Lead2Pass.com

First Test, First Pass!

http://www.lead2pass.com

LEAD2PASS

First Test, First Pass!

Vendor: Amazon

Exam Code: SAA-C03

Exam Name: AWS Certified Solutions Architect - Associate (SAA-C03) Exam

Version: 23.041

Important Notice

Product

Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within 150 days 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 suggestions, please feel free to contact us at support@lead2pass.com

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 technology@lead2pass.com and our technical experts will provide support in 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently.

If anyone who share the file we will disable the free update and account access.

Any unauthorized changes will be inflicted legal punishment. We will reserve the right of final explanation for this statement.

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

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

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

QUESTION 1
A company has a website hosted on AWS The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS.
What should a solutions architect do to meet this requirement?

A. Update the ALB's network ACL to accept only HTTPS traffic
B. Create a rule that replaces the HTTP in the URL with HTTPS.
C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

Answer: C
Explanation:
To redirect HTTP traffic to HTTPS, a solutions architect should create a listener rule on the ALB to redirect HTTP traffic to HTTPS. Option A is not correct because network ACLs do not have the ability to redirect traffic. Option B is not correct because it does not redirect traffic, it only replaces the URL. Option D is not correct because a Network Load Balancer does not have the ability to handle HTTPS traffic.
https://docs.aws.amazon.com/fr_fr/elasticloadbalancing/latest/application/create-https-listener.html
https://aws.amazon.com/fr/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/

QUESTION 2
A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis.

Which solution will meet these requirements with the LEAST operational overhead?

A. Store the database credentials in the instance metadata.
Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and instance metadata at the same time.
B. Store the database credentials in a configuration file in an encrypted Amazon S3 bucket.
Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and the credentials in the configuration file at the same time.
Use S3 Versioning to ensure the ability to fall back to previous values.
C. Store the database credentials as a secret in AWS Secrets Manager.
Turn on automatic rotation for the secret.
Attach the required permission to the EC2 role to grant access to the secret.
D. Store the database credentials as encrypted parameters in AWS Systems Manager Parameter Store.
Turn on automatic rotation for the encrypted parameters.
Attach the required permission to the EC2 role to grant access to the encrypted parameters.

Answer: C
Explanation:
Secrets manager supports Autorotation unlike Parameter store.
AWS Secrets Manager is a service that enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. By storing the database credentials as a secret in Secrets Manager, you can ensure that they are not

hardcoded in the application and that they are automatically rotated on a regular basis. To grant the EC2 instance access to the secret, you can attach the required permission to the EC2 role. This will allow the application to retrieve the secret from Secrets Manager as needed.
https://docs.aws.amazon.com/secretsmanager/latest/userguide/create_database_secret.html

QUESTION 3
A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB).
The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA).
The certificate must be rotated each year before the certificate expires.

What should a solutions architect do to meet these requirements?

A. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate.
Apply the certificate to the ALB.
Use the managed renewal feature to automatically rotate the certificate.
B. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate.
Import the key material from the certificate. Apply the certificate to the ALB.
Use the managed renewal feature to automatically rotate the certificate.
C. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root CA.
Apply the certificate to the ALB.
Use the managed renewal feature to automatically rotate the certificate.
D. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate.
Apply the certificate to the ALB.
Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration.
Rotate the certificate manually.

Answer: D
Explanation:
ACM does not manage the renewal process for imported certificates. You are responsible for monitoring the expiration date of your imported certificates and for renewing them before they expire.
Check this question on the link below:
Q: What types of certificates can I create and manage with ACM?
https://www.amazonaws.cn/en/certificate-manager/faqs/#Managed_renewal_and_deployment

QUESTION 4
A company runs its infrastructure on AWS and has a registered base of 700,000 users for its document management application. The company intends to create a product that converts large .pdf files to .jpg image files. The .pdf files average 5 MB in size. The company needs to store the original files and the converted files. A solutions architect must design a scalable solution to accommodate demand that will grow rapidly over time.
Which solution meets these requirements MOST cost-effectively?

A. Save the .pdf files to Amazon S3.
Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to .jpg format and store them back in Amazon S3.
B. Save the .pdf files to Amazon DynamoDUse the DynamoDB Streams feature to invoke an AWS Lambda function to convert the files to .jpg format and store them back in DynamoDB.

C. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic Block Store (Amazon EBS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the files to .jpg format. Save the .pdf files and the .jpg files in the EBS store.
D. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the file to .jpg format. Save the .pdf files and the .jpg files in the EBS store.

Answer: A
Explanation:
Elastic BeanStalk is expensive, and DocumentDB has a 400KB max to upload files. So Lambda and S3 should be the one.

QUESTION 5
A company has more than 5 TB of file data on Windows file servers that run on premises. Users and applications interact with the data each day.
The company is moving its Windows workloads to AWS. As the company continues this process, the company requires access to AWS and on-premises file storage with minimum latency. The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns. The company uses an AWS Site-to-Site VPN connection for connectivity to AWS.
What should a solutions architect do to meet these requirements?

A. Deploy and configure Amazon FSx for Windows File Server on AWS.
Move the on-premises file data to FSx for Windows File Server.
Reconfigure the workloads to use FSx for Windows File Server on AWS.
B. Deploy and configure an Amazon S3 File Gateway on premises.
Move the on-premises file data to the S3 File Gateway.
Reconfigure the on-premises workloads and the cloud workloads to use the S3 File Gateway
C. Deploy and configure an Amazon S3 File Gateway on premises.
Move the on-premises file data to Amazon S3.
Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway, depending on each workload's location.
D. Deploy and configure Amazon FSx for Windows File Server on AWS.
Deploy and configure an Amazon FSx File Gateway on premises.
Move the on-premises file data to the FSx File Gateway.
Configure the cloud workloads to use FSx for Windows File Server on AWS.
Configure the on-premises workloads to use the FSx File Gateway.

