QUESTION 21
A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative. A solutions architect needs to share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account. The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses a customer managed customer master key (CMK) to encrypt EBS volume snapshots.
What is the MOST secure way for the solutions architect to share the AMI with the MSP Partner's AWS account?

A. Make the encrypted AMI and snapshots publicly available.
Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key
B. Modify the launchPermission property of the AMI.
Share the AMI with the MSP Partner's AWS account only.
Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key.
C. Modify the launchPermission property of the AMI.
Share the AMI with the MSP Partner's AWS account only.
Modify the CMK's key policy to trust a new CMK that is owned by the MSP Partner for encryption.
D. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account.
Encrypt the S3 bucket with a CMK that is owned by the MSP Partner.
Copy and launch the AMI in the MSP Partner's AWS account.

Answer: B

QUESTION 22
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:
"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"
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

QUESTION 23
A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificate that are imported into AWS Certificate Manager (ACM). The company's security team must be notified 30 days before the expiration of each certificate.
What should a solutions architect recommend to meet the requirement?

A. Add a rule m ACM to publish a custom message to an Amazon Simple Notification Service (Amazon SNS) topic every day beginning 30 days before any certificate will expire.
B. Create an AWS Config rule that checks for certificates that will expire within 30 days.
Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a noncompliant resource
C. Use AWS trusted Advisor to check for certificates that will expire within to days.
Create an Amazon CloudWatch alarm that is based on Trusted Advisor metrics for check status changes.
Configure the alarm to send a custom alert by way of Amazon Simple rectification Service (Amazon SNS)
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days.
Configure the rule to invoke an AWS Lambda function.
Configure the Lambda function to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).

Answer: B
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/

QUESTION 24
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 geo-proximity routing policy pointing to on-premises servers.

Answer: C
Explanation:
https://aws.amazon.com/pt/blogs/aws/amazon-cloudfront-support-for-custom-origins/
You can now create a CloudFront distribution using a custom origin. Each distribution will can point to an S3 or to a custom origin. This could be another storage service, or it could be something more interesting and more dynamic, such as an EC2 instance or even an Elastic Load Balancer

QUESTION 25
A company wants to reduce the cost of its existing three-tier web architecture. The web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours.
The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use.
Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?

A. Use Spot Instances for the production EC2 instances.
Use Reserved Instances for the development and test EC2 instances.
B. Use Reserved Instances for the production EC2 instances.
Use On-Demand Instances for the development and test EC2 instances.
C. Use Spot blocks for the production EC2 instances.
Use Reserved Instances for the development and test EC2 instances.
D. Use On-Demand Instances for the production EC2 instances.
Use Spot blocks for the development and test EC2 instances.

Answer: B

QUESTION 26
A company has a production web application in which users upload documents through a web interlace or a mobile app.
According to a new regulatory requirement, new documents cannot be modified or deleted after they are stored.
What should a solutions architect do to meet this requirement?

A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled
B. Store the uploaded documents in an Amazon S3 bucket.
Configure an S3 Lifecycle policy to archive the documents periodically.
C. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled.
Configure an ACL to restrict all access to read-only.
D. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume.
Access the data by mounting the volume in read-only mode.

Answer: A
Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html

QUESTION 27
A company has several web servers that need to frequently access a common Amazon RDS MySQL Multi-AZ DB

instance. The company wants a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently.
Which solution meets these requirements?

A. Store the database user credentials in AWS Secrets Manager.
Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.
B. Store the database user credentials in AWS Systems Manager OpsCenter.
Grant the necessary IAM permissions to allow the web servers to access OpsCenter.
C. Store the database user credentials in a secure Amazon S3 bucket.
Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database.
D. Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system. The web server should be able to decrypt the files and access the database.

Answer: A
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://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

QUESTION 28
A company hosts an application on AWS Lambda functions mat are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data Is not recorded for some of the event.
A solutions architect needs to design a solution that stores customer data that is created during database upgrades.
Which solution will meet these requirements?

