorrect as S3 is not suitable for running high-performance computing jobs.
INCORRECT: "Amazon FSx for Windows for high-performance parallel storage" is incorrect as FSx for Lustre should be used for HPC use cases and use cases that require storing data on S3.
References:
https://aws.amazon.com/fsx/lustre/

QUESTION 48
A company has on-premises servers running a relational database.
The current database serves high read traffic for users in different locations.
The company wants to migrate to AWS with the least amount of effort.
The database solution should support disaster recovery and not affect the company's current traffic flow.
Which solution meets these requirements?

A. Use a database in Amazon RDS with Multi-AZ and at least one read replica
B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica
C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions
D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones

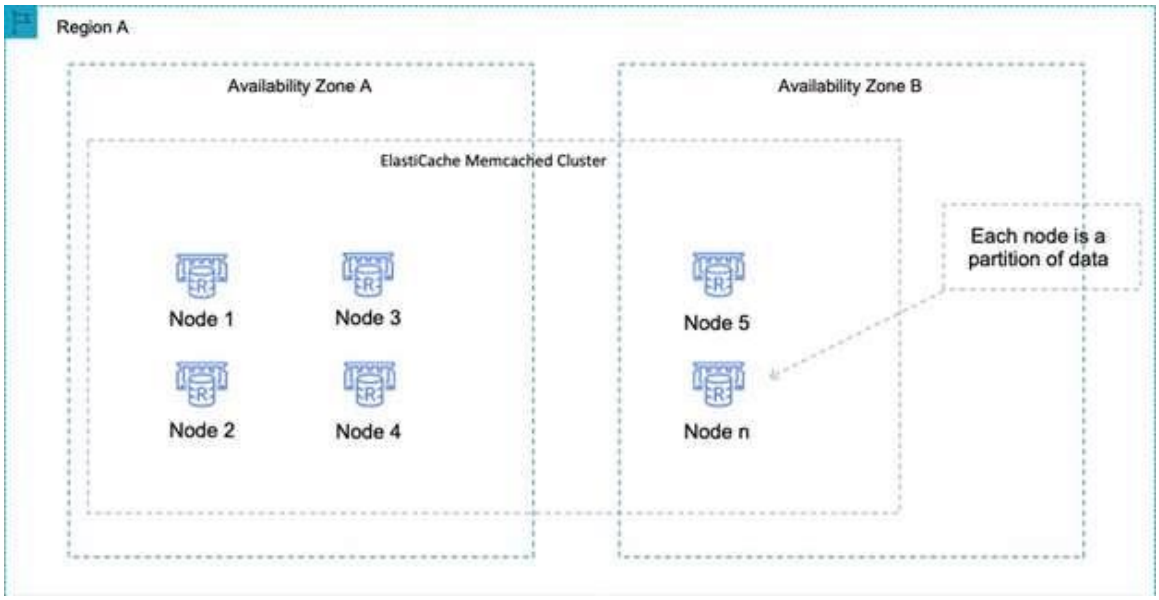
Answer: A

Explanation:
https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/

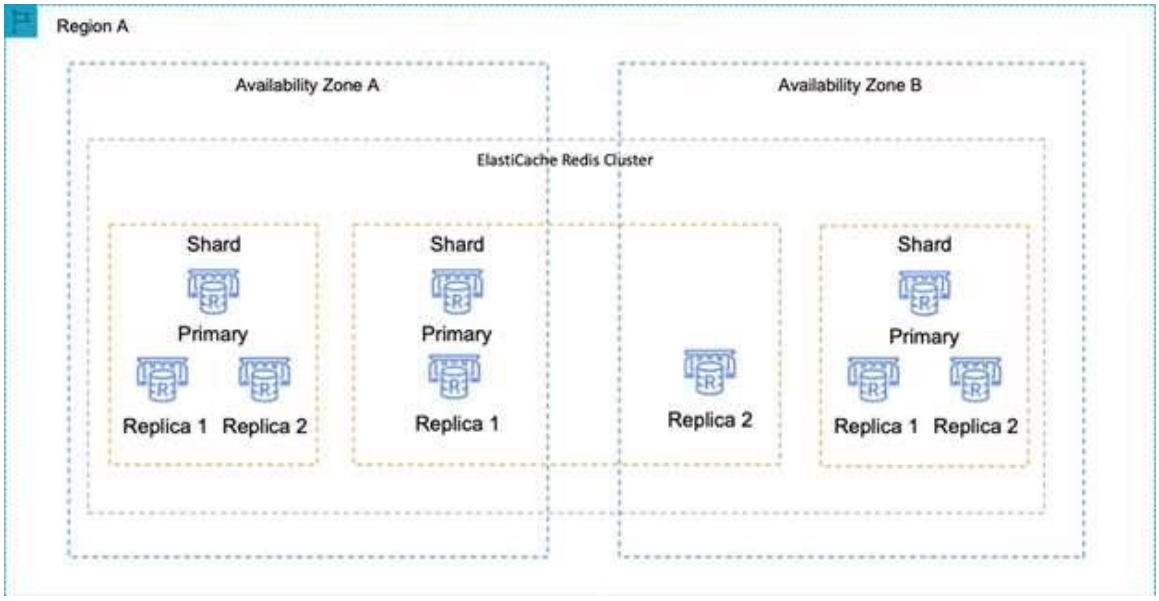
QUESTION 49
A media streaming company collects real-time data and stores it in a disk-optimized database system.
The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.
Which database should a solutions architect recommend'?

A. Amazon RDS for MySQL
B. Amazon RDS for PostgreSQL
C. Amazon ElastiCache for Redis
D. Amazon ElastiCache for Memcached

Answer: C
Explanation:
Amazon ElastiCache is an in-memory database. With ElastiCache Memcached there is no data replication or high availability. As you can see in the diagram, each node is a separate partition of data:



Therefore, the Redis engine must be used which does support both data replication and clustering. The following diagram shows a Redis architecture with cluster mode enabled:



CORRECT: "Amazon ElastiCache for Redis" is the correct answer.
INCORRECT: "Amazon ElastiCache for Memcached" is incorrect as Memcached does not support data replication or high availability.
INCORRECT: "Amazon RDS for MySQL" is incorrect as this is not an in-memory database.
INCORRECT: "Amazon RDS for PostgreSQL" is incorrect as this is not an in-memory database.
References:
https://aws.amazon.com/elasticache/redis/

QUESTION 50
A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer.
Based on the application's history, the company anticipates a spike in traffic during a holiday each year.
A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.
Which solution will meet these requirements?

A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%
B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand
C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period
D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are auto scaling EC2_INSTANCE_LAUNCH events

Answer: B
Explanation:
AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. AWS Auto Scaling refers to a collection of Auto Scaling capabilities across several AWS services.

The services within the AWS Auto Scaling family include:
・Amazon EC2 (known as Amazon EC2 Auto Scaling).

- Amazon ECS.
- Amazon DynamoDB.
- Amazon Aurora.

The scaling options define the triggers and when instances should be provisioned/de-provisioned.

There are four scaling options:

- Maintain – keep a specific or minimum number of instances running.
- Manual – use maximum, minimum, or a specific number of instances.
- Scheduled – increase or decrease the number of instances based on a schedule.
- Dynamic – scale based on real-time system metrics (e.g. CloudWatch metrics).

The following table describes the scaling options available and when to use them:

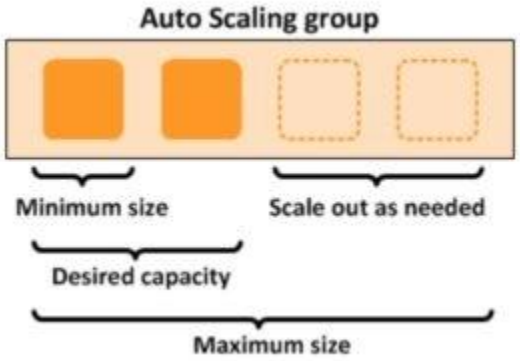
Scaling	What it is	When to use
Maintain	Ensures the required number of instances are running	Use when you always need a known number of instances running at all times
Manual	Manually change desired capacity via the console or CLI	Use when your needs change rarely enou that you're OK to make manual changes
Scheduled	Adjust min/max instances on specific dates/times or recurring time periods	Use when you know when your busy and quiet times are. Useful for ensuring enou instances are available *before* very busy times
Dynamic	Scale in response to system load or other triggers using metrics	Useful for changing capacity based on system utilization, e.g. CPU hits 80%

The scaling options are configured through Scaling Policies which determine when, if, and how the ASG scales and shrinks.

The following table describes the scaling policy types available for dynamic scaling policies and when to use them (more detail further down the page):

Scaling Policy	What it is	When to use
Target Tracking Policy	The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value	A use case is that you want to keep the aggregate CPU usage of your ASG at 70%
Simple Scaling Policy	Waits until health check and cool down period expires before re-evaluating	This is a more conservative way to add/remove instances. Useful when load is erratic. AWS recommend step scaling instead of simple in most cases
Step Scaling Policy	Increase or decrease the current capacity of your Auto Scaling group based on a set of scaling adjustments, known as step adjustments	Useful when you want to vary adjustments based on the size of the alarm breach

The diagram below depicts an Auto Scaling group with a Scaling policy set to a minimum size of 1 instance, a desired capacity of 2 instances, and a maximum size of 4 instances:



Amazon EC2 Auto Scaling supports sending Amazon SNS notifications when the following events occur.

QUESTION 51
A company has a two-tier application architecture that runs in public and private subnets Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet.
The web application instances and the database are running in a single Availability Zone (AZ).
Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

A. Create new public and private subnets in the same AZ for high availability
B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs

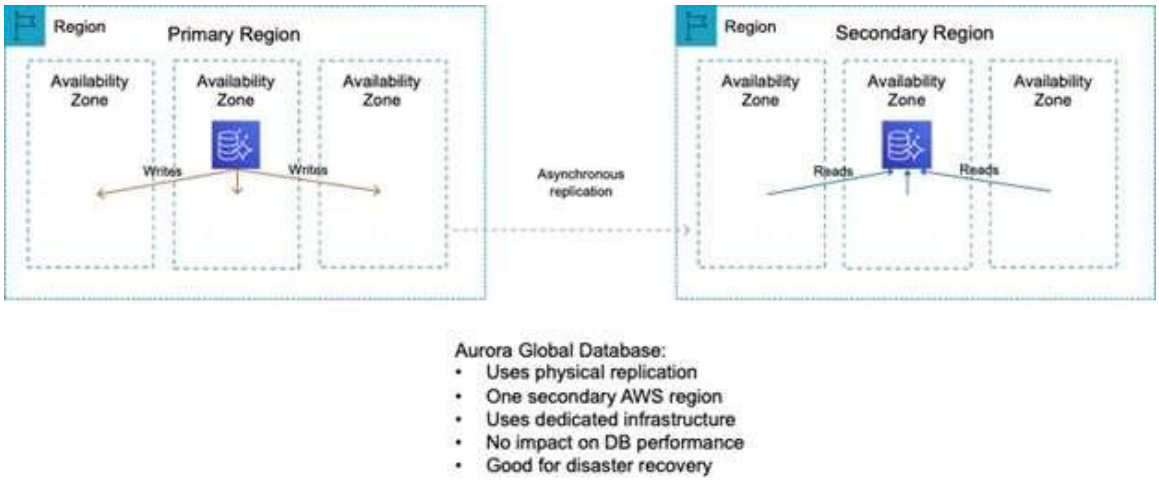
C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer
D. Create new public and private subnets in a new AZ Create a database using Amazon EC2 in one AZ
E. Create new public and private subnets in the same VPC each in a new AZ Migrate the database to an Amazon RDS multi-AZ deployment

Answer: BE
Explanation:
You would the EC2 instances to have high availability by placing them in multiple AZs.

QUESTION 52
A financial services company has a web application that serves users in the United States and Europe.
The application consists of a database tier and a web server tier.
The database tier consists of a MySQL database hosted in us-east-1 Amazon Route 53 geoproximity routing is used to direct traffic to instances in the closest Region.
A performance review of the system reveals that European users are not receiving the same level of query performance as those in the United States.
Which changes should be made to the database tier to improve performance?

A. Migrate the database to Amazon RDS for MySQL.
Configure Multi-AZ in one of the European Regions.
B. Migrate the database to Amazon DynamoDB.
Use DynamoDB global tables to enable replication to additional Regions.
C. Deploy MySQL instances in each Region.
Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance.
D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode.
Configure read replicas in one of the European Regions.

Answer: D
Explanation:
The issue here is latency with read queries being directed from Australia to UK which is great physical distance. A solution is required for improving read performance in Australia.
An Aurora global database consists of one primary AWS Region where your data is mastered, and up to five read-only, secondary AWS Regions.
Aurora replicates data to the secondary AWS Regions with typical latency of under a second. You issue write operations directly to the primary DB instance in the primary AWS Region.



This solution will provide better performance for users in the Australia Region for queries. Writes must still take place in the UK Region but read performance will be greatly improved.
CORRECT: "Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2" is the correct answer.
INCORRECT: "Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region" is incorrect. The database is located in UK. If the database is migrated to Australia then the reverse problem will occur. Multi-AZ does not assist with improving query performance across Regions.
INCORRECT: "Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions" is incorrect as a relational database running on MySQL is unlikely to be compatible with DynamoDB.
INCORRECT: "Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance" is incorrect as you can only put ALBs in front of the web tier, not the DB tier.
References:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html

QUESTION 53
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. 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.
B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint.
C. 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.
D. 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.

Answer: D
Explanation:
As the company's internet link is low-bandwidth uploading directly to Amazon S3 (ready for transition to Glacier) would saturate the link. The best alternative is to use AWS Snowball appliances. The Snowball edge appliance can hold up to 75 TB of data so 10 devices would be

required to migrate 750 TB of data.
Snowball moves data into AWS using a hardware device and the data is then copied into an Amazon S3 bucket of your choice. From there, lifecycle policies can transition the S3 objects to Amazon S3 Glacier.
CORRECT: "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" is the correct answer.
INCORRECT: "Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint" is incorrect as you cannot set a Glacier vault as the destination, it must be an S3 bucket. You also can't enforce a VPC endpoint using a bucket policy.
INCORRECT: "Create an AWS Direct Connect connection and migrate the data straight into Amazon Glacier" is incorrect as this is not the most cost- effective option and takes time to setup.
INCORRECT: "Use AWS Global Accelerator to accelerate upload and optimize usage of the available bandwidth" is incorrect as this service is not used for accelerating or optimizing the upload of data from on-premises networks.
References:
https://docs.aws.amazon.com/snowball/latest/developer-guide/specifications.html

QUESTION 54
A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance.
The company is launching a new reporting tool that will access the same data.
The reporting tool must be highly available and not impact the performance of the production application
How can this be achieved'?

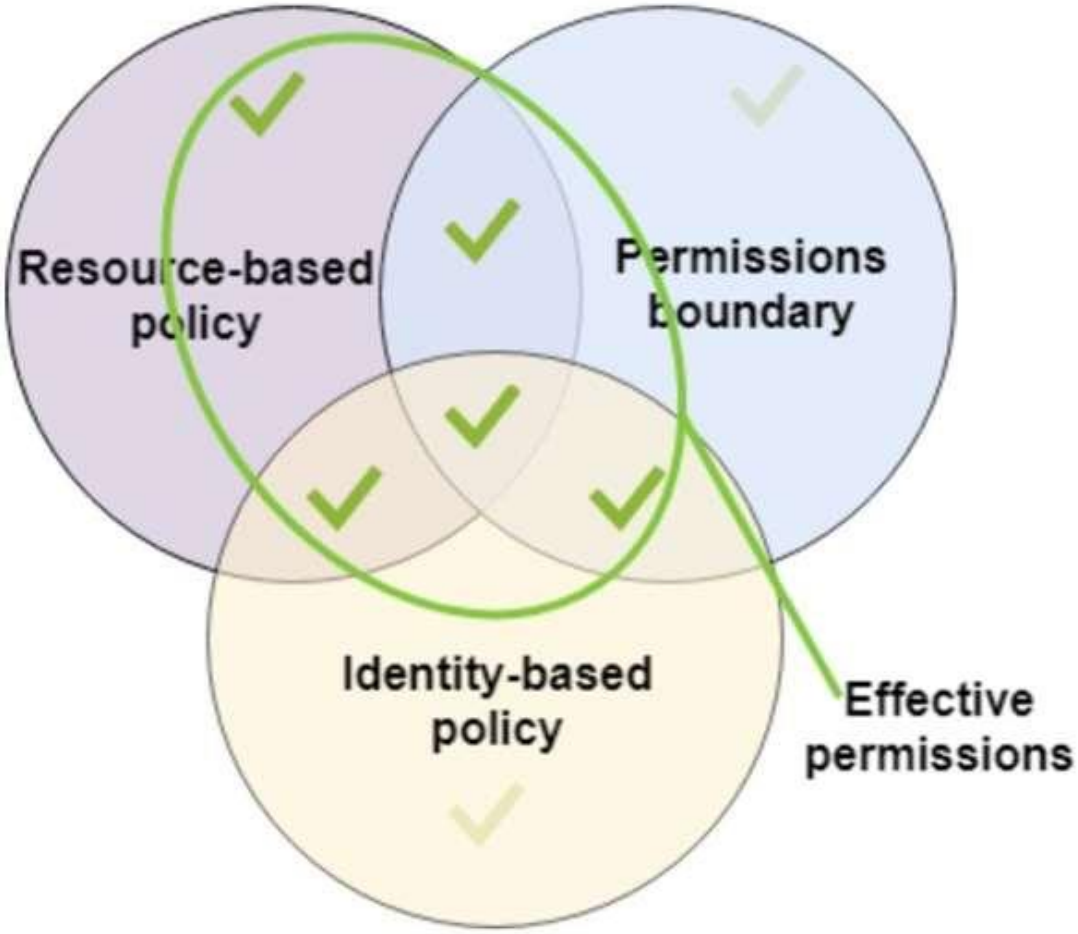
A. Create hourly snapshots of the production RDS DB instance.
B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance.
C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.
D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.

Answer: B
Explanation:
You can create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.
CORRECT: "Create a Multi-AZ RDS Read Replica of the production RDS DB instance" is the correct answer.
INCORRECT: "Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica" is incorrect. Read replicas are primarily used for horizontal scaling. The best solution for high availability is to use a Multi-AZ read replica.
INCORRECT: "Create a cross-region Multi-AZ deployment and create a read replica in the second region" is incorrect as you cannot create a cross- region Multi-AZ deployment with RDS.
INCORRECT: "Use Amazon Data Lifecycle Manager to automatically create and manage snapshots" is incorrect as using snapshots is not the best solution for high availability.
References:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html#USER_MySQL.Replication.ReadReplicas.MultiAZ

QUESTION 55
A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility.
However the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.
How should a solutions architect address this issue?

A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy
B. Use service control policies to disable IAM activity across all accounts in the organizational unit
C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team
D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

Answer: D
Explanation:
The permissions boundary for an IAM entity (user or role) sets the maximum permissions that the entity can have. This can change the effective permissions for that user or role. The effective permissions for an entity are the permissions that are granted by all the policies that affect the user or role. Within an account, the permissions for an entity can be affected by identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, or session policies.



Therefore, the solutions architect can set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.
CORRECT: "Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy" is the correct answer.
INCORRECT: "Create an Amazon SNS topic to send an alert every time a developer creates a new policy" is incorrect as this would mean investigating every incident which is not an efficient solution.
INCORRECT: "Use service control policies to disable IAM activity across all accounts in the organizational unit" is incorrect as this would prevent the developers from being able to work with IAM completely.
INCORRECT: "Prevent the developers from attaching any policies and assign all IAM duties to the security operations team" is incorrect as this is not necessary. The requirement is to allow developers to work with policies, the solution needs to find a secure way of achieving this.
References:
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

QUESTION 56
A user is storing a large number of objects on AWS S3. The user wants to implement the search functionality among the objects. How can the user achieve this?

A. Use the indexing feature of S3.
B. Tag the objects with the metadata to search on that.
C. Use the query functionality of S3.
D. Make your own DB system which stores the S3 metadata for the search functionality.

Answer: D
Explanation:
In Amazon Web Services, AWS S3 does not provide any query facility. To retrieve a specific object the user needs to know the exact bucket / object key. In this case it is recommended to have an own DB system which manages the S3 metadata and key mapping.
Reference: http://media.amazonwebservices.com/AWS_Storage_Options.pdf

QUESTION 57
After setting up a Virtual Private Cloud (VPC) network, a more experienced cloud engineer suggests that to achieve low network latency and high network throughput you should look into setting up a placement group. You know nothing about this, but begin to do some research about it and are especially curious about its limitations. Which of the below statements is wrong in describing the limitations of a placement group?

A. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed.
B. A placement group can span multiple Availability Zones.
C. You can't move an existing instance into a placement group.
D. A placement group can span peered VPCs

Answer: B
Explanation:
A placement group is a logical grouping of instances within a single Availability Zone. Using placement groups enables applications to participate in a low-latency, 10 Gbps network. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking.
Placement groups have the following limitations:
The name you specify for a placement group a name must be unique within your AWS account. A placement group can't span multiple Availability Zones. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed. We recommend using the same instance type for all instances in a placement group. You can't merge placement groups. Instead, you must terminate the instances in one placement group, and then relaunch those instances into the other placement group. A placement group can span peered VPCs; however, you will not get full-bisection bandwidth between instances in peered VPCs. For more information about VPC peering connections, see VPC Peering in the Amazon VPC User Guide. You can't move an existing instance into a placement group. You can create an AMI from your existing instance, and then launch a new instance from the AMI into a placement group.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

QUESTION 58
What is a placement group in Amazon EC2?

A. It is a group of EC2 instances within a single Availability Zone.

B. It the edge location of your web content.
C. It is the AWS region where you run the EC2 instance of your web content.
D. It is a group used to span multiple Availability Zones.

Answer: A
Explanation:
A placement group is a logical grouping of instances within a single Availability Zone.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

QUESTION 59
You are migrating an internal server on your DC to an EC2 instance with EBS volume. Your server disk usage is around 500GB so you just copied all your data to a 2TB disk to be used with AWS Import/Export. Where will the data be imported once it arrives at Amazon?

A. to a 2TB EBS volume
B. to an S3 bucket with 2 objects of 1TB
C. to an 500GB EBS volume
D. to an S3 bucket as a 2TB snapshot

Answer: B
Explanation:
An import to Amazon EBS will have different results depending on whether the capacity of your storage device is less than or equal to 1 TB or greater than 1 TB. The maximum size of an Amazon EBS snapshot is 1 TB, so if the device image is larger than 1 TB, the image is chunked and stored on Amazon S3. The target location is determined based on the total capacity of the device, not the amount of data on the device.
Reference: http://docs.aws.amazon.com/AWSImportExport/latest/DG/Concepts.html

QUESTION 60
A client needs you to import some existing infrastructure from a dedicated hosting provider to AWS to try and save on the cost of running his current website. He also needs an automated process that manages backups, software patching, automatic failure detection, and recovery. You are aware that his existing set up currently uses an Oracle database. Which of the following AWS databases would be best for accomplishing this task?

A. Amazon RDS
B. Amazon Redshift
C. Amazon SimpleDB
D. Amazon ElastiCache

Answer: A
Explanation:
Amazon RDS gives you access to the capabilities of a familiar MySQL, Oracle, SQL Server, or PostgreSQL database engine. This means that the code, applications, and tools you already use today with your existing databases can be used with Amazon RDS. Amazon RDS automatically patches the database software and backs up your database, storing the backups for a user-defined retention period and enabling point-in-time recovery.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

QUESTION 61
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.

Answer: C
Explanation:
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/

QUESTION 62
An edge location refers to which Amazon Web Service?

A. An edge location is refered to the network configured within a Zone or Region
B. An edge location is an AWS Region
C. An edge location is the location of the data center used for Amazon CloudFront.
D. An edge location is a Zone within an AWS Region

Answer: C
Explanation:
Amazon CloudFront is a content distribution network. A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers across the world. The location of the data center used for CDN is called edge location. Amazon CloudFront can cache static content at each edge location. This means that your popular static content (e.g., your site's logo, navigational images, cascading style sheets, JavaScript code, etc.) will be available at a nearby edge location for the browsers to download with low latency and improved performance for viewers. Caching popular static content with Amazon CloudFront also helps you offload requests for such files from your origin sever - CloudFront serves the cached copy when available and only makes a request to your origin server if the edge location receiving the browser's request does not have a copy of the file.
Reference: http://aws.amazon.com/cloudfront/

QUESTION 63
You are looking at ways to improve some existing infrastructure as it seems a lot of engineering resources are being taken up with basic management and monitoring tasks and the costs seem to be excessive. You are thinking of deploying Amazon ElasticCache to help. Which of the following statements is true in regards to ElasticCache?

A. You can improve load and response times to user actions and queries however the cost associated with scaling web applications will be more.
B. You can't improve load and response times to user actions and queries but you can reduce the cost associated with scaling web applications.
C. You can improve load and response times to user actions and queries however the cost associated with scaling web applications will remain the same.
D. You can improve load and response times to user actions and queries and also reduce the cost associated with scaling web applications.

Answer: D
Explanation:

Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory caching system, instead of relying entirely on slower disk-based databases. The service simplifies and offloads the management, monitoring and operation of in-memory cache environments, enabling your engineering resources to focus on developing applications. Using Amazon ElastiCache, you can not only improve load and response times to user actions and queries, but also reduce the cost associated with scaling web applications.
Reference: https://aws.amazon.com/elasticache/faqs/

QUESTION 64
Do Amazon EBS volumes persist independently from the running life of an Amazon EC2 instance?

A. Yes, they do but only if they are detached from the instance.
B. No, you cannot attach EBS volumes to an instance.
C. No, they are dependent.
D. Yes, they do.

Answer: D
Explanation:
An Amazon EBS volume behaves like a raw, unformatted, external block device that you can attach to a single instance. The volume persists independently from the running life of an Amazon EC2 instance.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION 65
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

Answer: A
Explanation:
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

QUESTION 66
A product team is creating a new application that will store a large amount of data.
The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances.
The application team believes the amount of space needed will continue to grow for the next 6 months.
Which set of actions should a solutions architect take to support these needs'?

A. Store the data in an Amazon EBS volume.

Mount the EBS volume on the application instances

B. Store the data in an Amazon EFS file system.
Mount the file system on the application instances.

C. Store the data in Amazon S3 Glacier.
Update the vault policy to allow access to the application instances.

D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
Update the bucket policy to allow access to the application instances.

Answer: B
Explanation:
Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on- premises resources. "It is built to scale on demand to petabytes without disrupting applications", "growing and shrinking automatically as you add and remove files", eliminating the need to provision and manage capacity to accommodate growth.
"The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances."

QUESTION 67
A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4.
The chief technology officer (CTO) wants to make the architecture highly available and cost-effective.
What should a solutions architect do to meet these requirements? (Select TWO.)

A. Increase the number of EC2 instances.
B. Decrease the number of EC2 instances
C. Configure a Network Load Balancer in front of the EC2 instances.
D. Configure an Application Load Balancer in front of the EC2 instances
E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

Answer: CE
Explanation:
The solutions architect must enable high availability for the architecture and ensure it is cost-effective. To enable high availability an Amazon EC2 Auto Scaling group should be created to add and remove instances across multiple availability zones.
In order to distribute the traffic to the instances the architecture should use a Network Load Balancer which operates at Layer 4. This architecture will also be cost-effective as the Auto Scaling group will ensure the right number of instances are running based on demand.
CORRECT: "Configure a Network Load Balancer in front of the EC2 instances" is a correct answer.
CORRECT: "Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically" is also a correct answer.
INCORRECT: "Increase the number of instances and use smaller EC2 instance types" is incorrect as this is not the most cost-effective option. Auto Scaling should be used to maintain the right number of active instances.
INCORRECT: "Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically" is incorrect as this is not highly available as it's a single AZ.
INCORRECT: "Configure an Application Load Balancer in front of the EC2 instances" is incorrect as an ALB operates at Layer 7 rather than Layer 4.
References:
https://docsaws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html

QUESTION 68
A company hosts an application on multiple Amazon EC2 instances.
The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue Occasional duplicate records are found in the RDS table.
The SQS queue does not contain any duplicate messages.
What should a solutions archived do to ensure messages are being processed once only?

A. Use the CreateQueue API call to create a new queue
B. Use the AddPermission API call to add appropriate permissions
C. Use the ReceiveMessage API call to set an appropriate wait time.
D. Use the ChangeMessageVisibility API call to increase the visibility timeout

Answer: D
Explanation:
Keyword: SQS queue writes to an Amazon RDS

From this, Option D best suite & other Options ruled out [Option A - You can't intruduce one more Queue in the existing one; Option B - only Permission & Option C - Only Retrieves Messages]

FIFO queues are designed to never introduce duplicate messages. However, your message producer might introduce duplicates in certain scenarios: for example, if the producer sends a message, does not receive a response, and then resends the same message. Amazon SQS APIs provide deduplication functionality that prevents your message producer from sending duplicates. Any duplicates introduced by the message producer are removed within a 5-minute deduplication interval.

For standard queues, you might occasionally receive a duplicate copy of a message (at-least-once delivery). If you use a standard queue, you must design your applications to be idempotent (that is, they must not be affected adversely when processing the same message more than once).

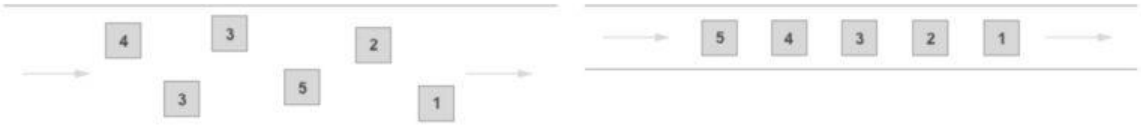
CreateQueue - You can't change the queue type after you create it and you can't convert an existing standard queue into a FIFO queue. You must either create a new FIFO queue for your application or delete your existing standard queue and recreate it as a FIFO queue.

AddPermission - You create a queue, you have full control access rights for the queue. Only you, the owner of the queue, can grant or deny permissions to the queue.

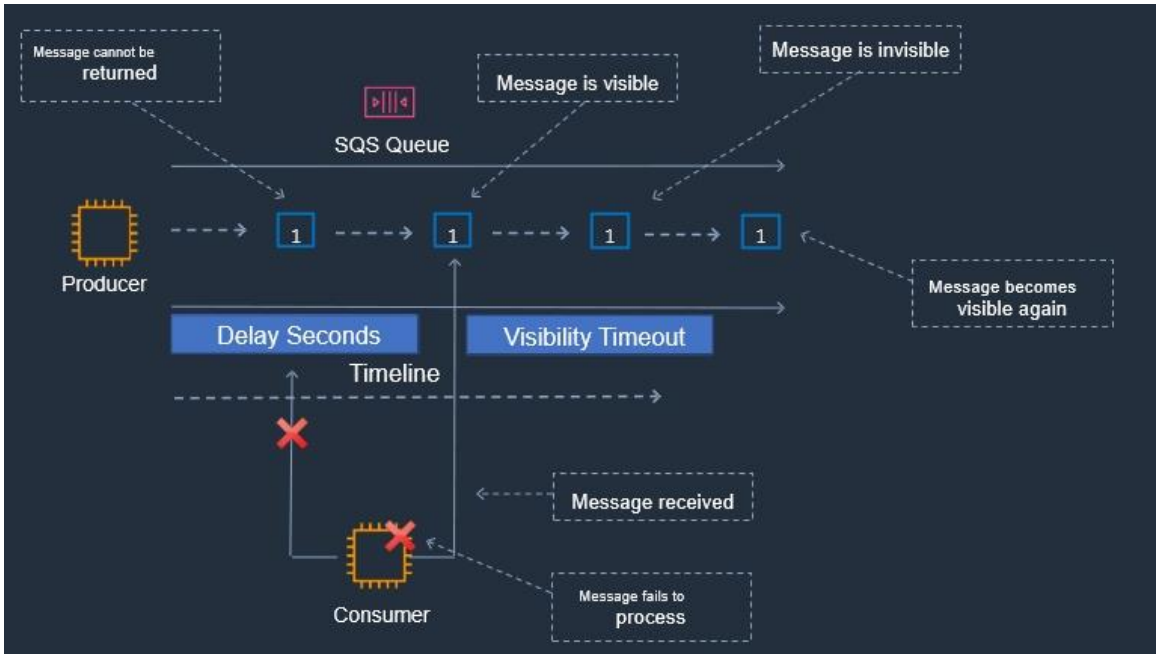
ReceiveMessage - Retrieves one or more messages (up to 10), from the specified queue.

FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it.

Standard Queues	FIFO Queues
Unlimited Throughput: Standard queues support a nearly unlimited number of transactions per second (TPS) per API action.	**High Throughput:** By default, FIFO queues support up to 300 messages per second (300 send, receive, or delete operations per second). When you batch 10 messages per operation (maximum), FIFO queues can support up to 3,000 messages per second. To request a limit increase, file a support request.
At-Least-Once Delivery: A message is delivered at least once, but occasionally more than one copy of a message is delivered.	**Exactly-Once Processing:** A message is delivered once and remains available until a consumer processes and deletes it. Duplicates aren't introduced into the queue.
Best-Effort Ordering: Occasionally, messages might be delivered in an order different from which they were sent.	**First-In-First-Out Delivery:** The order in which messages are sent and received is strictly preserved (i.e. First-In-First-Out).



Amazon SQS – Visibility Timeout



References:
https://aws.amazon.com/sqs/?nc2=h_ql_prod_ap_sqs
https://aws.amazon.com/sqs/faqs/
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html#FIFO-queues-exactly-once-processing
https://youtu.be/XrX7rb6M3jw
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_ChangeMessageVisibility.html

QUESTION 69
A solutions architect is designing an application for a two-step order process.

The first step is synchronous and must return to the user with little latency.
The second step takes longer, so it will be implemented in a separate component Orders must be processed exactly once and in the order in which they are received.
How should the solutions architect integrate these components?

A. Use Amazon SQS FIFO queues.
B. Use an AWS Lambda function along with Amazon SQS standard queues
C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic
D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Answer: A
Explanation:
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html "Standard queues provide at-least-once delivery, which means that each message is delivered at least once.
FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it. Duplicates are not introduced into the queue."

QUESTION 70
A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2.
The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.
Which EC2 configuration meets these requirements?

A. Launch the EC2 instances in a cluster placement group in one Availability Zone
B. Launch the EC2 instances in a spread placement group in one Availability Zone
C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs
D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones

Answer: A
Explanation:
When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload.
Depending on the type of workload, you can create a placement group using one of the following placement strategies:
Cluster - packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.
Partition - spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.
Spread - strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.
For this scenario, a cluster placement group should be used as this is the best option for providing low-latency network performance for a HPC application.
CORRECT: "Launch the EC2 instances in a cluster placement group in one Availability Zone" is the correct answer.
INCORRECT: "Launch the EC2 instances in a spread placement group in one Availability Zone" is incorrect as the spread placement group is used to spread instances across distinct underlying

hardware.
INCORRECT: "Launch the EC2 instances in an Auto Scaling group in two Regions. Place a Network Load Balancer in front of the instances" is incorrect as this does not achieve the stated requirement to provide low-latency, high throughput network performance between instances. Also, you cannot use an ELB across Regions.
INCORRECT: "Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones" is incorrect as this does not reduce network latency or improve performance.
References:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

QUESTION 71
A company is planning to use Amazon S3 lo store images uploaded by its users.
The images must be encrypted at rest in Amazon S3.
The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.
What should a solutions architect use to accomplish this?

A. Server-Side Encryption with keys stored in an S3 bucket
B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Answer: D
Explanation:
SSE-KMS requires that AWS manage the data key but you manage the customer master key (CMK) in AWS KMS. You can choose a customer managed CMK or the AWS managed CMK for Amazon S3 in your account.
Customer managed CMKs are CMKs in your AWS account that you create, own, and manage. You have full control over these CMKs, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the CMK, and scheduling the CMKs for deletion.
For this scenario, the solutions architect should use SSE-KMS with a customer managed CMK. That way KMS will manage the data key but the company can configure key policies defining who can access the keys.
CORRECT: "Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)" is the correct answer.
INCORRECT: "Server-Side Encryption with keys stored in an S3 bucket" is incorrect as you cannot store your keys in a bucket with server-side encryption
INCORRECT: "Server-Side Encryption with Customer-Provided Keys (SSE-C)" is incorrect as the company does not want to manage the keys.
INCORRECT: "Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)" is incorrect as the company needs to manage access control for the keys which is not possible when they're managed by Amazon.
References:
https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse
https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys

QUESTION 72
An Amazon EC2 administrator created the following policy associated with an IAM group containing several users.