Answer: D
Explanation:
Amazon FSx File Gateway (FSx File Gateway) is a new File Gateway type that provides low latency and efficient access to in-cloud FSx for Windows File Server file shares from your on-premises facility. If you maintain on-premises file storage because of latency or bandwidth requirements, you can instead use FSx File Gateway for seamless access to fully managed, highly reliable, and virtually unlimited Windows file shares provided in the AWS Cloud by FSx for Windows File Server.
https://docs.aws.amazon.com/filegateway/latest/filefsxw/what-is-file-fsxw.html

QUESTION 6
A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda. The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG

format. The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports. Which solution will meet these requirements with the LEAST operational overhead?

A. Use existing Python libraries to extract the text from the reports and to identify the PHI from the extracted text.
B. Use Amazon Textract to extract the text from the reports.
Use Amazon SageMaker to identify the PHI from the extracted text.
C. Use Amazon Textract to extract the text from the reports.
Use Amazon Comprehend Medical to identify the PHI from the extracted text.
D. Use Amazon Rekognition to extract the text from the reports.
Use Amazon Comprehend Medical to identify the PHI from the extracted text.

Answer: C
Explanation:
Using Amazon Textract to extract the text from the reports, and Amazon Comprehend Medical to identify the PHI from the extracted text, would be the most efficient solution as it would involve the least operational overhead. Textract is specifically designed for extracting text from documents, and Comprehend Medical is a fully managed service that can accurately identify PHI in medical text. This solution would require minimal maintenance and would not incur any additional costs beyond the usage fees for Textract and Comprehend Medical.

QUESTION 7
A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted. Immediate accessibility is always required as the 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 Mm from S3 Standard to S3 Glacier 30 days from object creation.
Delete the Tiles 4 years after object creation
B. Create an S3 bucket lifecycle policy to move tiles from S3 Standard to S3 One Zone-infrequent Access (S3 One Zone-IA) 30 days from object creation.
Delete the fees 4 years after object creation
C. Create an S3 bucket lifecycle policy to move files from S3 Standard-infrequent Access (S3 Standard -IA) 30 from object creation.
Delete the ties 4 years after 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 files to S3 Glacier 4 years after object carton.

Answer: C
Explanation:
Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce.
If they do not explicitly mention that they are using Glacier Instant Retrieval, we should assume that Glacier -> takes more time to retrieve and may not meet the requirements.

QUESTION 8
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 architect do to ensure messages are being processed once only?

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

Answer: D
Explanation:
The visibility timeout begins when Amazon SQS returns a message. During this time, the consumer processes and deletes the message. However, if the consumer fails before deleting the message and your system doesn't call the DeleteMessage action for that message before the visibility timeout expires, the message becomes visible to other consumers and the message is received again. If a message must be received only once, your consumer should delete it within the duration of the visibility timeout.
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html

Keyword: SQS queue writes to an Amazon RDS From this, Option D best suite &amp; other Options ruled out [Option A -You can't intruduce one more Queue in the existing one; Option B -only Permission &amp; Option C -Only Retrieves Messages] FIF O 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).

QUESTION 9
A solutions architect is designing a new hybrid architecture to extend a company s on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.
What should the solutions architect do to meet these requirements?

A. Provision an AWS Direct Connect connection to a Region.
Provision a VPN connection as a backup if the primary Direct Connect connection fails.
B. Provision a VPN tunnel connection to a Region for private connectivity.
Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.
C. Provision an AWS Direct Connect connection to a Region.
Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.
D. Provision an AWS Direct Connect connection to a Region.
Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

Answer: A
Explanation:

"In some cases, this connection alone is not enough. It is always better to guarantee a fallback connection as the backup of DX. There are several options, but implementing it with an AWS Site-To-Site VPN is a real cost-effective solution that can be exploited to reduce costs or, in the meantime, wait for the setup of a second DX."
https://www.proud2becloud.com/hybrid-cloud-networking-backup-aws-direct-connect-network-connection-with-aws-site-to-site-vpn/

QUESTION 10
A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data.

Which solution will meet these requirements with the LEAST operational effort?

A. Place the EC2 instances in different AWS Regions.
Use Amazon Route 53 health checks to redirect traffic.
Use Aurora PostgreSQL Cross-Region Replication.
B. Configure the Auto Scaling group to use multiple Availability Zones.
Configure the database as Multi-AZ.
Configure an Amazon RDS Proxy instance for the database.
C. Configure the Auto Scaling group to use one Availability Zone.
Generate hourly snapshots of the database.
Recover the database from the snapshots in the event of a failure.
D. Configure the Auto Scaling group to use multiple AWS Regions.
Write the data from the application to Amazon S3.
Use S3 Event Notifications to launch an AWS Lambda function to write the data to the database.

Answer: B
Explanation:
By configuring the Auto Scaling group to use multiple Availability Zones, the application will be able to continue running even if one Availability Zone goes down. Configuring the database as Multi-AZ will also ensure that the database remains available in the event of a failure in one Availability Zone. Using an Amazon RDS Proxy instance for the database will allow the application to automatically route traffic to healthy database instances, further increasing the availability of the application. This solution will meet the requirements for high availability with minimal operational effort.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html

QUESTION 11
A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service.

The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code.

What should a solutions architect do to meet these requirements?

A. Enable HTTP health checks on the NLB. supplying the URL of the company's application.

B. Add a cron job to the EC2 instances to check the local application's logs once each minute.
   If HTTP errors are detected, the application will restart.
C. Replace the NLB with an Application Load Balancer.
   Enable HTTP health checks by supplying the URL of the company's application.
   Configure an Auto Scaling action to replace unhealthy instances.
D. Create an Amazon Cloud Watch alarm that monitors the UnhealthyHostCount metric for the NLB.
   Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Answer: C
Explanation:
NLB does not handle HTTP (layer 7) listerns errors only TCP (layer 4) listeners.
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-nlb.html

QUESTION 12
A company runs a shopping application that uses Amazon DynamoDB to store customer information. In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour.