A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database.
Configure the Lambda functions to connect to the RDS proxy.
B. Increase the run time of me Lambda functions to the maximum.
Create a retry mechanism in the code that stores the customer data in the database.
C. Persist the customer data to Lambda local storage.
Configure new Lambda functions to scan the local storage to save the customer data to the database.
D. Store the customer data m an Amazon Simple Queue Service (Amazon SOS) FIFO queue.
Create a new Lambda function that polls the queue and stores the customer data in the database.

Answer: D
Explanation:
https://www.learnaws.org/2020/12/13/aws-rds-proxy-deep-dive/
RDS proxy can improve application availability in such a situation by waiting for the new database instance to be functional and maintaining any requests received from the application during this time. The end result is that the application is more resilient to issues with the underlying database. This will enable solution to hold data till the time DB comes back to normal. RDS proxy is to optimally utilize the connection between Lambda and DB. Lambda can open multiple connection concurrently which can be taxing on DB compute resources, hence RDS proxy was introduced to manage and leverage these connections efficiently.

QUESTION 29
A survey company has gathered data for several years from areas m\ the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB m size and growing. The company has started to share the data with a European marketing firm that has S3 buckets. The company wants to ensure that its data transfer costs remain as low as possible.

Which solution will meet these requirements?

A. Configure the Requester Pays feature on the company's S3 bucket
B. Configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.
C. Configure cross-account access for the marketing firm so that the marketing firm has access to the company's S3 bucket.
D. Configure the company's S3 bucket to use S3 Intelligent-Tiering Sync the S3 bucket to one of the marketing firm's S3 buckets

Answer: A

QUESTION 30
A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM 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 IAM user credentials for each audit team IAM user account.
C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.
D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Answer: A

QUESTION 31
A company is using a SQL database to store movie data that is publicly accessible. The database runs on an Amazon RDS Single-AZ DB instance. A script runs queries at random intervals each day to record the number of new movies that have been added to the database. The script must report a final total during business hours. The company's development team notices that the database performance is inadequate for development tasks when the script is running. A solutions architect must recommend a solution to resolve this issue.
Which solution will meet this requirement with the LEAST operational overhead?

A. Modify the DB instance to be a Multi-AZ deployment
B. Create a read replica of the database.
Configure the script to query only the read replica.
C. Instruct the development team to manually export the entries in the database at the end of each day
D. Use Amazon ElastiCache to cache the common queries that the script runs against the database

Answer: D

QUESTION 32
A company has applications that run on Amazon EC2 instances in a VPC. One of the applications needs to call the Amazon S3 API to store and read objects. According to the company's security regulations, no traffic from the applications is allowed to travel across the internet.
Which solution will meet these requirements?

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: A
Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3

QUESTION 33
A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Ama2on EC2 instances inside a VPC.
Which combination of steps should a solutions architect take to accomplish this? (Select TWO.)

A. Configure a VPC gateway endpoint for Amazon S3 within the VPC
B. Create a bucket policy to make the objects to the S3 bucket public
C. Create a bucket policy that limits access to only the application tier running in the VPC
D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance
E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket

Answer: AC
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/s3-private-connection-no-authentication/

QUESTION 34
A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to Increase the application's elasticity and availability. The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours the company's development team pulls a full export of the production database to populate a database in the staging environment. During this period, users experience unacceptable application latency. The development team is unable to use the staging environment until the procedure completes.
A solutions architect must recommend replacement architecture that alleviates the application latency issue.
The replacement architecture also must give the development team the ability to continue using the staging environment without delay.
Which solution meets these requirements?

A. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production.
Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.
B. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production.
Use database cloning to create the staging database on-demand
C. Use Amazon RDS for MySQL with a Mufti AZ deployment and read replicas for production.
Use the standby instance tor the staging database.
D. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production.
Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

Answer: B

QUESTION 35
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 tor auditing purposes. Keys must be rotated every year.
Which solution meets these requirements and the MOST operationally efferent?