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Effect": "Allow",
               "Action": "ec2:TerminateInstances",
               "Resources": "*",
               "Condition": {
                    "IpAddress": {
                         "aws:SourceIp": "10.100.100.0/24"
                    }
               }
          },
          {
               "Effect": "Deny",
               "Action": "ec2:*",
               "Resources": "*",
               "Condition": {
                    "StringNotEquals": {
                         "ec2:Region": "us-east-1"
                    }
               }
          }
     ]
}
```

What is the effect of this policy?

A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
B. Users can terminate an EC2 instance with the IP address 10.100. 1001 in the us-east-1 Region.
C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

Answer: C
Explanation:
What the policy means:
1. Allow termination of any instance if user's source ip address is 10.100.100.254.
2. Deny termination of instances that are not in the us-east-1 region.
Combining this two, you get:
"Allow instance termination in the us-east-1 region if the user's source ip address is 10.100.100.254. Deny termination operation on other regions."

QUESTION 73
A company is running an ecommerce application on Amazon EC2.
The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage.
The application requires 50 instances 80% of the time.
Which solution should be used to minimize costs?

A. Purchase Reserved Instances to cover 250 instances
B. Purchase Reserved Instances to cover 80 instances.
Use Spot Instances to cover the remaining instances
C. Purchase On-Demand Instances to cover 40 instances.
Use Spot Instances to cover the remaining instances
D. Purchase Reserved Instances to cover 50 instances.
Use On-Demand and Spot Instances to cover the remaining instances

Answer: D

QUESTION 74
Does DynamoDB support in-place atomic updates?

A. Yes
B. No
C. It does support in-place non-atomic updates
D. It is not defined

Answer: A
Explanation:
DynamoDB supports in-place atomic updates.
Reference:
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WorkingWithItems.html#WorkingWithItems.AtomicCounters

QUESTION 75
Your manager has just given you access to multiple VPN connections that someone else has recently set up between all your company's offices. She needs you to make sure that the communication between the VPNs is secure. Which of the following services would be best for providing a low-cost hub-and-spoke model for primary or backup connectivity between these remote offices?

A. Amazon CloudFront
B. AWS Direct Connect
C. AWS CloudHSM
D. AWS VPN CloudHub

Answer: D
Explanation:
If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who would like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

QUESTION 76
Amazon EC2 provides a ____. It is an HTTP or HTTPS request that uses the HTTP verbs GET or POST.

A. web database
B. .net framework
C. Query API
D. C library

Answer: C
Explanation:
Amazon EC2 provides a Query API. These requests are HTTP or HTTPS requests that use the HTTP verbs GET or POST and a Query parameter named Action.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/APIReference/making-api-requests.html

QUESTION 77
In Amazon AWS, which of the following statements is true of key pairs?

A. Key pairs are used only for Amazon SDKs.
B. Key pairs are used only for Amazon EC2 and Amazon CloudFront.
C. Key pairs are used only for Elastic Load Balancing and AWS IAM.
D. Key pairs are used for all Amazon services.

Answer: B
Explanation:
Key pairs consist of a public and private key, where you use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.
Reference: http://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html

QUESTION 78
Does Amazon DynamoDB support both increment and decrement atomic operations?

A. Only increment, since decrement are inherently impossible with DynamoDB's data model.
B. No, neither increment nor decrement operations.
C. Yes, both increment and decrement operations.
D. Only decrement, since increment are inherently impossible with DynamoDB's data model.

Answer: C
Explanation:
Amazon DynamoDB supports increment and decrement atomic operations.
Reference:
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/APISummary.html

QUESTION 79
An organization has three separate AWS accounts, one each for development, testing, and production. The organization wants the testing team to have access to certain AWS resources in the production account. How can the organization achieve this?

A. It is not possible to access resources of one account with another account.
B. Create the IAM roles with cross account access.
C. Create the IAM user in a test account, and allow it access to the production environment with the IAM policy.
D. Create the IAM users with cross account access.

Answer: B
Explanation:
An organization has multiple AWS accounts to isolate a development environment from a testing or production environment. At times the users from one account need to access resources in the other account, such as promoting an update from the development environment to the production environment. In this case the IAM role with cross account access will provide a solution. Cross account access lets one account share access to their resources with users in the other AWS accounts.
Reference: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 80
You need to import several hundred megabytes of data from a local Oracle database to an Amazon RDS DB instance. What does AWS recommend you use to accomplish this?

A. Oracle export/import utilities
B. Oracle SQL Developer
C. Oracle Data Pump
D. DBMS_FILE_TRANSFER

Answer: C
Explanation:
How you import data into an Amazon RDS DB instance depends on the amount of data you have and the number and variety of database objects in your database. For example, you can use Oracle SQL Developer to import a simple, 20 MB database; you want to use Oracle Data Pump to import complex databases or databases that are several hundred megabytes or several terabytes in size.
Reference:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Oracle.Procedural.Importing.html

QUESTION 81
A user has created an EBS volume with 1000 IOPS. What is the average IOPS that the user will get for most of the year as per EC2 SLA if the instance is attached to the EBS optimized instance?

A. 950
B. 990
C. 1000
D. 900

Answer: D
Explanation:
As per AWS SLA if the instance is attached to an EBS-Optimized instance, then the Provisioned IOPS volumes are designed to deliver within 10% of the provisioned IOPS performance 99.9% of the time in a given year. Thus, if the user has created a volume of 1000 IOPS, the user will get a minimum 900 IOPS 99.9% time of the year.
Reference: http://aws.amazon.com/ec2/faqs/

QUESTION 82
You need to migrate a large amount of data into the cloud that you have stored on a hard disk and you decide that the best way to accomplish this is with AWS Import/Export and you mail the hard disk to AWS. Which of the following statements is incorrect in regards to AWS

Import/Export?

A. It can export from Amazon S3
B. It can Import to Amazon Glacier
C. It can export from Amazon Glacier.
D. It can Import to Amazon EBS

Answer: C
Explanation:
AWS Import/Export supports:
Import to Amazon S3
Export from Amazon S3
Import to Amazon EBS
Import to Amazon Glacier
AWS Import/Export does not currently support export from Amazon EBS or Amazon Glacier.
Reference: https://docs.aws.amazon.com/AWSImportExport/latest/DG/whatisdisk.html

QUESTION 83
You are in the process of creating a Route 53 DNS failover to direct traffic to two EC2 zones. Obviously, if one fails, you would like Route 53 to direct traffic to the other region. Each region has an ELB with some instances being distributed. What is the best way for you to configure the Route 53 health check?

A. Route 53 doesn't support ELB with an internal health check.You need to create your own Route 53 health check of the ELB
B. Route 53 natively supports ELB with an internal health check. Turn "Evaluate target health" off and "Associate with Health Check" on and R53 will use the ELB's internal health check.
C. Route 53 doesn't support ELB with an internal health check. You need to associate your resource record set for the ELB with your own health check
D. Route 53 natively supports ELB with an internal health check. Turn "Evaluate target health" on and "Associate with Health Check" off and R53 will use the ELB's internal health check.

Answer: D
Explanation:
With DNS Failover, Amazon Route 53 can help detect an outage of your website and redirect your end users to alternate locations where your application is operating properly. When you enable this feature, Route 53 uses health checks--regularly making Internet requests to your application's endpoints from multiple locations around the world--to determine whether each endpoint of your application is up or down. To enable DNS Failover for an ELB endpoint, create an Alias record pointing to the ELB and set the "Evaluate Target Health" parameter to true. Route 53 creates and manages the health checks for your ELB automatically. You do not need to create your own Route 53 health check of the ELB. You also do not need to associate your resource record set for the ELB with your own health check, because Route 53 automatically associates it with the health checks that Route 53 manages on your behalf. The ELB health check will also inherit the health of your backend instances behind that ELB.
Reference: http://aws.amazon.com/about-aws/whats-new/2013/05/30/amazon-route-53-adds-elb-integration-for-dns- failover/

QUESTION 84
A user wants to use an EBS-backed Amazon EC2 instance for a temporary job. Based on the input data, the job is most likely to finish within a week. Which of the following steps should be followed to terminate the instance automatically once the job is finished?

A. Configure the EC2 instance with a stop instance to terminate it.
B. Configure the EC2 instance with ELB to terminate the instance when it remains idle.
C. Configure the CloudWatch alarm on the instance that should perform the termination action once the instance is idle.
D. Configure the Auto Scaling schedule activity that terminates the instance after 7 days.

Answer: C
Explanation:
Auto Scaling can start and stop the instance at a pre-defined time. Here, the total running time is unknown. Thus, the user has to use the CloudWatch alarm, which monitors the CPU utilization. The user can create an alarm that is triggered when the average CPU utilization percentage has been lower than 10 percent for 24 hours, signaling that it is idle and no longer in use. When the utilization is below the threshold limit, it will terminate the instance as a part of the instance action.
Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html

QUESTION 85
Which of the following is true of Amazon EC2 security group?

A. You can modify the outbound rules for EC2-Classic.
B. You can modify the rules for a security group only if the security group controls the traffic for just one instance.
C. You can modify the rules for a security group only when a new instance is created.
D. You can modify the rules for a security group at any time.

Answer: D
Explanation:
A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 86
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

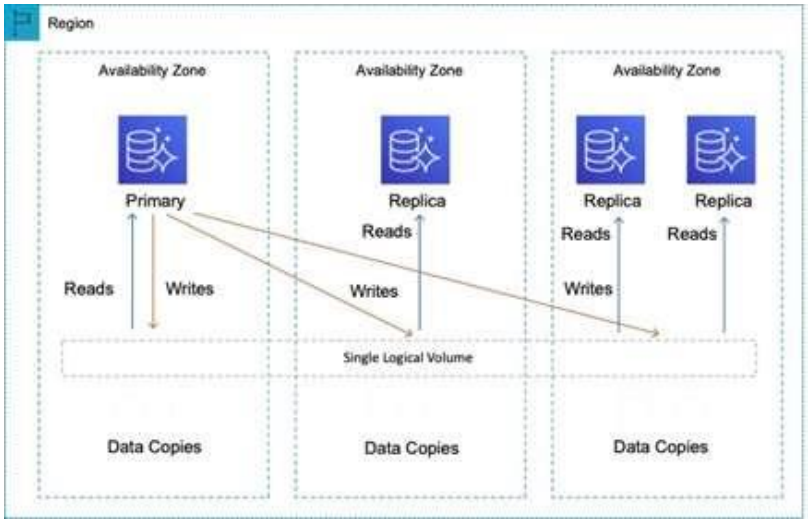
Answer: B
Explanation:
By default, all AWS accounts are limited to 5 Elastic IP addresses per region for each AWS account, because public (IPv4) Internet addresses are a scarce public resource. AWS strongly encourages you to use an EIP primarily for load balancing use cases, and use DNS hostnames

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

QUESTION 87
An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database.
What should the solutions architect do to separate the read requests from the write requests?

A. Enable read-through caching on the Amazon Aurora database
B. Update the application to read from the Multi-AZ standby instance
C. Create a read replica and modify the application to use the appropriate endpoint
D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Answer: C
Explanation:
Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region.
The DB cluster volume is made up of multiple copies of the data for the DB cluster. However, the data in the cluster volume is represented as a single, logical volume to the primary instance and to Aurora Replicas in the DB cluster.



Aurora Fault Tolerance
- Fault tolerance across 3 AZs
- Single logical volume
- Aurora Replicas scale-out read requests
- Up to 15 Aurora Replicas with sub-10ms replica lag
- Aurora Replicas are independent endpoints
- Can promote Aurora Replica to be a new primary or create new primary
- Set priority (tiers) on Aurora Replicas to control order of promotion
- Can use Auto Scaling to add replicas

As well as providing scaling for reads, Aurora Replicas are also targets for multi-AZ. In this case the solutions architect can update the application to read from the Multi-AZ standby instance.
References:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html

QUESTION 88
An application runs on Amazon EC2 instances across multiple Availability Zones.
The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer.
The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances m the group?

A. Use a simple scaling policy to dynamically scale the Auto Scaling group
B. Use a target tracking policy to dynamically scale the Auto Scaling group
C. Use an AWS Lambda function to update the desired Auto Scaling group capacity
D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group

Answer: B
Explanation:
With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value.
The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to the changes in the metric due to a changing load pattern.
CORRECT: "Use a target tracking policy to dynamically scale the Auto Scaling group" is the correct answer.
INCORRECT: "Use a simple scaling policy to dynamically scale the Auto Scaling group" is incorrect as target tracking is a better way to keep the aggregate CPU usage at around 40%
INCORRECT: "Use an AWS Lambda function to update the desired Auto Scaling group capacity" is incorrect as this can be done automatically.
INCORRECT: "Use scheduled scaling actions to scale up and scale down the Auto Scaling group" is incorrect as dynamic scaling is required to respond to changes in utilization.
References:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html

QUESTION 89
A company runs a multi-tier web application that hosts news content.
The application runs on Amazon EC2 instances behind an Application Load Balancer.
The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database.
A solutions architect needs to make the application more resilient to periodic increases in request rates.
Which architecture should the solutions architect implement? (Select TWO)

A. Add AWS Shield.
B. Add Aurora Replicas
C. Add AWS Direct Connect
D. Add AWS Global Accelerator.
E. Add an Amazon CloudFront distribution in front of the Application Load Balancer

Answer: BE
Explanation
The architecture is already highly resilient but the may be subject to performance degradation if there are sudden increases in request rates. To resolve this situation Amazon Aurora Read Replicas can be used to serve read traffic which offloads requests from the main database. On the frontend an Amazon CloudFront distribution can be placed in front of the ALB and this will cache content for better performance and also offloads requests from the backend.

CORRECT: "Add Amazon Aurora Replicas" is the correct answer.
CORRECT: "Add an Amazon CloudFront distribution in front of the ALB" is the correct answer.

INCORRECT: "Add and Amazon WAF in front of the ALB" is incorrect. A web application firewall protects applications from malicious attacks. It does not improve performance.
INCORRECT: "Add an Amazon Transit Gateway to the Availability Zones" is incorrect as this is used to connect on-premises networks to VPCs.
INCORRECT: "Add an Amazon Global Accelerator endpoint" is incorrect as this service is used for directing users to different instances of the application in different regions based on latency.

References:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

QUESTION 90
A solutions architect is optimizing a website for an upcoming musical event Videos of the performances will be streamed in real time and then will be available on demand.
The event is expected to attract a global online audience.
Which service will improve the performance of both the real-time and on-demand streaming?

A. Amazon CloudFront
B. AWS Global Accelerator
C. Amazon Route 53
D. Amazon S3 Transfer Acceleration

Answer: A
Explanation:
Amazon CloudFront can be used to stream video to users across the globe using a wide variety of protocols that are layered on top of HTTP. This can include both on-demand video as well as real time streaming video.
CORRECT: "Amazon CloudFront" is the correct answer.
INCORRECT: "AWS Global Accelerator" is incorrect as this would be an expensive way of getting the content closer to users compared to using CloudFront. As this is a use case for CloudFront and there are so many edge locations it is the better option.
INCORRECT: "Amazon Route 53" is incorrect as you still need a solution for getting the content closer to users.
INCORRECT: "Amazon S3 Transfer Acceleration" is incorrect as this is used to accelerate uploads of data to Amazon S3 buckets.
References:
https://aws.amazon.com/cloudfront/streaming/
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html

QUESTION 91
A company serves content to its subscribers across the world using an application running on AWS.
The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB).
Due to a recent change in copyright restrictions the chief information officer (CIO) wants to block access for certain countries.
Which action will meet these requirements?

A. Modify the ALB security group to deny incoming traffic from blocked countries
B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries
C. Use Amazon CloudFront to serve the application and deny access to blocked countries
D. Use ALB listener rules to return access denied responses to incoming traffic from blocked

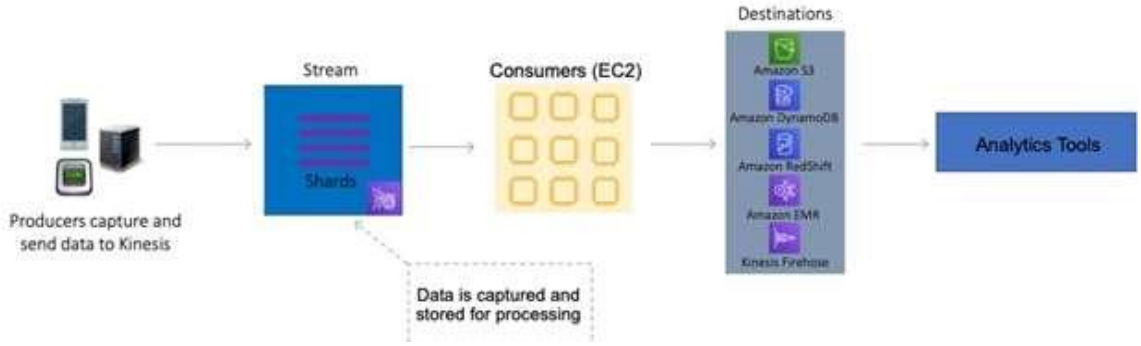
countries

Answer: C
Explanation:
When a user requests your content, CloudFront typically serves the requested content regardless of where the user is located. If you need to prevent users in specific countries from accessing your content, you can use the CloudFront geo restriction feature to do one of the following:
Allow your users to access your content only if they're in one of the countries on a whitelist of approved countries.
Prevent your users from accessing your content if they're in one of the countries on a blacklist of banned countries.
For example, if a request comes from a country where, for copyright reasons, you are not authorized to distribute your content, you can use CloudFront geo restriction to block the request. This is the easiest and most effective way to implement a geographic restriction for the delivery of content.
CORRECT: "Use Amazon CloudFront to serve the application and deny access to blocked countries" is the correct answer.
INCORRECT: "Use a Network ACL to block the IP address ranges associated with the specific countries" is incorrect as this would be extremely difficult to manage.
INCORRECT: "Modify the ALB security group to deny incoming traffic from blocked countries" is incorrect as security groups cannot block traffic by country.
INCORRECT: "Modify the security group for EC2 instances to deny incoming traffic from blocked countries" is incorrect as security groups cannot block traffic by country.
References:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html

QUESTION 92
A manufacturing company wants to implement predictive maintenance on its machinery equipment.
The company will install thousands of IoT sensors that will send data to AWS in real time.
A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.
Which solution would be MOST efficient?

A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.
B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS.
C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.
D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset.
Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Answer: A
Explanation:
Amazon Kinesis Data Streams collect and process data in real time. A Kinesis data stream is a set of shards. Each shard has a sequence of data records. Each data record has a sequence number that is assigned by Kinesis Data Streams. A shard is a uniquely identified sequence of data records in a stream.
A partition key is used to group data by shard within a stream. Kinesis Data Streams segregates the data records belonging to a stream into multiple shards. It uses the partition key that is associated with each data record to determine which shard a given data record belongs to.



For this scenario, the solutions architect can use a partition key for each device. This will ensure the records for that device are grouped by shard and the shard will ensure ordering. Amazon S3 is a valid destination for saving the data records.
CORRECT: "Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose to save data to Amazon S3" is the correct answer.
INCORRECT: "Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS" is incorrect as you cannot save data to EBS from Kinesis.
INCORRECT: "Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS" is incorrect as SQS is not the most efficient service for streaming, real time data.
INCORRECT: "Use an Amazon SQS standard queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3" is incorrect as SQS is not the most efficient service for streaming, real time data.
References:
https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html

QUESTION 93
A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB).
An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway.
When requests to the client application increase, the NAT gateway costs are higher than expected.
A solutions architect has configured the ALB to be internal.
Which combination of architectural changes will reduce the NAT gateway costs'? (Select TWO)

A. Configure a VPC peering connection between the two VPCs.
Access the API using the private address
B. Configure an AWS Direct Connect connection between the two VPCs.
Access the API using the private address.
C. Configure a ClassicLink connection for the API into the client VPC.
Access the API using the ClassicLink address.
D. Configure a PrivateLink connection for the API into the client VPC.
Access the API using the PrivateLink address.
E. Configure an AWS Resource Access Manager connection between the two accounts.
Access the API using the private address

Answer: AD
Explanation:

PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify the network architecture.
https://www.levvel.io/resource-library/aws-api-gateway-for-multi-account-architecture
There is no API listed in shareable resources for RAM.
https://docs.aws.amazon.com/ram/latest/userguide/shareable.html

QUESTION 94
In Amazon EC2, partial instance-hours are billed _____.

A. per second used in the hour
B. per minute used
C. by combining partial segments into full hours
D. as full hours

Answer: D
Explanation:
Partial instance-hours are billed to the next hour.
Reference: http://aws.amazon.com/ec2/faqs/

QUESTION 95
In EC2, what happens to the data in an instance store if an instance reboots (either intentionally or unintentionally)?

A. Data is deleted from the instance store for security reasons.
B. Data persists in the instance store.
C. Data is partially present in the instance store.
D. Data in the instance store will be lost.

Answer: B
Explanation:
The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists. However, data on instance store volumes is lost under the following circumstances.
Failure of an underlying drive
Stopping an Amazon EBS-backed instance
Terminating an instance
Reference:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/InstanceStorage.html

QUESTION 96
You are setting up a VPC and you need to set up a public subnet within that VPC. Which following requirement must be met for this subnet to be considered a public subnet?

A. Subnet's traffic is not routed to an internet gateway but has its traffic routed to a virtual private gateway.
B. Subnet's traffic is routed to an internet gateway.
C. Subnet's traffic is not routed to an internet gateway.
D. None of these answers can be considered a public subnet.

Answer: B
Explanation:

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can configure your VPC: you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings. A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the Internet. If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet. If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet. If a subnet doesn't have a route to the internet gateway, but has its traffic routed to a virtual private gateway, the subnet is known as a VPN-only subnet.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

QUESTION 97
Can you specify the security group that you created for a VPC when you launch an instance in EC2-Classic?

A. No, you can specify the security group created for EC2-Classic when you launch a VPC instance.
B. No
C. Yes
D. No, you can specify the security group created for EC2-Classic to a non-VPC based instance only.

Answer: B
Explanation:
If you're using EC2-Classic, you must use security groups created specifically for EC2-Classic. When you launch an instance in EC2-Classic, you must specify a security group in the same region as the instance. You can't specify a security group that you created for a VPC when you launch an instance in EC2-Classic.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#ec2-classic-securit y-groups

QUESTION 98
While using the EC2 GET requests as URLs, the _____ is the URL that serves as the entry point for the web service.

A. token
B. endpoint
C. action
D. None of these

Answer: B
Explanation:
The endpoint is the URL that serves as the entry point for the web service.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-query-api.html

QUESTION 99
You have been asked to build a database warehouse using Amazon Redshift. You know a little about it, including that it is a SQL data warehouse solution, and uses industry standard ODBC and JDBC connections and PostgreSQL drivers. However you are not sure about what sort of storage it uses for database tables. What sort of storage does Amazon Redshift use for database

tables?

A. InnoDB Tables
B. NDB data storage
C. Columnar data storage
D. NDB CLUSTER Storage

Answer: C
Explanation:
Amazon Redshift achieves efficient storage and optimum query performance through a combination of massively parallel processing, columnar data storage, and very efficient, targeted data compression encoding schemes.
Columnar storage for database tables is an important factor in optimizing analytic query performance because it drastically reduces the overall disk I/O requirements and reduces the amount of data you need to load from disk.
Reference:
http://docs.aws.amazon.com/redshift/latest/dg/c_columnar_storage_disk_mem_mgmnt.html

QUESTION 100
You are checking the workload on some of your General Purpose (SSD) and Provisioned IOPS (SSD) volumes and it seems that the I/O latency is higher than you require. You should probably check the _____ to make sure that your application is not trying to drive more IOPS than you have provisioned.

A. Amount of IOPS that are available
B. Acknowledgement from the storage subsystem
C. Average queue length
D. Time it takes for the I/O operation to complete

Answer: C
Explanation:
In EBS workload demand plays an important role in getting the most out of your General Purpose (SSD) and Provisioned IOPS (SSD) volumes. In order for your volumes to deliver the amount of IOPS that are available, they need to have enough I/O requests sent to them. There is a relationship between the demand on the volumes, the amount of IOPS that are available to them, and the latency of the request (the amount of time it takes for the I/O operation to complete).
Latency is the true end-to-end client time of an I/O operation; in other words, when the client sends a IO, how long does it take to get an acknowledgement from the storage subsystem that the IO read or write is complete.
If your I/O latency is higher than you require, check your average queue length to make sure that your application is not trying to drive more IOPS than you have provisioned. You can maintain high IOPS while keeping latency down by maintaining a low average queue length (which is achieved by provisioning more IOPS for your volume).
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-workload-demand.html

QUESTION 101
Which of the below mentioned options is not available when an instance is launched by Auto Scaling with EC2 Classic?

A. Public IP
B. Elastic IP
C. Private DNS

D. Private IP

Answer: B
Explanation:
Auto Scaling supports both EC2 classic and EC2-VPC. When an instance is launched as a part of EC2 classic, it will have the public IP and DNS as well as the private IP and DNS.
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html

QUESTION 102
You have been given a scope to deploy some AWS infrastructure for a large organisation. The requirements are that you will have a lot of EC2 instances but may need to add more when the average utilization of your Amazon EC2 fleet is high and conversely remove them when CPU utilization is low. Which AWS services would be best to use to accomplish this?

A. Auto Scaling, Amazon CloudWatch and AWS Elastic Beanstalk
B. Auto Scaling, Amazon CloudWatch and Elastic Load Balancing.
C. Amazon CloudFront, Amazon CloudWatch and Elastic Load Balancing.
D. AWS Elastic Beanstalk , Amazon CloudWatch and Elastic Load Balancing.

Answer: B
Explanation:
Auto Scaling enables you to follow the demand curve for your applications closely, reducing the need to manually provision Amazon EC2 capacity in advance. For example, you can set a condition to add new Amazon EC2 instances in increments to the Auto Scaling group when the average utilization of your Amazon EC2 fleet is high; and similarly, you can set a condition to remove instances in the same increments when CPU utilization is low. If you have predictable load changes, you can set a schedule through Auto Scaling to plan your scaling activities. You can use Amazon CloudWatch to send alarms to trigger scaling activities and Elastic Load Balancing to help distribute traffic to your instances within Auto Scaling groups. Auto Scaling enables you to run your Amazon EC2 fleet at optimal utilization.
Reference: http://aws.amazon.com/autoscaling/

QUESTION 103
A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption.
Due to new compliance requirements, all existing and new data in this database must be encrypted.
How should this be accomplished?

A. Create an Amazon S3 bucket with server-side encryption enabled.
Move all the data to Amazon S3 Delete the RDS instance.
B. Enable RDS Multi-AZ mode with encryption at rest enabled.
Perform a failover to the standby instance to delete the original instance.
C. Take a snapshot of the RDS instance Create an encrypted copy of the snapshot.
Restore the RDS instance from the encrypted snapshot.
D. Create an RDS read replica with encryption at rest enabled.
Promote the read replica to master and switch the application over to the new master Delete the old RDS instance.

Answer: C

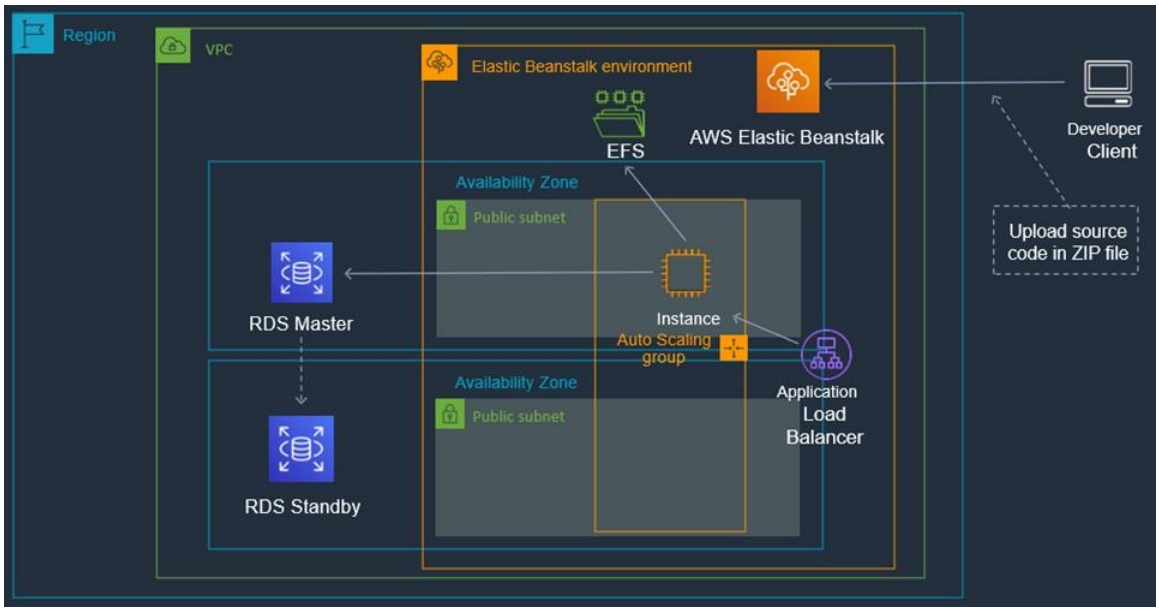
QUESTION 104
A company has a three-tier image-sharing application it uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database.
A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application.
Which solution meets these requirements'?

A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.
B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers.
Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer.
Move the database to a memory optimized instance type to store and serve users' images.
D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers.
Move the database to an Amazon RDS instance with a Multi-AZ deployment Use Amazon S3 to store and serve users' images.

Answer: D
Explanantion
Keyword: Highly available + Least amount of changes to the application
・High Availability = Multi-AZ
・Least amount of changes to the application = Elastic Beanstalk Automatically handles the deployment, from Capacity provisioning, Load Balancing, Auto Scaling to application health monitoring

Option - D will be the right choice and Option - A; Option - B and Option - C out of race due to Cost & inter-operability.

HA with Elastic Beanstalk and RDS



AWS Elastic Beanstalk
AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.

You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.

There is no additional charge for Elastic Beanstalk - you pay only for the AWS resources needed to store and run your applications.

AWS RDS
Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.

Amazon RDS is available on several database instance types - optimized for memory, performance or I/O - and provides you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server. You can use the AWS Database Migration Service to easily migrate or replicate your existing databases to Amazon RDS.

AWS S3
Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

References:
https://aws.amazon.com/elasticbeanstalk/?nc2=h_ql_prod_cp_ebs
https://aws.amazon.com/rds/?nc2=h_ql_prod_db_rds
https://aws.amazon.com/s3/?nc2=h_ql_prod_st_s3

QUESTION 105
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.

Answer: C
Explanation:
The AWS Web Application Firewall (WAF) is available on the Application Load Balancer (ALB). You can use AWS WAF directly on Application Load Balancers (both internal and external) in a VPC, to protect your websites and web services.
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 to inspect for possible malicious scripts.
CORRECT: "Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is the correct answer.
INCORRECT: "Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is incorrect as you cannot use AWS WAF with a classic load balancer.
INCORRECT: "Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is incorrect as you cannot use AWS WAF with a network load balancer.
INCORRECT: "Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard" is incorrect as you cannot use AWS Shield to protect against XSS attacks. Shield is used to protect against DDoS attacks.
References:
https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html

QUESTION 106
A recently acquired company is required to buikl its own infrastructure on AWS and migrate multiple applications to the cloud within a month.
Each application has approximately 50 TB of data to be transferred.
After the migration is complete this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications.
A solutions architect must ensure one-time data migration and ongoing network connectivity.
Which solution will meet these requirements"

A. AWS Direct Connect for both the initial transfer and ongoing connectivity
B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity

C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity
D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity

Answer: C
Explanation:
"Each application has approximately 50 TB of data to be transferred" = AWS Snowball; "secure network connectivity with consistent throughput from their data centers to the applications"
What are the benefits of using AWS Direct Connect and private network connections? In many circumstances, private network connections can reduce costs, increase bandwidth, and provide a more consistent network experience than Internet-based connections. "more consistent network experience", hence AWS Direct Connect.
Direct Connect is better than VPN; reduced cost+increased bandwith+(remain connection or consistent network) = direct connect

QUESTION 107
Organizers for a global event want to put daily reports online as static HTML pages.
The pages are expected to generate millions of views from users around the world The files are stored in an Amazon S3 bucket.
A solutions architect has been asked to design an efficient and effective solution.
Which action should the solutions architect take to accomplish this?

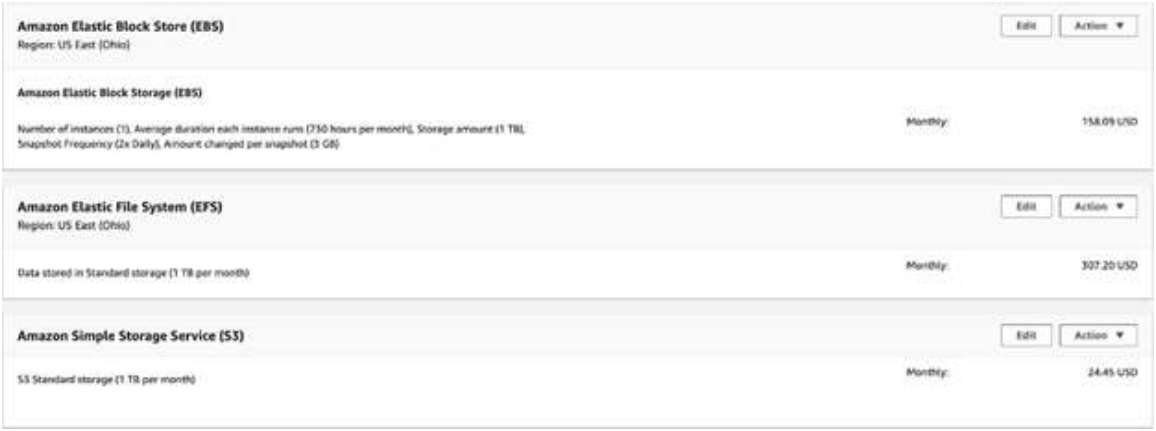
A. Generate presigned URLs for the files
B. Use cross-Region replication to all Regions
C. Use the geoproximity feature of Amazon Route 53
D. Use Amazon CloudFront with the S3 bucket as its origin

Answer: D
Explanation:
Amazon CloudFront can be used to cache the files in edge locations around the world and this will improve the performance of the webpages.
To serve a static website hosted on Amazon S3, you can deploy a CloudFront distribution using one of these configurations:
Using a REST API endpoint as the origin with access restricted by an origin access identity (OAI)
Using a website endpoint as the origin with anonymous (public) access allowed
Using a website endpoint as the origin with access restricted by a Referer header CORRECT: "Use Amazon CloudFront with the S3 bucket as its origin" is the correct answer.
INCORRECT: "Generate presigned URLs for the files" is incorrect as this is used to restrict access which is not a requirement.
INCORRECT: "Use cross-Region replication to all Regions" is incorrect as this does not provide a mechanism for directing users to the closest copy of the static webpages.
INCORRECT: "Use the geoproximity feature of Amazon Route 53" is incorrect as this does not include a solution for having multiple copies of the data in different geographic locations.
References:
https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/

QUESTION 108
A company runs an application on a group of Amazon Linux EC2 instances,
The application writes log files using standard API calls For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently.
Which storage service should a solutions architect use to provide the MOST cost-effective solution?

A. Amazon EBS
B. Amazon EFS
C. Amazon EC2 instance store
D. Amazon S3

Answer: D
Explanation:
The application is writing the files using API calls which means it will be compatible with Amazon S3 which uses a REST API. S3 is a massively scalable key-based object store that is well-suited to allowing concurrent access to the files from many instances.
Amazon S3 will also be the most cost-effective choice. A rough calculation using the AWS pricing calculator shows the cost differences between 1TB of storage on EBS, EFS, and S3 Standard.



CORRECT: "Amazon S3" is the correct answer.
INCORRECT: "Amazon EFS" is incorrect as though this does offer concurrent access from many EC2 Linux instances, it is not the most cost-effective solution.
INCORRECT: "Amazon EBS" is incorrect. The Elastic Block Store (EBS) is not a good solution for concurrent access from many EC2 instances and is not the most cost-effective option either. EBS volumes are mounted to a single instance except when using multi-attach which is a new feature and has several constraints.
INCORRECT: "Amazon EC2 instance store" is incorrect as this is an ephemeral storage solution which means the data is lost when powered down.
Therefore, this is not an option for long-term data storage.
References:
https://docs.aws.amazon.com/AmazonS3/latest/dev/optimizing-performance.html

QUESTION 109
A company's application is running on Amazon EC2 instances m a single Region in the event of a disaster a solutions architect needs to ensure that the resources can also be deployed to a second Region.
Which combination of actions should the solutions architect take to accomplish this-? (Select TWO)

A. Detach a volume on an EC2 instance and copy it to Amazon S3
B. Launch a new EC2 instance from an Amazon Machine image (AMI) in a new Region
C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance
D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination

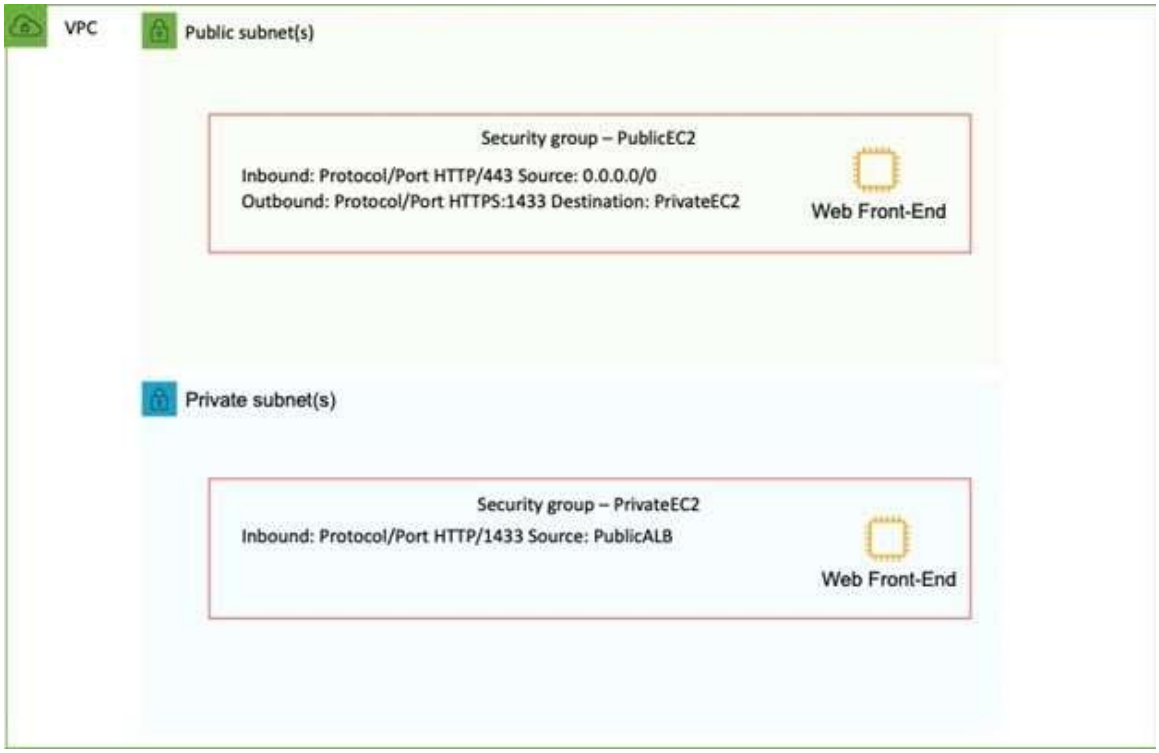
E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume

Answer: BD

QUESTION 110
A solutions architect is designing a two-tier web application.
The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets.
The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet
Security is a high priority for the company.
How should security groups be configured in this situation? (Select TWO)

A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/70
B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0
C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier
D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier
E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier

Answer: AC
Explanation:
In this scenario an inbound rule is required to allow traffic from any internet client to the web front end on SSL/TLS port 443. The source should therefore be set to 0.0.0.0/0 to allow any inbound traffic.
To secure the connection from the web frontend to the database tier, an outbound rule should be created from the public EC2 security group with a destination of the private EC2 security group. The port should be set to 1433 for MySQL. The private EC2 security group will also need to allow inbound traffic on 1433 from the public EC2 security group.
This configuration can be seen in the diagram:



CORRECT: "Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0" is a correct answer.
CORRECT: "Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier" is also a correct answer.
INCORRECT: "Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0" is incorrect as this is configured backwards.
INCORRECT: "Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier" is incorrect as the MySQL database instance does not need to send outbound traffic on either of these ports.
INCORRECT: "Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier" is incorrect as the database tier does not need to allow inbound traffic on port 443.
References:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

QUESTION 111
A data science team requires storage for nightly log processing.
The size and number of logs is unknown and will persist for 24 hours only.
What is the MOST cost-effective solution?

A. Amazon S3 Glacier
B. Amazon S3 Standard
C. Amazon S3 intelligent-Tiering
D. Amazon S3 One Zone-Infrequent Access {S3 One Zone-IA)

Answer: B
Explanation:
S3 standard is the best choice in this scenario for a short term storage solution. In this case the size and number of logs is unknown and it would be difficult to fully assess the access patterns at

this stage. Therefore, using S3 standard is best as it is cost-effective, provides immediate access, and there are no retrieval fees or minimum capacity charge per object.
CORRECT: "Amazon S3 Standard" is the correct answer.
INCORRECT: "Amazon S3 Intelligent-Tiering" is incorrect as there is an additional fee for using this service and for a short-term requirement it may not be beneficial.
INCORRECT: "Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as this storage class has a minimum capacity charge per object (128 KB) and a per GB retrieval fee.
INCORRECT: "Amazon S3 Glacier Deep Archive" is incorrect as this storage class is used for archiving data. There are retrieval fees and it take hours to retrieve data from an archive.
References:
https://aws.amazon.com/s3/storage-classes/

QUESTION 112
A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user- uploaded documents in an Amazon EBS volume.
For better scalability and availability the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone: placing both behind an Application Load Balancer.
After completing this change users reported that each time they refreshed the website they could see one subset of their documents or the other but never all of the documents at the same time.
What should a solutions architect propose to ensure users see all of their documents at once"

A. Copy the data so both EBS volumes contain all the documents.
B. Configure the Application Load Balancer to direct a user to the server with the documents.
C. Copy the data from both EBS volumes to Amazon EFS.
Modify the application to save new documents to Amazon EPS.
D. Configure the Application Load Balancer to send the request to both servers.
Return each document from the correct server.

Answer: C

QUESTION 113
You are building infrastructure for a data warehousing solution and an extra request has come through that there will be a lot of business reporting queries running all the time and you are not sure if your current DB instance will be able to handle it. What would be the best solution for this?

A. DB Parameter Groups
B. Read Replicas
C. Multi-AZ DB Instance deployment
D. Database Snapshots

Answer: B
Explanation:
Read Replicas make it easy to take advantage of MySQL's built-in replication functionality to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. There are a variety of scenarios where deploying one or more Read Replicas for a given source DB Instance may make sense. Common reasons for deploying a Read Replica include:
Scaling beyond the compute or I/O capacity of a single DB Instance for read-heavy database workloads. This excess read traffic can be directed to one or more Read Replicas. Serving read traffic while the source DB Instance is unavailable. If your source DB Instance cannot take I/O requests (e.g. due to I/O suspension for backups or scheduled maintenance), you can direct read traffic to your Read Replica(s). For this use case, keep in mind that the data on the Read Replica

may be "stale" since the source DB Instance is unavailable. Business reporting or data warehousing scenarios; you may want business reporting queries to run against a Read Replica, rather than your primary, production DB Instance.
Reference: https://aws.amazon.com/rds/faqs/

QUESTION 114
In DynamoDB, could you use IAM to grant access to Amazon DynamoDB resources and API actions?

A. In DynamoDB there is no need to grant access
B. Depended to the type of access
C. No
D. Yes

Answer: D
Explanation:
Amazon DynamoDB integrates with AWS Identity and Access Management (IAM). You can use AWS IAM to grant access to Amazon DynamoDB resources and API actions. To do this, you first write an AWS IAM policy, which is a document that explicitly lists the permissions you want to grant. You then attach that policy to an AWS IAM user or role.
Reference:
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/UsingIAMWithDDB.html

QUESTION 115
Much of your company's data does not need to be accessed often, and can take several hours for retrieval time, so it's stored on Amazon Glacier. However someone within your organization has expressed concerns that his data is more sensitive than the other data, and is wondering whether the high level of encryption that he knows is on S3 is also used on the much cheaper Glacier service. Which of the following statements would be most applicable in regards to this concern?

A. There is no encryption on Amazon Glacier, that's why it is cheaper.
B. Amazon Glacier automatically encrypts the data using AES-128 a lesser encryption method than Amazon S3 but you can change it to AES-256 if you are willing to pay more.
C. Amazon Glacier automatically encrypts the data using AES-256, the same as Amazon S3.
D. Amazon Glacier automatically encrypts the data using AES-128 a lesser encryption method than Amazon S3.

Answer: C
Explanation:
Like Amazon S3, the Amazon Glacier service provides low-cost, secure, and durable storage. But where S3 is designed for rapid retrieval, Glacier is meant to be used as an archival service for data that is not accessed often, and for which retrieval times of several hours are suitable.
Amazon Glacier automatically encrypts the data using AES-256 and stores it durably in an immutable form. Amazon Glacier is designed to provide average annual durability of 99.999999999% for an archive. It stores each archive in multiple facilities and multiple devices. Unlike traditional systems which can require laborious data verification and manual repair, Glacier performs regular, systematic data integrity checks, and is built to be automatically self-healing.
Reference: http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

QUESTION 116
Your EBS volumes do not seem to be performing as expected and your team leader has requested you look into improving their performance. Which of the following is not a true

statement relating to the performance of your EBS volumes?

A. Frequent snapshots provide a higher level of data durability and they will not degrade the performance of your application while the snapshot is in progress.
B. General Purpose (SSD) and Provisioned IOPS (SSD) volumes have a throughput limit of 128 MB/s per volume.
C. There is a relationship between the maximum performance of your EBS volumes, the amount of I/O you are driving to them, and the amount of time it takes for each transaction to complete.
D. There is a 5 to 50 percent reduction in IOPS when you first access each block of data on a newly created or restored EBS volume

Answer: A
Explanation:
Several factors can affect the performance of Amazon EBS volumes, such as instance configuration, I/O characteristics, workload demand, and storage configuration. Frequent snapshots provide a higher level of data durability, but they may slightly degrade the performance of your application while the snapshot is in progress. This trade off becomes critical when you have data that changes rapidly. Whenever possible, plan for snapshots to occur during off-peak times in order to minimize workload impact.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html

QUESTION 117
You've created your first load balancer and have registered your EC2 instances with the load balancer. Elastic Load Balancing routinely performs health checks on all the registered EC2 instances and automatically distributes all incoming requests to the DNS name of your load balancer across your registered, healthy EC2 instances. By default, the load balancer uses the ___ protocol for checking the health of your instances.

A. HTTPS
B. HTTP
C. ICMP
D. IPv6

Answer: B
Explanation:
In Elastic Load Balancing a health configuration uses information such as protocol, ping port, ping path (URL), response timeout period, and health check interval to determine the health state of the instances registered with the load balancer.
Currently, HTTP on port 80 is the default health check.
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/TerminologyandKeyConcepts.html

QUESTION 118
A major finance organisation has engaged your company to set up a large data mining application. Using AWS you decide the best service for this is Amazon Elastic MapReduce(EMR) which you know uses Hadoop. Which of the following statements best describes Hadoop?

A. Hadoop is 3rd Party software which can be installed using AMI
B. Hadoop is an open source python web framework
C. Hadoop is an open source Java software framework
D. Hadoop is an open source javascript framework

Answer: C
Explanation:
Amazon EMR uses Apache Hadoop as its distributed data processing engine. Hadoop is an open source, Java software framework that supports data-intensive distributed applications running on large clusters of commodity hardware. Hadoop implements a programming model named "MapReduce," where the data is divided into many small fragments of work, each of which may be executed on any node in the cluster.
This framework has been widely used by developers, enterprises and startups and has proven to be a reliable software platform for processing up to petabytes of data on clusters of thousands of commodity machines.
Reference: http://aws.amazon.com/elasticmapreduce/faqs/

QUESTION 119
In Amazon EC2 Container Service, are other container types supported?

A. Yes, EC2 Container Service supports any container service you need.
B. Yes, EC2 Container Service also supports Microsoft container service.
C. No, Docker is the only container platform supported by EC2 Container Service presently.
D. Yes, EC2 Container Service supports Microsoft container service and Openstack.

Answer: C
Explanation:
In Amazon EC2 Container Service, Docker is the only container platform supported by EC2 Container Service presently.
Reference: http://aws.amazon.com/ecs/faqs/

QUESTION 120
A Solutions Architect is designing the architecture for a web application that will be hosted on AWS. Internet users will access the application using HTTP and HTTPS.

How should the Architect design the traffic control requirements?

A. Use a network ACL to allow outbound ports for HTTP and HTTPS. Deny other traffic for inbound and outbound.
B. Use a network ACL to allow inbound ports for HTTP and HTTPS. Deny other traffic for inbound and outbound.
C. Allow inbound ports for HTTP and HTTPS in the security group used by the web servers.
D. Allow outbound ports for HTTP and HTTPS in the security group used by the web servers.

Answer: C

QUESTION 121
A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed.
The system will run a series of compute-intensive jobs for 4 hours every night.
The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started.
Once completed, the system is expected to run for a minimum of 1 year.
Which type of Amazon EC2 instances should be used to reduce the cost of the system?

A. Spot Instances
B. On-Demand Instances
C. Standard Reserved Instances
D. Scheduled Reserved Instances

Answer: D
Explanation:
Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.
Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week.
CORRECT: "Scheduled Reserved Instances" is the correct answer.
INCORRECT: "Standard Reserved Instances" is incorrect as the workload only runs for 4 hours a day this would be more expensive.
INCORRECT: "On-Demand Instances" is incorrect as this would be much more expensive as there is no discount applied.
INCORRECT: "Spot Instances" is incorrect as the workload cannot be interrupted once started. With Spot instances workloads can be terminated if the Spot price changes or capacity is required.
References:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html

QUESTION 122
A company hosts a static website on-premises and wants to migrate the website to AWS.
The website should load as quickly as possible for users around the world.
The company also wants the most cost- effective solution.
What should a solutions architect do to accomplish this?

A. Copy the website content to an Amazon S3 bucket.
Configure the bucket to serve static webpage content.
Replicate the S3 bucket to multiple AWS Regions
B. Copy the website content to an Amazon S3 bucket.
Configure the bucket to serve static webpage content.
Configure Amazon CloudFront with the S3 bucket as the origin
C. Copy the website content to an Amazon EBS-backed.
Amazon EC2 instance running Apache HTTP Server.
Configure Amazon Route 53 geolocation routing policies to select the closest origin
D. Copy the website content to multiple Amazon EBS-backed.
Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions.
Configure Amazon CloudFront geolocation routing policies to select the closest origin

Answer: B
Explanation:
The most cost-effective option is to migrate the website to an Amazon S3 bucket and configure that bucket for static website hosting. To enable good performance for global users the solutions architect should then configure a CloudFront distribution with the S3 bucket as the origin. This will cache the static content around the world closer to users.
CORRECT: "Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin" is the correct answer.

INCORRECT: "Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions" is incorrect as there is no solution here for directing users to the closest region. This could be a more cost-effective (though less elegant) solution if AWS Route 53 latency records are created.
INCORRECT: "Copy the website content to an Amazon EC2 instance. Configure Amazon Route 53 geolocation routing policies to select the closest origin" is incorrect as using Amazon EC2 instances is less cost-effective compared to hosting the website on S3. Also, geolocation routing does not achieve anything with only a single record.
INCORRECT: "Copy the website content to multiple Amazon EC2 instances in multiple AWS Regions. Configure AWS Route 53 geolocation routing policies to select the closest region" is incorrect as using Amazon EC2 instances is less cost-effective compared to hosting the website on S3.
References:
https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/

QUESTION 123
A solutions architect is implementing a document review application using an Amazon S3 bucket for storage.
The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available.
Users must be able to download, modify, and upload documents.
Which combination of actions should be taken to meet these requirements'? (Select TWO)

A. Enable a read-only bucket ACL
B. Enable versioning on the bucket
C. Attach an IAM policy to the bucket
D. Enable MFA Delete on the bucket
E. Encrypt the bucket using AWS KMS

Answer: BD
Explanation:
None of the options present a good solution for specifying permissions required to write and modify objects so that requirement needs to be taken care of separately. The other requirements are to prevent accidental deletion and the ensure that all versions of the document are available. The two solutions for these requirements are versioning and MFA delete. Versioning will retain a copy of each version of the document and multi-factor authentication delete (MFA delete) will prevent any accidental deletion as you need to supply a second factor when attempting a delete.
CORRECT: "Enable versioning on the bucket" is a correct answer.
CORRECT: "Enable MFA Delete on the bucket" is also a correct answer.
INCORRECT: "Set read-only permissions on the bucket" is incorrect as this will also prevent any writing to the bucket which is not desired.
INCORRECT: "Attach an IAM policy to the bucket" is incorrect as users need to modify documents which will also allow delete. Therefore, a method must be implemented to just control deletes.
INCORRECT: "Encrypt the bucket using AWS SSE-S3" is incorrect as encryption doesn't stop you from deleting an object.
References:
https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html

QUESTION 124
A company built a food ordering application that captures user data and stores it for future analysis.

The application's static front end is deployed on an Amazon EC2 instance.
The front-end application sends the requests to the backend application running on separate EC2 instance.
The backend application then stores the data in Amazon RDS
What should a solutions architect do to decouple the architecture and make it scalable"

A. Use Amazon S3 to serve the front-end application which sends requests to Amazon EC2 to execute the backend application.
The backend application will process and store the data in Amazon RDS
B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic.
Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic and process and store the data in Amazon RDS
C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue.
Place the backend instance in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS
D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway which writes the requests to an Amazon SQS queue.
Place the backend instances in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS

Answer: D
Explanation
Keyword: Static + Decouple + Scalable
Static=S3
Decouple=SQS Queue
Scalable=ASG

Option B will not be there in the race due to Auto-Scaling unavailability.
Option A will not be there in the race due to Decouple unavailability.
Option C & D will be in the race and Option D will be correct answers due to all 3 combination matches [Static=S3; Decouple=SQS Queue; Scalable=ASG] & Option C will loose due to Static option unavailability

QUESTION 125
A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket.
Upon payment, content will be available for download for 14 days before the user is denied access.
Which of the following would be the LEAST complicated implementation?

A. Use an Amazon CloudFront distribution with an origin access identity (OAI)
Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs
Design a Lambda function to remove data that is older than 14 days
B. Use an S3 bucket and provide direct access to the tile
Design the application to track purchases in a DynamoDH table
Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB
C. Use an Amazon CloudFront distribution with an OAI
Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs
Design the application to sot an expiration of 14 days for the URL
D. Use an Amazon CloudFront distribution with an OAI

Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs
Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary

Answer: C

QUESTION 126
A company wants to host a scalable web application on AWS.
The application will be accessed by users from different geographic regions of the world.
Application users will be able to download and upload unique data up to gigabytes in size.
The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.
What should a solutions architect do to accomplish this?

A. Use Amazon S3 with Transfer Acceleration to host the application.
B. Use Amazon S3 with CacheControl headers to host the application.
C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Answer: A
Explanation:
The maximum size of a single file that can be delivered through Amazon CloudFront is 20 GB.
This limit applies to all Amazon CloudFront distributions.

QUESTION 127
A company captures clickstream data from multiple websites and analyzes it using batch processing.
The data is loaded nightly into Amazon Redshift and is consumed by business analysts.
The company wants to move towards near-real-time data processing for timely insights.
The solution should process the streaming data with minimal effort and operational overhead.
Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

A. Amazon EC2
B. AWS Lambda
C. Amazon Kinesis Data Streams
D. Amazon Kinesis Data Firehose
E. Amazon Kinesis Data Analytics

Answer: DE
Explanation:
https://d0.awsstatic.com/whitepapers/whitepaper-streaming-data-solutions-on-aws-with-amazonkinesis.pdf (9)
https://aws.amazon.com/kinesis/#Evolve_from_batch_to_real-time_analytics

QUESTION 128
A company is migrating a three-tier application to AWS.
The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries.
These performance issues were caused by users generating different real-time reports from the application duringworking hours.

Which solution will improve the performance of the application when it is moved to AWS?

A. Import the data into an Amazon DynamoDB table with provisioned capacity.
Refactor the application to use DynamoDB for reports.
B. Create the database on a compute optimized Amazon EC2 instance.
Ensure compute resources exceed the on-premises database.
C. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas.
Configure the application reader endpoint for reports.
D. Create an Amazon Aurora MySQL Multi-AZ DB cluster.
Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Answer: C
Explanation:
The MySQL-compatible edition of Aurora delivers up to 5X the throughput of standard MySQL running on the same hardware, and enables existing MySQL applications and tools to run without requiring modification.
https://aws.amazon.com/rds/aurora/mysql-features/

QUESTION 129
A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs a solution with low latency and high availability.
What should a solutions architect do to accomplish this?

A. Provision EC2 instances in us-west-1.
Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.
B. Provision EC2 instances and an Application Load Balancer in us-west-1.
Make the load balancer distribute the traffic based on the location of the request.
C. Provision EC2 instances and configure an Application Load Balancer in us-west-1.
Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.
D. Provision EC2 instances and configure an Application Load Balancer in us-west-1.
Configure Amazon Route 53 with a weighted routing policy.
Create alias records in Route 53 that point to the Application Load Balancer.

Answer: C
Explanation:
"ELB provides load balancing within one Region, AWS Global Accelerator provides traffic management across multiple Regions [...] AWS Global Accelerator complements ELB by extending these capabilities beyond a single AWS Region, allowing you to provision a global interface for your applications in any number of Regions. If you have workloads that cater to a global client base, we recommend that you use AWS Global Accelerator. If you have workloads hosted in a single AWS Region and used by clients in and around the same Region, you can use an Application Load Balancer or Network Load Balancer to manage your resources."
https://aws.amazon.com/global-accelerator/faqs/

QUESTION 130
A company is planning to migrate a business-critical dataset to Amazon S3.
The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset.
The company's disaster recovery policy states that all data multiple AWS Regions.

How should a solutions architect design the S3 solution?

A. Create an additional S3 bucket in another Region and configure cross-Region replication.
B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Answer: C
Explanation:
Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region. Both source and destination buckets must have versioning enabled.
CORRECT: "Create an additional S3 bucket with versioning in another Region and configure cross-Region replication" is the correct answer.
INCORRECT: "Create an additional S3 bucket in another Region and configure cross-Region replication" is incorrect as the destination bucket must also have versioning enabled.
INCORRECT: "Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS)" is incorrect as CORS is not related to replication.
INCORRECT: "Create an additional S3 bucket with versioning in another Region and configure cross-origin resource sharing (CORS)" is incorrect as CORS is not related to replication.
References:
https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html

QUESTION 131
A company has application running on Amazon EC2 instances in a VPC.
One of the applications needs to call an Amazon S3 API to store and read objects.
The company's security policies restrict any internet-bound traffic from the applications.
Which action will fulfill these requirements and maintain security?

A. Configure an S3 interface endpoint.
B. Configure an S3 gateway endpoint.
C. Create an S3 bucket in a private subnet.
D. Create an S3 bucket in the same Region as the EC2 instance.

Answer: B
Explanation:
Gateway Endpoint for S3 and DynamoDB
https://medium.com/tensult/aws-vpc-endpoints-introduction-ef2bf85c4422
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html
https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html

QUESTION 132
A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data.
During the financial closing period at the start of every month. Accountants run large queries that impact the database's performance due to high usage.
The company wants to minimize the impact that the reporting activity has on the web application.
What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

A. Create a read replica and direct reporting traffic to the replica.
B. Create a Multi-AZ database and direct reporting traffic to the standby.
C. Create a cross-Region read replica and direct reporting traffic to the replica.
D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Answer: A
Explanation:
Amazon RDS uses the MariaDB, MySQL, Oracle, PostgreSQL, and Microsoft SQL Server DB engines' built-in replication functionality to create a special type of DB instance called a read replica from a source DB instance. Updates made to the source DB instance are asynchronously copied to the read replica. You can reduce the load on your source DB instance by routing read queries from your applications to the read replica.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

QUESTION 133
A company must generate sales reports at the beginning of every month.
The reporting process launches 20 Amazon EC2 instances on the first of the month.
The process runs for 7 days and cannot be interrupted. The company wants to minimize costs.
Which pricing model should the company choose?

A. Reserved Instances
B. Spot Block Instances
C. On-Demand Instances
D. Scheduled Reserved Instances

Answer: D
Explanation:
Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.
Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html

QUESTION 134
A company is hosting a website behind multiple Application Load Balancers.
The company has different distribution rights for its content around the world.
A solutions architect needs to ensure that users are served the correct content without violating distribution rights.
Which configuration should the solutions architect choose to meet these requirements?

A. Configure Amazon CloudFront with AWS WAF.
B. Configure Application Load Balancers with AWS WAF.
C. Configure Amazon Route 53 with a geolocation policy.
D. Configure Amazon Route 53 with a geoproximity routing policy.

Answer: C

Explanation:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html (geolocation routing)

QUESTION 135
A company's website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage.
There are other internal systems that query this DB instance to fetch data for internal batch processing.
The RDS DB instance slows down significantly the internal systems fetch data.
This impacts the website's read and write performance, and the users experience slow response times.
Which solution will improve the website's performance?

A. Use an RDS PostgreSQL DB instance instead of a MySQL database.
B. Use Amazon ElastiCache to cache the query responses for the website.
C. Add an additional Availability Zone to the current RDS MySQL Multi.AZ DB instance.
D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

Answer: D

QUESTION 136
A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux.
The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing.
Which storage option would be the optimal solution?

A. Amazon Elastic File System (Amazon EFS)
B. Amazon FSx for Lustre
C. Amazon EC2 instance store
D. Amazon EBS Provisioned IOPS SSD (io1)

Answer: B
Explanation:
https://d1.awsstatic.com/whitepapers/AWS%20Partner%20Network_HPC%20Storage%20Options_2019_FINAL.pdf (p.8)

QUESTION 137
A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS.
The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was install recently to support other AWS services.
A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff.
What should the solutions architect recommend?

A. Use AWS Directory Service to create a managed Active Directory.
Uninstall Active Directory on the current EC2 instance.

B. Create another EC2 instance in the same subnet and reinstall Active Directory on it.
Uninstall Active Directory.
C. Use AWS Directory Service to create an Active Directory connector.
Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
D. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller.
Modify the EC2 instance's security group to deny public access to Active Directory.

Answer: A
Explanation:
Migrate AD to AWS Managed AD and keep the webserver alone.. Reduce risk = remove AD from that EC2. Minimize admin = remove AD from any EC2
-> use AWS Directory Service
Active Directory connector is only for ON-PREM AD. The one they have exists in the cloud already.

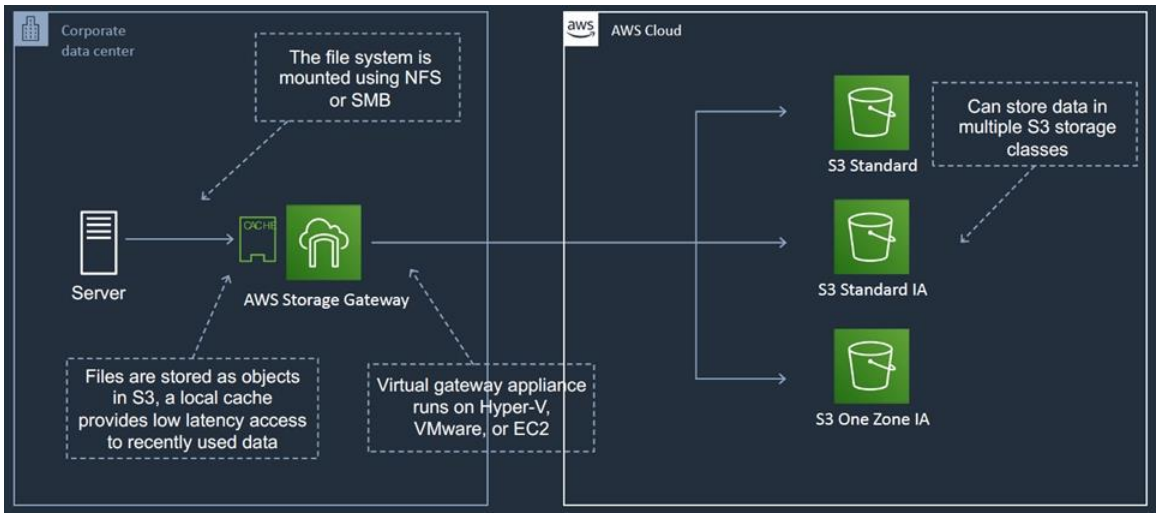
QUESTION 138
A company runs an application in a branch office within a small data closet with no virtualized compute resources.
The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.
Which solution meet these requirements?

A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Answer: B
Explanation
Keyword: NFS + Compliance

File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3. It can be used for on-premises applications, and for Amazon EC2-resident applications that need file storage in S3 for object based workloads. Used for flat files only, stored directly on S3. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching.

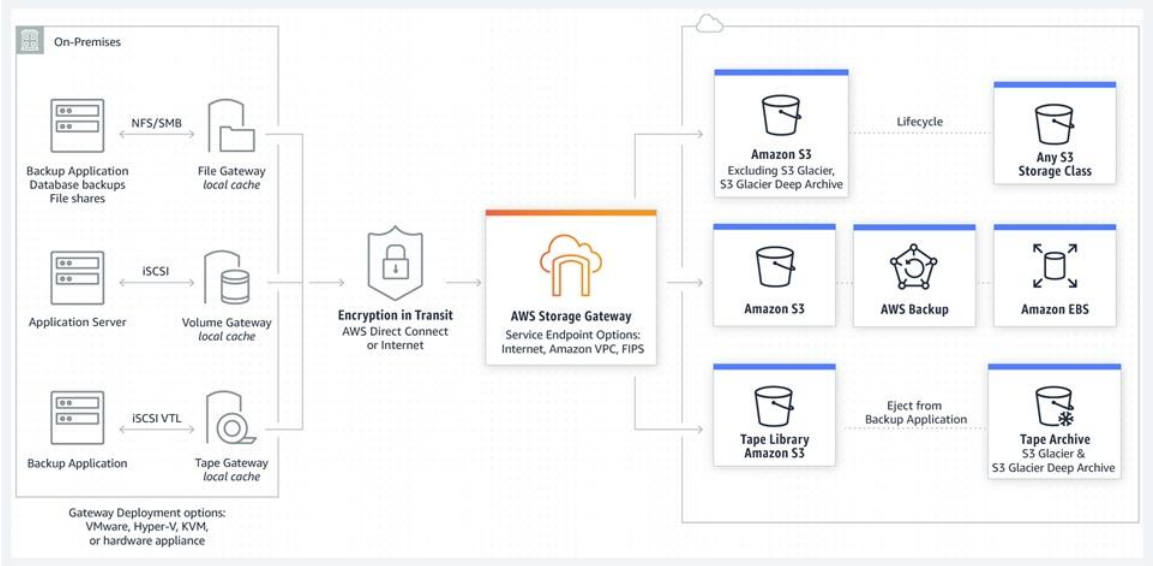
AWS Storage Gateway – File Gateway



The table below shows the different gateways available and the interfaces and use cases:

New Name	Old Name	Interface	Use Case
File Gateway	None	NFS, SMB	Allow on-prem or EC2 instances to store objects in S3 via NFS or SMB mount points
Volume Gateway Stored Mode	Gateway-Stored Volumes	iSCSI	Asynchronous replication of on-prem data to S3
Volume Gateway Cached Mode	Gateway-Cached Volumes	iSCSI	Primary data stored in S3 with frequently accessed data cached locally on-prem
Tape Gateway	Gateway-Virtual Tape Library	ISCSI	Virtual media changer and tape library for use with existing backup software

Storage Gateway Overview



CORRECT: "Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3" is the correct answer.

INCORRECT: "Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3" is incorrect.
INCORRECT: "Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3" is incorrect as unsupported NFS.
INCORRECT: "Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3" is incorrect as unsupported NFS.

References:
https://aws.amazon.com/blogs/aws/file-interface-to-aws-storage-gateway/
https://d0.awsstatic.com/whitepapers/aws-storage-gateway-file-gateway-for-hybrid-architectures.pdf

QUESTION 139
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 multifactor authentication.

Answer: C

QUESTION 140
A company hosts its product information webpages on AWS.
The existing solution uses multiple Amazon C2 instances behind an Application Load Balancer in an Auto Scaling group.

The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate.
The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website.
What should a solutions architect do to meet these requirements?

A. Redesign the application to use Amazon CloudFront.
B. Redesign the application to use AWS Elastic Beanstalk.
C. Redesign the application to use a Network Load Balancer.
D. Redesign the application to use Amazon S3 static website hosting.

Answer: A

QUESTION 141
A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.
What should the solutions architect do to meet these requirements?

A. Increase the minimum capacity for the Auto Scaling group.
B. Increase the maximum capacity for the Auto Scaling group.
C. Configure scheduled scaling to scale up to the desired compute level.
D. Change the scaling policy to add more EC2 instances during each scaling operation.

Answer: C

QUESTION 142
An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2. and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns.
Which action should be taken to improve the performance of the backend?

A. Implement Amazon SNS to store the database calls.
B. Implement Amazon ElastiCache to cache the large datasets.
C. Implement an RDS for MySQL read replica to cache database calls.
D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Answer: B

QUESTION 143
A company's application hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Due to data sensitivity, traffic cannot traverse the internet How should a solutions architect configure access?

A. Create a private hosted zone using Amazon Route 53.
B. Configure a VPC gateway endpoint for Amazon S3 in the VPC.
C. Configure AWS PrivateLink between the EC2 instance and the S3 bucket.

D. Set up a site-to-site VPN connection between the VPC and the S3 bucket.

Answer: B

QUESTION 144
An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table.
What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

A. Use a VPC endpoint for DynamoDB.
B. Use a NAT gateway in a public subnet.
C. Use a NAT instance in a private subnet.
D. Use the internet gateway attached to the VPC.

Answer: A
Explanantion
VPC Enpoint
An Interface endpoint uses AWS PrivateLink and is an elastic network interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service.

Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services.

AWS PrivateLink access over Inter-Region VPC Peering:
- Applications in an AWS VPC can securely access AWS PrivateLink endpoints across AWS Regions using Inter-Region VPC Peering.
- AWS PrivateLink allows you to privately access services hosted on AWS in a highly available and scalable manner, without using public IPs, and without requiring the traffic to traverse the Internet.
- Customers can privately connect to a service even if the service endpoint resides in a different AWS Region.
- Traffic using Inter-Region VPC Peering stays on the global AWS backbone and never traverses the public Internet.
- A gateway endpoint is a gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service.
- An interface VPC endpoint (interface endpoint) enables you to connect to services powered by AWS PrivateLink.

The table below highlights some key information about both types of endpoint:

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

References:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html

QUESTION 145
A solutions architect needs to design a low-latency solution for a static single-page application accessed by users utilizing a custom domain name. The solution must be serverless, encrypted in transit, and cost-effective.
Which combination of AWS services and features should the solutions architect use? (Select TWO.)

A. Amazon S3
B. Amazon EC2
C. AWS Fargate
D. Amazon CloudFront
E. Elastic Load Balancer

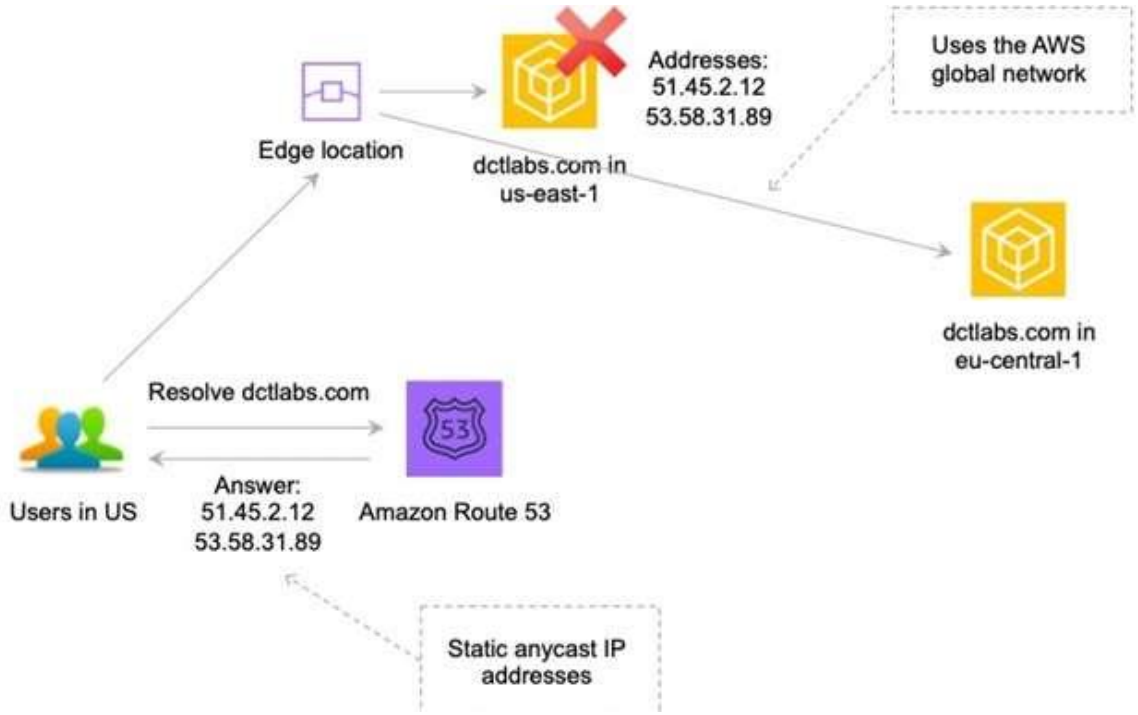
Answer: AD

QUESTION 146
A company has global users accessing an application deployed in different AWS Regions, exposing public static IP addresses. The users are experiencing poor performance when accessing the application over the internet.
What should a solutions architect recommend to reduce internet latency?

A. Set up AWS Global Accelerator and add endpoints.
B. Set up AWS Direct Connect locations in multiple Regions.
C. Set up an Amazon CloudFront distribution to access an application.
D. Set up an Amazon Route 53 geoproximity routing policy to route traffic.

Answer: A
Explanation:
AWS Global Accelerator is a service in which you create accelerators to improve availability and performance of your applications for local and global users. Global Accelerator directs traffic to optimal endpoints over the AWS global network. This improves the availability and performance of your internet applications that are used by a global audience. Global Accelerator is a global service that supports endpoints in multiple AWS Regions, which are listed in the AWS Region

Table.
By default, Global Accelerator provides you with two static IP addresses that you associate with your accelerator. (Or, instead of using the IP addresses that Global Accelerator provides, you can configure these entry points to be IPv4 addresses from your own IP address ranges that you bring to Global Accelerator.)



The static IP addresses are anycast from the AWS edge network and distribute incoming application traffic across multiple endpoint resources in multiple AWS Regions, which increases the availability of your applications. Endpoints can be Network Load Balancers, Application Load Balancers, EC2 instances, or Elastic IP addresses that are located in one AWS Region or multiple Regions.
CORRECT: "Set up AWS Global Accelerator and add endpoints" is the correct answer.
INCORRECT: "Set up AWS Direct Connect locations in multiple Regions" is incorrect as this is used to connect from an on-premises data center to AWS. It does not improve performance for users who are not connected to the on-premises data center.
INCORRECT: "Set up an Amazon CloudFront distribution to access an application" is incorrect as CloudFront cannot expose static public IP addresses.
INCORRECT: "Set up an Amazon Route 53 geoproximity routing policy to route traffic" is incorrect as this does not reduce internet latency as well as using Global Accelerator. GA will direct users to the closest edge location and then use the AWS global network.
References:
https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html

QUESTION 147
An application requires a development environment (DEV) and production environment (PROD) for several years. The DEV instances will run for 10 hours each day during normal business hours, while the PROD instances will run 24 hours each day. A solutions architect needs to determine a compute instance purchase strategy to minimize costs.
Which solution is the MOST cost-effective?

A. DEV with Spot Instances and PROD with On-Demand Instances

B. DEV with On-Demand Instances and PROD with Spot Instances
C. DEV with Scheduled Reserved Instances and PROD with Reserved Instances
D. DEV with On-Demand Instances and PROD with Scheduled Reserved Instances

Answer: C

QUESTION 148
A solutions architect is designing a customer-facing application. The application is expected to have a variable amount of reads and writes depending on the time of year and clearly defined access patterns throughout the year. Management requires that database auditing and scaling be managed in the AWS Cloud. The Recovery Point Objective (RPO) must be less than 5 hours.
Which solutions can accomplish this? (Select TWO.)

A. Use Amazon DynamoDB with auto scaling.
Use on-demand backups and AWS CloudTrail.
B. Use Amazon DynamoDB with auto scaling.
Use on-demand backups and Amazon DynamoDB Streams.
C. Use Amazon Redshift Configure concurrency scaling.
Enable audit logging.
Perform database snapshots every 4 hours.
D. Use Amazon RDS with Provisioned IOPS.
Enable the database auditing parameter.
Perform database snapshots every 5 hours.
E. Use Amazon RDS with auto scaling.
Enable the database auditing parameter.
Configure the backup retention period to at least 1 day.

Answer: AE
Explanation:
A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail.
CORRECT - Scalable, with backup and AWS Managed Auditing
B. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.
INCORRECT - AWS DDB Streams can be used for auditing, but its not AWS managed auditing.
C. Use Amazon Redshift Configure concurrency scaling. Enable audit logging. Perform database snapshots every 4 hours.
INCORRECT - Not a database. Datalake
D. Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter. Perform database snapshots every 5 hours.
INCORRECT - This does not scale
E. Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backup retention period to at least 1 day.
CORRECT - Scalable, AWS managed auditing and backup. The backup frequency is not stated but have no technical limitation which states it cannot be less 5 hours (1 day is retention period of the backup).

QUESTION 149
A company hosts its website on Amazon S3. The website serves petabytes of outbound traffic monthly, which accounts for most of the company's AWS costs.
What should a solutions architect do to reduce costs?

A. Configure Amazon CloudFront with the existing website as the origin.

B. Move the website to Amazon EC2 with Amazon EBS volumes for storage.
C. Use AWS Global Accelerator and specify the existing website as the endpoint.
D. Rearchitect the website to run on a combination of Amazon API Gateway and AWS Lambda.

Answer: A
Explanation:
A textbook case for CloudFront. The data transfer cost in CloudFront is lower than in S3. With heavy read operations of static content, it's more economical to add CloudFront in front of you S3 bucket.

QUESTION 150
A solution architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.

Policy1