What should the solutions architect recommend to meet these requirements?

A. Configure DynamoDB global tables.
   For RPO recovery, point the application to a different AWS Region.
B. Configure DynamoDB point-in-time recovery.
   For RPO recovery, restore to the desired point in time.
C. Export the DynamoDB data to Amazon S3 Glacier on a daily basis.
   For RPO recovery, import the data from S3 Glacier to DynamoDB.
D. Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes.
   For RPO recovery, restore the DynamoDB table by using the EBS snapshot.

Answer: B
Explanation:
Point in Time Recovery is designed as a continuous backup juts to recover it fast. It covers perfectly the RPO, and probably the RTO.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/PointInTimeRecovery.html

QUESTION 13
A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs.

How can the solutions architect meet this requirement?

A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through It.
B. Deploy a NAT gateway into a public subnet and attach an end point policy that allows access to the S3 buckets.
C. Deploy the application Into a public subnet and allow it to route through an internet gateway to

access the S3 Buckets

D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

Explanation:
By deploying an S3 VPC gateway endpoint, the application can access the S3 buckets over a private network connection within the VPC, eliminating the need for data transfer over the internet. This can help reduce data transfer fees as well as improve the performance of the application. The endpoint policy can be used to specify which S3 buckets the application has access to.

QUESTION 14
A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.
Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances
B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company
C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company
D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host
E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host

Answer: CD
Explanation:
C because from on-prem network to bastion through internet (using on-prem resource's public IP).
D because bastion and ec2 is in same VPC, meaning bastion can communicate to EC2 via it's private IP address.

QUESTION 15
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? (Choose two.)

A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
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:
"Security groups create an outbound rule for every inbound rule." Not completely right. Statefull does NOT mean that if you create an inbound (or outbound) rule, it will create an outbound (or inbound) rule. What it does mean is: suppose you create an inbound rule on port 443 for the X ip. When a request enters on port 443 from X ip, it will allow traffic out for that request in the port 443. However, if you look at the outbound rules, there will not be any outbound rule on port 443 unless explicitly create it. In ACLs, which are stateless, you would have to create an inbound rule to allow incoming requests and an outbound rule to allow your application responds to those incoming requests.
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#SecurityGroupRules

QUESTION 16
A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.

Which solution meets these requirements and is the MOST operationally efficient?

A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer.
Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server's peak utilization during the performance failures.
Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group.
Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group.
Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Answer: A
Explanation:
Lambda = serverless + autoscale (modernize), SQS= decouple (no more drops)
https://aws.amazon.com/getting-started/hands-on/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-4/

QUESTION 17
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: B
Explanation:
These are some of the main use cases for AWS DataSync:
- Data migration
- Move active datasets rapidly over the network into Amazon S3, Amazon EFS, or FSx for Windows File Server.
DataSync includes automatic encryption and data integrity validation to help make sure that your data arrives securely, intact, and ready to use.
DataSync includes encryption and integrity validation to help make sure your data arrives securely, intact, and ready to use.
https://aws.amazon.com/datasync/faqs/

QUESTION 18
A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data.

Which solution will meet these requirements with the LEAST operational overhead?

A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream.
Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source.
Use AWS Lambda functions to transform the data.
Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue.
Stop source/destination checking on the EC2 instance.
Use AWS Glue to transform the data and to send the data to Amazon S3.
C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream.
Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source.
Use AWS Lambda functions to transform the data.
Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
D. Configure an Amazon API Gateway API to send data to AWS Glue.
Use AWS Lambda functions to transform the data.
Use AWS Glue to send the data to Amazon S3.

Answer: C
Explanation:
It uses fully managed services for the API, data transformation, and data delivery, which minimizes operational overhead.

QUESTION 19
A company needs to keep user transaction data in an Amazon DynamoDB table.
The company must retain the data for 7 years.
What is the MOST operationally efficient solution that meets these requirements?

A. Use DynamoDB point-in-time recovery to back up the table continuously.
B. Use AWS Backup to create backup schedules and retention policies for the table.
C. Create an on-demand backup of the table by using the DynamoDB console.
Store the backup in an Amazon S3 bucket.
Set an S3 Lifecycle configuration for the S3 bucket.
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function.
Configure the Lambda function to back up the table and to store the backup in an Amazon S3 bucket.
Set an S3 Lifecycle configuration for the S3 bucket.

Answer: B
Explanation:
We recommend you use AWS Backup to automatically delete the backups that you no longer need by configuring your lifecycle when you created your backup plan.
https://docs.aws.amazon.com/aws-backup/latest/devguide/deleting-backups.html

QUESTION 20
A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings. In the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur, they will happen very quickly.

What should a solutions architect recommend?

A. Create a DynamoDB table in on-demand capacity mode.
B. Create a DynamoDB table with a global secondary index.
C. Create a DynamoDB table with provisioned capacity and auto scaling.
D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Answer: A
Explanation:
On-demand mode is a good option if any of the following are true:
- You create new tables with unknown workloads.
- You have unpredictable application traffic.
- You prefer the ease of paying for only what you use.

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
Explanation:
Share the existing KMS key with the MSP external account because it has already been used to encrypt the AMI snapshot.
https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html

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 in 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
Explanation:
Spot blocks are not longer available, and you can't use spot instances on Prod machines 24x7.

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:
You can use S3 Object Lock to store objects using a write-once-read-many (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use S3 Object Lock to meet regulatory requirements that require WORM storage, or add an extra layer of protection against object changes and deletion.
Versioning is required and automatically activated as Object Lock is enabled.

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:
Secrets Manager enables you to replace hardcoded credentials in your code, including passwords, with an API call to Secrets Manager to retrieve the secret programmatically. This helps ensure the secret can't be compromised by someone examining your code, because the secret no longer exists in the code. Also, you can configure Secrets Manager to automatically rotate the secret for you according to a specified schedule. This enables you to replace long-term secrets with short-term ones, significantly reducing the risk of compromise.
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 in 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:
SQS maintains the data if the lambda function fails, RDS Proxy just reuses db connections for performance.