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

automate rotation

Answer: D
Explanation:
https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html
When you enable automatic key rotation for a customer managed key, AWS KMS generates new cryptographic material for the KMS key every year. AWS KMS also saves the KMS key's older cryptographic material in perpetuity so it can be used to decrypt data that the KMS key encrypted.
Key rotation in AWS KMS is a cryptographic best practice that is designed to be transparent and easy to use. AWS KMS supports optional automatic key rotation only for customer managed CMKs. Enable and disable key rotation. Automatic key rotation is disabled by default on customer managed CMKs.
When you enable (or re-enable) key rotation, AWS KMS automatically rotates the CMK 365 days after the enable date and every 365 days thereafter.

QUESTION 36
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: D
Explanation:
https://aws.amazon.com/solutions/implementations/aws-streaming-data-solution-for-amazon-kinesis/

QUESTION 37
A company has an automobile sales website that stores its listings in a 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: D
Explanation:
https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html
https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html

QUESTION 38
A company needs to store data in Amazon S3 and must prevent the data from being changed. The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the

company decides to modify the objects.
Only specific users in the company's AWS account can have the ability to delete the objects.
What should a solutions architect do to meet these requirements?

A. Create an S3 Glacier vault Apply a write-once, read-many (WORM) vault lock policy to the objects.
B. Create an S3 bucket with S3 Object Lock enabled Enable versioning.
Set a retention period of 100 years.
Use governance mode as the S3 bucket's default retention mode for new objects.
C. Create an S3 bucket.
Use AWS CloudTrail to track any S3 API events that modify the objects.
Upon notification, restore the modified objects from any backup versions that the company has.
D. Create an S3 bucket with S3 Object Lock enabled.
Enable versioning.
Add a legal hold to the objects.
Add the s3:PutObjectLegalHold permission to the IAM policies of users who need to delete the objects.

Answer: D

QUESTION 39
A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3.
Users are experiencing slow upload requests to the website.
The company needs to reduce coupling within the application and improve website performance.
A solutions architect must design the most operationally efficient process for image uploads.
Which combination of actions should the solutions architect take to meet these requirements? (Choose two.)

A. Configure the application to upload images to S3 Glacier.
B. Configure the web server to upload the original images to Amazon S3.
C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL.
D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded.
Use the function to resize the image
E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

Answer: BD

QUESTION 40
A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database funning on Amazon EC2. The company wants this application to be highly available with tow operational complexity Which architecture otters the HGHEST availability?

A. Add a second ActiveMQ server to another Availably Zone.
Add an additional consumer EC2 instance in another Availability Zone.
Replicate the MySQL database to another Availability Zone.
B. Use Amazon MO with active/standby brokers configured across two Availability Zones.
Add an additional consumer EC2 instance in another Availability Zone.
Replicate the MySQL database to another Availability Zone.
C. Use Amazon MO with active/standby blotters configured across two Availability Zones.
Add an additional consumer EC2 instance in another Availability Zone.
Use Amazon ROS tor MySQL with Multi-AZ enabled.

D. Use Amazon MQ with active/standby brokers configured across two Availability Zones.d
Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones.
Use Amazon RDS for MySQL with Multi-AZ enabled.

Answer: D

QUESTION 41
A company hosts a containerized web application on a fleet of on-premises servers that process incoming requests. The number of requests is growing quickly. The on-premises servers cannot handle the increased number of requests. The company wants to move the application to AWS with minimum code changes and minimum development effort. Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling.
Use an Application Load Balancer to distribute the incoming requests.
B. Use two Amazon EC2 instances to host the containerized web application.
Use an Application Load Balancer to distribute the incoming requests.
C. Use AWS Lambda with a new code that uses one of the supported languages.
Create multiple Lambda functions to support the load.
Use Amazon API Gateway as an entry point to the Lambda functions.
D. Use a high performance computing (HPC) solution such as AWS ParallelClusterto establish an HPC cluster that can process the incoming requests at the appropriate scale.

Answer: A