```
{
    "Version": "2012-10-17", "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:Get*",
                "iam:List*",
                "kms:List*",
                "ec2:*",
                "ds:*",
                "logs:Get*",
                "logs:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

Policy2

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ds:Delete*",
            "Resource": "*"
        }
    ]
}
```

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 IAM users
B. Deleting directories
C. Deleting Amazon EC2 instances
D. Deleting logs from Amazon CloudWatch Logs

Answer: C

QUESTION 151
A solutions architect is helping a developer design a new ecommerce shopping cart application using AWS services. The developer is unsure of the current database schema and expects to make changes as the ecommerce site grows. The solution needs to be highly resilient and capable of automatically scaling read and write capacity.
Which database solution meets these requirements?

A. Amazon Aurora PostgreSQL
B. Amazon DynamoDB with on-demand enabled
C. Amazon DynamoDB with DynamoDB Streams enabled
D. Amazon SQS and Amazon Aurora PostgreSQL

Answer: B
Explanation:
https://aws.amazon.com/pt/about-aws/whats-new/2018/11/announcing-amazon-dynamodb-on-demand/

QUESTION 152
A solutions architect is designing an architecture for a new application that requires low network latency and high network throughput between Amazon EC2 instances. Which component should be included in the architectural design?

A. An Auto Scaling group with Spot Instance types.
B. A placement group using a cluster placement strategy.
C. A placement group using a partition placement strategy.
D. An Auto Scaling group with On-Demand instance types.

Answer: B

QUESTION 153
A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications.
Which solution will meet these requirements?

A. Amazon DynamoDB
B. Amazon RDS for MySQL

C. MySQL-compatible Amazon Aurora Serverless
D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Answer: C

QUESTION 154
A solutions architect is designing a mission-critical web application. It will consist of Amazon EC2 instances behind an Application Load Balancer and a relational database. The database should be highly available and fault tolerant.
Which database implementations will meet these requirements? (Select TWO.)

A. Amazon Redshift
B. Amazon DynamoDB
C. Amazon RDS for MySQL
D. MySQL-compatible Amazon Aurora Multi-AZ
E. Amazon RDS for SQL Server Standard Edition Mufti-AZ

Answer: DE

QUESTION 155
A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing. 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.
Which set of services should a solutions architect recommend to meet these requirements?

A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
B. Amazon EBS for maximum performance. Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage
C. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage
D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Answer: A

QUESTION 156
A company hosts an application on an Amazon EC2 instance that requires a maximum of 200 GB storage space. The application is used infrequently, with peaks during mornings and evenings. Disk I/O varies, but peaks at 3,000 IOPS. The chief financial officer of the company is concerned about costs and has asked a solutions architect to recommend the most cost-effective storage option that does not sacrifice performance.
Which solution should the solutions architect recommend?

A. Amazon EBS Cold HDD (sc1)
B. Amazon EBS General Purpose SSD (gp2)
C. Amazon EBS Provisioned IOPS SSD (io1)
D. Amazon EBS Throughput Optimized HDD (st1)

Answer: B
Explanation:
General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time.
Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 16,000 IOPS (at 5,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver their provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.
In this case the volume would have a baseline performance of 3 x 200 = 600 IOPS. The volume could also burst to 3,000 IOPS for extended periods. As the I/O varies, this should be suitable.
CORRECT: "Amazon EBS General Purpose SSD (gp2)" is the correct answer.
INCORRECT: "Amazon EBS Provisioned IOPS SSD (io1) " is incorrect as this would be a more expensive option and is not required for the performance characteristics of this workload.
INCORRECT: "Amazon EBS Cold HDD (sc1)" is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload.
INCORRECT: "Amazon EBS Throughput Optimized HDD (st1)" is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload.
References:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

QUESTION 157
A company delivers files in Amazon S3 to certain users who do not have AWS credentials. These users must be given access for a limited lime. What should a solutions architect do to securely meet these requirements?

A. Enable public access on an Amazon S3 bucket.
B. Generate a presigned URL to share with the users.
C. Encrypt files using AWS KMS and provide keys to the users.
D. Create and assign IAM roles that will grant GetObject permissions to the users.

Answer: B

QUESTION 158
A leasing company generates and emails PDF statements every month for all its customers. Each statement is about 400 KB in size. Customers can download their statements from the website for up to 30 days from when the statements were generated. At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements.
What is the MOST cost-effective storage solution for this situation?

A. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.
B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.
C. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.
D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class.
Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

Answer: D

QUESTION 159
A solutions architect is moving the static content from a public website hosted on Amazon EC2 instances to an Amazon S3 bucket. An Amazon CloudFront distribution will be used to deliver the static assets. The security group used by the EC2 instances restricts access to a limited set of IP ranges. Access to the static content should be similarly restricted.
Which combination of steps will meet these requirements? (Select TWO.)

A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.
B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.
C. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the CloudFront distribution.
D. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the S3 bucket hosting the static content.
E. Create a new IAM role and associate the role with the distribution. Change the permissions either on the S3 bucket or on the files within the S3 bucket so that only the newly created IAM role has read and download permissions.

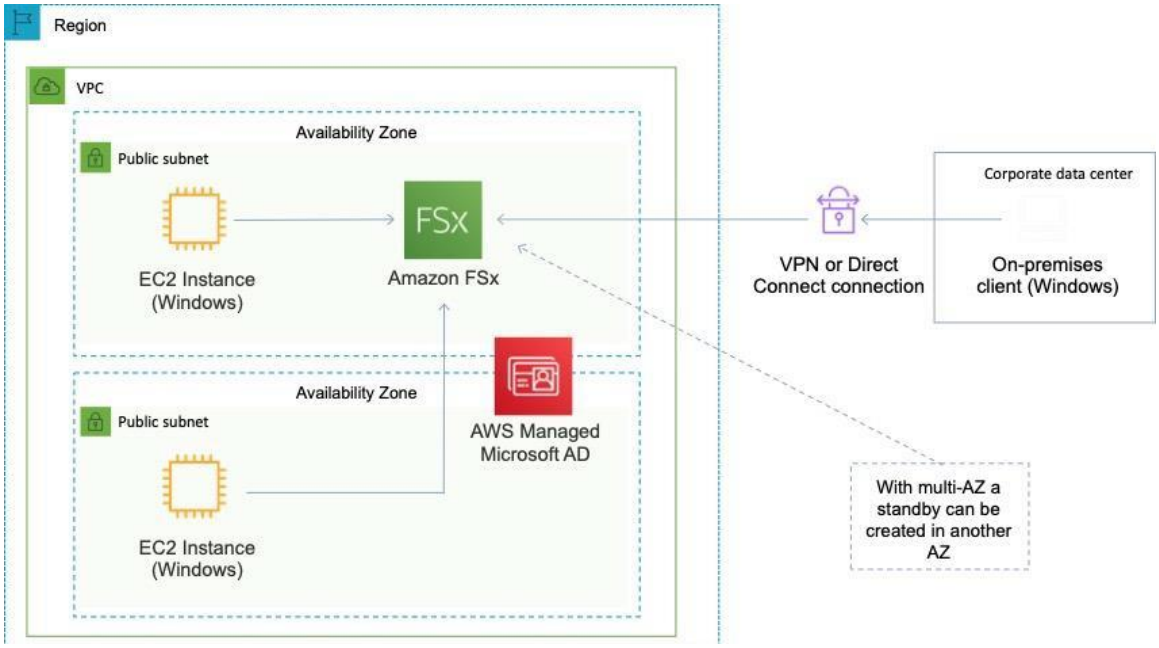
Answer: AB

QUESTION 160
A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.
Which solution will satisfy these requirements?

A. Configure Amazon EFS storage and set the Active Directory domain for authentication.
B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.
C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Answer: D
Explanation
Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. It offers single-AZ and multi-AZ deployment options, fully managed backups, and encryption of data at rest and in transit. You can optimize cost and performance for your workload needs with SSD and HDD storage options; and you can scale storage and change the throughput performance of your file system at any time. Amazon FSx file storage is accessible from Windows, Linux, and MacOS compute instances and devices running on AWS or on premises.

Works with Microsoft Active Directory (AD) to easily integrate file systems with Windows environments.



CORRECT: "Amazon FSx" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect as EFS only supports Linux systems.
INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.
INCORRECT: "AWS Storage Gateway" is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on-premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company need to replace the file server farm and Amazon FSx is the best choice for this job.

References:
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html

QUESTION 161
A company runs multiple Amazon EC2 Linux instances in a VPC with applications that use a hierarchical directory structure. The applications need to rapidly and concurrently read and write to shared storage How can this be achieved?

A. Create an Amazon EFS file system and mount it from each EC2 instance.
B. Create an Amazon S3 bucket and permit access from all the EC2 instances in the VPC.
C. Create a file system on an Amazon EBS Provisioned IOPS SSD (io1) volume. Attach the volume to all the EC2 instances.
D. Create file systems on Amazon EBS volumes attached to each EC2 instance. Synchronize the Amazon EBS volumes across the different EC2 instances.

Answer: A

QUESTION 162
A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon

S3. How can a solutions architect ensure that the application has permission to access Amazon S3?

A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.
C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.
D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Answer: B

QUESTION 163
A solutions architect has configured the following IAM policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lambda:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction"
            ],
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "220.100.16.0/20"
                }
            }
        }
    ]
}
```

Which action will be allowed by the policy?

A. An AWS Lambda function can be deleted from any network.
B. An AWS Lambda function can be created from any network.
C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.
D. An AWS Lambda function can be deleted from the 220.100.16.0/20 network

Answer: C

QUESTION 164
A website runs a web application that receives a burst of traffic each day at noon. The users upload new pictures and content daily, but have been complaining of timeouts. The architecture uses Amazon EC2 Auto Scaling groups, and the custom application consistently takes 1 minute to initiate upon boot up before responding to user requests.
How should a solutions architect redesign the architecture to better respond to changing traffic?