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 in 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
Explanation:
Typically, you configure buckets to be Requester Pays buckets when you want to share data but not incur charges associated with others accessing the data. For example, you might use Requester Pays buckets when making available large datasets, such as zip code directories, reference data, geospatial information, or web crawling data.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/RequesterPaysBuckets.html

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
Explanation:
This will secure the audit documents by providing an additional layer of protection against accidental deletion. With versioning enabled, any deleted or overwritten objects in the S3 bucket will be preserved as previous versions, allowing the company to recover them if needed. With MFA Delete enabled, any delete request made to the S3 bucket will require the use of an MFA code, which provides an additional layer of security.

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: B
Explanation:
Elasti Cache if for reading common results. The script is looking for new movies added. Read replica would be the best choice.

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: B
Explanation:
Gateway endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC.
https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html

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 Amazon EC2 instances inside a VPC.
Which combination of steps should a solutions architect take to accomplish this? (Choose 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
Explanation:
To alleviate the application latency issue, the recommended solution is to use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production, and use database cloning to create the staging database on-demand. This allows the development team to continue using the staging environment without delay, while also providing elasticity and availability for the production application.

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:

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.
https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html

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: B
Explanation:
Kinesis Data Streams does not persist data. It also only ingests data from Kinesis Data Stream and Firehose, and outputs to Kinesis Data Stream, Firehose and Lambda.

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:
Amazon RDS uses the SNS to provide notification when an Amazon event occurs.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.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 10 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
Explanation:
"The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed."
https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-legal-hold.html

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
Explanation:
Remember to have operationally efficiency in mind. It usually goes with configure rather than create. For Presigned URL's you have to assign it individually to the user. Example of Presiged URL's use case: For access to premium users on a premium content on a website .

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 running on Amazon EC2. The company wants this application to be highly available with low operational complexity.
Which architecture offers the HIGHEST 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.
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
Explanation:
Amazon MQ with active/standby brokers configured across two Availability Zones ensures that the message queue is available even if one Availability Zone experiences an outage.
An Auto Scaling group for the consumer EC2 instances across two Availability Zones ensures that the consumer application is able to continue processing messages even if one Availability Zone experiences an outage.
Amazon RDS for MySQL with Multi-AZ enabled ensures that the database is available even if one Availability Zone experiences an outage.

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
Explanation:
Less operational overhead means A: Fargate (no EC2), move the containers on ECS, autoscaling for growth and ALB to balance consumption.

QUESTION 42
A company uses 50 TB of data for reporting. The company wants to move this data from on premises to AWS A custom application in the company's data center runs a weekly data transformation job. The company plans to pause the application until the data transfer is complete and needs to begin the transfer process as soon as possible.
The data center does not have any available network bandwidth for additional workloads.
A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud.
Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS DataSync to move the data.
Create a custom transformation job by using AWS Glue.
B. Order an AWS Snowcone device to move the data.
Deploy the transformation application to the device.
C. Order an AWS Snowball Edge Storage Optimized device.
Copy the data to the device.
Create a custom transformation job by using AWS Glue.
D. Order an AWS D. Snowball Edge Storage Optimized device that includes Amazon EC2 compute.
Copy the data to the device.
Create a new EC2 instance on AWS to run the transformation application.

Answer: C
Explanation:
SnowBall can store 80TB (ok), takes around 1 week to move the device (faster than A), and AWS Glue allows to do ETL jobs.

QUESTION 43
A company has created an image analysis application in which users can upload photos and add photo frames to their images. The users upload images and metadata to indicate which photo frames they want to add to their images. The application uses a single Amazon EC2 instance and Amazon DynamoDB to store the metadata.

The application is becoming more popular, and the number of users is increasing. The company expects the number of concurrent users to vary significantly depending on the time of day and day of week. The company must ensure that the application can scale to meet the needs of the growing user base.

Which solution meats these requirements?

A. Use AWS Lambda to process the photos.
Store the photos and metadata in DynamoDB.
B. Use Amazon Kinesis Data Firehose to process the photos and to store the photos and metadata.
C. Use AWS Lambda to process the photos.

Store the photos in Amazon S3.
Retain DynamoDB to store the metadata.

D. Increase the number of EC2 instances to three.
Use Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volumes to store the photos and metadata.

Answer: C
Explanation:
Storing image in DB won't be very scalable compared to S3 metadata does not take up much space and is more efficiently stored in DB.

QUESTION 44
A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.
A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.
Which change to the network architecture should a solutions architect recommend to meet this requirement?

A. Create a NAT gateway.
Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.
B. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.
C. Move the EC2 instances to private subnets.
Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets
D. Remove the internet gateway from the VPC.
Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

Answer: C
Explanation:
VPC endpoint is the best choice to route S3 traffic without traversing internet.

QUESTION 45
A company uses a popular content management system (CMS) for its corporate website. However, the required patching and maintenance are burdensome. The company is redesigning its website and wants anew solution. The website will be updated four times a year and does not need to have any dynamic content available. The solution must provide high scalability and enhanced security.

Which combination of changes will meet these requirements with the LEAST operational overhead? (Choose two.)

A. Deploy an AWS WAF web ACL in front of the website to provide HTTPS functionality
B. Create and deploy an AWS Lambda function to manage and serve the website content
C. Create the new website and an Amazon S3 bucket Deploy the website on the S3 bucket with static website hosting enabled
D. Create the new website.

Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer.

Answer: AD
Explanation:
A -> We can configure CloudFront to require HTTPS from clients (enhanced security)
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-viewers-to-cloudfront.html
D -> storing static website on S3 provides scalability and less operational overhead, then configuration of Application LB and EC2 instances.

QUESTION 46
A company stores its application logs in an Amazon CloudWatch Logs log group.
A new policy requires the company to store all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) in near-real time.

Which solution will meet this requirement with the LEAST operational overhead?

A. Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
B. Create an AWS Lambda function.
Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
C. Create an Amazon Kinesis Data Firehose delivery stream.
Configure the log group as the delivery stream's source.
Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.
D. Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams.
Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service)

Answer: A
Explanation:
CloudWatch has a native feature to stream logs to OpenSearch, when you enable this setting it creates a Lambda Function automatically with pre-populated code which streams the logs to OpenSearch Cluster.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

QUESTION 47
A company is building a web-based application running on Amazon EC2 instances in multiple Availability Zones. The web application will provide access to a repository of text documents totaling about 900 TB in size. The company anticipates that the web application will experience periods of high demand. A solutions architect must ensure that the storage component for the text documents can scale to meet the demand of the application at all times. The company is concerned about the overall cost of the solution.

Which storage solution meets these requirements MOST cost-effectively?

A. Amazon Elastic Block Store (Amazon EBS)
B. Amazon Elastic File System (Amazon EFS)
C. Amazon Elasticsearch Service (Amazon ES)

D. Amazon S3

Answer: D
Explanation:
Amazon S3 is an object storage service that can store and retrieve large amounts of data at any time, from anywhere on the web. It is designed for high durability, scalability, and cost-effectiveness, making it a suitable choice for storing a large repository of text documents. With S3, you can store and retrieve any amount of data, at any time, from anywhere on the web, and you can scale your storage up or down as needed, which will help to meet the demand of the web application. Additionally, S3 allows you to choose between different storage classes, such as standard, infrequent access, and archive, which will enable you to optimize costs based on your specific use case.

QUESTION 48
A global company is using Amazon API Gateway to design REST APIs for its loyalty club users in the us-east-1 Region and the ap-southeast-2 Region. A solutions architect must design a solution to protect these API Gateway managed REST APIs across multiple accounts from SQL injection and cross-site scripting attacks.

Which solution will meet these requirements with the LEAST amount of administrative effort?

A. Set up AWS WAF in both Regions.
Associate Regional web ACLs with an API stage.
B. Set up AWS Firewall Manager in both Regions.
Centrally configure AWS WAF rules.
C. Set up AWS Shield in bath Regions.
Associate Regional web ACLs with an API stage.
D. Set up AWS Shield in one of the Regions.
Associate Regional web ACLs with an API stage.

Answer: B
Explanation:
Using AWS WAF has several benefits. Additional protection against web attacks using criteria that you specify. You can define criteria using characteristics of web requests such as the following:
- Presence of SQL code that is likely to be malicious (known as SQL injection).
- Presence of a script that is likely to be malicious (known as cross-site scripting).
AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for a variety of protections.
https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

QUESTION 49
A company has implemented a self-managed DNS solution on three Amazon EC2 instances behind a Network Load Balancer (NLB) in the us-west-2 Region. Most of the company's users are located in the United States and Europe. The company wants to improve the performance and availability of the solution. The company launches and configures three EC2 instances in the eu-west-1 Region and adds the EC2 instances as targets for a new NLB.

Which solution can the company use to route traffic to all the EC2 instances?

A. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs.
Create an Amazon CloudFront distribution.

Use the Route 53 record as the distribution's origin.

B. Create a standard accelerator in AWS Global Accelerator.
Create endpoint groups in us-west-2 and eu-west-1.
Add the two NLBs as endpoints for the endpoint groups.

C. Attach Elastic IP addresses to the six EC2 instances.
Create an Amazon Route 53 geolocation routing policy to route requests to one of the six EC2 instances.
Create an Amazon CloudFront distribution.
Use the Route 53 record as the distribution's origin.

D. Replace the two NLBs with two Application Load Balancers (ALBs).
Create an Amazon Route 53 latency routing policy to route requests to one of the two ALBs.
Create an Amazon CloudFront distribution.
Use the Route 53 record as the distribution's origin.

Answer: B
Explanation:
WS Global Accelerator is a networking service that helps you improve the availability and performance of the applications that you offer to your global users. AWS Global Accelerator is easy to set up, configure, and manage. It provides static IP addresses that provide a fixed entry point to your applications and eliminate the complexity of managing specific IP addresses for different AWS Regions and Availability Zones. AWS Global Accelerator always routes user traffic to the optimal endpoint based on performance, reacting instantly to changes in application health, your user’s location, and policies that you configure.
https://aws.amazon.com/global-accelerator/faqs/

QUESTION 50
A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

A. Encrypt a copy of the latest DB snapshot.
Replace existing DB instance by restoring the encrypted snapshot

B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it.
Enable encryption on the DB instance.

C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS).
Restore encrypted snapshot to an existing DB instance.

D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS)

Answer: A
Explanation:
You can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created. However, you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance.
https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html

QUESTION 51

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 multifactor 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
Explanation:
If you are responsible for securing your data across AWS services, you should use it to centrally manage the encryption keys that control access to your data. If you are a developer who needs to encrypt data in your applications, you should use the AWS Encryption SDK with AWS KMS to easily generate, use and protect symmetric encryption keys in your code.

QUESTION 52
A company has a dynamic web application hosted 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 connections to the existing EC2 instances
D. Import the SSL certificate into AWS Certificate Manager (ACM).
Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

Answer: D
Explanation:
https://aws.amazon.com/certificate-manager/:
"With AWS Certificate Manager, you can quickly request a certificate, deploy it on ACM-integrated AWS resources, such as Elastic Load Balancers, Amazon CloudFront distributions, and APIs on API Gateway, and let AWS Certificate Manager handle certificate renewals. It also enables you to create private certificates for your internal resources and manage the certificate lifecycle centrally."

QUESTION 53
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:
EC2 Spot Instances allow users to bid on spare Amazon EC2 computing capacity and can be a cost-effective solution for stateless, interruptible workloads that can be started and stopped at any time. Since the batch processing job is stateless, can be started and stopped at any time, and typically takes upwards of 60 minutes to complete, EC2 Spot Instances would be a good fit for this workload.

QUESTION 54
A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.

Which combination of configuration options will meet these requirements? (Choose two.)