A. Configure a Network Load Balancer with a slow start configuration.
B. Configure AWS ElastiCache for Redis to offload direct requests to the servers.
C. Configure an Auto Scaling step scaling policy with an instance warmup condition.
D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

Answer: C

QUESTION 165
A company has a website running on Amazon EC2 instances across two Availability Zones. The company is expecting spikes in traffic on specific holidays, and wants to provide a consistent user experience. How can a solutions architect meet this requirement?

A. Use step scaling.
B. Use simple scaling.
C. Use lifecycle hooks.
D. Use scheduled scaling.

Answer: D

QUESTION 166
A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.
Which configuration will meet this requirement?

A. Configure the security group for the EC2 instances.
B. Configure the security group on the Application Load Balancer.
C. Configure AWS WAF on the Application Load Balancer in a VPC.
D. Configure the network ACL for the subnet that contains the EC2 instances.

Answer: C

QUESTION 167
A company has 150 TB of archived image data stored on-premises that needs to be mowed to the AWS Cloud within the next month. The company's current network connection allows up to 100 Mbps uploads for this purpose during the night only.
What is the MOST cost-effective mechanism to move this data and meet the migration deadline?

A. Use AWS Snowmobile to ship the data to AWS.
B. Order multiple AWS Snowball devices to ship the data to AWS.

C. Enable Amazon S3 Transfer Acceleration and securely upload the data.
D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

Answer: B

QUESTION 168
A three-tier web application processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer, a middle tier of three EC2 instances decoupled from the web tier using Amazon SQS. and an Amazon DynamoDB backend. At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy processing times. A solutions architect needs to reduce these processing times. Which action will be MOST effective in accomplishing this?

A. Replace the SQS queue with Amazon Kinesis Data Firehose.
B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier.
C. Add an Amazon CloudFront distribution to cache the responses for the web tier.
D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SOS queue depth.

Answer: D

QUESTION 169
A company wants to host a web application on AWS that will communicate to a database within a VPC.
The application should be highly available.
What should a solutions architect recommend?

A. Create two Amazon EC2 instances to host the web servers behind a load balancer, and then deploy the database on a large instance.
B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones.
C. Deploy a load balancer in the public subnet with an Auto Scaling group for the web servers, and then deploy the database on an Amazon EC2 instance in the private subnet.
D. Deploy two web servers with an Auto Scaling group, configure a domain that points to the two web servers, and then deploy a database architecture in multiple Availability Zones.

Answer: B

QUESTION 170
A company is migrating to the AWS Cloud. A file server is the first workload to migrate. Users must be able to access the file share using the Server Message Block (SMB) protocol. Which AWS managed service meets these requirements?

A. Amazon EBS
B. Amazon EC2
C. Amazon FSx
D. Amazon S3

Answer: C
Explanation

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.

Amazon FSx is built on Windows Server and provides a rich set of administrative features that include end-user file restore, user quotas, and Access Control Lists (ACLs).

Additionally, Amazon FSX for Windows File Server supports Distributed File System Replication (DFSR) in both Single-AZ and Multi-AZ deployments as can be seen in the feature comparison table below.

CORRECT: "Amazon FSx" is the correct answer.

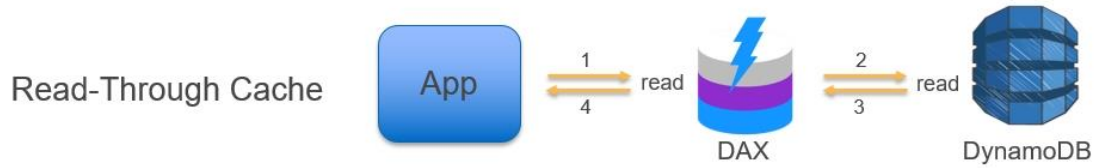
INCORRECT: "Amazon Elastic Block Store (EBS)" is incorrect. EFS and EBS are not good use cases for this solution. Neither storage solution is capable of presenting Amazon S3 objects as files to the application.
INCORRECT: "Amazon EC2" is incorrect as no SMB support.
INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.

References:
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html

QUESTION 171
A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes.
Which method should the solutions architect select?

A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
B. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.
D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.

Answer: A
Explanation
Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache that can reduce Amazon DynamoDB response times from milliseconds to microseconds, even at millions of requests per second.



Amazon ElastiCache is incorrect because although you may use ElastiCache as your database cache, it will not reduce the DynamoDB response time from milliseconds to microseconds as compared with DynamoDB DAX.

AWS Device Farm is incorrect because this is an app testing service that lets you test and interact with your Android, iOS, and web apps on many devices at once, or reproduce issues on a device in real time.

DynamoDB Read Replica is incorrect because this is primarily used to automate capacity management for your tables and global secondary indexes.

References:
https://aws.amazon.com/dynamodb/dax
https://aws.amazon.com/device-farm
Check out this Amazon DynamoDB Cheat Sheet:
https://tutorialsdojo.com/aws-cheat-sheet-amazon-dynamodb/

QUESTION 172
A company wants to use an AWS Region as a disaster recovery location for its on-premises infrastructure. The company has 10 TB of existing data, and the on-premise data center has a 1 Gbps internet connection. A solutions architect must find a solution so the company can have its existing data on AWS in 72 hours without transmitting it using an unencrypted channel.
Which solution should the solutions architect select?

A. Send the initial 10 TB of data to AWS using FTP.
B. Send the initial 10 TB of data to AWS using AWS Snowball.
C. Establish a VPN connection between Amazon VPC and the company's data center.
D. Establish an AWS Direct Connect connection between Amazon VPC and the company's data center.

Answer: C
Explanation:
Keyword: AWS Region as DR for On-premises DC (Existing Data=10TB) + 1G Internet Connection

Condition: 10TB on AWS in 72 Hours + Without Unencrypted Channel

Without Unencrypted Channel = VPN

FTP = Unencrypted Channel

Options - A - Out of race, since this is unencrypted channel & not matching the condition
Options - B - Out of race due to the timebound target & order /delivering AWS Snowball device will take time
Options - C - Win th race, using the existing 1G Internet Link we can transfer this 10TB data within 24Hrs using encrypted Channel
Options - D - Out of race due to the timebound target & order /delivering AWS Direct Connect will take time

References:
https://docs.aws.amazon.com/snowball/latest/ug/mailing-storage.html
https://tutorialsdojo.com/aws-direct-connect/
https://tutorialsdojo.com/amazon-vpc/

QUESTION 173
A web application runs on Amazon EC2 instances behind an Application Load Balancer. The application allows users to create custom reports of historical weather data. Generating a report

can take up to 5 minutes. These long-running requests use many of the available incoming connections, making the system unresponsive to other users.
How can a solutions architect make the system more responsive?

A. Use Amazon SQS with AWS Lambda lo generate reports.
B. Increase the idle timeout on the Application Load Balancer to 5 minutes.
C. Update the client-side application code to increase its request timeout to 5 minutes.
D. Publish the reports to Amazon S3 and use Amazon CloudFront for downloading to the user.

Answer: A

QUESTION 174
A company decides to migrate its three-tier web application from on premises to the AWS Cloud. The new database must be capable of dynamically scaling storage capacity and performing table joins.
Which AWS service meets these requirements?

A. Amazon Aurora
B. Amazon RDS for SqlServer
C. Amazon DynamoDB Streams
D. Amazon DynamoDB on-demand

Answer: A

QUESTION 175
A company runs a website on Amazon EC2 instances behind an ELB Application Load Balancer. Amazon Route 53 is used for the DNS. The company wants to set up a backup website with a message including a phone number and email address that users can reach if the primary website is down.
How should the company deploy this solution?

A. Use Amazon S3 website hosting for the backup website and Route 53 failover routing policy.
B. Use Amazon S3 website hosting for the backup website and Route 53 latency routing policy.
C. Deploy the application in another AWS Region and use ELB health checks for failover routing.
D. Deploy the application in another AWS Region and use server-side redirection on the primary website.

Answer: A

QUESTION 176
A company needs to implement a relational database with a multi-Region disaster recovery Recovery Point Objective (RPO) of 1 second and an Recovery Time Objective (RTO) of 1 minute.
Which AWS solution can achieve this?

A. Amazon Aurora Global Database
B. Amazon DynamoDB global tables.
C. Amazon RDS for MySQL with Multi-AZ enabled.
D. Amazon RDS for MySQL with a cross-Region snapshot copy.

Answer: A

Explanation:
Cross-Region Disaster Recovery
If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage. This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.

QUESTION 177
A company running an on-premises application is migrating the application to AWS to increase its elasticity and availability. The current architecture uses a Microsoft SQL Server database with heavy read activity. The company wants to explore alternate database options and migrate database engines, if needed. Every 4 hours, the development team does a full copy of the production database to populate a test database. During this period, users experience latency.
What should a solution architect recommend as replacement database?

A. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore from mysqldump for the test database.
B. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore snapshots from Amazon RDS for the test database.
C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas, and use the standby instance for the test database.
D. Use Amazon RDS for SQL Server with a Multi-AZ deployment and read replicas, and restore snapshots from RDS for the test database.

Answer: D

QUESTION 178
A company currently stores symmetric encryption keys in a hardware security module (HSM). A solution architect must design a solution to migrate key management to AWS. The solution should allow for key rotation and support the use of customer provided keys. Where should the key material be stored to meet these requirements?

A. Amazon S3
B. AWS Secrets Manager
C. AWS Systems Manager Parameter store
D. AWS Key Management Service (AWS KMS)

Answer: B
Explanation:
AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.
https://aws.amazon.com/secrets-manager/

QUESTION 179
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 file gateway to provide file storage to AWS, then perform analytics on this data in the AWS Cloud.
B. 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.
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 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.

Answer: A

QUESTION 180
A company must re-evaluate its need for the Amazon EC2 instances it currently has provisioned in an Auto Scaling group. At present, the Auto Scaling group is configured for minimum of two instances and a maximum of four instances across two Availability zones. A Solutions architect reviewed Amazon CloudWatch metrics and found that CPU utilization is consistently low for the EC2 instances. What should the solutions architect recommend to maximize utilization while ensuring the application remains fault tolerant?

A. Remove some EC2 instances to increase the utilization of remaining instances.
B. Increase the Amazon Elastic Block Store (Amazon EBS) capacity of instances with less CPU utilization.
C. Modify the Auto Scaling group scaling policy to scale in and out based on a higher CPU utilization metric.
D. Create a new launch configuration that uses smaller instance types. Update the existing Auto Scaling group.

Answer: C

QUESTION 181
A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost effective, limit the? provisioning of Into and provide the fastest possible response time. Which combination should a solutions architect recommend to meet these requirements?

A. Amazon CloudFront and Amazon S3
B. AWS Lambda and Amazon Dynamo
C. Application Load Balancer with Amazon EC2 Auto Scaling
D. Amazon Route 53 with internal Application Load Balances

Answer: A

QUESTION 182
A company is developing a real-time multiplier game that uses UDP for communications between client and servers in an Auto Scaling group Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.
Which solution should a solution architect recommend?

A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.

B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
C. Use a Network Load Balancer for traffic distribution and amazon Aura Global for data storage.
D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage

Answer: B

QUESTION 183
A company currently has 250 TB of backup files stored in Amazon S3 in a vendor's proprietary format. Using a Linux-based software application provided by the vendor, the company wants to retrieve files from Amazon S3, transform the files to an industry-standard format, and re-upload them to Amazon S3. The company wants to minimize the data transfer charges associated with this conversation. What should a solution architect do to accomplish this?

A. Install the conversion software as an Amazon S3 batch operation so the data is transformed without leaving Amazon S3.
B. Install the conversion software onto an on-premises virtual machines. Perform the transformation and re-upload the files to Amazon S3 from the virtual machine.
C. Use AWS Snowball Edge device to expert the data and install the conversion software onto the devices. Perform the data transformation and re-upload the files to Amazon S3 from the Snowball devices.
D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re-upload the files to Amazon S3 from the EC2 instance.

Answer: D

QUESTION 184
A company has an Amazon EC2 instance running on a private subnet that needs to access a public websites to download patches and updates. The company does not want external websites to see the EC2 instance IP address or initiate connection to it.
How can a solution architect achieve this objective?

A. Create a site-to-site VPN connection between the private subnet and the network in which the public site is deployed
B. Create a NAT gateway in a public subnet Route outbound traffic from the private subnet through the NAI gateway
C. Create a network ACL for the private subnet where the EC2 instance deployed only allows access from the IP address range of the public website
D. Create a security group that only allows connections from the IP address range of the public website.
Attach the security group to the EC2 instance.

Answer: B

QUESTION 185
A company has created an isolated backup of its environment in another Region. The application is running in warm standby mode and is fronted by an Application Load Balancer (ALB). The current failover process is manual and requires updating a DNS alias record to point to the secondary ALB in another Region.

What should a solution architect do to automate the failover process?

A. Enable an ALB health check
B. Enable an Amazon Route 53 health check.
C. Crate an CNAME record on Amazon Route 53 pointing to the ALB endpoint.
D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server.

Answer: B
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/route-53-dns-health-checks/

QUESTION 186
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 be a Requester Pays bucket
B. Update the bucket to enable cross-origin resource sharing (CPORS)
C. Create a bucket policy to require users to grant bucket-owner-full when uploading objects
D. Create an IAM policy to require users to grant bucket-owner-full control when uploading objects.

Answer: C

QUESTION 187
A company uses Amazon S3 as its object storage solution. The company has thousands of S3 it uses to store data. Some of the S3 bucket have data that is accessed less frequently than others. A solutions architect found that lifecycle policies are not consistently implemented or are implemented partially. resulting in data being stored in high-cost storage.
Which solution will lower costs without compromising the availability of objects?

A. Use S3 ACLs
B. Use Amazon Elastic Block Store EBS) automated snapshots
C. Use S3 inteligent-Tiering storage
D. Use S3 One Zone-infrequent Access (S3 One Zone-IA).

Answer: C

QUESTION 188
A solution architect is performing a security review of a recently migrated workload. The workload is a web application that consists of amazon EC2 instances in an Auto Scaling group behind an Application Load balancer. The solution architect must improve the security posture and minimize the impact of a DDoS attack on resources.
Which solution is MOST effective?

A. Configure an AWS WAF ACL with rate-based rules Create an Amazon CloudFront distribution that points to the Application Load Balancer. Enable the EAF ACL on the CloudFront distribution
B. Create a custom AWS Lambda function that adds identified attacks into a common vulnerability pool to capture a potential DDoS attack. use the identified information to modify a network ACL to block access.

C. Enable VPC Flow Logs and store then in Amazon S3. Create a custom AWS Lambda functions that parses the logs looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.
D. Enable Amazon GuardDuty and , configure findings written 10 Amazon GloudWatch Create an event with Cloud Watch Events for DDoS alerts that triggers Amazon Simple Notification Service (Amazon SNS) Have Amzon SNS invoke a custom AWS lambda function that parses the logs looking for a DDoS attack Modify a network ACL to block identified source IP addresses

Answer: A

QUESTION 189
A company has a custom application running on an Amazon EC2 instance that:

- Reads a large amount of data from Amazon S3
- Performs a multi stage analysis
- Writes the results to Amazon DynamoDB

The application writes a significant number of large temporary files during the multi stage analysis The process performance depends on the temporary storage performance. What would be the fastest storage option for holding the temporary files?

A. Multiple Amazon S3 buckets with Transfer Acceleration for storage
B. Multiple Amazon EBS drives with Provisioned IOPS and EBS optimization
C. Multiple Amazon EFS volumes using the Network I lie System version 4.1 (NFSv4.1) protocol.
D. Multiple instance store volumes with software RAID 0.

Answer: D

QUESTION 190
A solution architect must migrate a Windows internet information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS). The solution architected has proposed migrating the IIS web servers Which replacement to the on-promises filo share is MOST resilient and durable?

A. Migrate the file Share to Amazon RDS.
B. Migrate the tile Share to AWS Storage Gateway
C. Migrate the file Share to Amazon FSx dor Windows File Server.
D. Migrate the tile share to Amazon Elastic File System (Amazon EFS)

Answer: C
Explanation:
https://aws.amazon.com/fsx/windows/

QUESTION 191
An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both are in separate AWS accounts.
The network administrator needs to design a solution to enable secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.
Which solution will meet these requirements?

A. Set up a VPC peering connection between VPC-A and VPC-B.
B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.
C. Attach a virtual private gateway to VPC-B and enable routing from VPC-A.
D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-B.

Answer: A
Explanation:
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The traffic remains in the private IP space. All inter-region traffic is encrypted with no single point of failure, or bandwidth bottleneck.
https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

QUESTION 192
A company is seeing access requests by some suspicious IP addresses. The security team discovers the requests are from different IP addresses under the same CIDR range. What should a solutions architect recommend to the team?

A. Add a rule in the inbound table of the security to deny the traffic from that CIDR range.
B. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range.
C. Add a deny rule in the inbound table of the network ACL with a lower number than other rules.
D. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules.

Answer: C
Explanation:
You can only create deny rules with network ACLs, it is not possible with security groups. Network ACLs process rules in order from the lowest numbered rules to the highest until they reach and allow or deny. The following table describes some of the differences between security groups and network ACLs:

Security Group	Network ACL
Operates at the instance (interface) level	Operates at the subnet level
Supports allow rules only	Supports allow and deny rules
Stateful	Stateless
Evaluates all rules	Processes rules in order
Applies to an instance only if associated with a group	Automatically applies to all instances in the subnets its associated with

Therefore, the solutions architect should add a deny rule in the inbound table of the network ACL with a lower rule number than other rules.

CORRECT: "Add a deny rule in the inbound table of the network ACL with a lower rule number than other rules" is the correct answer.
INCORRECT: "Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules" is incorrect as this will only block outbound traffic.
INCORRECT: "Add a rule in the inbound table of the security group to deny the traffic from that CIDR range" is incorrect as you cannot create a deny rule with a security group.
INCORRECT: "Add a rule in the outbound table of the security group to deny the traffic from that CIDR range" is incorrect as you cannot create a deny rule with a security group.
References:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

QUESTION 193
A company is using a VPC peering strategy to connect its VPCs in a single Region to allow for cross- communication. A recent increase in account creations and VPCs has made it difficult to maintain the VPC peering strategy, and the company expects to grow to hundreds of VPCs. There are also new requests to create site-to-site VPNs with some of the VPCs. A solutions architect has been tasked with creating a centrally networking setup for multiple accounts, VPNS, and VPNs.
Which networking solution meets these requirements?

A. Configure shared VPCs and VPNs and share to each other
B. Configure a hub-and-spoke and route all traffic through VPC peering.
C. Configure an AWS Direct Connect between all VPCs and VPNs.
D. Configure a transit gateway with AWS Transit Gateway and connected all VPCs and VPNs.

Answer: D

QUESTION 194
A monolithic application was recently migrated to AWS and is now running on a single Amazon EC2 instance. Due to application limitations, it is not possible to use automatic scaling to scale out the application. The chief technology officer (CTO) wants an automated solution to restore the EC2 instance in the unlikely event the underlying hardware fails.
What would allow for automatic recovery of the EC2 instance as quickly as possible?

A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.
B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired.
C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired, triggered instance recovery.
D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy.

Answer: A
Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html

QUESTION 195
A company has created a VPC with multiple private subnets in multiple Availability Zones (AZs) and one public subnet in one of the AZs. The public subnet is used to launch a NAT gateway. There are instance in the private subnet that use a NAT gateway to connect to the internet. In

case is used of an AZ failure, the company wants to ensure that the instance are not all experiencing internet connectivity issues and that there is a backup plan ready.
Which solution should a solutions architect recommend that is MOST highly available?

A. Create a new public subnet with a NAT gateway in the same AZ Distribute the traffic between the two NAT gateways
B. Create an Amazon EC2 NAT instance in a now public subnet Distribute the traffic between the NAT gateway and the NAT instance
C. Create public subnets In each f\Z and launch a NAT gateway in each subnet Configure the traffic from the private subnets In each A2 to the respective NAT gateway
D. Create an Amazon EC2 NAT instance in the same public subnet Replace the NAT gateway with the NAT instance and associate the instance with an Auto Scaling group with an appropriate scaling policy.

Answer: C

QUESTION 196
A company has multiple AWS accounts, for various departments. One of the departments wants to share an Amazon S3 bucket with all other department.
Which solution will require the LEAST amount of effort-?

A. Enable cross-account S3 replication for the bucket
B. Create a pre signed URL tor the bucket and share it with other departments
C. Set the S3 bucket policy to allow cross-account access to other departments
D. Create IAM users for each of the departments and configure a read-only IAM policy

Answer: C

QUESTION 197
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 site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
D. 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.

Answer: A

QUESTION 198
A company has implemented one of its microservices on AWS Lambda that accesses an Amazon DynamoDB table named Books. A solutions architect is design an IAM policy to be attached to the Lambda function's IAM role, giving it access to put, update, and delete items in the Books

table. the IAM policy must prevent function from performing any other actions on the Books table or any other. Which IAM policy would fulfill these needs and provide the LEAST privileged access?

A.
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PutUpdateDeleteOnBooks",
         "Effect": "Allow",
         "Action": [
            "dynamodb: PutItem",
            "dynamodb: UpdateItem",
            "dynamodb: DeleteItem"
         ],
         "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
      }
   ]
}
```

B.
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PutUpdateDeleteOnBooks",
         "Effect": "Allow",
         "Action": [
            "dynamodb: PutItem",
            "dynamodb: UpdateItem",
            "dynamodb: DeleteItem"
         ],
         "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/*"
      }
   ]
}
```

C.
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PutUpdateDeleteOnBooks",
         "Effect": "Allow",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
      }
   ]
}
```

D.
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PutUpdateDeleteOnBooks",
         "Effect": "Allow",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
      },
      {
         "Sid": "PutUpdateDeleteOnBooks",
         "Effect": "Deny",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
   ]
}
```

Answer: A

QUESTION 199
Application developers have noticed that a production application is very slow when business reporting users run large production reports against the Amazon RDS instance backing the application. the CPU and memory utilization metrics for the RDS instance-d not exceed 60% while the reporting queries are running. The business reporting users must be able to generate reports without affecting the applications performance.
Which action will accomplish this?

A. Increase the size of the RDS instance
B. Create a read replica and connect the application to it.
C. Enable multiple Availability Zones on the RDS instance
D. Create a read replication and connect the business reports to it.

Answer: D

QUESTION 200
A company's packaged application dynamically creates and returns single-use text files in response to user requests. The company is using Amazon CloudFront for distribution, but wants to future reduce data transfer costs. The company modify the application's source code.
What should a solution architect do to reduce costs?

A. Use Lambda@Edge to compress the files as they are sent to users.
B. Enable Amazon S3 Transfer Acceleration to reduce the response times.
C. Enable caching on the CloudFront distribution to store generated files at the edge.
D. Use Amazon S3 multipart uploads to move the files to Amazon S3 before returning them to users.

Answer: A
Explanation:
B seems more expensive; C does not seem right because they are single use files and will not be needed again from the cache; D multipart mainly for large files and will not reduce data and cost; A seems the best: change the application code to compress the files and reduce the amount of data transferred to save costs.

QUESTION 201
A public-facing web application queries a database hosted on a Amazon EC2 instance in a private subnet. A large number of queries involve multiple table joins, and the application performance has been degrading due to an increase in complex queries. The application team will be performing updates to improve performance.
What should a solutions architect recommend to the application team? (Select TWO.)

A. Cache query data in Amazon SQS
B. Create a read replica to offload queries
C. Migrate the database to Amazon Athena
D. Implement Amazon DynamoDB Accelerator to cache data.
E. Migrate the database to Amazon RDS

Answer: BE

QUESTION 202
A company has a Microsoft Windows-based application that must be migrated to AWS. This application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances. What should a solution architect do to accomplish this?

A. Configure a volume using Amazon EFS Mount the EPS volume to each Windows Instance
B. Configure AWS Storage Gateway in Volume Gateway mode Mount the volume to each Windows instance
C. Configure Amazon FSx for Windows File Server Mount the Amazon FSx volume to each Windows Instance
D. Configure an Amazon EBS volume with the required size Attach each EC2 instance to the volume Mount the file system within the volume to each Windows instance

Answer: C

QUESTION 203
A company recently expanded globally and wants to make its application accessible to users in those geographic locations. The application is deploying on Amazon EC2 instances behind an Application Load balancer in an Auto Scaling group. The company needs the ability shift traffic from resources in one region to another.
What should a solutions architect recommend?

A. Configure an Amazon Route 53 latency routing policy
B. Configure an Amazon Route 53 geolocation routing policy
C. Configure an Amazon Route 53 geoproximity routing policy.
D. Configure an Amazon Route 53 multivalue answer routing policy

Answer: C
Explanation:
Keyword: Users in those Geographic Locations

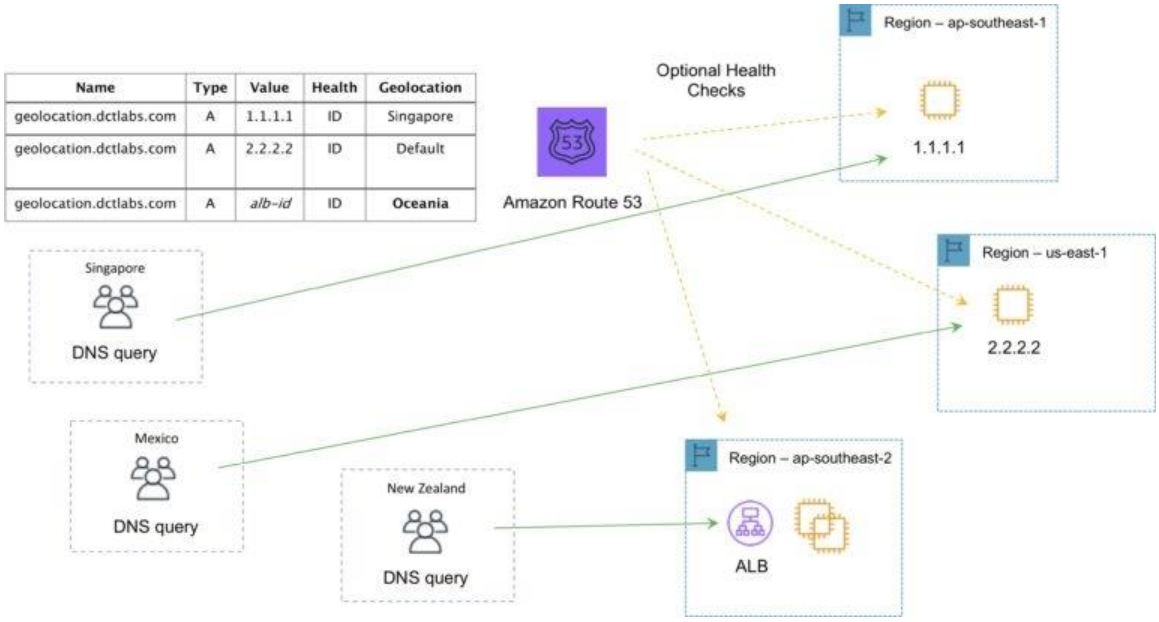
Condition: Ability Shift traffic from resources in One Region to Another Region

The following table highlights the key function of each type of routing policy:

Policy	What it Does
Simple	Simple DNS response providing the IP address associated with a name
Failover	If primary is down (based on health checks), routes to secondary destination
Geolocation	Uses geographic location you're in (e.g. Europe) to route you to the closest region
Geoproximity	Routes you to the closest region within a geographic area
Latency	Directs you based on the lowest latency route to resources
Multivalue answer	Returns several IP addresses and functions as a basic load balancer
Weighted	Uses the relative weights assigned to resources to determine which to route to

Geo-location:
- Caters to different users in different countries and different languages.
- Contains users within a particular geography and offers them a customized version of the workload based on their specific needs.
- Geolocation can be used for localizing content and presenting some or all of your website in the language of your users.
- Can also protect distribution rights.
- Can be used for spreading load evenly between regions.
- If you have multiple records for overlapping regions, Route 53 will route to the smallest geographic region.
- You can create a default record for IP addresses that do not map to a geographic location.

The following diagram depicts an Amazon Route 53 Geolocation routing policy configuration:



Reference:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html
https://aws.amazon.com/route53/?nc2=h_ql_prod_nt_r53

QUESTION 204
A company has several business systems that require access to data stored in a file share. the business systems will access the file share using the Server Message Block (SMB) protocol. The file share solution should be accessible from both of the company's legacy on-premises environment and with AWS. Which services mod the business requirements? (Select TWO.)

A. Amazon EBS
B. Amazon EFS
C. Amazon FSx for Windows
D. Amazon S3
E. AWS Storage Gateway file gateway

Answer: CE

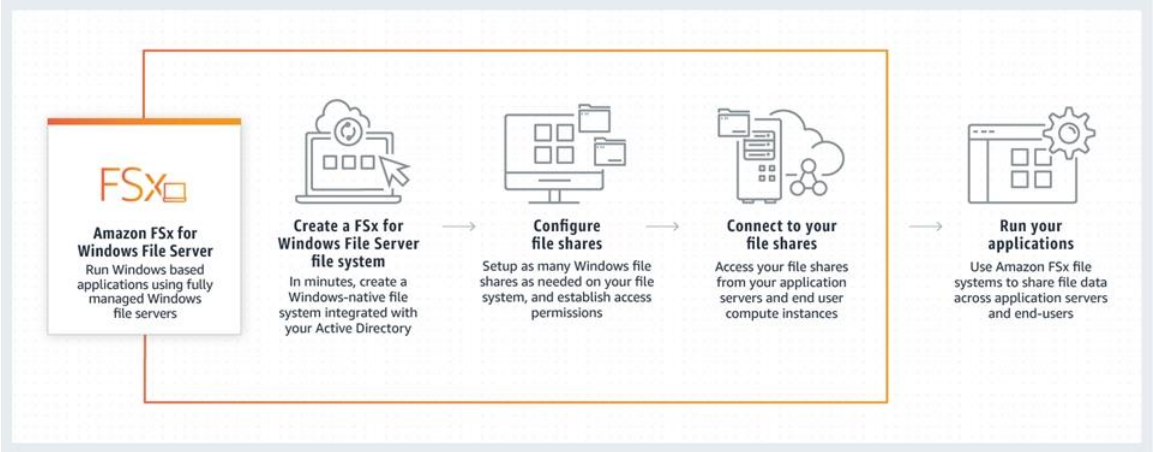
Explanation:
Keyword: SMB + On-premises

Condition: File accessible from both on-premises and AWS

Amazon FSx for Windows File Server

Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. It offers single-AZ and multi-AZ deployment options, fully managed backups, and encryption of data at rest and in transit. You can optimize cost and performance for your workload needs with SSD and HDD storage options; and you can scale storage and change the throughput performance of your file system at any time. Amazon FSx file storage is accessible from Windows, Linux, and MacOS compute instances and devices running on AWS or on premises.

How FSx for Windows File Server works

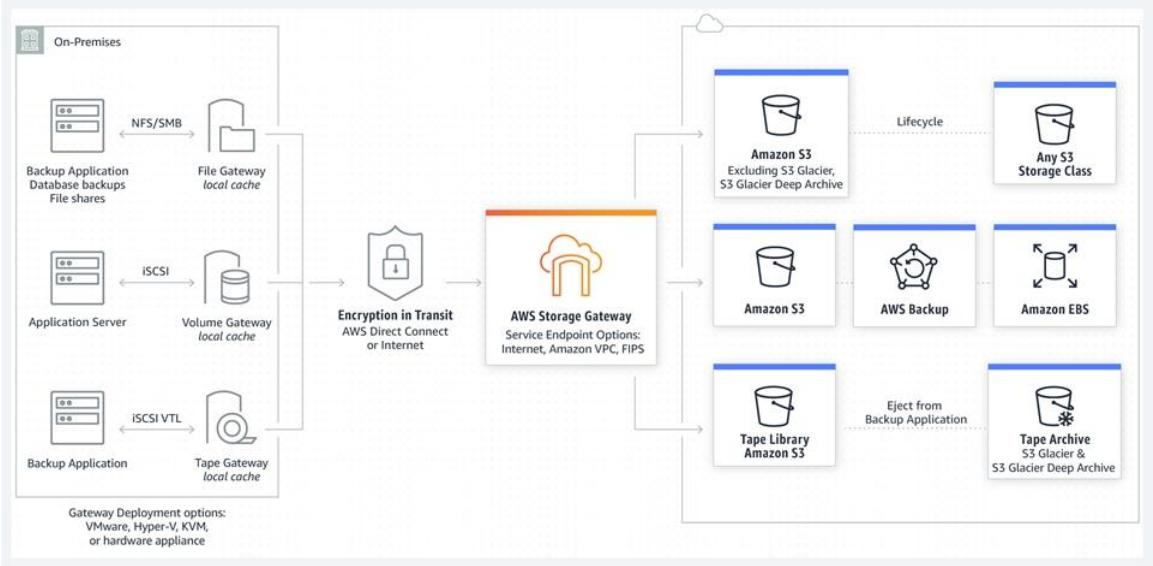


AWS Storage Gateway

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications.

To support these use cases, Storage Gateway offers three different types of gateways – File Gateway, Tape Gateway, and Volume Gateway – that seamlessly connect on-premises applications to cloud storage, caching data locally for low-latency access. Your applications connect to the service through a virtual machine or gateway hardware appliance using standard storage protocols, such as NFS, SMB, and iSCSI. The gateway connects to AWS storage services, such as Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Amazon EBS, and AWS Backup, providing storage for files, volumes, snapshots, and virtual tapes in AWS. The service includes a highly-optimized and efficient data transfer mechanism, with bandwidth management and automated network resilience.

How Storage Gateway works



The table below shows the different gateways available and the interfaces and use cases:

New Name	Old Name	Interface	Use Case
File Gateway	None	NFS, SMB	Allow on-prem or EC2 instances to store objects in S3 via NFS or SMB mount points
Volume Gateway Stored Mode	Gateway-Stored Volumes	iSCSI	Asynchronous replication of on-prem data to S3
Volume Gateway Cached Mode	Gateway-Cached Volumes	iSCSI	Primary data stored in S3 with frequently accessed data cached locally on-prem
Tape Gateway	Gateway-Virtual Tape Library	ISCSI	Virtual media changer and tape library for use with existing backup software

CORRECT: "Amazon FSx for Windows" is the correct answer.
CORRECT: "Amazon Storage File Gateway" is the correct answer.

INCORRECT: "Amazon EBS" is incorrect as unsupported NFS/SMB.
INCORRECT: "Amazon EFS" is incorrect as unsupported NFS/SMB.
INCORRECT: "Amazon S3" is incorrect as unsupported NFS/SMB.

References:
https://aws.amazon.com/fsx/windows/
https://aws.amazon.com/storagegateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc
https://aws.amazon.com/blogs/aws/file-interface-to-aws-storage-gateway/
https://d0.awsstatic.com/whitepapers/aws-storage-gateway-file-gateway-for-hybrid-architectures.pdf

https://youtu.be/T5KlnNj7-qg

QUESTION 205
A company's operations teams has an existing Amazon S3 bucket configured to notify an Amazon SQS queue when new object are created within the bucket. The development team also wants to receive events when new objects are created. The existing operations team workflow must remain intact.
Which solution would satisfy these requirements?

A. Create another SQS queue Update the S3 events in bucket to also update the new queue when a new object is created.
B. Create a new SQS queue that only allows Amazon S3 to access the queue, Update Amazon S3 update this queue when a new object is created
C. Create an Amazon SNS topic and SQS queue for the Update. Update the bucket to send events to the new topic. Updates both queues to poll Amazon SNS.
D. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic Add subscription for both queue in the topic.

Answer: D

QUESTION 206
A company wants to deploy a shared file system for its .NET application servers and Microsoft SQL Server database running on Amazon EC2 instance with Windows Server 2016. The solution must be able to be integrated in to the corporate Active Directory domain, be highly durable, be managed by AWS, and provided levels of throuput and IOPS.
Which solution meets these requirements?

A. Use Amazon FSx for Windows File Server
B. Use Amazon Elastic File System (Amazon EFS)
C. Use AWS Storage Gateway in file gateway mode.
D. Deploy a Windows file server on two On Demand instances across two Availability Zones.

Answer: A
Explanation:
https://aws.amazon.com/fsx/windows/

QUESTION 207
A company is designing a new service that will run on Amazon EC2 instance behind an Elastic Load Balancer. However, many of the web service clients can only reach IP addresses whitelisted on their firewalls.
What should a solution architect recommend to meet the clients' needs? What should a solution architect recommend to meet the clients' needs?

A. A Network Load Balancer with an associated Elastic IP address.
B. An Application Load Balancer with an a associated Elastic IP address
C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address
D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

Answer: C
Explanation:
Route 53 routes end users to Internet applications so the correct answer is C. Map one of the whitelisted IP addresses using an A record to the Elastic IP address.

QUESTION 208
A company is designing a new service that will run on Amazon EC2 instance behind an Elastic Load Balancer.
However, many of the web service clients can only reach IP addresses whitelisted on their firewalls.
What should a solution architect recommend to meet the clients' needs?

A. A Network Load Balancer with an associated Elastic IP address.
B. An Application Load Balancer with an a associated Elastic IP address
C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address
D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

Answer: A
Explanation:
https://acloud.guru/forums/aws-csysops-2019/discussion/-LzN1_Aw0dL3Z98CkBs1/Using%20EIP%20for%20ALB
https://www.bluematador.com/blog/static-ips-for-aws-application-load-balancer

QUESTION 209
A company is investigating potential solutions that would collect, process, and store users' service usage data.
The business objective is to create an analytics capability that will enable the company to gather operational insights quickly using standard SQL queries.
The solution should be highly available and ensure Atomicity, Consistency, Isolation, and Durability (ACID) compliance in the data tier.
Which solution should a solutions architect recommend?

A. Use Amazon DynamoDB transactions
B. Create an Amazon Neptune database in a Multi AZ design
C. Use a fully managed Amazon RDS for MySQL database in a Multi-AZ design
D. Deploy PostgreSQL on an Amazon EC2 instance that uses Amazon EBS Throughput Optimized HDD (st1) storage.

Answer: C

QUESTION 210
A company runs a web service on Amazon CC2 instances behind an Application Load Balancer.
The instances run in an Amazon EC2 Auto Scaling group across two Availability zones.
The company needs a minimum of tour instances a! all limes to meet the required service level agreement (SLA) while keeping costs low.
If an Availability Zone tails, how can the company remain compliant with the SLA?

A. Add a target tracking scaling policy with a short cooldown period
B. Change the Auto Scaling group launch configuration to use a larger instance type
C. Change the Auto Scaling group to use six servers across three Availability Zones
D. Change the Auto Scaling group to use eight servers across two Availability Zones

Answer: C

QUESTION 211
An ecommerce company has noticed performance degradation of its Amazon RDS based web application.
The performance degradation is attribute to an increase in the number of read-only SQL queries triggered by business analysts.
A solution architect needs to solve the problem with minimal changes to the existing web application.
What should the solution architect recommend?

A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
B. Load the data into Amazon ElasticCache and have the business analysts run their queries.
C. Create a read replica of the primary database and have the business analysts run their queries.
D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Answer: C

QUESTION 212
A company is building applications in containers.
The company wants to migrate its on-premises development and operations services from its on-premises data center to AWS.
Management states that production system must be cloud agnostic and use the same configuration and administrator tools across production systems.
A solutions architect needs to design a managed solution that will align open-source software.
Which solution meets these requirements?

A. Launch the containers on Amazon EC2 with EC2 instance worker nodes.
B. Launch the containers on Amazon Elastic Kubernetes Service (Amazon EKS) and EKS workers nodes.
C. Launch the containers on Amazon Elastic Containers service (Amazon ECS) with AWS Fargate instances.
D. Launch the containers on Amazon Elastic Container Service (Amazon EC) with Amazon EC2 instance worker nodes.

Answer: B
Explanation:
When talking about containerized applications, the leading technologies which will always come up during the conversation are Kubernetes and Amazon ECS (Elastic Container Service).
While Kubernetes is an open-sourced container orchestration platform that was originally developed by Google, Amazon ECS is AWS' proprietary, managed container orchestration service.

QUESTION 213
A company is running a two-tier ecommerce website using services.
The current architect uses a publish- facing Elastic Load Balancer that sends traffic to Amazon EC2 instances in a private subnet.
The static content is hosted on EC2 instances, and the dynamic content is retrieved from a MYSQL database.
The application is running in the United States. The company recently started selling to users in Europe and Australia.
A solution architect needs to design solution so their international users have an improved browsing experience.
Which solution is MOST cost-effective?

A. Host the entire website on Amazon S3.
B. Use Amazon CloudFront and Amazon S3 to host static images.
C. Increase the number of public load balancers and EC2 instances
D. Deploy the two-tier website in AWS Regions in Europe and Austraila.

Answer: B

QUESTION 214
A database is on an Amazon RDS MYSQL 5.6 Multi-AZ DB instance that experience highly dynamic reads.
Application developers notice a significant slowdown when testing read performance from a secondary AWS Region.
The developers want a solution that provides less than 1 second of read replication latency.
What should the solutions architect recommend?

A. Install MySQL on Amazon EC2 in (he secondary Region.
B. Migrate the database to Amazon Aurora with cross-Region replicas.
C. Create another RDS for MySQL read replica in the secondary.
D. Implement Amazon ElastiCache to improve database query performance.

Answer: B

QUESTION 215
An operations team has a standard that states IAM policies should not be applied directly to users.
Some new members have not been following this standard.
The operation manager needs a way to easily identify the users with attached policies.
What should a solutions architect do to accomplish this?