A. Use an Auto Scaling group to launch the EC2 instances in private subnets.
Deploy an RDS Multi-AZ DB instance in private subnets.
B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones.
Deploy an Application Load Balancer in the private subnets.
C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones.
Deploy an RDS Multi-AZ DB instance in private subnets.
D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones.
Deploy an Application Load Balancer in the public subnet.
E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones.
Deploy an Application Load Balancer in the public subnets.

Answer: AE
Explanation:
Before you begin: Decide which two Availability Zones you will use for your EC2 instances. Configure your virtual private cloud (VPC) with at least one public subnet in each of these Availability Zones. These public subnets are used to configure the load balancer. You can launch your EC2 instances in other subnets of these Availability Zones instead.

QUESTION 55
A solutions architect needs to implement a solution to reduce a company's storage costs. All the company's data is in the Amazon S3 Standard storage class. The company must keep all data for at least 25 years. Data from the most recent 2 years must be highly available and immediately retrievable.

Which solution will meet these requirements?

A. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive immediately.
B. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years.
C. Use S3 Intelligent-Tiering. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.
D. Set up an S3 Lifecycle policy to transition objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately and to S3 Glacier Deep Archive after 2 years.

Answer: B

QUESTION 56
A company runs its ecommerce application on AWS. Every new order is published as a message in a RabbitMQ queue that runs on an Amazon EC2 instance in a single Availability Zone. These messages are processed by a different application that runs on a separate EC2 instance. This application stores the details in a PostgreSQL database on another EC2 instance. All the EC2 instances are in the same Availability Zone.
The company needs to redesign its architecture to provide the highest availability with the least operational overhead.
What should a solutions architect do to meet these requirements?

A. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group (or EC2 instances that host the application. Create another Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.
B. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
C. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS fqjPostgreSQL.
D. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Create a third Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.

Answer: B
Explanation:
Migrating to Amazon MQ reduces the overhead on the queue management. C and D are dismissed.
Deciding between A and B means deciding to go for an AutoScaling group for EC2 or an RDS for Postgress (both multi- AZ). The RDS option has less operational impact, as provide as a service the tools and software required. Consider for instance, the effort to add an additional node like a read replica, to the DB.
https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/active-standby-broker-deployment.html
https://aws.amazon.com/rds/postgresql/

QUESTION 57
A reporting team receives files each day in an Amazon S3 bucket. The reporting team manually reviews and copies the files from this initial S3 bucket to an analysis S3 bucket each day at the same time to use with Amazon QuickSight. Additional teams are starting to send more files in larger sizes to the initial S3 bucket.

The reporting team wants to move the files automatically analysis S3 bucket as the files enter the initial S3 bucket. The reporting team also wants to use AWS Lambda functions to run pattern-matching code on the copied data. In addition, the reporting team wants to send the data files to a pipeline in Amazon SageMaker Pipelines.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

A. Create a Lambda function to copy the files to the analysis S3 bucket.
Create an S3 event notification for the analysis S3 bucket.
Configure Lambda and SageMaker Pipelines as destinations of the event notification.
Configure s30bjectCreated:Put as the event type.
B. Create a Lambda function to copy the files to the analysis S3 bucket.
Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events).
Configure an ObjectCreated rule in EventBridge (CloudWatch Events).
Configure Lambda and SageMaker Pipelines as targets for the rule.
C. Configure S3 replication between the S3 buckets.
Create an S3 event notification for the analysis S3 bucket.
Configure Lambda and SageMaker Pipelines as destinations of the event notification.
Configure s30bjectCreated:Put as the event type.
D. Configure S3 replication between the S3 buckets.
Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events).
Configure an ObjectCreated rule in EventBridge (CloudWatch Events).
Configure Lambda and SageMaker Pipelines as targets for the rule.

Answer: D
Explanation:
The files are getting large, less operational overhead - so will choose S3 replication. Event bridge is far more advanced than S3 event notification and they support multiple targets. S3 Event notification may not support Sagemaker. Also filtering and pattern matching available in Event bridge.

QUESTION 58
A solutions architect needs to help a company optimize the cost of running an application on AWS. The application will use Amazon EC2 instances, AWS Fargate, and AWS Lambda for compute within the architecture.

The EC2 instances will run the data ingestion layer of the application. EC2 usage will be sporadic and unpredictable. Workloads that run on EC2 instances can be interrupted at any time. The application front end will run on Fargate, and Lambda will serve the API layer. The front-end utilization and API layer utilization will be predictable over the course of the next year.

Which combination of purchasing options will provide the MOST cost-effective solution for hosting this application? (Choose two.)

A. Use Spot Instances for the data ingestion layer
B. Use On-Demand Instances for the data ingestion layer
C. Purchase a 1-year Compute Savings Plan for the front end and API layer.
D. Purchase 1-year All Upfront Reserved instances for the data ingestion layer.
E. Purchase a 1-year EC2 instance Savings Plan for the front end and API layer.

Answer: AC
Explanation:
EC2 instance Savings Plan saves 72% while Compute Savings Plans saves 66%. But according to link, it says "Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, region, OS or tenancy, and also apply to Fargate and Lambda usage." EC2 instance Savings Plans are not applied to Fargate or Lambda.
https://aws.amazon.com/savingsplans/faq/
https://aws.amazon.com/savingsplans/compute-pricing/

QUESTION 59
A company runs a web-based portal that provides users with global breaking news, local alerts, and weather updates. The portal delivers each user a personalized view by using mixture of static and dynamic content. Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB). The company wants the portal to provide this content to its users across the world as quickly as possible.

How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

A. Deploy the application stack in a single AWS Region.
Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin.
B. Deploy the application stack in two AWS Regions.
Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region.
C. Deploy the application stack in a single AWS Region.
Use Amazon CloudFront to serve the static content.
Serve the dynamic content directly from the ALB.
D. Deploy the application stack in two AWS Regions.
Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region.