A. Monitor using AWS CloudTrail
B. Create an AWS Config rule to run daily
C. Publish IAM user changes lo Amazon SNS
D. Run AWS Lambda when a user is modified

Answer: B
Explanation:
A new AWS Config rule is deployed in the account after you enable AWS Security Hub. The AWS Config rule reacts to resource configuration and compliance changes and send these change items to AWS CloudWatch. When AWS CloudWatch receives the compliance change, a CloudWatch event rule triggers the AWS Lambda function.

QUESTION 216
A company has established a new AWS account.
The account is newly provisioned and no changed have been made to the default settings.
The company is concerned about the security of the AWS account root user.
What should be done to secure the root user?

A. Create IAM users for daily administrative tasks.
Disable the root user.
B. Create IAM users for daily administrative tasks.
Enable multi-factor authentication on the root user.

C. Generate an access key for the root user.
Use the access key for daily administration tasks instead of the AWS Management Console.
D. Provide the root user credentials to the most senior solution architect.
Have the solution architect use the root user for daily administration tasks.

Answer: B

QUESTION 217
A healthcare company stores highly sensitive patient records.
Compliance requires that multiple copies be stored in different locations Each record must be stored for 7 years.
The company has a service level agreement (SLA) to provide records to government agencies immediately for the first 30 days and then within 4 hours of a request thereafter.
What should a solutions architect recommend?

A. Use Amazon S3 with cross-Region replication enabled.
After 30 days, transition the data to Amazon S3 Glacier using lifecycle policy
B. Use Amazon S3 with cross-origin resource sharing (CORS) enabled.
After 30 days, transition the data to Amazon S3 Glacier using a lifecycle policy.
C. Use Amazon S3 with cross-Region replication enabled.
After 30 days, transition the data to Amazon S3 Glacier Deep Achieve using a lifecycle policy
D. Use Amazon S3 with cross-origin resource sharing (GORS) enabled.
After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy

Answer: A

QUESTION 218
A solutions architect must create a highly available bastion host architecture.
The solution needs to be resilient within a single AWS Region and should require only minimal effort to maintain.
What should the solutions architect do to meet these requirements?

A. Create a Network Load Balancer backed by an Auto Scaling group with a UDP listener.
B. Create a Network Load Balancer backed by a Spot Fleet with instances in a group with instances in a partition placement group.
C. Create a Network Load Balancer backed by the existing serves in different Availability Zones as the target.
D. Create a Network Load Balancer backed by an Auto Scaling with instances in multiple Availability zones as the target

Answer: D

QUESTION 219
A solution architect is designing a hybrid application using the AWS cloud.
The network between the on- premises data center and AWS will use an AWS Direct Connect (DX) connection.
The application connectivity between AWS and the on-premises data center must be highly resilient.
Which DX configuration should be implemented to meet these requirements?

A. Configure a DX connection with a VPN on top of it.

B. Configure DX connections at multiple DX locations.
C. Configure a DX connection using the most reliable DX partner.
D. Configure multiple virtual interfaces on top of a DX connection.

Answer: B

QUESTION 220
A company plans to store sensitive user data on Amazon S3.
Internal security compliance requirement mandata encryption of data before sending it to Amazon S3.
What should a solution architect recommend to satisfy these requirements?

A. Server-side encryption with customer-provided encryption keys
B. Client-side encryption with Amazon S3 managed encryption keys
C. Server-side encryption with keys stored in AWS key Management Service (AWS KMS)
D. Client-side encryption with a master key stored in AWS Key Management Service (AWS KMS)

Answer: D
Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html

QUESTION 221
A company is using Amazon EC2 to run its big data analytics workloads.
These variable workloads run each night, and it is critical they finish by the start of business the following day.
A solutions architect has been tasked with designing the MOST cost-effective solution.
Which solution will accomplish this?

A. Spot Fleet
B. Spot Instances
C. Reserved Instances
D. On-Demand Instances

Answer: C

QUESTION 222
A company mandates that an Amazon S3 gateway endpoint must allow traffic to trusted buckets only.
Which method should a solutions architect implement to meet this requirement?

A. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's trusted VPCs
B. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's S3 gateway endpoint IDs
C. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that blocks access from any VPC other than the company's trusted VPCs
D. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that provides access to the Amazon Resource Name (ARN) of the trusted S3 buckets

Answer: D

QUESTION 223
A company is designing a web application using AWS that processes insurance quotes Users will request quotes from the application.
Quotes must be separated by quote type must be responded to within 24 hours, and must not be lost.
The solution should be simple to set up and maintain.
Which solution meets these requirements?

A. Create multiple Amazon Kinesis data streams based on the quote type.
Configure the web application to send messages to the proper data stream.
Configure each backend group of application servers to pool messages from its own data stream using the Kinesis Client Library (KCL)
B. Create multiple Amazon Simple Notification Service (Amazon SNS) topics and register Amazon SQS queues to their own SNS topic based on the quote type.
Configure the web application to publish messages to the SNS topic queue.
Configure each backend application server to work its own SQS queue
C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic.
Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type.
Configure each backend application server to work its own SQS queue.
D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasticsearch Service (Amazon ES) cluster.
Configure the web application to send messages to the proper delivery stream.
Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly

Answer: C
Explanation:
https://docs.aws.amazon.com/sns/latest/dg/sns-message-filtering.html
It all depends on where you want to do the quote type classification i.e. in the app and send to a different/multiple SNS topics (B) or use SNS filtering to do the type classification (C). The question doesn't really give you enough info to make a clear choice but configuring SNS filtering is probablgt less work and easier to maintain than maintaining app code.

QUESTION 224
A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database Compliance regulations mandate that all personally identifiable information (Pll) be encrypted at rest.
Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure"

A. Deploy AWS Certificate Manager to generate certificates.
Use the certificates to encrypt the database volume
B. Deploy AWS CloudHSM. generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.
C. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes
D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

Answer: D

QUESTION 225
A company is creating an architecture for a mobile app that requires minimal latency for its users. The company's architecture consists of Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group.
The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data However the metrics indicate that the EC2 instances do not cross any CPU utilization thresholds
How can this issue be addressed1?

A. Reduce the threshold for CPU utilization in the Auto Scaling group
B. Replace the Application Load Balancer with a Network Load Balancer.
C. Add read replicas for the RDS instances and direct read traffic to the replica.
D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance.

Answer: C

QUESTION 226
A company recently released a new type of internet-connected sensor.
The company is expecting lo sell thousands of sensors, which are designed to stream high volumes of data each second to a central location.
A solutions architect must design a solution that ingests and stores data so that engineering teams can analyze it in near-real time with millisecond responsiveness.
Which solution should the solutions architect recommend?

A. Use an Amazon SQS queue to ingest the data.
Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
B. Use an Amazon SOS queue to ingest the data.
Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.
C. Use Amazon Kinesis Data Streams to ingest the data.
Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
D. Use Amazon Kinesis Data Streams to ingest the data.
Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.

Answer: D
Explanation:
https://aws.amazon.com/blogs/big-data/analyze-data-in-amazon-dynamodb-using-amazon-sagemaker-for-real-time-prediction/

QUESTION 227
A company is migrating a NoSQL database cluster to Amazon EC2.
The database automatically replicates data to maintain at least three copies of the data. I/O throughput of the servers is the highest priority.
Which instance type should a solutions architect recommend for the migration?

A. Storage optimized instances with instance store

B. Burstable general purpose instances with an Amazon Elastic Block Store (Amazon EBS) volume
C. Memory optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled
D. Compute optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled

Answer: A

QUESTION 228
A company operates a website on Amazon EC2 Linux instances.
Some of the instances are faring Troubleshooting points to insufficient swap space on the failed instances.
The operations team lead needs a solution to monitor this.
What should a solutions architect recommend?

A. Configure an Amazon CloudWatch SwapUsage metric dimension.
Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.
B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics.
Monitor SwapUsage metrics in CloudWatch.
C. Install an Amazon CloudWatch agent on the instances.
Run an appropriate script on a set schedule.
Monitor SwapUtilizalion metrics in CloudWatch.
D. Enable detailed monitoring in the EC2 console.
Create an Amazon CloudWatch SwapUtilizalion custom metric.
Monitor SwapUtilization metrics in CloudWatch.

Answer: C
Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html

QUESTION 229
A company has two applications it wants to migrate to AWS.
Both applications process a large set of files by accessing the same files at the same time.
Both applications need to read the files with low latency.
Which architecture should a solutions architect recommend for this situation?

A. Configure two AWS Lambda functions to run the applications.
Create an Amazon EC2 instance with an instance store volume to store the data.
B. Configure two AWS Lambda functions to run the applications.
Create an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume to store the data.
C. Configure one memory optimized Amazon EC2 instance to run both applications simultaneously.
Create an Amazon Elastic Block Store (Amazon EBS) volume with Provisioned IOPS to store the data.
D. Configure two Amazon EC2 instances to run both applications.
Configure Amazon Elastic File System (Amazon EFS) with General Purpose performance mode and Bursting.
Throughput mode to store the data.

Answer: D

QUESTION 230
A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances.
A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.
Which solution achieves these goals MOST efficiently?

A. Use a scheduled AWS Lambda function and execute a script remotely on all EC2 instances to send data to the audit system.
B. Use EC2 Auto Scaling lifecycle hooks to execute a custom script to send data to the audit system when instances are launched and terminated.
C. Use an EC2 Auto Scaling launch configuration to execute a custom script through user data to send data to the audit system when instances are launched and terminated.
D. Execute a custom script on the instance operating system to send data to the audit system. Configure the script to be executed by the EC2 Auto Scaling group when the instance starts and is terminated.

Answer: B

QUESTION 231
A company requires a durable backup storage solution for its on-premises database servers while ensuring on-premises applications maintain access to these backups for quick recovery.
The company will use AWS storage services as the destination for these backups.
A solutions architect is designing a solution with minimal operational overhead.
Which solution should the solutions architect implement?

A. Deploy an AWS Storage Gateway file gateway on-premises and associate it with an Amazon S3 bucket
B. Back up the databases to an AWS Storage Gateway volume gateway and access it using the Amazon S3 API.
C. Transfer the database backup files to an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance.
D. Back up the database directly to an AWS Snowball device and uss lifecycle rules to move the data to Amazon S3 Glacier Deep Archive.

Answer: A

QUESTION 232
A company has a web server running on an Amazon EC2 instance in a public subnet with an Elastic IP address.
The default security group is assigned to the EC2 instance.
The default network ACL has been modified to block all traffic.
A solutions architect needs to make the web server accessible from everywhere on port 443.
Which combination of steps will accomplish this task? (Select TWO.)

A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.
B. Create a security group with a rule to allow TCP port 443 to destination 0 0 0 0/0.
C. Update the network ACL to allow TCP port 443 from source 0.0 0 0/0.
D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0 0/0 and outbound TCP port 32768-65535 to destination 0 0 0.0/0

Answer: AE

QUESTION 233
A company hosts its website on AWS. To address the highly variable demand, the company has implemented Amazon EC2 Auto Scaling.
Management is concerned that the company is over- provisioning its infrastructure, especially at the front end of the three-tier application.
A solutions architect needs to ensure costs are optimized without impacting performance.
What should the solutions architect do to accomplish this?

A. Use Auto Scaling with Reserved Instances.
B. Use Auto Scaling with a scheduled scaling policy.
C. Use Auto Scaling with the suspend-resume feature
D. Use Auto Scaling with a target tracking scaling policy.

Answer: D
Explanation:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html

QUESTION 234
A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application.
A solutions architect wants to implement a solution that is highly available fault tolerant, and automatically scalable.
What should the solutions architect recommend?

A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.
D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

Answer: C

QUESTION 235
A solutions architect is working on optimizing a legacy document management application running on Microsoft Windows Server in an on-premises data center.
The application stores a large number of files on a network file share.
The chief information officer wants to reduce the on-premises data center footprint and minimize storage costs by moving on-premises storage to AWS.
What should the solutions architect do to meet these requirements?

A. Set up an AWS Storage Gateway file gateway.
B. Set up Amazon Elastic File System (Amazon EFS)
C. Set up AWS Storage Gateway as a volume gateway
D. Set up an Amazon Elastic Block Store (Amazon EBS) volume.

Answer: A

QUESTION 236
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 Glacier after 30 days.
C. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) 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.

Answer: C

QUESTION 237
A recent analysis of a company's IT expenses highlights the need to reduce backup costs.
The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes.
The company must preserve the existing investment in the on-premises backup applications and workflows.
What should a solutions architect recommend?

A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface
C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface
D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

Answer: D
Explanation:

Tape Gateway

- Some companies have backup processes using physical tapes (!)
- With Tape Gateway, companies use the same processes but in the cloud
- Virtual Tape Library (VTL) backed by Amazon S3 and Glacier
- Back up data using existing tape-based processes (and iSCSI interface)
- Works with leading backup software vendors

QUESTION 238
A company wants to replicate its data to AWS to recover in the event of a disaster.
Today, a system administrator has scripts that copy data to a NFS share Individual backup files need to be accessed with low latency by application administrators to deal with errors in processing.
What should a solutions architect recommend to meet these requirements?

A. Modify the script to copy data to an Amazon S3 bucket instead of the on-premises NFS share
B. Modify the script to copy data to an Amazon S3 Glacier Archive instead of the on-premises NFS share
C. Modify the script to copy data to an Amazon Elastic File System (Amazon EFS) volume instead of the on-premises NFS share.
D. Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises NFS share.

Answer: D

QUESTION 239
A solutions architect is designing the storage architecture for a new web application used for stonng and viewing engineering drawings.
All application components will be deployed on the AWS infrastructure.
The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load.
The application must be able to store petabytes of data.
Which combination of storage and caching should the solutions architect use?

A. Amazon S3 with Amazon CloudFront
B. Amazon S3 Glacier with Amazon ElastiCache
C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
D. AWS Storage Gateway with Amazon ElastiCache

Answer: A

Explanation:
CloudFront for caching and S3 as the origin. Glacier is used for archiving which is not the case for this scenario.

QUESTION 240
A company that develops web applications has launched hundreds of Application Load Balancers (ALBs) in multiple Regions.
The company wants to create an allow list (or the IPs of all the load balancers on its firewall device.
A solutions architect is looking for a one-time, highly available solution to address this request, which will also help reduce the number of IPs that need to be allowed by the firewall.
What should the solutions architect recommend to meet these requirements?

A. Create a AWS Lambda function to keep track of the IPs for all the ALBs in different Regions Keep refreshing this list.
B. Set up a Network Load Balancer (NLB) with Elastic IPs.
Register the private IPs of all the ALBs as targets to this NLB.
C. Launch AWS Global Accelerator and create endpoints for all the Regions.
Register all the ALBs in different Regions to the corresponding endpoints
D. Set up an Amazon EC2 instance, assign an Elastic IP to this EC2 instance, and configure the instance as a proxy to forward traffic to all the ALBs.

Answer: C

QUESTION 241
A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3.
The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services.
Which solution should a solutions architect recommend to keep the data private?

A. Deploy an AWS DataSync agent tor the on-premises environment.
Configure a sync job to replicate the data and connect it with an AWS service endpoint.
B. Deploy an AWS DataSync agent for the on-premises environment.
Schedule a batch job to replicate point-ln-time snapshots to AWS.
C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment.
Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.
D. Deploy an AWS Storage Gateway file gateway for the on-premises environment.
Configure it to store data locally, and asynchronously back up point-in-lime snapshots to AWS.

Answer: A
Explanation:
You can use AWS DataSync with your Direct Connect link to access public service endpoints or private VPC endpoints. When using VPC endpoints, data transferred between the DataSync agent and AWS services does not traverse the public internet or need public IP addresses, increasing the security of data as it is copied over the network.

QUESTION 242
A company has an on-premises data center that is running out of storage capacity.
The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs.
The solution must allow for immediate retrieval of data at no additional cost.

How can these requirements be met?

A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval.
Enable provisioned retrieval capacity for the workload
B. Deploy AWS Storage Gateway using cached volumes.
Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.
C. Deploy AWS Storage Gateway using stored volumes to store data locally.
Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3
D. Deploy AWS Direct Connect to connect with the on-premises data center.
Configure AWS Storage Gateway to store data locally.
Use Storage Gateway to asynchronously bacK up potnt-tn-time snapshots of the data to Amazon S3.

Answer: C
Explanation:
Volume Gateway provides an iSCSI target, which enables you to create block storage volumes and mount them as iSCSI devices from your on-premises or EC2 application servers. The Volume Gateway runs in either a cached or stored mode:
In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access.
In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

QUESTION 243
A company Is reviewing Its AWS Cloud deployment to ensure its data is not accessed by anyone without appropriate authorization.
A solutions architect is tasked with identifying all open Amazon S3 buckets and recording any S3 bucket configuration changes.

What should the solutions architect do to accomplish this?

A. Enable AWS Config service with the appropriate rules
B. Enable AWS Trusted Advisor with the appropriate checks.
C. Write a script using an AWS SDK to generate a bucket report
D. Enable Amazon S3 server access logging and configure Amazon CloudWatch Events.

Answer: A
Explanation:

QUESTION 244
A company built an application that lets users check in to places they visit, rank the places, and add reviews about their experiences.
The application is successful with a rapid increase in the number of users every month.
The chief technology officer fears the database supporting the current Infrastructure may not handle the new load the following month because the single Amazon RDS for MySQL instance has triggered alarms related lo resource exhaustion due to read requests.
What can a solutions architect recommend to prevent service Interruptions at the database layer with minimal changes to code?

A. Create RDS read replicas and redirect read-only traffic to the read replica endpoints.
Enable a Multi-AZ deployment.
B. Create an Amazon EMR cluster and migrate the data to a Hadoop Distributed File System (HDFS) with a replication factor of 3.
C. Create an Amazon ElastiCache cluster and redirect all read-only traffic to the cluster.
Set up the cluster to be deployed m three Availability Zones.
D. Create an Amazon DynamoDB table to replace the RDS instance and redirect all read-only traffic to the DynamoDB table.
Enable DynamoDB Accelerator to offload traffic from the main table.

Answer: A

QUESTION 245
A company runs an application on Amazon EC2 Instances.
The application is deployed in private subnets in three Availability Zones of the us-east-1 Region.
The instances must be able to connect to the internet to download files.
The company wants a design that Is highly available across the Region.
Which solution should be implemented to ensure that there are no disruptions to Internet connectivity?

A. Deploy a NAT Instance In a private subnet of each Availability Zone.
B. Deploy a NAT gateway in a public subnet of each Availability Zone.

C. Deploy a transit gateway in a private subnet of each Availability Zone.
D. Deploy an internet gateway in a public subnet of each Availability Zone.

Answer: B

QUESTION 246
A company has migrated an on-premises Oracle database to an Amazon RDS (or Oracle Multi-AZ DB instance In the us-east-l Region.
A solutions architect is designing a disaster recovery strategy to have the database provisioned In the us-west-2 Region In case the database becomes unavailable in the us-east-1 Region.
The design must ensure the database is provisioned in the us-west-2 Region in a maximum of 2 hours, with a data loss window of no more than 3 hours.
How can these requirements be met?

A. Edit the DB instance and create a read replica in us-west-2.
Promote the read replica to master In us- west-2 in case the disaster recovery environment needs to be activated.
B. Select the multi-Region option to provision a standby instance in us-west-2.
The standby Instance will be automatically promoted to master In us-west-2 in case the disaster recovery environment needs to be created.
C. Take automated snapshots of the database instance and copy them to us-west-2 every 3 hours.
Restore the latest snapshot to provision another database instance in us-west-2 in case the disaster recovery environment needs to be activated.
D. Create a multimaster read/write instances across multiple AWS Regions Select VPCs in us-east-1 and us-west-2 lo make that deployment.
Keep the master read/write instance in us-west-2 available to avoid having to activate a disaster recovery environment.

Answer: A

QUESTION 247
A company has an application with a REST-based Interface that allows data to be received in near-real time from a third-party vendor.
Once received, the application processes and stores the data for further analysis.
The application Is running on Amazon EC2 instances.
The third-party vendor has received many 503 Service Unavailable Errors when sending data to the application.
When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests.
Which design should a solutions architect recommend to provide a more scalable solution?

A. Use Amazon Kinesis Data Streams to ingest the data.
Process the data using AWS Lambda functions.
B. Use Amazon API Gateway on top of the existing application.
Create a usage plan with a quota limit for the third-party vendor.
C. Use Amazon Simple Notification Service (Amazon SNS) to ingest the data.
Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.
D. Repackage the application as a container.
Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

Answer: A

QUESTION 248
A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days.
The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization.
What should a solutions architect do to meet these requirements?

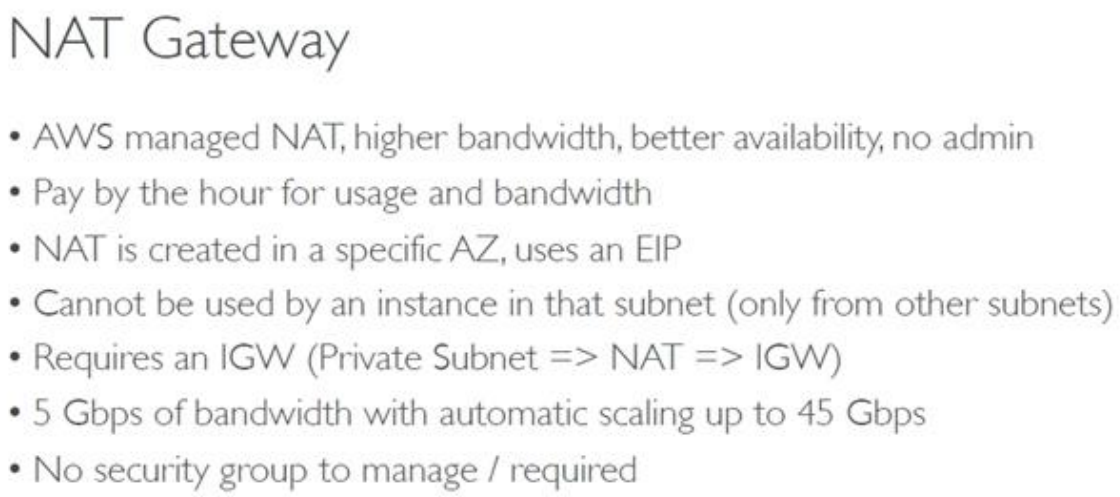
A. Use AWS Snowball.
B. Use AWS DataSync.
C. Use a secure VPN connection.
D. Use Amazon S3 Transfer Acceleration.

Answer: A

QUESTION 249
A company recently deployed a two-tier application in two Availability Zones in the us-east-1 Region.
The databases are deployed in a private subnet while the web servers are deployed in a public subnet.
An internet gateway is attached to the VPC. The application and database run on Amazon EC2 instances.
The database servers are unable to access patches on the internet.
A solutions architect needs to design a solution that maintains database security with the least operational overhead.
Which solution meets these requirements?

A. Deploy a NAT gateway inside the public subnet for each Availability Zone and associate it with an Elastic IP address.
Update the routing table of the private subnet to use it as the default route.
B. Deploy a NAT gateway inside the private subnet for each Availability Zone and associate it with an Elastic IP address.
Update the routing table of the private subnet to use it as the default route.
C. Deploy two NAT instances inside the public subnet for each Availability Zone and associate them with Elastic IP addresses.
Update the routing table of the private subnet to use it as the default route.
D. Deploy two NAT instances inside the private subnet for each Availability Zone and associate them with Elastic IP addresses.
Update the routing table of the private subnet to use it as the default route.

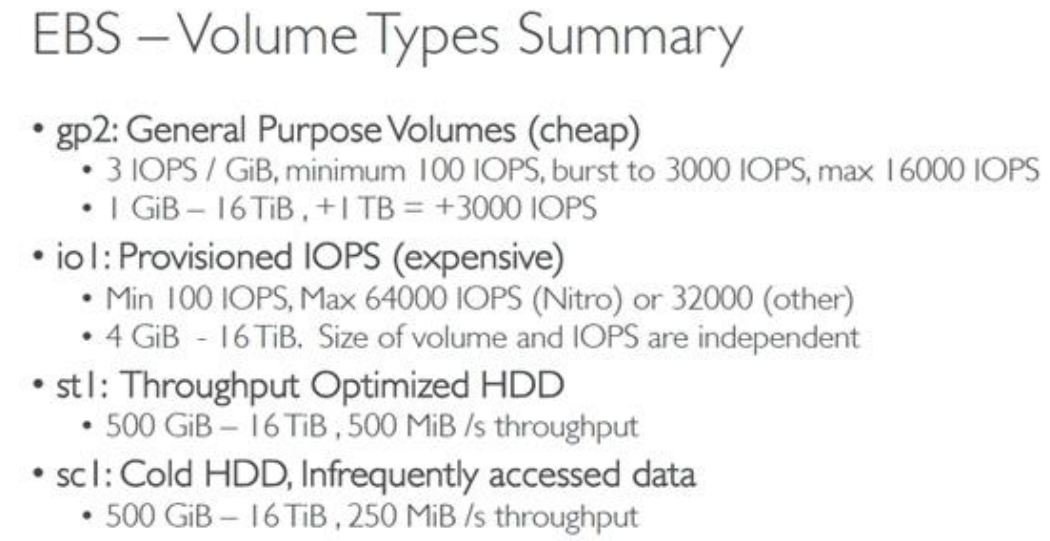
Answer: B
Explanation:



QUESTION 250
A solutions architect must design a solution for a persistent database that is being migrated from on- premises to AWS.
The database requires 64,000 IOPS according to the database administrator.
If possible, the database administrator wants to use a single Amazon Elastic Block Store (Amazon EBS) volume to host the database instance.
Which solution effectively meets the database administrator's criteria?

A. Use an instance from the 13 I/O optimized family and leverage local ephemeral storage to achieve the IOPS requirement.
B. Create an Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1) volume attached. Configure the volume to have 64,000 IOPS.
C. Create and map an Amazon Elastic File System (Amazon EFS) volume to the database instance and use the volume to achieve the required IOPS for the database.
D. Provision two volumes and assign 32,000 IOPS to each. Create a logical volume at the operating system level that aggregates both volumes to achieve the IOPS requirements.

Answer: B
Explanation:



QUESTION 251
A company recently launched its website to serve content to its global user base.
The company wants to store and accelerate the delivery of static content to its users by leveraging Amazon CloudFront with an Amazon EC2 instance attached as its origin.
How should a solutions architect optimize high availability for the application?

A. Use Lambda@Edge for CloudFront.
B. Use Amazon S3 Transfer Acceleration for CloudFront.
C. Configure another EC2 instance in a different Availability Zone as part of the origin group.
D. Configure another EC2 instance as part of the origin server cluster in the same Availability Zone.

Answer: A

QUESTION 252
A company is planning to build a new web application on AWS.
The company expects predictable traffic most of the year and very high traffic on occasion.
The web application needs to be highly available and fault tolerant with minimal latency.
What should a solutions architect recommend to meet these requirements?

A. Use an Amazon Route 53 routing policy to distribute requests to two AWS Regions, each with one Amazon EC2 instance.
B. Use Amazon EC2 instances in an Auto Scaling group with an Application Load Balancer across multiple Availability Zones.
C. Use Amazon EC2 instances in a cluster placement group with an Application Load Balancer across multiple Availability Zones.
D. Use Amazon EC2 instances in a cluster placement group and include the cluster placement group within a new Auto Scaling group.

Answer: C

QUESTION 253
A company wants to migrate a workload to AWS.

The chief information security officer requires that all data be encrypted at rest when stored in the cloud.
The company wants complete control of encryption key lifecycle management.
The company must be able to immediately remove the key material and audit key usage independently of AWS CloudTrail.
The chosen services should integrate with other storage services that will be used on AWS.
Which services satisfies these security requirements?

A. AWS CloudHSM with the CloudHSM client
B. AWS Key Management Service (AWS KMS) with AWS CloudHSM
C. AWS Key Management Service (AWS KMS) with an external key material origin
D. AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs)

Answer: B
Explanation:
Took a bit of reading. Key points in question:
"The company must be able to immediately remove the key material and audit key usage independently"
"The chosen services should integrate with other storage services that will be used on AWS"
Point 1: Q: Can I use CloudHSM to store keys or encrypt data used by other AWS services?
Ans: Yes. You can do all encryption in your CloudHSM-integrated application. In this case, AWS services such as Amazon S3 or Amazon Elastic Block Store (EBS) would only see your data encrypted.
Point 2: AWS manages the hardware security module (HSM) appliance, but does not have access to your keys. You control and manage your own keys
Ref: https://aws.amazon.com/cloudhsm/features/
Ref: https://aws.amazon.com/cloudhsm/faqs/

QUESTION 254
A company is looking for a solution that can store video archives in AWS from old news footage.
The company needs to minimize costs and will rarely need to restore these files.
When the files are needed, they must be available in a maximum of five minutes.
What is the MOST cost-effective solution?

A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: A

QUESTION 255
A company wants to use Amazon S3 for the secondary copy of its on-premises dataset.
The company would rarely need to access this copy.
The storage solution's cost should be minimal.
Which storage solution meets these requirements?

A. S3 Standard
B. S3 Intelligent-Tiering
C. S3 Standard-Infrequent Access (S3 Standard-IA)
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: D

QUESTION 256
A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts.
The company has created a central AWS account for streamlining management and audit reviews.
An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users.
The solution must be secure and optimized. How should a solutions architect meet these requirements?

A. Configure an AWS Lambda function in each developer account to copy the log files to the central account.
Create an IAM role in the central account for the auditor.
Attach an IAM policy providing read- only permissions to the bucket.
B. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account.
Create an IAM user in the central account for the auditor.
Attach an IAM policy providing full permissions to the bucket.
C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account.
Create an IAM role in the central account for the auditor.
Attach an IAM policy providing read- only permissions to the bucket.
D. Configure an AWS Lambda function in the central account to copy the log files from the S3 bucket in each developer account.
Create an IAM user in the central account for the auditor.
Attach an IAM policy providing full permissions to the bucket.

Answer: C

QUESTION 257
A company has an application that posts messages to Amazon SQS Another application polls the queue and processes the messages in an I/O-intensive operation.
The company has a service level agreement (SLA) that specifies the maximum amount of time that can elapse between receiving the messages and responding to the users.
Due to an increase in the number of messages the company has difficulty meeting its SLA consistently.
What should a solutions architect do to help improve the application's processing time and ensure it can handle the load at any level?

A. Create an Amazon Machine Image (AMI) from the instance used for processing.
Terminate the instance and replace it with a larger size.
B. Create an Amazon Machine Image (AMI) from the instance used for processing.
Terminate the instance and replace it with an Amazon EC2 Dedicated Instance
C. Create an Amazon Machine image (AMI) from the instance used for processing.
Create an Auto Scaling group using this image in its launch configuration.
Configure the group with a target tracking policy to keep us aggregate CPU utilization below 70%.
D. Create an Amazon Machine Image (AMI) from the instance used for processing.
Create an Auto Scaling group using this image in its launch configuration.
Configure the group with a target tracking policy based on the age of the oldest message in the SQS queue.

Answer: C

QUESTION 258
A company is planning to deploy an Amazon RDS DB instance running Amazon Aurora.
The company has a backup retention policy requirement of 90 days.
Which solution should a solutions architect recommend?

A. Set the backup retention period to 90 days when creating the RDS DB instance
B. Configure RDS to copy automated snapshots to a user-managed Amazon S3 bucket with a lifecycle policy set to delete after 90 days.
C. Create an AWS Backup plan to perform a daily snapshot of the RDS database with the retention set to 90 days.
Create an AWS Backup job to schedule the execution of the backup plan daily
D. Use a daily scheduled event with Amazon CloudWatch Events to execute a custom AWS Lambda function that makes a copy of the RDS automated snapshot Purge snapshots older than 90 days

Answer: B

QUESTION 259
A company is using a tape backup solution to store its key application data offsite.
The daily data volume is around 50 TB.
The company needs to retain the backups for 7 years for regulatory purposes.
The backups are rarely accessed and a week's notice is typically given if a backup needs to be restored.
The company is now considering a cloud-based option to reduce the storage costs and operational burden of managing tapes.
The company also wants to make sure that the transition (rom tape backups to the cloud minimizes disruptions.
Which storage solution is MOST cost-effective'?

A. Use Amazon Storage Gateway to back up to Amazon Glacier Deep Archive
B. Use AWS Snowball Edge to directly integrate the backups with Amazon S3 Glacier.
C. Copy the backup data to Amazon S3 and create a lifecycle policy to move the data to Amazon S3 Glacier
D. Use Amazon Storage Gateway to back up to Amazon S3 and create a lifecycle policy to move the backup to Amazon S3 Glacier

Answer: A

QUESTION 260
A company relies on an application that needs at least 4 Amazon EC2 instances during regular traffic and must scale up to 12 EC2 instances during peak loads.
The application is critical to the business and must be highly available
Which solution will meet these requirements?

A. Deploy the EC2 instances in an Auto Scaling group.
Set the minimum to 4 and the maximum to M, with 2 in Availability Zone A and 2 in Availability Zone B
B. Deploy the EC2 instances in an Auto Scaling group.
Set the minimum to 4 and the maximum to 12, with all 4 in Availability Zone A
C. Deploy the EC2 instances in an Auto Scaling group.

Set the minimum to 8 and the maximum to 12, with 4 in Availability Zone A and 4 in Availability Zone B

D. Deploy the EC2 instances in an Auto Scaling group.
Set the minimum to 8 and the maximum to 12 with all 8 in Availability Zone A

Answer: C
Explanation:
It requires HA and if one AZ is down then at least 4 instances will be active in another AZ which is key for this question.

QUESTION 261
A company is planning to migrate its virtual server-based workloads to AWS The company has internet-facing load balancers backed by application servers.
The application servers rely on patches from an internet-hosted repository
Which services should a solutions architect recommend be hosted on the public subnet? (Select TWO.)

A. NAT gateway
B. Amazon RDS DB instances
C. Application Load Balancers
D. Amazon EC2 application servers
E. Amazon Elastic File System (Amazon EFS) volumes

Answer: AC

QUESTION 262
An application is running on Amazon EC2 instances Sensitive information required for the application is stored in an Amazon S3 bucket.
The bucket needs to be protected from internet access while only allowing services within the VPC access to the bucket.
Which combination of actions should a solutions archived take to accomplish this'' (Select TWO.)

A. Create a VPC endpoint for Amazon S3.
B. Enable server access logging on the bucket
C. Apply a bucket policy to restrict access to the S3 endpoint.
D. Add an S3 ACL to the bucket that has sensitive information
E. Restrict users using the IAM policy to use the specific bucket

Answer: AC
Explanation:
ACL is a property at object level not at bucket level .Also by just adding ACL you cant let the services in VPC allow access to the bucket .

QUESTION 263
A solutions architect is designing a multi-Region disaster recovery solution for an application that will provide public API access.
The application will use Amazon EC2 instances with a userdata script to load application code and an Amazon RDS for MySQL database.
The Recovery Time Objective (RTO) is 3 hours and the Recovery Point Objective (RPO) is 24 hours.
Which architecture would meet these requirements at the LOWEST cost?

A. Use an Application Load Balancer for Region failover.
Deploy new EC2 instances with the userdata script.
Deploy separate RDS instances in each Region
B. Use Amazon Route 53 for Region failover.
Deploy new EC2 instances with the userdata script.
Create a read replica of the RDS instance in a backup Region
C. Use Amazon API Gateway for the public APIs and Region failover.
Deploy new EC2 instances with the userdata script.
Create a MySQL read replica of the RDS instance in a backup Region
D. Use Amazon Route 53 for Region failover.
Deploy new EC2 instances with the userdata scnpt for APIs, and create a snapshot of the RDS instance daily for a backup.
Replicate the snapshot to a backup Region

Answer: D

QUESTION 264
A solutions architect is designing a new API using Amazon API Gateway that will receive requests from users.
The volume of requests is highly variable, several hours can pass without receiving a single request.
The data processing will take place asynchronously but should be completed within a few seconds after a request is made
Which compute service should the solutions architect have the API invoke to deliver the requirements at the lowest cost?

A. An AWS Glue job
B. An AWS Lambda function
C. A containerized service hosted in Amazon Elastic Kubernetes Service (Amazon EKS)
D. A containerized service hosted in Amazon ECS with Amazon EC2

Answer: B

QUESTION 265
A development team needs to host a website that will be accessed by other teams.
The website contents.consist of HTML. CSS, client side JavaScript, and images.
Which method is the MOST cost-effective for hosting the website?

A. Containerize the website and host it in AWS Fargate
B. Create an Amazon S3 bucket and host the website there.
C. Deploy a web server on an Amazon EC2 instance to host the website.
D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express is framework

Answer: B

QUESTION 266
A company has media and application files that need to be shared internally.
Users currently are authenticated using Active Directory and access files from a Microsoft Windows platform.

The chief execute officer wants to keep the same user permissions, but wants the company to improve the process as the company is reaching its storage capacity limit.
What should a solutions architect recommend?

A. Set up a corporate Amazon S3 bucket and move and media and application files.
B. Configure Amazon FSx for Windows File Server and move all the media and application files.
C. Configure Amazon Elastic File System (Amazon EFS) and move all media and application files.
D. Set up Amazon EC2 on Windows, attach multiple Amazon Elastic Block Store (Amazon EBS) volumes and, and move all media and application files.

Answer: B

QUESTION 267
A company is moving its legacy workload to the AWS Cloud.
The workload files will be shared, appended, and frequently accessed through Amazon EC2 instances when they are first created.
The files will be accessed occasionally as they age
What should a solutions architect recommend?

A. Store the data using Amazon EC2 instances with attached Amazon Elastic Block Store (Amazon EBS) data volumes
B. Store the data using AWS Storage Gateway volume gateway and export rarely accessed data to Amazon S3 storage
C. Store the data using Amazon Elastic File System (Amazon EFS) with lifecycle management enabled for rarely accessed data
D. Store the data using Amazon S3 with an S3 lifecycle policy enabled to move data to S3 Standard-Infrequent Access (S3 Standard-IA)

Answer: D

QUESTION 268
A company is deploying a multi-instance application within AWS that requires minimal latency between the instances.
What should a solutions architect recommend?

A. Use an Auto Scaling group with a cluster placement group.
B. Use an Auto Scaling group with single Availability Zone in the same AWS Region.
C. Use an Auto Scaling group with multiple Availability Zones in the same AWS Region.
D. Use a Network Load Balancer with multiple Amazon EC2 Dedicated Hosts as the targets

Answer: A

QUESTION 269
A company receives structured and semi-structured data from various sources once every day.
A solutions architect needs to design a solution that leverages big data processing frameworks.
The data should be accessible using SQL queries and business intelligence tools.
What should the solutions architect recommend to build the MOST high-performing solution?

A. Use AWS Glue to process data and Amazon S3 to store data
B. Use Amazon EMR to process data and Amazon Redshift to store data

C. Use Amazon EC2 to process data and Amazon Elastic Block Store (Amazon EBS) to store data
D. Use Amazon Kinesis Data Analytics to process data and Amazon Elastic File System (Amazon EFS) to store data

Answer: B

QUESTION 270
Company is designing a website that uses an Amazon S3 bucket to store static images.
The company wants ail future requests have taster response times while reducing both latency and cost.
Which service configuration should a solutions architect recommend?

A. Deploy a NAT server in front of Amazon S3.
B. Deploy Amazon CloudFront in front of Amazon S3.
C. Deploy a Network Load Balancer in front of Amazon S3.
D. Configure Auto Scaling to automatically adjust the capacity of the website.

Answer: B

QUESTION 271
What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

A. Update the bucket policy to deny if the PutObject does not have an s3 x-amz-acl header set
B. Update the bucket policy to deny if the PutObject does not have an s3 x-amz-acl header set to private
C. Update the bucket policy to deny if the PutObject does not have an aws SecureTransport header set to true
D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set

Answer: D

QUESTION 272
A company runs a high performance computing (HPC) workload on AWS.
The workload required low- latency network performance and high network throughput with tightly coupled node-to-node communication.
The Amazon EC2 instances are properly sized for compute and storage capacity, and are launched using default options.
What should a solutions architect propose to improve the performance of the workload'?

A. Choose a cluster placement group while launching Amazon EC2 instances
B. Choose dedicated instance tenancy while launching Amazon EC2 instances
C. Choose an Elastic Inference accelerator while launching Amazon EC2 instances
D. Choose the required capacity reservation while launching Amazon EC2 instances.

Answer: A

QUESTION 273
A company's dynamic website is hosted using on-premises servers in the United States.

The company is launching its product in Europe and it wants to optimize site loading times for new European users.
The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed
What should the solutions architect recommend?

A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it
B. Move the website to Amazon S3 Use cross-Region replication between Regions.
C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers
D. Use an Amazon Route 53 geoproximity routing policy pointing to on-premises servers

Answer: C

QUESTION 274
A company is building a media-sharing application and decides to use Amazon S3 for storage. When a media file is uploaded the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions and extract and store the metadata to an Amazon DynamoDB table.
The metadata is used for searching and navigation. The amount of traffic is variable The solution must be able to scale to handle spikes in load without unnecessary expenses.
What should a solutions architect recommend to support this workload?

A. Build the processing into the website or mobile app used to upload the content to Amazon S3. Save the required data to the DynamoDB table when the objects are uploaded
B. Trigger AWS Step Functions when an object is stored in the S3 bucket.
Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table
C. Trigger an AWS Lambda function when an object is stored in the S3 bucket.
Have the Lambda function start AWS Batch to perform the steps to process the object.
Place the object data in the DynamoDB table when complete
D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3.
Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocess use the program to perform the processing

Answer: C

QUESTION 275
A company has recently updated its internal security standards.
The company must now ensure all Amazon S3 buckets and Amazon Elastic Block Store (Amazon EBS) volumes are encrypted with keys created and periodically rotated by internal security specialists.
The company is looking for a native, software-based AWS service to accomplish this goal.
What should a solutions architect recommend as a solution?

A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager.
B. Use AWS Key Management Service (AWS KMS) with customer master keys (CMKs) to store master key material and apply a routing to re-create a new key periodically and replace it in AWS KMS.
C. Use an AWS CloudHSM cluster with customer master keys (CMKs) to store master key material and apply a routine a re-create a new key periodically and replace it in the CloudHSM cluster

nodes.

D. Use AWS Systems Manager Parameter Store with customer master keys (CMKs) keys to store master key material and apply a routine to re-create a new periodically and replace it in the Parameter Store.

Answer: A
Explanation:
AWS Secrets Manager provides full lifecycle management for secrets within your environment. In this post, Maitreya and I will show you how to use Secrets Manager to store, deliver, and rotate SSH keypairs used for communication within compute clusters. Rotation of these keypairs is a security best practice, and sometimes a regulatory requirement. Traditionally, these keypairs have been associated with a number of tough challenges. For example, synchronizing key rotation across all compute nodes, enable detailed logging and auditing, and manage access to users in order to modify secrets.

QUESTION 276
A solution architect must design a solution that uses Amazon CloudFront with an Amazon S3 to store a static website.
The company security policy requires that all websites traffic be inspected by AWS WAF.
How should the solution architect company with these requirements?

A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only
B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin,
C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only Associate AWS WAF to CloudFront.
D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Answer: D

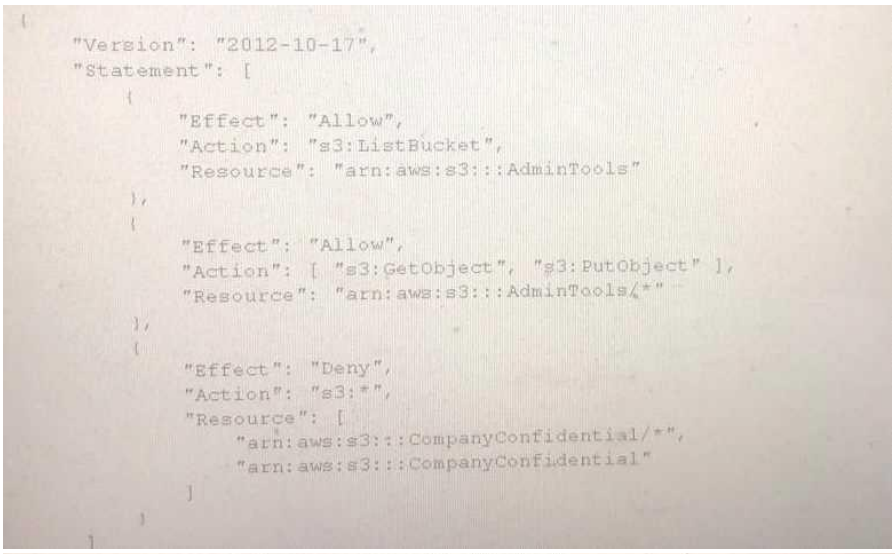
QUESTION 277
A company has copied 1 PB of data from a colocation facility to an Amazon S3 bucket in the us-east-1 Region using an AWS Direct Connect link.
The company now wants to copy the data to another S3 bucket in the us-west-2 Region.
The colocation facility does not allow the use AWS Snowball.
What should a solutions architect recommend to accomplish this?

A. Order a Snowball Edge device to copy the data from one Region to another Region.
B. Transfer contents from the source S3 bucket to a target S3 bucket using the S3 console.
C. Use the aws S3 sync command to copy data from the source bucket to the destination bucket.
D. Add a cross-Region replication configuration to copy objects across S3 buckets in different Reg.

Answer: D

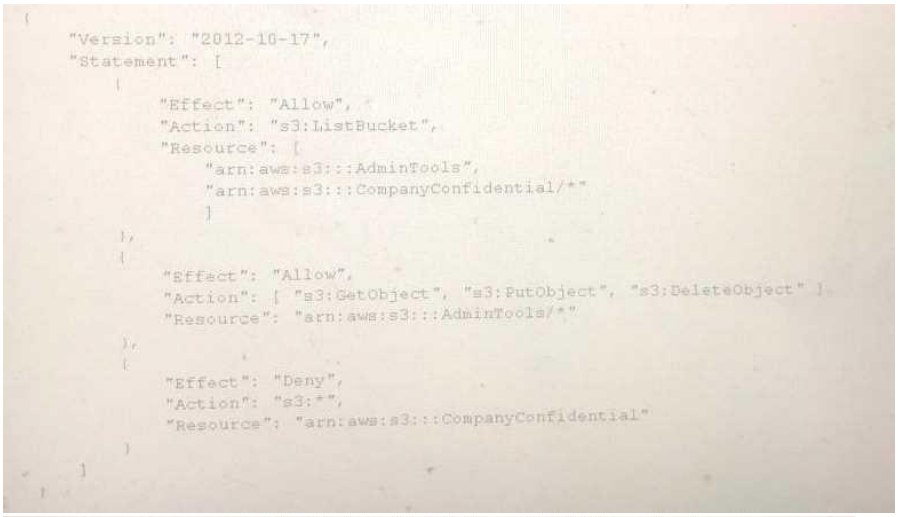
QUESTION 278
A company has hired a new cloud engineer who should not have access to an Amazon S3 bucket named Company Confidential.
The cloud engineer must be able to read from and write to an S3 bucket called AdminTools.
Which IAM policy will meet these requirements?

A.



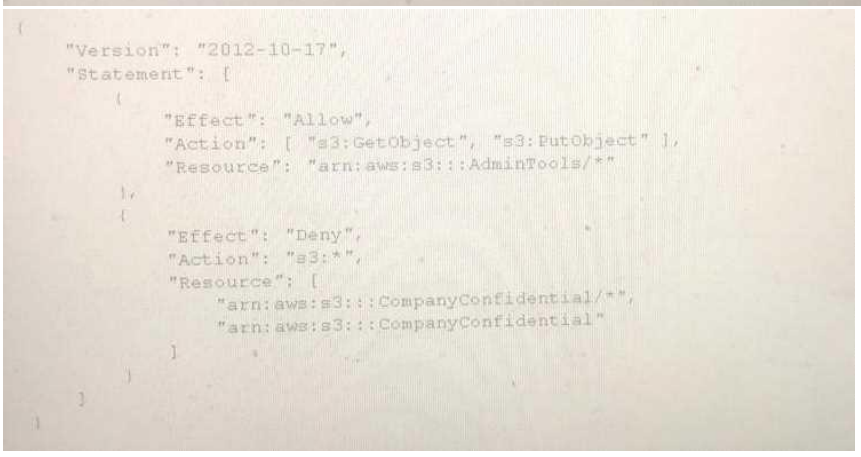
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::AdminTools"
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

B.



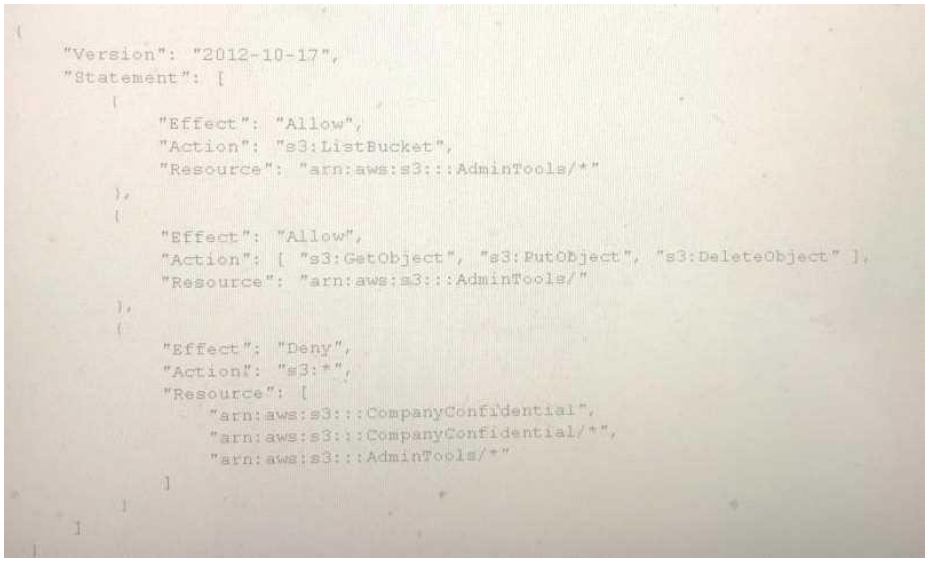
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::AdminTools",
                "arn:aws:s3:::CompanyConfidential/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::CompanyConfidential"
        }
    ]
}
```

C.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

D.



Answer: A

QUESTION 279
An engineering team is developing and deploying AWS Lambda functions.
The team needs to create roles and manage policies in AWS IAM to configure the permissions of the Lambda functions.
How should the permissions for the team be configured so they also adhere to the concept of least privilege?

A. Create an IAM role with a managed policy attached.
Allow the engineering team and the Lambda functions to assume this role
B. Create an IAM group for the engineering team with an IAMFullAccess policy attached.
Add all the users from the team to this IAM group
C. Create an execution role for the Lambda functions.
Attach a managed policy that has permission boundaries specific to these Lambda functions
D. Create an IAM role with a managed policy attached that has permission boundaries specific to the Lambda functions.
Allow the engineering team to assume this role.

Answer: D

QUESTION 280
A company needs a secure connection between its on-premises environment and AWS.
This connection does not need high bandwidth and will handle a small amount of traffic.
The connection should be set up quickly.
What is the MOST cost-effective method to establish this type of connection?

A. Implement a client VPN
B. Implement AWS Direct Connect
C. Implement a bastion host on Amazon EC2 53D.
D. Implement an AWS Site-to-Site VPN connection.

Answer: D

QUESTION 281
A company is building a payment application that must be highly available even during regional service disruptions.
A solutions architect must design a data storage solution that can be easily replicated and used in other AWS Regions.
The application also requires low-latency atomicity, consistency, isolation, and durability (ACID) transactions that need to be immediately available to generate reports.
The development team also needs to use SQL.
Which data storage solution meets these requirements'?

A. Amazon Aurora Global Database
B. Amazon DynamoDB global tables
C. Amazon S3 with cross-Region replication and Amazon Athena
D. MySQL on Amazon EC2 instances with Amazon Elastic Block Store (Amazon EBS) snapshot replication

Answer: D

QUESTION 282
A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application.
The media files must be resilient to the loss of an Availability Zone Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern.
The solutions architect must minimize the costs of storing and retrieving the media files.
Which storage option meets these requirements?

A. S3 Standard
B. S3 Intelligent-Tiering
C. S3 Standard-Infrequent Access (S3 Standard-IA)
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

QUESTION 283
A company uses a legacy on-premises analytics application that operates on gigabytes of csv files and represents months of data.
The legacy application cannot handle the growing size of csv files New csv files are added daily from various data sources to a central on-premises storage location.
The company wants to continue to support the legacy application while users learn AWS analytics services.
To achieve this, a solutions architect wants to maintain two synchronized copies of all the csv files on-premises and in Amazon S3.
Which solution should the solutions architect recommend?

A. Deploy AWS DataSync on-premises.
Configure DataSync to continuously replicate the csv files between the company's on-premises storage and the company's S3 bucket
B. Deploy an on-premises file gateway.
Configure data sources to write the csv files to the file gateway.
Point the legacy analytics application to the file gateway.

The file gateway should replicate the csv files to Amazon S3

C. Deploy an on-premises volume gateway.
Configure data sources to write the csv files to the volume gateway.
Point the legacy analytics application to the volume gateway.
The volume gateway should replicate data to Amazon S3.

D. Deploy AWS DataSync on-premises.
Configure DataSync to continuously replicate the csv files between on-premises and Amazon Elastic File System (Amazon EFS).
Enable replication from Amazon EFS to the company's S3 bucket.

Answer: A

QUESTION 284
An application allows users at a company's headquarters to access product data.
The product data is stored in an Amazon RDS MySQL DB instance.
The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic.
A solutions architect needs to optimize the application's performance quickly.
What should the solutions architect recommend?

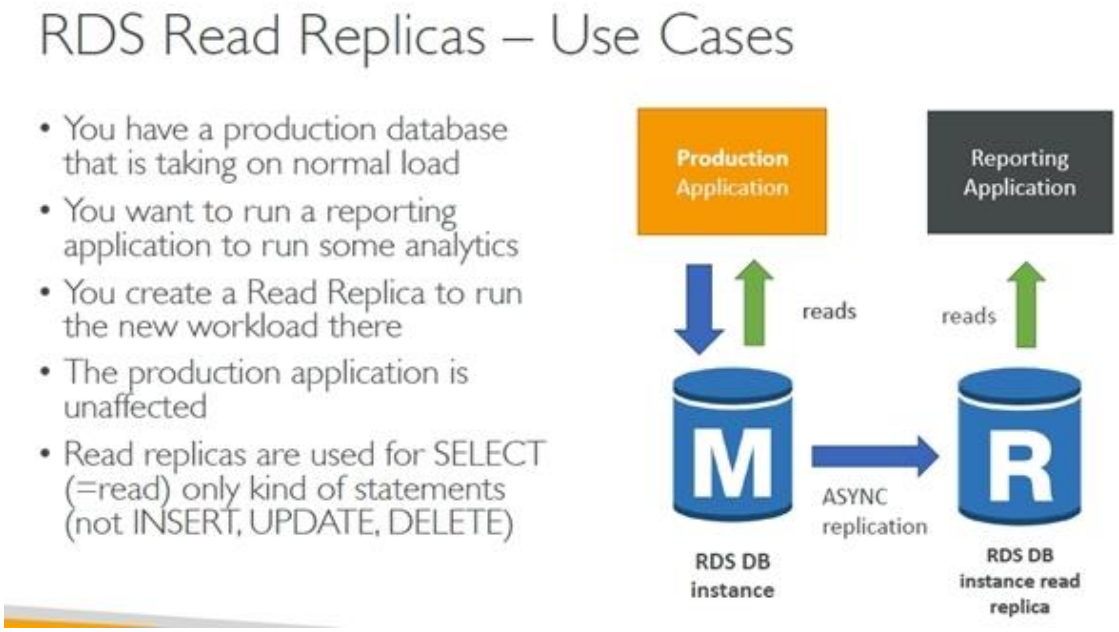
A. Change the existing database to a Multi-AZ deployment.
Serve the read requests from the primary Availability Zone.

B. Change the existing database to a Multi-AZ deployment.
Serve the read requests from the secondary Availability Zone.

C. Create read replicas for the database.
Configure the read replicas with half of the compute and storage resources as the source database.

D. Create read replicas for the database.
Configure the read replicas with the same compute and storage resources as the source database.

Answer: D
Explanation:



QUESTION 285
A company wants to optimize the cost of its data storage for data that is accessed quarterly.
The company requires high throughput, low latency, and rapid access, when needed.
Which Amazon S3 storage class should a solutions architect recommend?

A. Amazon S3 Glacier (S3 Glacier)
B. Amazon S3 Standard (S3 Standard)
C. Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)
D. Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

Answer: B

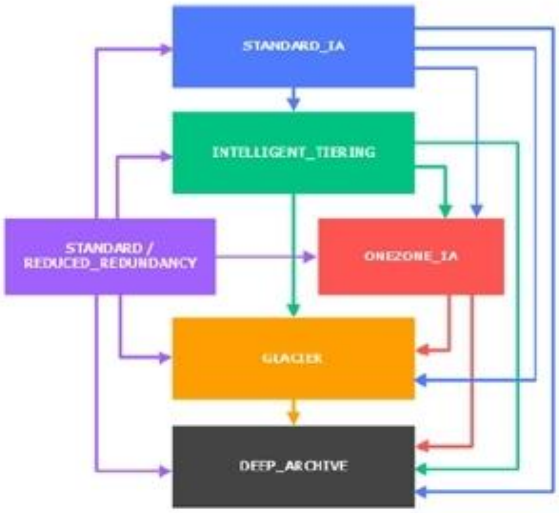
QUESTION 286
A company requires that all versions of objects in its Amazon S3 bucket be retained.
Current object versions will be frequently accessed during the first 30 days, after which they will be rarely accessed and must be retrievable within 5 minutes.
Previous object versions need to be kept forever, will be rarely accessed, and can be retrieved within 1 week. All storage solutions must be highly available and highly durable.
What should a solutions architect recommend to meet these requirements in the MOST cost-effective manner?

A. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier after 1 day.
B. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day
C. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Standard-infrequent Access (S3 Standard-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day
D. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day

Answer: B
Explanation:

S3 – Moving between storage classes

- You can transition objects between storage classes
- For infrequently accessed object, move them to STANDARD_IA
- For archive objects you don't need in real-time, GLACIER or DEEP_ARCHIVE
- Moving objects can be automated using a **lifecycle configuration**



S3 Storage Classes – Price Comparison Example us-east-2

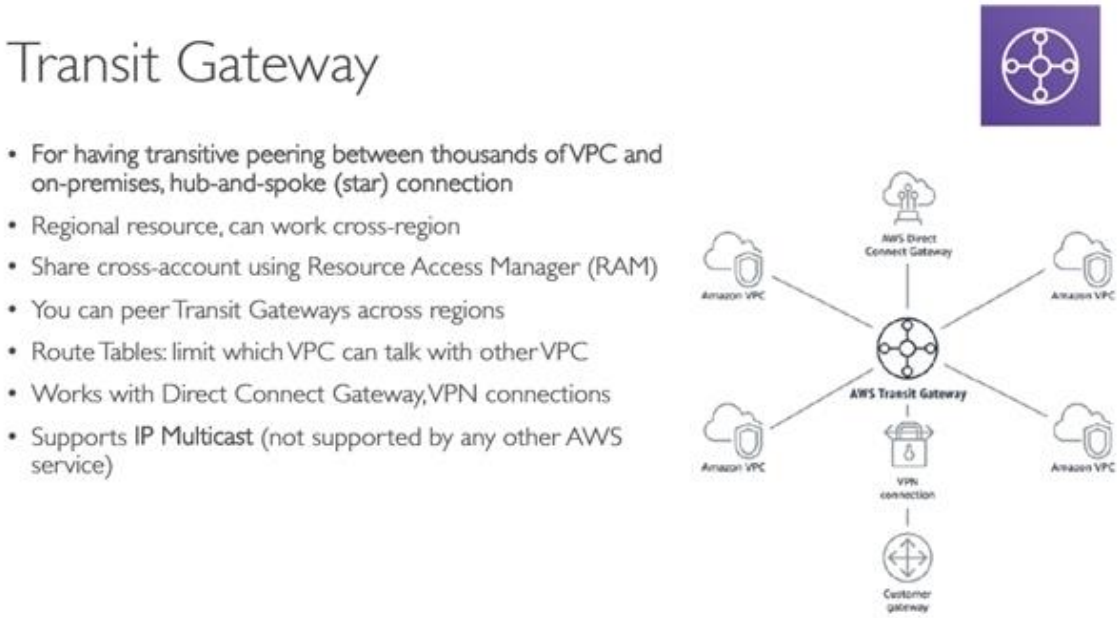
	S3 Standard	S3 Intelligent-Tiering	S3 Standard-IA	S3 One Zone-IA	S3 Glacier	S3 Glacier Deep Archive
Storage Cost (per GB per month)	$0.023	$0.0125 - $0.023	$0.0125	$0.01	$0.004 Minimum 90 days	$0.00099 Minimum 180 days
Retrieval Cost (per 1000 requests)	GET $0.0004	GET $0.0004	GET $0.001	GET $0.001	GET $0.0004 + Expedited - $10.00 Standard - $0.05 Bulk - $0.025	GET $0.0004 + Standard - $0.10 Bulk - $0.025
Time to retrieve	instantaneous	Instantaneous	Instantaneous	Instantaneous	Expedited (1 to 5 minutes) Standard (3 to 5 hours) Bulk (5 to 12 hours)	Standard (12 hours) Bulk (48 hours)
Monitoring Cost (per 1000 objects)		$0.0025				

QUESTION 287
A company hosts its core network services, including directory services and DNS. in its on-premises data center.
The data center is connected to the AWS Cloud using AWS Direct Connect (DX) Additional AWS accounts are planned that will require quick, cost-effective, and consistent access to these network services
What should a solutions architect implement to meet these requirements with the LEAST amount of operational overhead?

A. Create a DX connection in each new account.
Route the network traffic to the on-premises servers
B. Configure VPC endpoints in the DX VPC for all required services.
Route the network traffic to the on- premises servers

C. Create a VPN connection between each new account and the DX VPp
Route the network traffic to the on-premises servers
D. Configure AWS Transit Gateway between the accounts.
Assign DX to the transit gateway and route network traffic to the on-premises servers

Answer: D
Explanation:



QUESTION 288
A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances. Amazon RDS DB instances and Amazon Redshift clusters are configured with tags.
The company wants to minimize the effort of configuring and operating this check.
What should a solutions architect do to accomplish this"

A. Use AWS Config rules to define and detect resources that are not property tagged
B. Use Cost Explorer to display resources that are not properly tagged Tag those resources manually.
C. Write API calls to check all resources for proper tag allocation.
Periodically run the code on an EC2 instance.
D. Write API calls to check all resources for proper tag allocation.
Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code

Answer: C
Explanation:

QUESTION 289
An application running on an Amazon EC2 instance needs to access an Amazon DynamoDB table.
Both the EC2 instance and the DynamoDB table are in the same AWS account.
A solutions architect must configure the necessary permissions.
Which solution will allow least privilege access to the DynamoDB table from the EC2 instance?

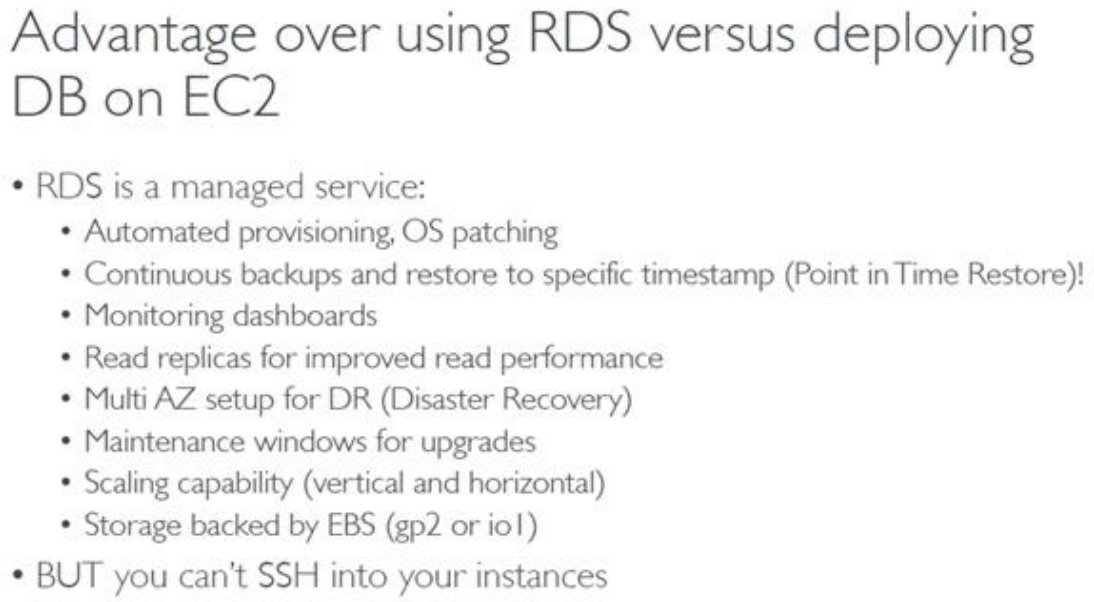
A. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Create an instance profile to assign this IAM role to the EC2 instance
B. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Add the EC2 instance to the trust relationship policy document to allow it to assume the role
C. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Store the credentials in an Amazon S3 bucket and read them from within the application code directly.
D. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Ensure that the application stores the IAM credentials securely on local storage and uses them to make the DynamoDB calls

Answer: A

QUESTION 290
An application uses an Amazon RDS MySQL DB instance.
The RDS database is becoming low on disk space.
A solutions architect wants to increase the disk space without downtime.
Which solution meets these requirements with the LEAST amount of effort?

A. Enable storage auto scaling in RDS.
B. Increase the RDS database instance size
C. Change the RDS database instance storage type to Provisioned IOPS.
D. Back up the RDS database, increase the storage capacity, restore the database and stop the previous instance

Answer: A
Explanation:



QUESTION 291
A company uses an Amazon S3 bucket to store static images for its website. The company configured permissions to allow access to Amazon S3 objects by privileged users only.

What should a solutions architect do to protect against data loss? (Choose two.)

A. Enable versioning on the S3 bucket.
B. Enable access logging on the S3 bucket.
C. Enable server-side encryption on the S3 bucket.
D. Configure an S3 lifecycle rule to transition objects to Amazon S3 Glacier.
E. Use MFA Delete to require multi-factor authentication to delete an object.

Answer: AE

QUESTION 292
A company has an application that runs on Amazon EC2 instances within a private subnet in a VPC.
The instances access data in an Amazon S3 bucket in the same AWS Region.
The VPC contains a NAT gateway in a public subnet to access the S3 bucket.
The company wants to reduce costs by replacing the NAT gateway without compromising security or redundancy
Which solution meets these requirements?

A. Replace the NAT gateway with a NAT instance
B. Replace the NAT gateway with an internet gateway.
C. Replace the NAT gateway with a gateway VPC endpoint
D. Replace the NAT gateway with an AWS Direct Connect connection

Answer: C
Explanation:

QUESTION 293
A company is designing a message-driven order processing application on AWS.
The application consists of many services and needs to communicate the results of its processing to multiple consuming services.
Each of the consuming services may take up to 5 days to receive the messages.
Which process will meet these requirements?

A. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic.
Each consuming service subscribes to this SNS topic and consumes the results
B. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic.
Each consuming service consumes the messages directly from its corresponding SNS topic.
C. The application sends the results of its processing to an Amazon Simple Queue Service (Amazon SQS) queue.
Each consuming service runs as an AWS Lambda function that consumes this single SQS queue.
D. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic.
An Amazon Simple Queue Service (Amazon SQS) queue is created for each service and each queue is configured to be a subscriber of the SNS topic.

Answer: C

QUESTION 294
A company stores call recordings on a monthly basis Statistically, the recorded data may be referenced randomly within a year but accessed rarely after 1 year.
Files that are newer than 1 year old must be queried and retrieved as quickly as possible.
A delay in retrieving older files is acceptable A solutions architect needs to store the recorded data at a minimal cost.
Which solution is MOST cost-effective?

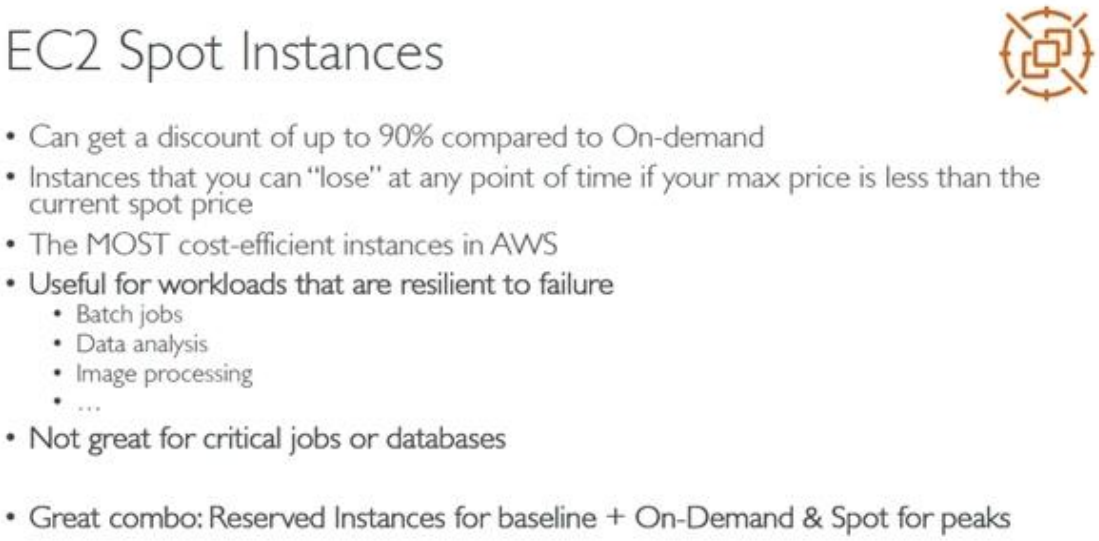
A. Store individual files in Amazon S3 Glacier and store search metadata in object tags created in S3 Glacier.
Query S3 Glacier tags and retrieve the files from S3 Glacier
B. Store individual files in Amazon S3 Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year.
Query and retrieve the files from Amazon S3 or S3 Glacier.
C. Archive individual files and store search metadata for each archive in Amazon S3.
Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year.
Query and retrieve the files by searching for metadata from Amazon S3
D. Archive individual files in Amazon S3.
Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year.
Store search metadata in Amazon DynamoDB Query the files from DynamoDB and retrieve them from Amazon S3 or S3 Glacier

Answer: B

QUESTION 295
A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it.
The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete.
The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.
What should the solutions architect recommend?

A. Implement EC2 Spot Instances
B. Purchase EC2 Reserved Instances
C. Implement EC2 On-Demand Instances
D. Implement the processing on AWS Lambda

Answer: A
Explanation:



QUESTION 296
An online photo application lets users upload photos and perform image editing operations.
The application offers two classes of service free and paid Photos submitted by paid users are processed before those submitted by free users.
Photos are uploaded to Amazon S3 and the job information is sent to Amazon SQS.
Which configuration should a solutions architect recommend?

A. Use one SQS FIFO queue.
Assign a higher priority to the paid photos so they are processed first
B. Use two SQS FIFO queues: one for paid and one for free.
Set the free queue to use short polling and the paid queue to use long polling
C. Use two SQS standard queues one for paid and one for free.
Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.
D. Use one SQS standard queue. Set the visibility timeout of the paid photos to zero.
Configure Amazon EC2 instances to prioritize visibility settings so paid photos are processed first

Answer: C

QUESTION 297
A company has an application hosted on Amazon EC2 instances in two VPCs across different AWS Regions.
To communicate with each other, the instances use the internet for connectivity.
The security team wants to ensure that no communication between the instances happens over the internet.
What should a solutions architect do to accomplish this"

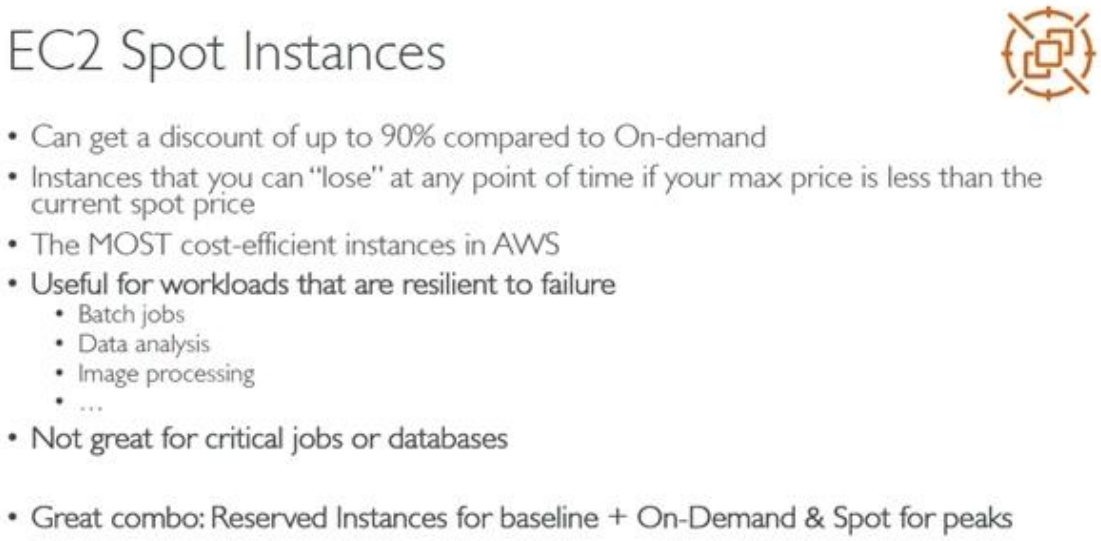
A. Create a NAT gateway and update the route table of the EC2 instances' subnet
B. Create a VPC endpoint and update the route table of the EC2 instances' subnet
C. Create a VPN connection and update the route table of the EC2 instances' subnet
D. Create a VPC peering connection and update the route table of the EC2 instances' subnet

Answer: D

QUESTION 298
A company runs a production application on a fleet of Amazon EC2 instances.
The application reads the data from an Amazon SQS queue and processes the messages in parallel.
The message volume is unpredictable and often has intermittent traffic.
This application should continually process messages without any downtime
Which solution meets these requirements MOST cost-effectively?

A. Use Spot Instances exclusively to handle the maximum capacity required
B. Use Reserved Instances exclusively to handle the maximum capacity required
C. Use Reserved Instances for the baseline capacity and use Spot InstaKes to handle additional capacity
D. Use Reserved instances for the baseline capacity and use On-Demand Instances to handle additional capacity

Answer: D
Explanation:

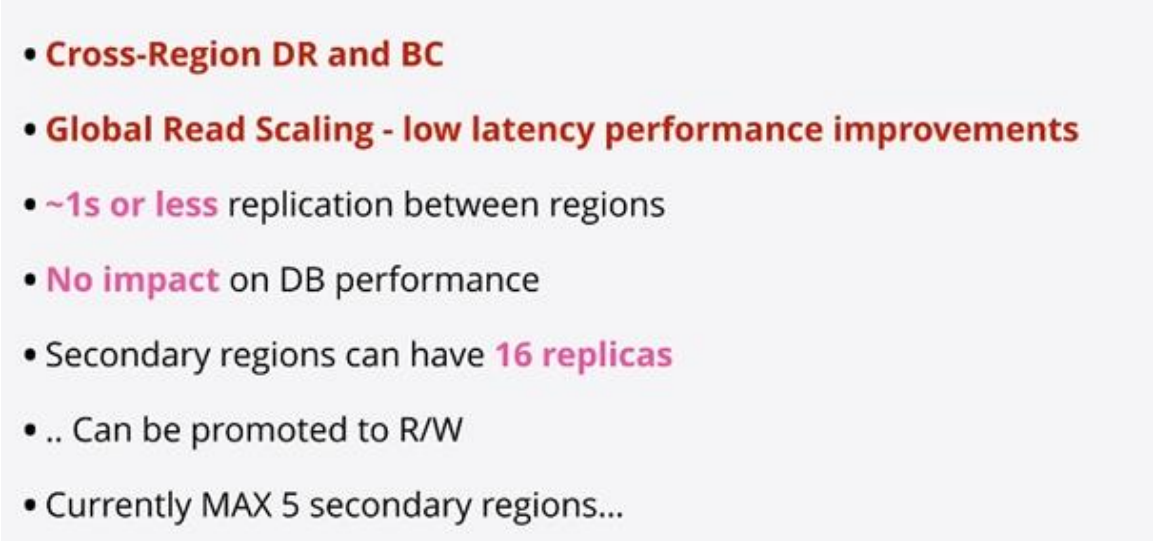


QUESTION 299
A company with facilities in North America. Europe, and Asia is designing new distributed application to optimize its global supply chain and manufacturing process.
The orders booked on one continent should be visible to all Regions in a second or less. The database should be able to support failover with a short Recovery Time Objective (RTO).
The uptime of the application is important to ensure that manufacturing is not impacted.
What should a solutions architect recommend?

A. Use Amazon DynamoDB global tables
B. Use Amazon Aurora Global Database
C. Use Amazon RDS for MySQL with a cross-Region read replica
D. Use Amazon RDS for PostgreSQL with a cross-Region read replica

Answer: B
Explanation:
Cross-Region Disaster Recovery

If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage. This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.



QUESTION 300
A company has several Amazon EC2 instances set up in a private subnet for security reasons. These instances host applications that read and write large amounts of data to and from Amazon S3 regularly.
Currently, subnet routing directs all the traffic destined for the internet through a NAT gateway. The company wants to optimize the overall cost without impacting the ability of the application to communicate with Amazon S3 or the outside internet.
What should a solutions architect do to optimize costs?

A. Create an additional NAT gateway Update the route table to route to the NAT gateway. Update the network ACL to allow S3 traffic
B. Create an internet gateway Update the route table to route traffic to the internet gateway. Update the network ACL to allow S3 traffic.
C. Create a VPC endpoint for Amazon S3 Attach an endpoint policy to the endpoint. Update the route table to direct traffic to the VPC endpoint
D. Create an AWS Lambda function outside of the VPC to handle S3 requests. Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

Answer: C

QUESTION 301
A company hosts a training site on a fleet of Amazon EC2 instances.
The company anticipates that its new course, which consists of dozens of training videos on the site, will be extremely popular when it is released in 1 week.
What should a solutions architect do to minimize the anticipated server load?

A. Store the videos in Amazon ElastiCache for Redis. Update the web servers to serve the videos using the Elastic ache API
B. Store the videos in Amazon Elastic File System (Amazon EFS). Create a user data script for the web servers to mount the EFS volume.
C. Store the videos in an Amazon S3 bucket. Create an Amazon CloudFlight distribution with an origin access identity (OAI) of that S3 bucket. Restrict Amazon S3 access to the OAI.
D. Store the videos in an Amazon S3 bucket.

Create an AWS Storage Gateway file gateway to access the S3 bucket.
Create a user data script for the web servers to mount the file gateway

Answer: C

QUESTION 302
A media company stores video content in an Amazon Elastic Block Store (Amazon EBS) volume. A certain video file has become popular and a large number of users across the world are accessing this content.
This has resulted in a cost increase.

Which action will DECREASE cost without compromising user accessibility?

A. Change the EBS volume to Provisioned IOPS (PIOPS).
B. Store the video in an Amazon S3 bucket and create an Amazon CloudFront distribution.
C. Split the video into multiple, smaller segments so users are routed to the requested video segments only.
D. Clear an Amazon S3 bucket in each Region and upload the videos so users are routed to the nearest S3 bucket.

Answer: B

QUESTION 303
A solutions architect is designing the cloud architecture for a new application being deployed to AWS. The application allows users to interactively download and upload files. Files older than 2 years will be accessed less frequently. The solutions architect needs to ensure that the application can scale to any number of files while maintaining high availability and durability.

Which scalable solutions should the solutions architect recommend? (Choose two.)

A. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Glacier.
B. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard-Infrequent Access (S3 Standard-IA)
C. Store the files on Amazon Elastic File System (Amazon EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA).
D. Store the files in Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.
E. Store the files in RAID-striped Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.

Answer: AB
Explanation:
https://docs.aws.amazon.com/efs/latest/ug/enable-lifecycle-management.html
https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html

QUESTION 304
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? (Choose two.)

A. AWS Batch
B. Network Load Balancer
C. Application Load Balancer
D. Amazon EC2 Auto Scaling
E. Amazon S3 website hosting

Answer: CD
Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html
https://medium.com/awesome-cloud/aws-difference-between-application-load-balancer-and-network-load-balancer-cb8b6cd296a4

QUESTION 305
A solutions architect is creating an application that will handle batch processing of large amounts of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple Amazon EC2 instances.

What should the solutions architect do to reduce the overall data transfer costs?

A. Place all the EC2 instances in an Auto Scaling group.
B. Place all the EC2 instances in the same AWS Region.
C. Place all the EC2 instances in the same Availability Zone.
D. Place all the EC2 instances in private subnets in multiple Availability Zones.

Answer: B
Explanation:
There is no data transfer cost between eC2 & S3 with in same region.

QUESTION 306
A company is hosting an election reporting website on AWS for users around the world. The website uses Amazon EC2 instances for the web and application tiers in an Auto Scaling group with Application Load Balancers. The database tier uses an Amazon RDS for MySQL database. The website is updated with election results once an hour and has historically observed hundreds of users accessing the reports.

The company is expecting a significant increase in demand because of upcoming elections in different countries. A solutions architect must improve the website's ability to handle additional demand while minimizing the need for additional EC2 instances.

Which solution will meet these requirements?

A. Launch an Amazon ElastiCache cluster to cache common database queries.
B. Launch an Amazon CloudFront web distribution to cache commonly requested website content.
C. Enable disk-based caching on the EC2 instances to cache commonly requested website content.

D. Deploy a reverse proxy into the design using an EC2 instance with caching enabled for commonly requested website content.

Answer: B

QUESTION 307
A company is running a three-tier web application to process credit card payments. The front-end user interface consists of static webpages. The application tier can have long-running processes. The database tier uses MySQL.

The application is currently running on a single, general purpose large Amazon EC2 instance. A solutions architect needs to decouple the services to make the web application highly available.

Which solution would provide the HIGHEST availability?

A. Move static assets to Amazon CloudFront.
Leave the application in EC2 in an Auto Scaling group.
Move the database to Amazon RDS to deploy Multi-AZ.
B. Move static assets and the application into a medium EC2 instance.
Leave the database on the large instance.
Place both instances in an Auto Scaling group.
C. Move static assets to Amazon S3, Move the application to AWS Lambda with the concurrency limit set.
Move the database to Amazon DynamoDB with on-demand enabled.
D. Move static assets to Amazon S3.
Move the application to Amazon Elastic Container Service (Amazon ECS) containers with Auto Scaling enabled.
Move the database to Amazon RDS to deploy Multi-AZ.

Answer: D

QUESTION 308
A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.

What should a solutions architect recommend?

A. Deploy Amazon Inspector and associate it with the ALB.
B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

Answer: B
Explanation:
Rate limit
For a rate-based rule, enter the maximum number of requests to allow in any five-minute period from an IP address that matches the rule's conditions. The rate limit must be at least 100.

You can specify a rate limit alone, or a rate limit and conditions. If you specify only a rate limit, AWS WAF places the limit on all IP addresses. If you specify a rate limit and conditions, AWS WAF places the limit on IP addresses that match the conditions.

When an IP address reaches the rate limit threshold, AWS WAF applies the assigned action (block or count) as quickly as possible, usually within 30 seconds. Once the action is in place, if five minutes pass with no requests from the IP address, AWS WAF resets the counter to zero.

QUESTION 309
A company is creating an architecture for a mobile app that requires minimal latency for its users. The company's architecture consists of Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group. The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data. However, the metrics indicate that the EC2 instances do not cross any CPU utilization thresholds.

How can this issue be addressed?

A. Reduce the threshold for CPU utilization in the Auto Scaling Group
B. Replace the Application Load Balancer with a Network Load Balancer
C. Add read replica for the RDS instances and direct read traffic to the replica
D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance

Answer: C

QUESTION 310
A company is hosting its static website in an Amazon S3 bucket, which is the origin for Amazon CloudFront. The company has users in the United States, Canada, and Europe and wants to reduce.

What should a solutions architect recommend?

A. Adjust the CloudFront caching time to live (TTL) from the default to a longer timeframe
B. Implement CloudFront events with Lambda@edge to run the website's data processing
C. Modify the CloudFront price class to include only the locations of the countries that are served
D. Implement a CloudFront Secure Socket Layer (SSL) certificate to push security closer to the locations of the countries that are served

Answer: C

QUESTION 311
A media company stores video content in an Amazon Elastic Block Store (Amazon EBS) volume. A certain video files has become popular and a large number of user across the world are accessing this content.
This has resulted in a cost increase.

Which action will DECREASE cost without compromising user accessibility?

A. Change the EBS volume to provisioned IOPS (PIOPS)
B. Store the video in an Amazon S3 bucket and create and Amazon CloudFront distribution
C. Split the video into multiple, smaller segments so users are routed to the requested video segments only

D. Create an Amazon S3 bucket in each Region and upload the videos so users are routed to the nearest S3 bucket

Answer: B

QUESTION 312
A company built a new VPC with the intention of the hosting Amazon EC2 based workloads on AWS. A solutions architect specified that an Amazon S3 gateway endpoint be created and attached to this new VPC. Once the first Application server is built, developers report that server time out when accessing data stored in the S3 bucket.

Which scenario could be causing this issue? (Select TWO)

A. The S3 bucket is in a region other than the VPC
B. The endpoint has a policy that blocks the CIDR of the VPC
C. The route to the S3 endpoint is not configured in the route table
D. The access is routed through an internet gateway rather than the endpoint
E. The S3 bucket has a bucket policy that does not allow access to the CIDR of the VPC

Answer: CE

QUESTION 313
A solution architect is designing a shared storage solution for an Auto Scaling web application. The company anticipates making frequent changes to the content, so the solution must have strong consistency.

Which solution requires the LEAST amount of effort?

A. Create an Amazon S3 bucket to store the web content and use Amazon Cloudfront to deliver the content
B. Create an Amazon Elastic File system (Amazon EFS) file system and mount it on the individual Amazon EC2 instance
C. Create a shared Amazon Elastic Block store (Amazon EBS) volume and mount it on the individual Amazon EC2 instance
D. Use AWS Datasync to perform continuous synchronization of data between Amazon EC2 hosts in the Auto scaling group.

Answer: B

QUESTION 314
A solution architect creating an application that will handle batch processing of large amount of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing the application will transfer the data over the network between multiple Amazon EC2 instances.

What should the solution architect do to reduce the overall data transfer costs ?

A. Place all the EC2 instances in an Auto scaling group.
B. Place all the EC2 instance in the same AWS Region
C. Place all the EC2 instance in the same Availability Zone
D. Place all the EC2 instances in private subnets in multiple Availability zones

Answer: B

QUESTION 315
A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection Corparate office user query the data warehouse using a visulization tool. Th average size of a query returned by th data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

A. Host the visualization tool on-premises and query the data warehouse directly over the internet.
B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.
C. Host the visualization tool on-premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.
D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same AWS Region.

Answer: D

QUESTION 316
A company provides an API to its users that automates inquiries for tax complutations based on item prices. The company experiences a larger number of inquires during the holiday season only that cause slower response times. A solution architect needs to design a solution that is scalable and elastic.

What should the solutions architect do to accomplish this?

A. Provide an API hosted on an Amazon EC2 instance.
The EC2 instance performs the required computations when the API request is made.
B. Design a REST API using Amazon API Gateway that accepts the item names, API Gateway passes item names to AWS Lambada for tax computations.
C. Create ans Application Load Balancer that has two Amazon EC2 instances behind it.
The EC2 instances will compute the tax on the recieved item names.
D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance, API Gateway accepts and passes the item names to the EC2 instance for tax computations.

Answer: B

QUESTION 317
A company uses a legacy on-premises analytics application that operate on gigabytes of .csv and represents months of data. The legacy application cannit handle the growing size of .csv files. New CSV files added daily from various data sources to a central on-premises storage location. The company wants to continuew to support the legacy application while user learn AWS analytics services. To achieve this, a solution architect wants to maintain two synchronizes copies of all the .csv files on-premises and in Amazon S3.

Which solution should the solution architect recommend?

A. Deploy AWS Datasync on-premises.configure Datasync to continuously replicate the .csv files between the company's S3 bucket.
B. Deploye an on-premises file gateway, Configur data source to write the .csv files to the file gateway, point the legacy analytics application to the file gatway.
The file gaeway should replicate the .csv file to Amazon S3.
C. Deploy an on-premises volume gateway.configure data source to write the .csv files to the volume gateway.Point the legacy analytics application to the volume gateway.
The volume gateway should replicate data to Amazon S3.
D. Deploy AWS datasync on-premises. Configure datasync to continuously replicate the .csv files between on-premises and Amazon Elastic file system (Amazon EFS) enable replication from Amazon EFS to the comapny's S3 Bucket.

Answer: A

QUESTION 318
Management has decided to deploy all AWS VPCs with IPv6 enabled. After sometime, a solutions architect tries to launch a new instance and receives an error stating that there is no enough IP address space available in the subnet.

What should the solutions architect do to fix this?

A. Check to make sure that only IPv6 was used during the VPC creation
B. Create a new IPv4 subnet with a larger range, and then launch the instance
C. Create a new IPv6-only subnet with a larger range, and then launch the instance
D. Disable the IPv4 subnet and migrate all instances to IPv6 only. Once that is complete, launch the instance.

Answer: C

QUESTION 319
A company is developing a new machine learning model solution in AWS. The models are developed as independent microservices that fetch about 1 GB of model data from Amazon S3 at startup and load the data into memory. users access the models through an asychronous API. Users can send a request or a batch of requests and specify where the result should be sent. The comapny provides models to hundreds of users. The usage patterns for the models are irregular. somes models could be unused for days or weeks. other models could receive batches of thousands of requests at a time.

Which solution meets these requirements?

A. The requests from from the API are sent to an Application Load Balancer (ALB).Models are deployed as AWS lambda functions invoked by the ALB
B. The requests from the API are sent to the models Amazon Simple Queue service(Amazon SOS) queue.
Models are deployed as AWS Lambda functions trigeered by SOS events.
AWS auto scaling is enabled on Lambda to increse the number vCPUSs based on the SQS queue size.
C. The requests from the API are sent to the model's Amazon simple Queue service (Amazon SQS) queue.
Model are deployed as Amazon Elastic container service (AMAzon ECS) service reading from the queue.
AWS App Mesh scales the instances of the ECS cluster based on the SQS queue size.

D. The requests from the API are sent to the model's Amazon simple Queue service (Amazon SQS) queue.
Models are deployed as Amazon Elastics container service (Amazon ECS) services reading from the queue.
AWS Auto Scaling is enabled ECS for both the cluster and copies the service based on the queue size.

Answer: D

QUESTION 320
A company has a mobile game that reads most of its metadata from an Amazon RDS DB instances. As the game increased in popularity, developer noticed slowdowns related to the game's metadata load times. Performance metrics Indicate that simply scaling the database will not help. A solutions architect must explore all options that include capabilities for snapshots, replication, and sub-millisecond response times.

What should the solutions architect recommend to solve the issues?

A. Migrate the database to Amazon Aurora with Aurora Replicas.
B. Migrate the database to Amazon DynamoDB with global tables.
C. Add an Amazon ElastiCache for Redis layer in front of the database.
D. Add an Amazon ElastiCache for Memcached layer in front of the database.

Answer: C

QUESTION 321
A company runs and application that uses multiple Amazon EC2 instances to gather data from its users. The data is then processed and transferred to Amazon S3 for long-term storage. A review of the application shows that there were long periods of time when the EC2 instances were not being used. A solution architect needs to design a solution that optimizes utilization and reduces costs.

Which solution meets these requirements?

A. Use Amazon EC2 in an Auto Scaling group with On-Demand instances.
B. Build the application to use Amazon Lightsail with On-Demand instances.
C. Create an Amazon CloudWatch cros job to automatically stop the EC2 instance when there is no activity.
D. Redesign the application to use an event-driven design with Amazon Simple Queue Service (Amazon SQS) and AWS Lambda.

Answer: D

QUESTION 322
A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IP 4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zone (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

What should the solutions architect do to enable Intrnet access for the private subnets?

A. Create three NAT gateways, one for each public subnet in each AZ.
Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
B. Create three NAT gateways, one for each private subnet in each AZ.
Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
C. Create second internet gateway on one of the private subnets.
Update the rout table for the private subnets that forward non-VPC traffic to the private internt gateway.
D. Create an egress-only internet gateway on one of the public subnets.
Update the route table for the private subnets that forward non-VPC traffic to the egress-only internet gateway.

Answer: A

QUESTION 323
A solutions architect needs to design a network that will allow multiple Amazon EC2 instances to access a common data source used for mission-critical data that can be accessed by all the EC2 instances simultaneously. The solution must be highly scalable, easy to implement, and support the NFS protocol.

Which solution meets these requirements?

A. Create an Amazon EFS file system.
Configure a mount target in each Availability Zone.
Attach each instance to the appropriate mount target.
B. Create and additional EC2 instance and configure it as a file server.
Create security group that allows communication between the instances and apply that to the addiotional instance.
C. Create an Amazon S3 bucket with the appropriate permissions.
Create a role in AWS IAM that grants the correct permissions to the S3 bucket.
Attach the role to the EC2 instances that need access to the data.
D. Create an Amazon EBS volume with the appropriate permissions.
Crate a role in AWS IAM that grants the correct permissions to the EBS volume.
Attach the role to then EC2 instances that need access to the data.

Answer: A

QUESTION 324
A company has a multi-tier application deployed on several Amazon EC2 instance in an Auto Scaling group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PUISQL functions Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.

What should a solution architect do to ensure the system can automatically scale for the increased traffic? (Select TWO.)

A. Configure storage auto scaling on the RDS for Oracle instance.

B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
C. Configure an alarm on the RDS for Oracle instance for low free storage space.
D. Configure the Auto Scaling group to use the average CPU as the scaling metric.
E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

Answer: AD

QUESTION 325
A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third-party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks.

Which solution meets these requirements?

A. Enable Amazon Guard Duty on th account
B. Enable Amazon Inspector on the EC2 instances
C. Enable AWS Shield and assign Amazon Route 53 to it.
D. Enable AWS Shield Advancd and assign the ELB to it.

Answer: D

QUESTION 326
A company has a 10 Gbps AWS Direct Connect connection from its on-premises servers to AWS. Th workloads using the connection are critical. The company requires a disastr recovery strategy with maximum resiliency that maintains the current connection bandwidth at a minimum.

What should a solutions architect recommend?

A. Set up a new Direct Connect connection in anothr AWS Region.
B. Set up a new AWS managed VPN connection in another AWS Region.
C. Set up two new Direct Connect connections one in the currnt AWS Region and one in another Region.
D. Set up two new AWS managed VPN connctions one in the current AWS Region and one in another Region.

Answer: A

QUESTION 327
A company stores user data in AWS. The data is used continuously with peak usage during business hours. Access patterns vary, with some data not being used for months at a time. A solutions architect must choose a cost-effective solution that maintains the highest level of durability while maintaining high availability.

Which storage solution meets these requirements?

A. Amazon S3
B. Amazon S3 Intelligent-Tiering
C. Amazon S3 Glacier Deep Archive
D. Amazon S3 One Zone-Infequent Access (S3 One Zone-IA)

Answer: B

QUESTION 328
A company has no existing file share services. A new project requires access to file storage that is mountable as a drive for on-premises desktops. The file server must authenticate usrs to an Activ Directory domain before they are able to access the storage.

Which service will allow Active Directory users to mount storage as a drive on their desktops?

A. AWS S3 Glacier
B. AWS DataSync
C. AWS Snowball Edge
D. AWS Storage Gateway

Answer: B
Explanation:
https://docs.aws.amazon.com/storagegateway/latest/userguide/CreatingAnSMBFileShare.html

QUESTION 329
A company is planning to migrate a legacy application to AWS. The application currently uses NFS to communicate to an on-premises storage solution to store application data. The application cannot be modified to use any other communication protocols other than NFS for this purpose.

Which storage solution should a solutions architect recommend for use after the migrations?

A. AWS DataSync
B. Amazon Elastic Block Store (Amazon EBS)
C. Amazon Elastic File System (Amazon EFS)
D. Amazon EMR File System (Amazon EMRFS)

Answer: C
Explanation:
https://aws.amazon.com/efs/

QUESTION 330
A company has a dynamic web application hostes on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

What should a solutions architect do to increase the application's performance?

A. Create a new SSL certificate using AWS Certificate Manager (ACM).
Install the ACM certificate on each instance.
B. Create an Amazon S3 bucket Migrate the SSL certificate to the S3 bucket.
Configure the EC2 instances to reference the bucket for SSL termination.
C. Create another EC2 instance as a proxy server.
Migrate the SSL certificate to the new instance and configure it to direct connctions to the existing

EC2 instances.

D. Import the SSL certificate into AWS Crtificate Manager (ACM).
Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

Answer: C

QUESTION 331
A solutions architect is designing a security solution for a company that wants to provider developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own account, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.

Which action meets these requirements?

A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.
B. Create a new trail in ClouTrail from within the developer accounts with the organization trails options enabled.
C. Create a service control policy (SCP) the prohibits changes to CloudTrail, and attach it to the developer accounts.
D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master account.

Answer: C

QUESTION 332
A company is building a media sharing application and decides to use Amazon S3 for storage. When a media file uploaded, the company starts a multi-step to create thumbnails, identify obkects in the image, transcode videos into standard formats and resolutons, and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation. The amount of traffic is variable. the solution must be able to scale handle spikes in load without unnecessary expenses.

What should a solution architect recommend to support this workload?

A. Build the processing into the website or mobile app used to upload the content to Amazon S3 save the required data to the DynamDB table when the obkects are uploaded
B. Trigger an AWS Lambda function when an object is stored in the S3 bucket.
Have the step functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.
C. Trigger an AWS Lambda function when an object is stored in the S3 bucket.
Have the Lambda function start AWS batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.
D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amzon S3 use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the Index for unpr0cessed items, and use the program to perform the processing.

Answer: C

QUESTION 333

A company is preparing to migrate its on-premiss application to AWS. The application consists of application servers and a Microsoft SQL Server database. The database cannot be migrated to a different engine because SQL Server features are used in the application's NET code. The company wants to attain the greatest availability possible while minimizing operational and management overhead.

What should a solutions architect do to accomplish this?

A. Install SQL Server on Amazon C2 in a Multi-AZ deployment.
B. Migrate teh data to Amazon RDS for SQL Server in a Multi-AZ deployment.
C. Deploy the database on Amazon RDS for SQL Server with Multi-AZ Replicas.
D. Migrate the data to Amazon RDS for SQL Server in a cross-Region Multi-AZ deployment

Answer: B

QUESTION 334
A company is using Site-Site VPN connection for secure connectivity to its AWS cloud resource from on premises. Due to an increase in traffic across the VPN connections to the Amazon EC2 instances,users are experiencing slower VPN connectivity.

Which solution will improve the VPN throughput?

A. Implement multiple customer gateways for the same network to scale the throughput
B. Use a Transit Gateway with equal cost multipath routing and add additional VPN tunnels.
C. Configure a virtual gateway with equal cost multipath routing and multiple cahnnels.
D. Increase the number of tunnels in the VPN configuration to scale the throughput beyond the default limit.

Answer: B

QUESTION 335
A mobile gaming company runs apllication servers on Amazon EC2 instances. The servers reciev updates from players every 15 minutes. The mobile game creates a JSON object of the progress made in the game since the last update, and sends the JSON object an Application Load Balacer. As the mobile game is played, game updates are being lost. The company wants to create a durable way to get the updates in order.

What should a solution architect recommend to decouple the system?

A. Use Amazon Kinesis Data streams to capture the data and store the JSON object in Amazon S3.
B. Use Amazon Kinesis Data Firehouse to capture the data and store the JSON object in Amzon S3
C. Use Amazon simple Queue service (Amzon SQS) FIFO queue to captur the data and EC2 instances to process the messages in the queue.
D. Use Amazon simple Notification Service (Amazon SNS) to capture the data and EC2 instances to process the messages sent to Application Load balancer.

Answer: C

QUESTION 336
A recently created startup built a three-tier web application. The front end has staic content. The application layer is based on microservices. User data is stored as JSON documents that needs

to be access with low latency. The company expects regular traffic to be low during the first year, with peaks in traffic when it publicizes new features every month. The startup team needs to minimize operational overhead costs.

What should a solutions architect recommend to accomplish this?

A. Use Amazon S3 static website hosting to store and serve the front end.
Use AWS Elastic Benstalk for the applications layer.
Use Amazon DynamoDB to store user data.
B. Use Amazon S3 static website hosting to store and serve the front end.
Use Amazon Elastic Kubernets Service (Amazon EKS) for application layer.
Use Amazon DynamoDB to store user data.
C. Use Amazon S3 static website hosting to store and serve the front end.
Use Amazon API Gateway and Lambda functions for application layer.
Use Amazon DynamoDB to store user data.
D. Use Amazon S3 static website hosting to store and serve the front end.
Use Amazon API Gateway and Lambda functions for application layer.
Use Amazon RDS with read replica to store user data.

Answer: C

QUESTION 337
A company needs comply with a regulatory requirement that states all emails must be stored and archieved externally for 7 years. An administrator has created compressed email files on-premises and wants a managed service to transfer the files to AWS storage.

Which managed service should a solution architect recommend?

A. Amazon Elastic File System (Amazon EFS).
B. Amazon S3 Glacier.
C. AWS Backup.
D. AWS Storage Gateway.

Answer: D

QUESTION 338
Acompany's near-real-time streaming application is running on AWS. As the data is ingested, a job runs on the data and tales 30 minutes to complete. The workload frequently experiences high latency due to large amount of incoming data. A solutions architect needs to design a scalable and serverless solution to enhance performance.

Which combination of steps should the solutions architect take? (Select TWO)

A. Use Amazon Kinesis Data Firehose to ingest the data.
B. Use AWS Lambda with AWS Step Fucntions to process the data.
C. Use AWS Database Migration Service (AWS DMS) to ingest the data.
D. Use Amazon EC2 instances in an Auto Scaling group to process the data.
E. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

Answer: AB

QUESTION 339
A company company is planning to transfer multiple terabytes of data to AWS. The data is collected offline from ships. The company wants to run complex transformations before transferring the data.

Which AWS service should a solutions architect recommend for this migrations?

A. AWS Snowball.
B. AWS Snowmobile.
C. AWS Snowball Edge Storage Optimized.
D. AWS Snowball Edge Compute Optimized.

Answer: D

QUESTION 340
A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains over 10 million rows. The database has 2 TB of General Purpose SSD (gp2) storage. There are millions of updates against this data every day through the company's website. The company has noticed some operations are taking 10 seconds or longer, and has determined that the database storage performance is bottleneck.

Which solution addresses the performance issues?

A. Change the storage type to Provissioned IOPS SSD (io1).
B. Change the instance to a memory-optimized instance class.
C. Change the instance to a burstable performance DB instance class.
D. Enable Multi-AZ RDS read replicas with MySQL natice asynchronous replication.

Answer: A

QUESTION 341
A company has a hybrid application hosted on multiple on-premises servers with static IP addresses. There is already a VPN that provides connectivity between the VPC and the on-premises network. The company wants to distribute TCP traffic across the on-premises servers for internet users.

What should a solution architect recommend to provides a highly available and scalable solution?

A. Launch an internet-facing Network Load Balancer (NLB) and register on-premises IP addresses with the NLB.
B. Launch an internet-facing Application Load Balancer (ALB) and register on-premises IP addresses with the ALB.
C. Launch an Amazon EC2 instance, attach an Elastic IP address, and distribute traffic to the on-premises servers.
D. Launch and Amazon EC2 instance woth public IP addresses in an Auto Scaling group distribute traffic to the on-premises servers.

Answer: A

QUESTION 342
A company has na application that generates a large number of files, each approximately 5 MB in

size. The files are stored in Amazon S3. Company policy requires teh files to be stored for 4 years before they can be deleted. Immediate accessibility is always required as teh files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days.

Which storage solution is MOST cost effective?

A. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Glacier 30 days from object creation.
Delete the files 4 years after the object creation.
B. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days from object creation.
Delete the files 4 years after the object creation.
C. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation.
Delete the files 4 years after the object creation.
D. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation.
Move the file to S3 Glacier 4 years after object creation.

Answer: C

QUESTION 343
An online shopping application accesses an Amazon RDS Multi-AZ DB instance. Database performance is slowing down the application. After upgrading to the next generation instance type, there was no significant performance improvemnt.

Analysis shows approximately 700 IOPS are sustained, common queries run for long durations, and memory utilization is high.

Which application change should a solution architect recommend to resolve these issue?

A. Migrate the RDS instance to an Amazon Redshift cluster and enable weekly garbage collection.
B. Spearate teh long-running queries into a new Multi-AZ RDS database and modify the application to query whichever database only if needed.
C. Deploy a two-node Amazon ElastiCache cluster and modify the application to query whichever database only if needed.
D. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue for common queries and query it first and query the database only if needed

Answer: C

QUESTION 344
A company hosts its web application on AWS using server Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be refumed in response to DNS queries.

Which policy should be used to meet this requirement?

A. Simple routing policy.
B. Latency routing policy.
C. Multivalue routing policy.

D. Geolocation routing policy.

Answer: C

QUESTION 345
As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most effective way to obtain this report information.

Which solution meets these requirements?

A. Run a query with Amazon Athena to generate the report.
B. Create a report in Cost Explorer and download the report.
C. Access the bill details from the billing dashboard and download the bill.
D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Answer: B

QUESTION 346
A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Key must be rotated every year.

Which solution meets these requirements and is the MOST operationally effecient?

A. Server-side encryption with customer-provided keys (SSE-C)
B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation.
D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic rotation.

Answer: D

QUESTION 347
A company has 700 TB of backup data stored in network attached storage (NAS) in its data center. This backup data need to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migrations must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.

What should a solutions architect do to migrate and store the data at the LOWEST cost?

A. Order AWS Snowball devices to transfer the data.
Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
B. Deploy a VPN connection between the data center and Amazon VPC.
Use the AWS CLI to copy the data from on-premises to Amazon S3 Glacier.
C. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3.
Use a lifecycle policy to transistion the files to Amazon S3 Glacier Deep Archive.
D. Use AWS DataSync to transfer the data and deploy a DataSync agent on-premises.
Use the DataSync task to copy files from the on-premises NAS Storage to Amazon S3 Glacier.

Answer: A

QUESTION 348
A company wants to migrate its MySQL database from on-premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which solution meets these requirements?

A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
C. Create an Amazon RDS MySQL DB instance with Multi-AZ and the create a read replica in a separate AWS Region that synchronously replicates the data.
D. Create and Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda fucntion to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Answer: B

QUESTION 349
A application running on an Amazon EC2 instance needs to securely access files on an Amazon Elastic File System (Amazon EFS) file system. The EFS files are stores using encryptions at rest.

Which solution for accessing teh files in MOST secure?

A. Enable TLS when mounting Amazon EFS.
B. Store the encryption key in the code of the application.
C. Enable AWS Key MAnagement Service (AKS KMS) when mounting Amazon EFS.
D. Store the encryption key in an Amazon S3 bucket and use IAM roles to grand the EC2 instance access permission.

Answer: C

QUESTION 350
An ecommerce website is deploying its web application as Amazon Elastic Container Service (Amazon ECS) container instance behind an Application Load Balancer (ALB). During periods of high activity, the website slows down and availability is reduced. A solutions architect uses Amazon CloudWatch alarms to receive notifications whenever there is an availability issues so they can scale out resource Company management wants a solution that automatically responds to such events.

Which solution meets these requirements?

A. Set up AWS Auto Scaling to scale out the ECS service when there are timeouts on the ALB. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
B. Set up AWS Auto Scaling to scale out the ECS service when the ALB CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is

too high.

C. Set up AWS Auto Scaling to scale out the ECS service when the service's CPU utilization is too high.
Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.

D. Set up AWS Auto Scaling to scale out the ECS service when the ALB target group CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.

Answer: D

QUESTION 351
A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

A. Create security group rules using the instance ID as the source or destination.
B. Create security group rules using the security group ID as the source or destination.
C. Create security group rules using the VPC CIDR block as the source or destination.
D. Create security group rules using the subnet CIDR block as the source or destination.

Answer: B

QUESTION 352
A company is developing a video conversion application hosted on AWS. The application will be available in to tiers: a free tier and paid tier. User in teh paid tier will have their videos converted first, and then teh free tier users will have their videos converted.

Which solution meets these requirements and is MOST cost-effective?

A. One FIFO queue for the paid tier and one standard queue for the free tier
B. A single FIFO Amazon Simple Queue Service (Amazon SQS) queue for all files types.
C. A single standard Amazon Simple Queue Service (Amazon SQS) queue for all files types.
D. Two standard Amazon Simple Queue Service (Amazon SQS) queues with one for the paid tier and one for the free tier.

Answer: A

QUESTION 353
A company is building a website that relies on reading and writing to an Amazon DynamoDB database. The traffic associated with the website predictably peaks during business hours on weekdays and declines overnight and during weekends A solutions architect needs to design a cost-effective solution that can handle the load.

What should the solutions architect do to meet these requirements?

A. Enable DynamoDB Accelerator (DAX) to cache the data.
B. Enable Multi-AZ replication for the DynamoDB database.
C. Enable DynamoDB auto scaling when creating the tables.

D. Enable DynamoDB On-Demand capacity allocation when creating the tables.

Answer: C

QUESTION 354
A company is preparing to deploy a data lake on AWS. A solutions architect must define the encryption strategy for data at rest in Amazon S3. The company's security policy states.