Answer: A
Explanation:
Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content.
https://aws.amazon.com/blogs/networking-and-content-delivery/deliver-your-apps-dynamic-content-using-amazon-cloudfront-getting-started-template/

QUESTION 60
A gaming company is designing a highly available architecture. The application runs on a modified Linux kernel and supports only UDP-based traffic. The company needs the front-end tier to provide the best possible user experience. That tier must have low latency, route traffic to the nearest edge location, and provide static IP addresses for entry into the application endpoints.

What should a solutions architect do to meet these requirements?

A. Configure Amazon Route 53 to forward requests to an Application Load Balancer.
Use AWS Lambda for the application in AWS Application Auto Scaling.
B. Configure Amazon CloudFront to forward requests to a Network Load Balancer.
Use AWS Lambda for the application in an AWS Application Auto Scaling group.
C. Configure AWS Global Accelerator to forward requests to a Network Load Balancer.

Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.

D. Configure Amazon API Gateway to forward requests to an Application Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.

Answer: C
Explanation:
AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

QUESTION 61
A company wants to migrate its existing on-premises monolithic application to AWS. The company wants to keep as much of the front-end code and the backend code as possible. However, the company wants to break the application into smaller applications. A different team will manage each application. The company needs a highly scalable solution that minimizes operational overhead.
Which solution will meet these requirements?

A. Host the application on AWS Lambda Integrate the application with Amazon API Gateway.
B. Host the application with AWS Amplify. Connect the application to an Amazon API Gateway API that is integrated with AWS Lambda.
C. Host the application on Amazon EC2 instances. Set up an Application Load Balancer with EC2 instances in an Auto Scaling group as targets.
D. Host the application on Amazon Elastic Container Service (Amazon ECS) Set up an Application Load Balancer with Amazon ECS as the target.

Answer: D
Explanation:
https://aws.amazon.com/blogs/compute/microservice-delivery-with-amazon-ecs-and-application-load-balancers/

QUESTION 62
A company recently started using Amazon Aurora as the data store for its global ecommerce application.
When large reports are run developers report that the ecommerce application is performing poorly After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPUUtilization metrics are spiking when monthly reports run.
What is the MOST cost-effective solution?

A. Migrate the monthly reporting to Amazon Redshift.
B. Migrate the monthly reporting to an Aurora Replica
C. Migrate the Aurora database to a larger instance class
D. Increase the Provisioned IOPS on the Aurora instance

Answer: B
Explanation:

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html #Aurora.Replication.Replicas Aurora Replicas have two main purposes. You can issue queries to them to scale the read operations for your application. You typically do so by connecting to the reader endpoint of the cluster. That way, Aurora can spread the load for read-only connections across as many Aurora Replicas as you have in the cluster. Aurora Replicas also help to increase availability. If the writer instance in a cluster becomes unavailable, Aurora automatically promotes one of the reader instances to take its place as the new writer.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.html

QUESTION 63
A company hosts a website analytics application on a single Amazon EC2 On-Demand Instance. The analytics software is written in PHP and uses a MySQL database. The analytics software, the web server that provides PHP, and the database server are all hosted on the EC2 instance. The application is showing signs of performance degradation during busy times and is presenting 5xx errors.
The company needs to make the application scale seamlessly.

Which solution will meet these requirements MOST cost-effectively?

A. Migrate the database to an Amazon RDS for MySQL DB instance.
Create an AMI of the web application.
Use the AMI to launch a second EC2 On-Demand Instance.
Use an Application Load Balancer to distribute the load to each EC2 instance.
B. Migrate the database to an Amazon RDS for MySQL DB instance.
Create an AMI of the web application.
Use the AMI to launch a second EC2 On-Demand Instance.
Use Amazon Route 53 weighted routing to distribute the load across the two EC2 instances.
C. Migrate the database to an Amazon Aurora MySQL DB instance.
Create an AWS Lambda function to stop the EC2 instance and change the instance type.
Create an Amazon CloudWatch alarm to invoke the Lambda function when CPU utilization surpasses 75%.
D. Migrate the database to an Amazon Aurora MySQL DB instance.
Create an AMI of the web application.
Apply the AMI to a launch template.
Create an Auto Scaling group with the launch template.
Configure the launch template to use a Spot Fleet.
Attach an Application Load Balancer to the Auto Scaling group.

Answer: D
Explanation:
Spot Fleet can leverage both spot+on-demand instances, it should be the most cost-effective.

QUESTION 64
A company runs a stateless web application in production on a group of Amazon EC2 On-Demand Instances behind an Application Load Balancer. The application experiences heavy usage during an 8-hour period each business day. Application usage is moderate and steady overnight Application usage is low during weekends.
The company wants to minimize its EC2 costs without affecting the availability of the application.
Which solution will meet these requirements?

A. Use Spot Instances for the entire workload.
B. Use Reserved instances for the baseline level of usage.
Use Spot Instances for any additional capacity that the application needs.

C. Use On-Demand Instances for the baseline level of usage.
   Use Spot Instances for any additional capacity that the application needs.
D. Use Dedicated Instances for the baseline level of usage.
   Use On-Demand Instances for any additional capacity that the application needs.

Answer: B
Explanation:
They are currently using On Demand instances, so option C is out.
A uses Spot instances which is not recommended for PROD and D uses Dedicated instances which are expensive.
So option B should be the one.

QUESTION 65
A company needs to retain application logs files for a critical application for 10 years. The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed. The application generates more than 10 TB of logs per month.
Which storage option meets these requirements MOST cost-effectively?

A. Store the Iogs in Amazon S3.
   Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.
B. Store the logs in Amazon S3.
   Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.
C. Store the logs in Amazon CloudWatch Logs.
   Use AWS Backup to move logs more then 1 month old to S3 Glacier Deep Archive.
D. Store the logs in Amazon CloudWatch Logs.
   Use Amazon S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.

Answer: B
Explanation:
You need S3 to be able to archive the logs after one month. Cannot do that with CloudWatch Logs.