```
- Keys must be rotated every 90 days.
- Strict separation of duties between key users and key administrators
must be implemented.
- Auditing key usage must be possible.
```

What should the solutions architect recommend?

A. Server-side encryption with AWS KMS managed keys (SSE-KMS) with customer managed customer master keys (CMKs).
B. Server-side encryption with AWS KMS managed keys (SSE-KMS) with AWS managed customer master keys (CMKS).
C. Server-side encryption with Amazon S3 managed keys (SSE-S3) with customer managed customer master keys (CMKS).
D. Server-side encryption with Amazon S3 managed keys (SSE-S3) with AWS managed customer master keys (CMKs).

Answer: A

QUESTION 355
A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3. The application has grown and there are user complaints about internet bandwidth limitations. A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and with minimal impact on internet connectivity for internal users.

Which solution meets these requirements?

A. Establish AWS VPN connections and proxy all traffic through a VPC gateway endpoint
B. Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.
C. Order daily AWS Snowball devices Load the data onto the Snowball devices and return the devices to AWS each day.
D. Submit a support ticket through the AWS Management Console Request the removal of S3 service limits from the account.

Answer: B

QUESTION 356
A company uses Amazon Redshift for its data warehouse. The company wants to ensure high durability for its data in case of any component failure.

What should a solutions architect recommend?

A. Enable concurrency scaling.
B. Enable cross-Region snapshots.
C. Increase the data retention period.
D. Deploy Amazon Redshift in Multi-AZ.

Answer: B

QUESTION 357
A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content to meet the migration date, minimal changes can be made.

What should a solutions architect do to meet these requirements?

A. Create an Amazon S3 Standard bucket with access to the web server.
B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
C. Create an Amazon Elastic File System (Amazon EFS) volume and mount it on all web servers.
D. Configure Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volumes and mount them on all web servers.

Answer: C

QUESTION 358
A solutions architect is planning the deployment of a new static website. The solution must minimize costs and provide at least 99% availability.

Which solution meets these requirements?

A. Deploy the application to an Amazon S3 bucket in one AWS Region that has versioning disabled.
B. Deploy the application to Amazon EC2 instances that run in two AWS Regions and two Availability Zones.
C. Deploy the application to an Amazon S3 bucket that has versioning and cross-Region replication enabled.
D. Deploy the application to an Amazon EC2 instance that runs in one AWS Region and one Availability Zone.

Answer: A

QUESTION 359
A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.

Which solution meets these requirements?

A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
B. Create a new RDS Multi-AZ deployment.
Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.

C. Create a read-only replica of the PostgreSQL database in another Availability Zone.
Use Amazon Route 53 weighted record sets to distribute requests across the databases.
D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two.
Use Amazon Route 53 weighted record sets to distribute requests across instances.

Answer: A

QUESTION 360
A company is deploying an application in three AWS Regions using an Application Load Balancer. Amazon Route 53 will be used to distribute traffic between these Regions.

Which Route 53 configuration should a solutions architect use to provide the MOST high-performing experience?

A. Create an A record with a latency policy.
B. Create an A record with a geolocation policy
C. Create a CNAME record with a failover policy.
D. Create a CNAME record with a geoproximity policy.

Answer: A

QUESTION 361
A company hosts an application used to upload files to an Amazon S3 bucket. Once uploaded, the files are processed to extract metadata, which takes less than 5 seconds. The volume and frequency of the uploads varies from a few files each hour to hundreds of concurrent uploads. The company has asked a solutions architect to design a cost-effective architecture that will meet these requirements.

What should the solutions architect recommend?

A. Configure AWS Cloud Trail trails to log S3 API calls.
Use AWS AppSync to process the files.
B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.
C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3.
Invoke an AWS Lambda function to process the files.
D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3.
Invoke an AWS Lambda function to process the files.

Answer: B

QUESTION 362
A company has data stored in an on-premises data center that is used by several on-premises applications. The company wants to maintain its existing application environment and be able to use AWS services for data analytics and future visualizations.

Which storage service should a solutions architect recommend?

A. Amazon Redshift.

B. AWS Storage Gateway for files.
C. Amazon Elastic Block Store (Amazon EBS).
D. Amazon Elastic File System (Amazon EFS).

Answer: B

QUESTION 363
A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard. A solutions architect needs to design a solution that can handle large traffic spikes, process the mobile game updates in order of receipt, and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution.

What should the solutions architect do to meet these requirements?

A. Push score updates to Amazon Kinesis Data Streams.
Process the updates in Kinesis Data Streams with AWS Lambda.
Store the processed updates in Amazon DynamoDB.
B. Push score updates to Amazon Kinesis Data Streams.
Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling.
Store the processed updates in Amazon Redshift.
C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic.
Subscribe an AWS Lambda function to the SNS topic to process the updates.
Store the processed updates in a SQL database running on Amazon EC2.
D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue.
Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SOS queue.
Store the processed updates in an Amazon RDS Multi-AZ DB instance.

Answer: A
Explanation:
Keywords to focus on would be highly available database - DynamoDB would be a better choice for leaderboard.

QUESTION 364
A company has a three-tier environment on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB), then to Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier that makes database calls.

What should a solutions architect do to improve the security of data in transit to the web tier?

A. Configure a TLS listener and add the Server Certificate on the NLB.
B. Configure AWS Shield Advanced and enable AWS WAF on the NLB.
C. Change the Load Balancer to an Application Load Balancer and attach AWS WAF to it.
D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS)

Answer: A
Explanation:
User - NLB - EC2 (Web) + DB

QUESTION 365
A company uses Application Load Balancers (ALBs) in different AWS Regions.

The ALBs receive inconsistent traffic that can spike and drop throughout the year. The company's networking team needs to allow the IP addresses of the ALBs in the on-premises firewall to enable connectivity.

Which solution is the MOST scalable with minimal configuration changes?

A. Write an AWS Lambda script to get the IP addresses of the ALBs in different Regions.
Update the on- premises firewalls rule to allow the IP addresses of the ALBs.
B. Migrate all ALBs in different Regions to the Network Load Balancers (NLBs).
Update the on-premises firewall's rule to allow the Elastic IP addresses of all the NLBs.
C. Launch AWS Global Accelerator Register the ALBs in different Regions to the accelerator.
Update the on-premises firewall's rule to allow static IP addresses associated with the accelerator.
D. Launch a Network Load Balancer (NLB) in one Region Register the private IP addresses of the ALBs in different Regions with the NLB.
Update the on-premises firewall's rule to allow the Elastic IP address attached to the NLB.

Answer: C

QUESTION 366
A company receives inconsistent service from its data center provider because the company is headquartered in an area affected by natural disasters.

The company is not ready to fully migrate to the AWS Cloud, but it wants a failure environment on AWS in case the on-premises data center fails.

The company runs web servers that connect to external vendors. The data available on AWS and on premises must be uniform.

Which solution should a solutions architect recommend that has the LEAST amount of downtime?

A. Configure an Amazon Route 53 failover record.
Run application servers on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group.
Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
B. Configure an Amazon Route 53 failover record.
Execute an AWS CloudFormation template from a script to create Amazon EC2 instances behind an Application Load Balancer.
Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
C. Configure an Amazon Route 53 failover record.
Set up an AWS Direct Connect connection between a VPC and the data center.
Run application servers on Amazon EC2 in an Auto Scaling group.
Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer.
D. Configure an Amazon Route 53 failover record.
Run an AWS Lambda function to execute an AWS CloudFormation template to launch two Amazon EC2 instances.
Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
Set up an AWS Direct Connect connection between a VPC and the data center.

Answer: D

QUESTION 367
A company has two AWS accounts Production and Development.

There are code changes ready in the Development account to push to the Production account. In the alpha phase, only two senior developers on the development team need access to the Production account. In the beta phase, more developers might need access to perform testing as well.

What should a solutions architect recommend?

A. Create two policy documents using the AWS Management Console in each account.
Assign the policy to developers who need access.
B. Create an IAM role in the Development account Give one IAM role access to the Production account.
Allow developers to assume the role.
C. Create an IAM role in the Production account with the trust policy that specifies the Development account.
Allow developers to assume the role.
D. Create an IAM group in the Production account and add it as a principal in the trust policy that specifies the Production account.
Add developers to the group.

Answer: C

QUESTION 368
A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys.
Configure the application to load the database credentials from AWS KMS.
Enable automatic key rotation.
B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager.
Configure the application to load the database credentials from Secrets Manager.
Create an AWS Lambda function that rotates the credentials in Secret Manager.
C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager.
Configure the application to load the database credentials from Secrets Manager.
Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter.
Store Configure the application to load the database credentials from Parameter Store.
Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Answer: B

QUESTION 369
A web application must persist order data to Amazon S3 to support near-real-time processing.

A solutions architect needs create an architecture that is both scalable and fault tolerant.

Which solutions meet these requirements? (Select TWO.)

A. Write the order event to an Amazon DynamoDB table.
Use DynamoDB Streams to trigger an AWS Lambda function that parses the payload and writes the data to Amazon
B. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue.
Use the queue to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
C. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic.
Use the SNS topic to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
D. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue.
Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
E. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic.
Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

Answer: AD

QUESTION 370
A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS Key Management Service Customer Master Keys (AWS KMS CMKs).

A solutions architect needs to design a solution that will ensure the required permissions are set correctly.

Which combination of actions accomplish this? (Select TWO.)

A. Attach the kms.decrypt permission to the Lambda function's resource policy.
B. Grant the decrypt permission for the Lambda IAM role in the KMS key's policy.
C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.
E. Create a new IAM role with the kms decrypt permission and attach the execution role to the Lambda function.

Answer: BE

QUESTION 371
A company is building a document storage application on AWS. The application runs on Amazon EC2 instances in multiple Availability Zones. The company requires the document store to be highly available. The documents need to be returned immediately when requested.

The lead engineer has configured the application to use Amazon Elastic Block Store (Amazon EBS) to store the documents, but is willing to consider other options to meet the availability

requirement.

What should a solutions architect recommend?

A. Snapshot the EBS volumes regularly and build new volumes using those snapshots in additional Availability Zones.
B. Use Amazon EBS for the EC2 instance root volumes.
Configure the application to build the document store on Amazon S3.
C. Use Amazon EBS for the EC2 instance root volumes.
Configure the application to build the document store on Amazon S3 Glacier.
D. Use at least three Provisioned IOPS EBS volumes for EC2 instances.
Mount the volumes to the EC2 instances in a RAID 5 configuration.

Answer: B

QUESTION 372
A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost.

The company's data science team wants to query ingested data near-real time.

Which solution provides near-real-time data querying that is scalable with minimal data loss?

A. Publish data to Amazon Kinesis Data Streams.
Use Kinesis Data Analytics to query the data.
B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination.
Use Amazon Redshift to query the data.
C. Store ingested data in an EC2 instance store.
Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination.
Use Amazon Athena to query the data.
D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume.
Publish data to Amazon ElastiCache for Redis.
Subscribe to the Redis channel to query the data.

Answer: C

QUESTION 373
A company has a website deployed on AWS. The database backend is hosted on Amazon RDS for MySQL with a primary instance and five read replicas to support scaling needs. The read replicas should lag no more than 1 second behind the primary instance to support the user experience.

As traffic on the website continues to increase, the replicas are falling further behind during periods of peak load, resulting in complaints from users when searches yield inconsistent results.

A solutions architect needs to reduce the replication lag as much as possible, with minimal changes to the application code or operational requirements.

Which solution meets these requirements?

A. Migrate the database to Amazon Aurora MySQL.

Replace the MySQL read replicas with Aurora Replicas and enable Aurora Auto Scaling.

B. Deploy an Amazon ElastiCache for Redis cluster in front of the database.
Modify the website to check the cache before querying the database read endpoints.

C. Migrate the database from Amazon RDS to MySQL running on Amazon EC2 compute instances.
Choose very large compute optimized instances for all replica nodes.

D. Migrate the database to Amazon DynamoDB.
Initially provision a large number of read capacity units (RCUs) to support the required throughput with on-demand capacity.

Answer: A

QUESTION 374
A group requires permissions list an Amazon S3 bucket and delete objects from that bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket.

The company follows least-privilege access rules.

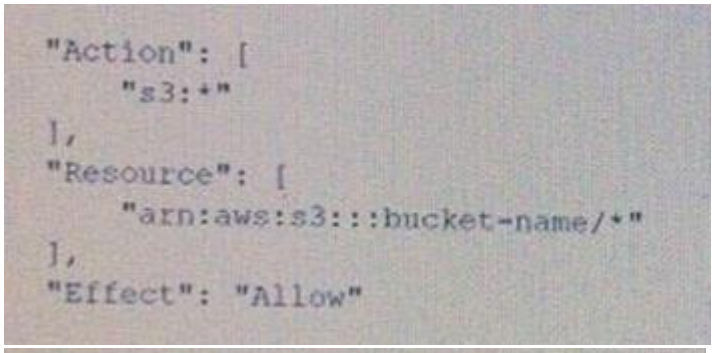
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Which statement should a solutions architect add to the policy to correct bucket access?

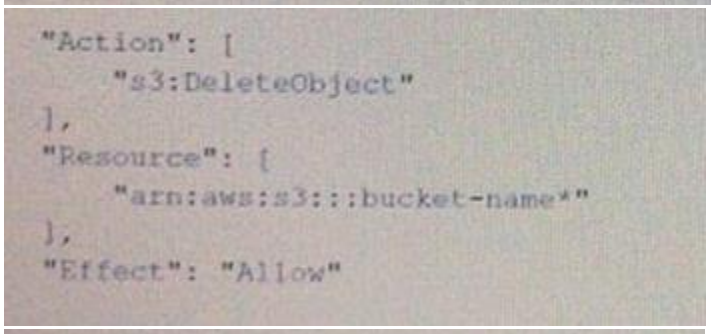
A.

```
"Action": [
    "s3:*Object"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

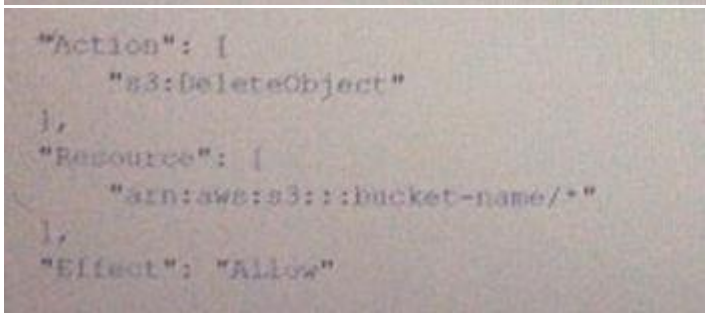
B.



C.



D.



Answer: B

QUESTION 375
A company has an API-based inventory reporting application running on Amazon EC2 instances. The application stores information in an Amazon DynamoDB table. The company's distribution centers have an on-premises shipping application that calls an API to update the inventory before printing shipping labels.

The company has been experiencing application interruptions several times each day, resulting in lost transactions.

What should a solutions architect recommend to improve application resiliency?

A. Modify the shipping application to write to a local database.
B. Modify the application APIs to run serverless using AWS Lambda.
C. Configure Amazon API Gateway to call the EC2 inventory application APIs.
D. Modify the application to send inventory updates using Amazon Simple Queue Service (Amazon SQS).

Answer: D

QUESTION 376
A user has underutilized on-premises resources.

Which AWS Cloud concept can BEST address this issue?

A. High Availability
B. Elasticity
C. Security
D. Loose Coupling

Answer: B

QUESTION 377
A company has an automobile sales website that stores its listings in an database on Amazon RDS When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems.

Which design should a solutions architect recommend?

A. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume.
B. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) FIFO queue for the targets to consume.
C. Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics. Use AWS Lambda functions to update the targets.
D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues Use AWS Lambda functions to update the targets.

Answer: B

QUESTION 378
An application is running on an Amazon EC2 instance and must have millisecond latency when running the workload. The application makes many small reads and writes to the file system, but the file system itself is small.

Which Amazon Elastic Block Store (Amazon EBS) volume type should a solutions architect attach to their EC2 instance?

A. Cold HDD (sc1)
B. General Purpose SSD (gp2)
C. Provisioned IOPS SSD (io1)
D. Throughput Optimized HDD (st1)

Answer: B

QUESTION 379

A company runs a static website through its on-premises data center. The company has multiple servers that handle all of its traffic, but on busy days, services are interrupted and the website becomes unavailable. The company wants to expand its presence globally and plans to triple its website traffic

What should a solutions architect recommend to meet these requirements?

A. Migrate the website content to Amazon S3 and host the website on Amazon CloudFront.
B. Migrate the website content to Amazon EC2 instances with public Elastic IP addresses in multiple AWS Regions.
C. Migrate the website content to Amazon EC2 instances and vertically scale as the load increases.
D. Use Amazon Route 53 to distribute the loads across multiple Amazon CloudFront distributions for each AWS Region that exists globally.

Answer: A

QUESTION 380
A company has a media catalog with metadata for each item in the catalog. Different types of metadata are extracted from the media items by an application running on AWS Lambda. Metadata is extracted according to a number of rules, with the output stored in an Amazon ElastiCache for Redis cluster. The extraction process is done in batches and takes around 40 minutes to complete. The update process is triggered manually whenever the metadata extraction rules change.

The company wants to reduce the amount of time it takes to extract metadata from its media catalog. To achieve this, a solutions architect has split the single metadata extraction Lambda function into a Lambda function for each type of metadata.

Which additional steps should the solutions architect take to meet the requirements?

A. Create an AWS Step Functions workflow to run the Lambda functions in parallel.
Create another Step Functions workflow that retrieves a list of media items and executes a metadata extraction workflow for each one.
B. Create an AWS Batch compute environment for each Lambda function.
Configure an AWS Batch job queue for the compute environment.
Create a Lambda function to retrieve a list of media items and write each item to the job queue.
C. Create an AWS Step Functions workflow to run the Lambda functions in parallel.
Create a Lambda
function to retrieve a list of media items and write each item to an Amazon SQS queue.
Configure the SQS queue as an input to the Step Functions workflow.
D. Create a Lambda function to retrieve a list of media items and write each item to an Amazon SQS queue.
Subscribe the metadata extraction Lambda functions to the SQS queue with a large batch size.

Answer: C

QUESTION 381
A company is deploying a public-facing global application on AWS using Amazon CloudFront. The application communicates with an external system. A solutions architect needs to ensure the data is secured during end-to-end transit and at rest.

Which combination of steps will satisfy these requirements? (Select TWO)

A. Create a public certificate for the required domain in AWS Certificate Manager and deploy it to CloudFront, an Application Load Balancer, and Amazon EC2 instances.
B. Acquire a public certificate from a third-party vendor and deploy it to CloudFront, an Application Load Balancer, and Amazon EC2 instances.
C. Provision Amazon EBS encrypted volumes using AWS KMS and ensure explicit encryption of data when writing to Amazon EBS.
D. Use SSL or encrypt data while communicating with the external system using a VPN.
E. Communicate with the external system using plaintext and use the VPN to encrypt the data in transit.

Answer: CD

QUESTION 382
A company's lease of a co-located storage facility will expire in 90 days. The company wants to move to AWS to avoid signing a contract extension. The company's environment consists of 200 virtual machines and a NAS with 40 TB of data. Most of the data is archival, yet instant access is required when data is requested.

Leadership wants to ensure minimal downtime during the migration. Each virtual machine has a number of customized configurations. The company's existing 1 Gbps network connection is mostly idle, especially after business hours.

Which combination of steps should the company take to migrate to AWS while minimizing downtime and operational impact? (Select TWO.)

A. Use new Amazon EC2 instances and reinstall all application code.
B. Use AWS SMS to migrate the virtual machines.
C. Use AWS Storage Gateway to migrate the data to cloud-native storage.
D. Use AWS Snowball to migrate the data.
E. Use AWS SMS to copy the infrequently accessed data from the NAS.

Answer: BC

QUESTION 383
A company is planning a large event where a promotional offer will be introduced. The company's website is hosted on AWS and backed by an Amazon RDS for PostgreSQL DB instance. The website explains the promotion and includes a sign-up page that collects user information and preferences. Management expects large and unpredictable volumes of traffic periodically, which will create many database writes.

A solutions architect needs to build a solution that does not change the underlying data model and ensures that submissions are not dropped before they are committed to the database.

Which solutions meets these requirements?

A. Immediately before the event, scale up the existing DB instance to meet the anticipated demand. Then scale down after the event.
B. Use Amazon SQS to decouple the application and database layers.
Configure an AWS Lambda function to write items from the queue into the database.
C. Migrate to Amazon DynamoDB and manage throughput capacity with automatic scaling.
D. Use Amazon ElastiCache for Memcached to increase write capacity to the DB instance.

Answer: B

QUESTION 384
A solutions architect is designing a publicly accessible web application that is on an Amazon CloudFront distribution with an Amazon S3 website endpoint as the origin.

When the solution is deployed, the website returns an Error 403: Access Denied message.

Which steps should the solutions architect take to correct the issue? (Select TWO.)

A. Remove the S3 block public access option from the S3 bucket.
B. Remove the requester pays option from the S3 bucket.
C. Remove the origin access identity (OAI) from the CloudFront distribution.
D. Change the storage class from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA).
E. Disable S3 object versioning

Answer: AB

QUESTION 385
A company is running a media store across multiple Amazon EC2 instances distributed across multiple Availability Zones in a single VPC.

The company wants a high-performing solution to share data between all the EC2 instances, and prefers to keep the data within the VPC only.

What should a solutions architect recommend?

A. Create an Amazon S3 bucket and call the service APIs from each instance's application.
B. Create an Amazon S3 bucket and configure all instances to access it as a mounted volume.
C. Configure an Amazon Elastic Block Store (Amazon EBS) volume and mount it across all instances.
D. Configure an Amazon Elastic File System (Amazon EFS) file system and mount it across all instances.

Answer: D

QUESTION 386
A company has a 143 TB MySQL database that it wants to migrate to AWS. The plan is to use Amazon Aurora MySQL as the platform going forward. The company has a 100 Mbps AWS Direct Connect connection to Amazon VPC.

Which solution meets the company's needs and takes the LEAST amount of time?

A. Use a gateway endpoint for Amazon S3.
Migrate the data to Amazon S3. Import the data into Aurora.
B. Upgrade the Direct Connect link to 500 Mbps.
Copy the data to Amazon S3 Import the data into Aurora.
C. Order an AWS Snowmobile and copy the database backup to it.
Have AWS import the data into Amazon S3. Import the backup into Aurora.
D. Order four 50-TB AWS Snowball devices and copy the database backup onto them.

Have AWS import the data into Amazon S3. Import the data into Aurora.

Answer: D

QUESTION 387
A media company has an application that tracks user clicks on its websites and performs analytics to provide near-real time recommendations. The application has a fleet of Amazon EC2 instances that receive data from the websites and send the data to an Amazon RDS DB instance.

Another fleet of EC2 instances hosts the portion of the application that is continuously checking changes in the database and executing SQL queries to provide recommendations. Management has requested a redesign to decouple the infrastructure.

The solution must ensure that data analysts are writing SQL to analyze the data only. No data can be lost during the deployment.

What should a solutions architect recommend?

A. Use Amazon Kinesis Data Streams to capture the data from the websites, Kinesis Data Firehose to persist the data on Amazon S3, and Amazon Athena to query the data.
B. Use Amazon Kinesis Data Streams to capture the data from the websites, Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3.
C. Use Amazon Simple Queue Service (Amazon SQS) to capture the data from the websites, keep the fleet of EC2 instances, and change to a bigger instance type in the Auto Scaling group configuration.
D. Use Amazon Simple Notification Service (Amazon SNS) to receive data from the websites and proxy the messages to AWS Lambda functions that execute the queries and persist the data. Change Amazon RDS to Amazon Aurora Serverless to persist the data.

Answer: B

QUESTION 388
A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.

What should a solutions architect do to mitigate any single point of failure in this architecture?

A. Add a set of VPNs between the Management and Production VPCs.
B. Add a second virtual private gateway and attach it to the Management VPC.
C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Answer: C

QUESTION 389
A solutions architect is designing a solution that involves orchestrating a series of Amazon Elastic Container Service (Amazon ECS) task types running on Amazon EC2 instances that are part of an ECS cluster. The output and state data for all tasks needs to be stored.

The amount of data output by each task is approximately 10MB, and there could be hundreds of tasks running at a time. The system should be optimized for high-frequency reading and writing. As old outputs are archived and deleted, the storage size is not expected to exceed 1TB.

Which storage solution should the solutions architect recommend?

A. An Amazon DynamoDB table accessible by all ECS cluster instances.
B. An Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.
C. An Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode.
D. An Amazon Elastic File System (Amazon EFS) volume mounted to the ECS cluster instances.

Answer: C

QUESTION 390
A company has three VPCs named Develpoment, Testing, and Production in the us-east-1 Region. The three VPCs need to be connected to and on-premesis data center and are designed to be separate to maintain security and prevent any resource sharing.

A solution architect needs to find a scalable and secure solution.

What should the solution archtect recommend?

A. Create an AWS Direct Connect connection and a VPN connection for each VPC to connect back to the data center.
B. Create VPC peers from all the VPCs to the Production VPC.
Use an AWS Direct Connect connection from the Production VPC back to the data center.
C. Connect VPN connections from all the VPCs to a VPN in the Production VPC.
Use a VPN connection from the Production VPC back to the data center.
D. Create a new VPC called Network. Within the Network VPC, create and AWS Transit Gateway with an AWS Direct Connect connection back to the data center.
Attach all the other VPCs to the Network VPC.

Answer: D

QUESTION 391
A company wants to build a scalable key management infrastructure to support developers who need to encrypt data in their applications.

What should a solutions architect do to reduce the operational burden?

A. Use multi-factor authentication (MFA) to protect the encryption keys
B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys
C. Use AWS Certificate Manager (ACM) to create, store and assign the encryption keys
D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys

Answer: B

QUESTION 392
A development team is collaborating with another company to create an integrated product. The

other company needs to access an Amazon Simple Queue Service (Amazon SQS) queue that is contained in the development team's account. The other company wants to poll the queue without giving up its own account permissions to do so.

How should a solutions architect provide access to the SQS queue?

A. Create an instance profile that provides the other company access to the SQS queue.
B. Create an IAM policy that provides the other company access to the SQS queue.
C. Create an SQS access policy that provides the other company access to the SQS queue.
D. Create an Amazon Simple Notification Service (Amazon SNS) access policy that provides the other company access to the SQS queue.

Answer: C

QUESTION 393
A disaster response team is using drones to collect images from recent storm damage. The response team's laptops lack the storage and compute capacity to transfer the images and process the data. While the team has Amazon EC2 instances for processing and Amazon S3 buckets for storage, network connectivity is intermittent and unreliable. The images need to be processed to evaluate the damage.

What should a solutions architect recommend?

A. Use AWS Snowball Edge devices to process and store the images.
B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.
C. Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separatelyat the S3 buckets for storage and the EC2 instances for processing the images.
D. Use AWS Storage Gateway pre-installed on a hardware appliance to cache the images locally for Amazon S3 to process the images when connectivity becomes available.

Answer: A

QUESTION 394
A company has a live chat application running on list on-premises servers that use WebSockets. The company wants to migrate the application to AWS Application traffic is inconsistent, and the company expects there to be more traffic with sharp spikes in the future. The company wants a highly scalable solution with no server maintenance nor advanced capacity planning.

Which solution meets these requirements?

A. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store Configure the DynamoDB table for provisioned capacity
B. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store Configure the DynaiWDB table for on-demand capacity
C. Run Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store Configure the DynamoDB table for on-demand capacity
D. Run Amazon EC2 instances behind a Network Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store Configure the DynamoDB table for provisioned capacity

Answer: B

QUESTION 395
A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However, the company's security policy states that any external service cannot initiate a connection to the EC2 instances.

What should a solutions architect recommend to resolve this issue?

A. Create a NAT gateway and make it the destination of the subnet's route table
B. Create an internet gateway and make it the destination of the subnet's route table
C. Create a virtual private gateway and make it the destination of the subnet's route table
D. Create an egress-only internet gateway and make it the destination of the subnet's route table

Answer: D

QUESTION 396
A company is deploying a web portal. The company wants to ensure that only the web portion of the application is publicly accessible. To accomplish this, the VPC was designed with two public subnets and two private subnets. The application will run on several Amazon EC2 instances in an Auto Scaling group. SSL termination must be offloaded from the EC2 instances.

What should a solutions architect do to ensure these requirements are met?

A. Configure the Network Load Balancer in the public subnets.
Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer
B. Configure the Network Load Balancer in the public subnets.
Configure the Auto Scaling group in the public subnets and associate it with the Application Load Balancer
C. Configure the Application Load Balancer in the public subnets.
Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer
D. Configure the Application Load Balancer in the private subnets.
Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer

Answer: C

QUESTION 397
A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.

Which combination of actions should the solutions architect take to accomplish this? (Select TWO.)

A. Migrate the PostgreSQL database to Amazon Aurora

B. Migrate the web application to be hosted on Amazon EC2 instances.
C. Set up an Amazon CloudFront distribution for the web application content.
D. Set up Amazon ElastiCache between the web application and the PostgreSQL database
E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS)

Answer: AE

QUESTION 398
A solutions architect needs to ensure that all Amazon Elastic Block Store (Amazon EBS) volumes restored from unencrypted EBS snapshots are encrypted.

What should the solutions architect do to accomplish this?

A. Enable EBS encryption by default for the AWS Region
B. Enable EBS encryption by default for the specific volumes
C. Create a new volume and specify the symmetric customer master key (CMK) to use for encryption
D. Create a new volume and specify the asymmetric customer master key (CMK) to use for encryption.

Answer: A

QUESTION 399
A company wants to share forensic accounting data is stored in an Amazon RDS DB instance with an external auditor. The Auditor has its own AWS account and requires its own copy of the database.

How should the company securely share the database with the auditor?

A. Create a read replica of the database and configure IAM standard database authentication to grant the auditor access.
B. Copy a snapshot of the database to Amazon S3 and assign an IAM role to the auditor to grant access to the object in that bucket.
C. Export the database contents to text files, store the files in Amazon S3, and create a new IAM user for the auditor with access to that bucket.
D. Make an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key.

Answer: C

QUESTION 400
A company is experiencing growth as demand for its product has increased The company's existing purchasing application is slow when traffic spikes The application is a monolithic three tier application that uses synchronous transactions and sometimes sees bottlenecks in the application tier A solutions architect needs to design a solution that can meet required application response times while accounting for traffic volume spikes.

Which solution will meet these requirements?

A. Vertically scale the application instance using a larger Amazon EC2 instance size.

B. Scale the application's persistence layer horizontally by introducing Oracle RAC on AWS
C. Scale the web and application tiers horizontally using Auto Scaling groups and an Application Load Balancer
D. Decouple the application and data tiers using Amazon Simple Queue Service (Amazon SQS) with asynchronous AWS Lambda calls.

Answer: A

QUESTION 401
A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.

What should a solutions architect recommend to meet these requirements?

A. Store the transactions data into Amazon DynamoDB.
Set up a rule in DynamoDB to remove sensitive data from every transaction upon write.
Use DynamoDB Streams to share the transactions data with other applications.
B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3.
Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data.
Other applications can consume the data stored in Amazon S3.
C. Stream the transactions data into Amazon Kinesis Data Streams.
Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB.
Other applications can consume the transactions data off the Kinesis data stream.
D. Store the batched transactions data in Amazon S3 as files.
Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3.
The Lambda function then stores the data in Amazon DynamoDB.
Other applications can consume transaction files stored in Amazon S3.

Answer: B

QUESTION 402
A solutions architect is creating a new VPC design. There are two public subnet for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web serves use only HTTPS. The solutions architect has already created a security group for the load Balancer allowing port 443 from 0.0 0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.
Which additional configuration strategy should the solution architect use to meet these requirements?

A. Create a security group far the web servers and allow port 443 from 0.0.0.0/0.
Create a security group tor the MySQL serve's aid allow port 3306 from the web servers security group.
B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0.
Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group
C. Create a security group for the web servers and allow port 443 from the load balancer.

Create a security group tor the MySQL servers and allow port 3306 from the web sewers security group

D. Create a network ACL for the web servers and allow port 443 from the web balancer.
Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

Answer: C

QUESTION 403
A company runs an application on an Amazon EC2 instance Backed by Amazon Elastic Block Store (Amazon EBS).
The instance needs to be available for 12 hours daily.
The company wants to save costs by making the instance unavailable outside the window required for the application.
However the contents of the instance's memory must be preserved whenever the instance is unavailable.
What should a solutions architect do lo meet this requirement?

A. Stop the instance outside the application's availability window.
Start up the Instance again when required.
B. Hibernate tie instance outside the application's availability window.
Start up the instance again when required.
C. Use Auto Scaling to scale down the instance outside the application's availability window.
Scale up the instance when required.
D. Terminate the instance outside the application's availability window.
Launch the instance by using a preconfigured Amazon Machine Image (AMI) when required.

Answer: B

QUESTION 404
A company Is migrating lo the AWS Cloud. A file server is the first workload to migrate.
Users must be able to access the file share using the Server Message Block (SMB) protocol.
Which AWS managed service meets these requirements"

A. Amazon EBS
B. Amazon EC2
C. Amazon FSx
D. Amazon S3

Answer: B

QUESTION 405
A solutions architect needs to design a resilient solution for Windows users' home directories.
The solution must provide fault tolerance, file-level backup and recovery, and access control, based upon the company's Active Directory.
Which storage solution meets these requirements?

A. Configure Amazon S3 to store the users' home directories.
Join Amazon S3 to Active Directory.
B. Configure a Multi-AZ file system with Amazon FSx for Windows File Server.
Join Amazon FSx to Active Directory.

C. Configure Amazon Elastic File System (Amazon EFS) for the users' home directories. Configure AWS Single Sign-On with Active Directory.
D. Configure Amazon Elastic Block Store (Amazon EBS) to store the users' home directories. Configure AWS Single Sign-On with Active Directory.

Answer: A

QUESTION 406
A company has a legacy application that processes data in two parts.
The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently.
How should a solutions architect integrate the microservices?

A. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2
B. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code In microservice 2 to subscribe to this topic.
C. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose.
D. Implement code in microservice 1 to send data to an Amazon SOS queue. Implement code in microservice 2 to process messages from the queue.

Answer: A

QUESTION 407
A company hosts its application using Amazon Elastic Container Service (Amazon ECS) and wants to ensure high availability.
The company wants to be able (o deploy updates to its application even if nodes in one Availability Zone are not accessible.
The expected request volume for the application is 100 requests per second, and each container task is able to serve at least 60 requests pet second.
The company set up Amazon ECS with a rolling update deployment type with the minimum healthy percent parameter set to 50% and the maximum percent set lo 100%.
Which configuration of tasks and Availability Zones meets these requirements?

A. Deploy the application across two Availability Zones, with one task in each Availability Zone
B. Deploy the application across two Availability Zones, with two tasks in each Availability Zone.
C. Deploy the application across three Availability Zones, with one task in each Availability Zone.
D. Deploy the application across three Availability Zones, with two tasks in each Availability Zone.

Answer: A

QUESTION 408
A web application runs on Amazon EC2 instances behind an Application Load Balancer.
The application allows users to create custom reports of historical weather data.
Generating a report can take up to 5 minutes.
These long-running requests use many of the available incoming connections, making the system unresponsive to other users.
How can a solutions architect make the system more responsive?

A. Use Amazon SOS with AWS Lambda to generate reports.

B. Increase the Idle timeout on the Application Load Balancer to 5 minutes.
C. Update the client-side application code to increase its request timeout to 5 minutes.
D. Publish the reports to Amazon S3 and use Amazon CloudFront for downloading lo the user.

Answer: A

QUESTION 409
A company is planning to use Amazon S3 to store images uploaded by its users.
The images must be encrypted at rest in Amazon S3.
The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.
What should a solutions architect use to accomplish this?

A. Server-Side Encryption with keys stored in an S3 bucket
B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Answer: D

QUESTION 410
A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer.
Based on the application's history, the company anticipates a spike in traffic during a holiday each year.
A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity lo minimize any performance impact on application users.
Which solution will meet these requirements?

A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.
B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.
C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.
D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there ate autoscaling:EC2_INSTANCE_LAUNCH events.

Answer: B

QUESTION 411
A website runs a web application that receives a burst of traffic each day at noon.
The users upload new pictures and content daily, but have been complaining of timeouts.
The architecture uses Amazon EC2 Auto Seating groups, and the custom application consistently takes 1 minute to initiate upon boot up before responding to user requests
How should a solutions architect redesign the architecture to better respond to changing traffic?

A. Configure a Network Load Balancer with a slow start configuration.
B. Configure AWS ElastiCache for Redis to offload direct requests to the servers
C. Configure an Auto Scaling step scaling policy with an instance warmup condition.

D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

Answer: B

QUESTION 412
A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning.
This application runs on AWS Fargate. and the connected storage needs to have concurrent access to files and deliver high performance.
Which storage option should the solutions architect recommend?

A. Create an Amazon S3 bucket for the application and establish an 1AM role for Fargate to communicate with Amazon S3.
B. Create an Amazon FSx for Lustre file share and establish an 1AM role that allows Fargate to communicate with FSx for Lustre
C. Create an Amazon Elastic File System (Amazon EFS> file share and establish an 1AM role that allows Fargate to communicate with Amazon EFS.
D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an 1AM role that allows Fargate to communicate with Amazon EBS.

Answer: B

QUESTION 413
A company Is launching an ecommerce website on AWS.
This website is built with a three-tier architecture that includes a MySQL database.
In a Multi-AZ deployment of Amazon Aurora MySQL.
The website application must be highly available and will initially be launched in an AWS Region with three Availability Zones.
The application produces a metric that describes the load the application experiences.
Which solution meets these requirements?

A. Configure an Application Load Balancer (ALB(with Amazon EC2 Auto Scaling behind the ALB with scheduled scaling
B. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a simple scaling policy.
C. Configure a Network Load Balancer (NLB) and launch a Spot Fleet with Amazon EC2 Auto Scaling behind the NL8.
D. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a target tracking scaling policy.

Answer: B

QUESTION 414
A company Is designing an internet-facing web application. The application runs on Amazon EC2 for Linux-based instances that store sensitive user data in Amazon RDS MySQL Multi-AZ DB instances.
The EC2 instances are in public subnets, and the RDS DB instances are in private subnets.
The security team has mandated that the DB instances be secured against web-based attacks.
What should a solutions architect recommend?

A. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load

Balancer.
Configure the EC2 instance iptables rules to drop suspicious web traffic.
Create a security group for the DB instances.
Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.

B. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer.
Move DB instances to the same subnets that EC2 instances are located in.
Create a security group for the DB instances.
Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.

C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer.
Use AWS WAF to monitor inbound web traffic for threats.
Create a security group for the web application servers and a security group for the DB instances.
Configure the RDS security group to only allow port 3306 inbound from the web application server security group.

D. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer.
Use AWS WAF to monitor inbound web traffic for threats.
Configure the Auto Scaling group lo automatically create new DB instances under heavy traffic.
Create a security group for the RDS DB instances. Configure the RDS security group to only allow port 3306 inbound.

Answer: D

QUESTION 415
A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs 3 solution with low latency and high availability.
What should a solutions architect do to accomplish this?

A. Provision EC2 instances in us-west-1.
Switch me Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.

B. Provision EC2 instances and an Application Load Balancer in us-west-1.
Make the load balancer distribute the traffic based on the location of the request

C. Provision EC2 instances and configure an Application Load Balancer in us-west-1.
Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.

D. Provision EC2 Instances and configure an Application Load Balancer in us-wesl-1.
Configure Amazon Route 53 with a weighted routing policy.
Create alias records in Route 53 that point to the Application Load Balancer

Answer: C
Explanation:
https://aws.amazon.com/global-accelerator/faqs/

QUESTION 416
A company has a custom application running on an Amazon EC2 instance that:

- Reads a large amount of data from Amazon S3

```
- Performs a multi-stage analysis.
- Writes the results to Amazon DynamoDB.
```

The application writes a significant number of large, temporary files during the multi-stage analysis.
The process performance depends on the temporary storage performance.
What would be the fastest storage option for holding the temporary files?

A. Multiple Amazon S3 buckets with Transfer Acceleration for storage
B. Multiple Amazon EBS drives with Provisioned IOPS and EBS optimization.
C. Multiple Amazon EFS volumes using the Network File System version 4.1 (NFSv4.1) protocol.
D. Multiple instance store volumes with software RAID 0

Answer: D

QUESTION 417
A company built a food ordering application that captures user data and stores it for future analysis.
The application's static front end is deployed on an Amazon EC? instance.
The front-end application sends the requests to the backend application running on separate EC2 instance.
The backend application then stores the data in Amazon RDS.
What should a solutions architect do to decouple the architecture and make it scalable?

A. Use Amazon S3 to serve the front-end application, which sends requests to Amazon EC2 to execute the backend application.
   The backend application will process and store the data in Amazon RDS.
B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic.
   Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint o(the topic, and process and store the data in Amazon RDS.
C. Use an EC2 instance lo serve the front end and write requests to an Amazon SOS queue.
   Place the backend Instance in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.
D. Use Amazon S3 to serve the static front-end application and send requests lo Amazon API Gateway which writes the requests to an Amazon SQS queue.
   Place the backend instances in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.

Answer: D

QUESTION 418
A company has an on-premises application that collects data and stores it to an on-premises NFS server.
The company recently set up a 10 Gbps AWS Direct Connect connection.
The company is running out of storage capacity on premises.
The company needs to migrate the application data from on premises to the AWS Cloud while maintaining low-latency access to the data from the on- premises application.
What should a solutions architect do to meet these requirements?

A. Deploy AWS Storage Gateway for the application data, and use the file gateway to store the data in Amazon S3.

Connect the on-premises application servers to the file gateway using NFS.

B. Attach an Amazon Elastic File System (Amazon EFS) file system to the NFS server, and copy the application data to the EFS file system.
Then connect the on-premises application to Amazon EFS.

C. Configure AWS Storage Gateway as a volume gateway.
Make the application data available to the on-premises application from the NFS server and with Amazon Elastic Block Store (Amazon EBS) snapshots.

D. Create an AWS DataSync agent with the NFS server as the source location and an Amazon Elastic File System (Amazon EFS) file system as the destination for application data transfer.
Connect the on- premises application to the EFS file system.

Answer: A

QUESTION 419
A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud.
The company uses tiered storage on-premises with hoi high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running.
Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO)

A. Amazon S3 for cold data storage
B. Amazon EFS for cold data storage
C. Amazon S3 for high-performance parallel storage
D. Amazon FSx for clustre tor high-performance parallel storage
E. Amazon FSx for Windows for high-performance parallel storage

Answer: AD
Explanation:
https://aws.amazon.com/fsx/lustre/
Amazon FSx for Lustre makes it easy and cost effective to launch and run the world's most popular high-performance file system. Use it for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.

QUESTION 420
A software vendor is deploying a new software-as-a-service (SaaS) solution that will be utilized by many AWS users.
The service is hosted in a VPC behind a Network Load Balancer.
The software vendor wants to provide access to this service to users with the least amount of administrative overhead and without exposing the service to the public internet.
What should a solutions architect do to accomplish this goal?

A. Create a peering VPC connection from each user's VPC to the software vendor s VPC.
B. Deploy a transit VPC in the software vendor's AWS account.
Create a VPN connection with each user account
C. Connect the service in the VPC with an AWS PrivateLink endpoint.
Have users subscribe to the endpoint.
D. Deploy a transit VPC in the software vendor's AWS account.
Create an AWS Direct Connect connection with each user account.

Answer: C

QUESTION 421
A company uses Amazon S3 to store its confidential audit documents.
The S3 bucket uses bucket policies to restrict access to audit team 1AM user credentials according to the principle of least privilege.
Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.
What should a solutions architect do to secure the audit documents?

A. Enable the versioning and MFA Delete features on the S3 bucket
B. Enable multi-factor authentication (MFA) on the 1AM user credentials for each audit team 1AM user account.
C. Add an S3 Lifecycle policy to the audit team's 1AM user accounts to deny the s3:DeleteOb|ect action during audit dates.
D. Use AWS Key Management Service (AWS KMS> to encrypt the S3 bucket and restrict audit team 1AM user accounts from accessing the KMS key.

Answer: A

QUESTION 422
A solutions architect is helping a developer design a new ecommerce shopping cart application using AWS services.
The developer is unsure of the current database schema and expects to make changes as the ecommerce site grows.
The solution needs to be highly resilient and capable of automatically scaling read and write capacity.
Which database solution meets these requirements?

A. Amazon Aurora PostgreSQL
B. Amazon DynamoDB with on-demand enabled
C. Amazon DynamoDB with DynamoDB Streams enabled
D. Amazon SQS and Amazon Aurora PostgreSQL

Answer: B

QUESTION 423
A company Is seeing access requests by some suspicious IP addresses.
The security team discovers the requests are horn different IP addresses under the same CIDR range.
What should a solutions architect recommend to the team?

A. Add a rule in the inbound table of the security group to deny the traffic from that CIDR range.
B. Add a rule In the outbound table of the security group to deny the traffic from that CIDR range
C. Add a deny rule in the Inbound table of the network ACL with a lower rule number than other rules.
D. Add a deny rule in the outbound table of the network ACL with a tower rule number than other rules.

Answer: C

QUESTION 424

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 fife gateway to provide file storage to AWS.
Then perform analytics on the data in the AWS Cloud.
B. 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.
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 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.

Answer: C
Explanation:
https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

QUESTION 425
A solutions architect is designing a solution that requires frequent updates to a website that is hosted on Amazon S3 with versioning enabled.
For compliance reasons, older versions of the objects will not be accessed frequently and will need to be deleted after 2 years.
What should the solutions architect recommend to meet these requirements at the LOWEST cost?

A. Use S3 batch operations to replace object tags.
Expire the objects based on the modified tags
B. Configure an S3 Lifecycle policy to transition older versions of objects to S3 Glacier.
Expire the objects after 2 years
C. Enable S3 Event Notifications on the bucket that sends older objects to the Amazon Simple Queue Service (Amazon SOS) queue for further processing.
D. Replicate older object versions to a new bucket.
Use an S3 Lifecycle policy to expire the objects In the new bucket after 2 years

Answer: B

QUESTION 426
A company receives 10 TB of instrumentation data each day from several machines located at a single factory.
The data consists of JSON files stored on a storage area network (SAN) in an on- premises data center located within the factory.
The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-lime analytics.
A secure transfer is important because the data is considered sensitive.
Which solution offers the MOST reliable data transfer?

A. AWS DataSync over public internet
B. AWS DataSync over AWS Direct Connect
C. AWS Database Migration Service (AWS DMS) over public internet
D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Answer: D

QUESTION 427
A company's web application is running on Amazon EC2 instances behind an Application Load Balancer.
The company recently changed its policy, which now requires the application to be accessed from one specific country only.
Which configuration will meet this requirement?

A. Configure the security group for the EC2 instances.
B. Configure the security group on the Application Load Balancer.
C. Configure AWS WAF on the Application Load Balancer in a VPC.
D. Configure the network ACL for the subnet that contains the EC2 instances.

Answer: C
Explanation:
https://aws.amazon.com/es/blogs/security/how-to-use-aws-waf-to-filter-incoming-traffic-from-embargoed-countries/

QUESTION 428
A leasing company generates and emails POF statements every month for all its customers. Each statement is about 400 KB in size. Customers can download their statements from the website for up to 30 days from when the statements were generated.
At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements.
What is the MOST cost-effective storage solution for this situation?

A. Store the statements using the Amazon S3 Standard storage class.
Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.
B. Store the statements using the Amazon S3 Glacier storage class.
Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.
C. Store the statements using the Amazon S3 Standard storage class.
Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.
D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class.
Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

Answer: B

QUESTION 429
A company is using a third-party vendor to manage its marketplace analytics.
The vendor needs limited programmatic access to resources in the company's account.
All the needed policies have been created to grant appropriate access.
Which additional component will provide the vendor with the MOST secure access to the account?

A. Create an 1AM user.
B. Implement a service control policy (SCP)

C. Use a cross-account role with an external ID.
D. Configure a single sign-on (SSO) identity provider.

Answer: C

QUESTION 430
A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month.
Each application has approximately 50 TB of data to be transferred After the migration ts complete this company and its parent company will Doth require secure network connectivity with consistent throughput from their data centers to the applications.
A solutions architect must ensure one-time data migration and ongoing network connectivity.
Which solution will meet these requirements?

A. AWS Direct Connect for both the initial transfer and ongoing connectivity.
B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity.
C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity.
D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity.

Answer: C

QUESTION 431
A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks.
The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch.
However, the company wants to reduce costs when utilization decreases.
What should a solutions architect recommend?

A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

Answer: D

QUESTION 432
A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage.
The chief information security officer has directed that no application traffic between the two services should traverse the public internet.
Which capability should the solutions architect use to meet the compliance requirements?

A. AWS Key Management Service (AWS KMS))
B. VPC endpoint
C. Private subnet
D. Virtual private gateway

Answer: A

QUESTION 433
A solutions architect must design a database solution for a high-traffic ecommerce web application.
The database stores customer profiles and shopping cart information.
The database must support a peak load of several million requests each second and deliver responses in milliseconds.
The operational overhead for managing and scaling the database must be minimized.
Which database solution should the solutions architect recommend?

A. Amazon Aurora
B. Amazon DynamoDB
C. Amazon RDS
D. Amazon Redshift

Answer: A

QUESTION 434
A company stores 200 GB of data each month in Amazon S3.
The company needs to perform analytics on this data at the end of each month to determine the number of items sold in each sales region for the previous month.
Which analytics strategy is MOST cost-effective for the company to use?

A. Create an Amazon Elasticsearch Service (Amazon ES) cluster.
Query the data in Amazon ES.
Visualize the data by using Kibana.
B. Create a table in the AWS Glue Data Catalog.
Query the data in Amazon S3 by using Amazon Athena.
Visualize the data in Amazon QuickSight
C. Create an Amazon EMR cluster.
Query the data by using Amazon EMR, and store the results in Amazon S3.
Visualize the data in Amazon QuickSight.
D. Create an Amazon Redshift cluster.
Query the data in Amazon Redshift, and upload the results to Amazon S3.
Visualize the data in Amazon QuickSight.

Answer: A

QUESTION 435
A company wants a storage option that enables its data science team to analyze its data on premises and in the AWS Cloud.
The team needs to be able to run statistical analyses by using the data on premises and by using a fleet of Amazon EC2 instances across multiple Availability Zones.
What should a solutions architect do to meet these requirements?

A. Use an AWS Storage Gateway tape gateway to copy the on-premises files into Amazon S3.
B. Use an AWS Storage Gateway volume gateway to copy the on-premises files into Amazon S3.
C. Use an AWS Storage Gateway file gateway to copy the on-premises files to Amazon Elastic Block Store (Amazon EBS).
D. Attach an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers.

Copy the files to Amazon EFS.

Answer: C

QUESTION 436
A company is planning on deploying a newly built application on AWS in a default VPC The application will consist of a web layer and database layer.
The web server was created in public subnets, and the MySQL database was created in private subnets. All subnets are created with the default network ACL settings, and the default security group in the VPC will be replaced with new custom security groups.
The following are the key requirements:

- The web servers must be accessible only to users on an SSL connection.
- The database should be accessible to the web layer, which is created in a public subnet only.
- All traffic to and from the IP range 182.20.0.0/16 subnet should be blocked.

Which combination of steps meets these requirements? (Select TWO.)

A. Create a database server security group with inbound and outbound rules for MySQL port 3306 traffic to and from anywhere (0 0.0.0/0)
B. Create a database server security group with an inbound rule for MySQL port 3306 and specify the source as a web server security group.
C. Create a web server security group with an inbound allow rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0) and an inbound deny rule for IP range 182.20.0 0/16.
D. Create a web server security group with an inbound rule for HTTPS port 443 traffic from anywhere (0.0 0 0/0).
Create network ACL inbound and outbound deny rules for IP range 182 20.00/16
E. Create a web server security group with inbound and outbound rules for HTTPS port 443 traffic to and from anywhere (0.0.0.0/0).
Create a network ACL inbound deny rule for IP range 182.20.0.0/16.

Answer: BD

QUESTION 437
A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for 1AM user passwords.
What should the solutions architect do to accomplish this?

A. Set an overall password policy for the entire AWS account
B. Set a password policy for each 1AM user in the AWS account.
C. Use third-party vendor software to set password requirements,
D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

Answer: A

QUESTION 438
The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        },
        {
            "Sid": "2",
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}
```

What are the effective IAM permissions of this policy for group members?

A. Group members are permitted any Amazon EC2 action within the uss-east-1 Region. Statements after The Allow permission are not applied
B. Group member are denied any Amazon EC2 permissions in the us-east-1 Region unless they are tagged in with multi-factor authentication (MFA).
C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members authorized any other Amazon EC2 action.
D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Groups are permitted any other Amazon EC2 action within the us-east-1 Region

Answer: D

QUESTION 439
A new employee has joined a company as a deployment engineer.
The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources.
A solutions architect wants the deployment engineer to perform job activities. While following the principle of least privilege.
Which combination of actions should the solutions architect take to accomplish this goal? (Select TWO.)

A. Have the deployment engineer use AWS account roof user credentials for performing AWS CloudFormation stack operations.
B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached
C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the

Administrate/Access IAM policy attached

D. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only
E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using Dial IAM role.

Answer: AE

QUESTION 440
A solutions architect is working on optimizing a legacy document management application running on Microsoft a network file share.
The chief information officer wants to reduce the on-premises data center footprint and minimize storage by moving on-premises storage to AWS.
What should the solution architect do to meet these requirements?

A. Sat up an AWS Storage Gateway file gateway.
B. Set up Amazon Elastic File System (Amazon EFS).
C. Set up AWS Storage Gateway as a volume gateway.
D. Set up an Amazon Elastic Block Store (Amazon EBS) volume.

Answer: A

QUESTION 441
A company is moving Its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables.
The applications need to be migrated one by one with a month in between each migration Management has expressed concerns that the database has a high number of reads and writes.
The data must be kept in sync across both databases throughout tie migration.
What should a solutions architect recommend?

A. Use AWS DataSync tor the initial migration.
Use AWS Database Migration Service (AWS DMS] to create a change data capture (CDC) replication task and a table mapping to select all cables.
B. UseAVVS DataSync for the initial migration.
Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select ail tables.
C. Use the AWS Schema Conversion led with AWS DataBase Migration Service (AWS DMS) using a memory optimized replication instance.
Create a tui load plus change data capture (CDC) replication task and a table mapping lo select all tables.
D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized implication instance.
Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Answer: B

QUESTION 442
A company wants to migrate its web application to AWS. The legacy web aoplication consists of a web tier, an appfccation tier, and a MySQL database.
The re-architectod application must consist of technologies that do not require the administration

team to manage instances or clusters.
Which combination of services should a solutions architect include in Ihe overall architecture? (Select TWO)

A. Amazon Aurora Serverless
B. Amazon EC2 Spot Instances
C. Amazon Elasticsearch Service (Amazon ES)
D. Amazon RDS for MySQL
E. AWS Fargate

Answer: DE

QUESTION 443
A company has multiple applications that use Amazon RDS lor MySQL as is database.
The company recently discovered that a new custom reporting application has Increased the number of Queries on the database.
This is slowing down performance.
How should a solutions architect resolve this issue with the LEAST amount of application changes?

A. Add a secondary DB instance using Multi-AZ
B. Set up a road replica ana Multi-AZ on Amazon RDS.
C. Set up a standby replica and Multi-AZ on Amazon RDS
D. Use caching on Amazon RDS to improve the overall performance

Answer: D

QUESTION 444
A company owns an asynchronous API that is used to ingest use requests and, based on the request type, dispatch requests to the appropriate microservice for processing.
The company is using Amazon API Gateway to deploy the API front end, and an AWS Lambda function that invokes Amazon DynamoDB to store user requests before dispatching them to the processing microservices.
The company provisioned as much DynamoDB throughput as its budget allows, but the company is still experiencing availability issues and is losing user requests.
What should a solutions architect do to address this Issue without impacting existing users?

A. Add throttling on the API Gateway with server-side throttling limits
B. Use DynamoDB Accelerator (DAX) and LamDda to buffer writes to DynamoDB
C. Create a secondary index in DynamoDB for the label with the user requests.
D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

Answer: B

QUESTION 445
A company is running a multi-tier ecommerce web application In the AWS Cloud. The application runs on Amazon EC2 Instances with an Amazon RDS MySQL Mutt>AZ DB instance.
Amazon RDS is configured with the latest generation instance with 2,000 GB of storage in an Amazon EBS General Purpose SSD (gp2) volume.
The database performance impacts the application during periods of high demand.

After analyzing the logs in Amazon CloudWatch Logs, a database administrator finds that the application performance always degrades when the number of read and write IOPS is higher than 6.000
What should a solutions architect do to improve the application performance?

A. Replace the volume with a Magnetic volume
B. Increase the number of IOPS on the gp2 volume
C. Replace the volume with a Provisioned IOPS (PIOPS) volume.
D. Replace the 2,000 GB gp2 volume with two 1,000 GBgp2 volumes.

Answer: C