QUESTION 66
A company has a data ingestion workflow that includes the following components:

- An Amazon Simple Notation Service (Amazon SNS) topic that receives notifications about new data deliveries.
- An AWS Lambda function that processes and stores the data

The ingestion workflow occasionally fails because of network connectivity issues.
When tenure occurs the corresponding data is not ingested unless the company manually reruns the job.

What should a solutions architect do to ensure that all notifications are eventually processed?

A. Configure the Lambda function for deployment across multiple Availability Zones
B. Modify me Lambda functions configuration to increase the CPU and memory allocations tor the function
C. Configure the SNS topic's retry strategy to increase both the number of retries and the wait time between retries
D. Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on failure

destination.
Modify the Lambda function to process messages in the queue.

Answer: D
Explanation:
To ensure that all notifications are eventually processed, the best solution would be to configure an Amazon Simple Queue Service (SQS) queue as the on-failure destination for the SNS topic. This will allow the notifications to be retried until they are successfully processed. The Lambda function can then be modified to process messages in the queue, ensuring that all notifications are eventually processed. Option D, "Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on-failure destination. Modify the Lambda function to process messages in the queue," is the correct answer.

QUESTION 67
A company has a service that produces event data. The company wants to use AWS to process the event data as it is received.
The data is written in a specific order that must be maintained throughout processing.
The company wants to implement a solution that minimizes operational overhead.
How should a solutions architect accomplish this?

A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages.
Set up an AWS Lambda function to process messages from the queue.
B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process.
Configure an AWS Lambda function as a subscriber.
C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages.
Set up an AWS Lambda function to process messages from the queue independently.
D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process.
Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Answer: A
Explanation:
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html
FIFO (First-In-First-Out) queues are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated. Examples of situations where you might use FIFO queues include the following: To make sure that user-entered commands are run in the right order. To display the correct product price by sending price modifications in the right order. To prevent a student from enrolling in a course before registering for an account.

QUESTION 68
A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms.

What should the solutions architect do to meet these requirements?

A. Create Amazon CloudWatch composite alarms where possible.

B. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.
C. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.
D. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.

Answer: A
Explanation:
Composite alarms determine their states by monitoring the states of other alarms. You can **use composite alarms to reduce alarm noise**. For example, you can create a composite alarm where the underlying metric alarms go into ALARM when they meet specific conditions. You then can set up your composite alarm to go into ALARM and send you notifications when the underlying metric alarms go into ALARM by configuring the underlying metric alarms never to take actions. Currently, composite alarms can take the following actions:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Create_Composite_Alarm.html

QUESTION 69
A company wants to migrate its on-premises data center to AWS. According to the company's compliance requirements, the company can use only the ap-northeast-3 Region. Company administrators are not permitted to connect VPCs to the internet.

Which solutions will meet these requirements? (Choose two.)

A. Use AWS Control Tower to implement data residency guardrails to deny internet access and deny access to all AWS Regions except ap-northeast-3.
B. Use rules in AWS WAF to prevent internet access.
Deny access to all AWS Regions except ap-northeast-3 in the AWS account settings.
C. Use AWS Organizations to configure service control policies (SCPS) that prevent VPCs from gaining internet access.
Deny access to all AWS Regions except ap-northeast-3.
D. Create an outbound rule for the network ACL in each VPC to deny all traffic from 0.0.0.0/0.
Create an IAM policy for each user to prevent the use of any AWS Region other than ap-northeast-3.
E. Use AWS Config to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3.

Answer: AC
Explanation:
Disallow internet access for an Amazon VPC instance managed by a customer.
https://aws.amazon.com/blogs/aws/new-for-aws-control-tower-region-deny-and-guardrails-to-help-you-meet-data-residency-requirements/

QUESTION 70
A company uses a three-tier web application to provide training to new employees. The application is accessed for only 12 hours every day. The company is using an Amazon RDS for MySQL DB instance to store information and wants to minimize costs.

What should a solutions architect do to meet these requirements?

A. Configure an IAM policy for AWS Systems Manager Session Manager.
Create an IAM role for the policy.
Update the trust relationship of the role.

Set up automatic start and stop for the DB instance.

B. Create an Amazon ElastiCache for Redis cache cluster that gives users the ability to access the data from the cache when the DB instance is stopped.
Invalidate the cache after the DB instance is started.

C. Launch an Amazon EC2 instance.
Create an IAM role that grants access to Amazon RDS.
Attach the role to the EC2 instance.
Configure a cron job to start and stop the EC2 instance on the desired schedule.

D. Create AWS Lambda functions to start and stop the DB instance.
Create Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions.
Configure the Lambda functions as event targets for the rules

Answer: D
Explanation:
AWS Lambda and Amazon EventBridge that allows you to schedule a Lambda function to stop and start the idle databases with specific tags to save on compute costs.
https://aws.amazon.com/blogs/database/schedule-amazon-rds-stop-and-start-using-aws-lambda/

QUESTION 71
A company sells ringtones created from clips of popular songs. The files containing the ringtones are stored in Amazon S3 Standard and are at least 128 KB in size. The company has millions of files, but downloads are infrequent for ringtones older than 90 days. The company needs to save money on storage while keeping the most accessed files readily available for its users.

Which action should the company take to meet these requirements MOST cost-effectively?

A. Configure S3 Standard-Infrequent Access (S3 Standard-IA) storage for the initial storage tier of the objects.

B. Move the files to S3 Intelligent-Tiering and configure it to move objects to a less expensive storage tier after 90 days.

C. Configure S3 inventory to manage objects and move them to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.

D. Implement an S3 Lifecycle policy that moves the objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.

Answer: D
Explanation:
The Question talks about downloads are infrequent older than 90 days which means files less than 90 days are accessed frequently. Standard-Infrequent Access (S3 Standard-IA) needs a minimum 30 days if accessed before, it costs more.
So to access the files frequently you need a S3 Standard. After 90 days you can move it to Standard-Infrequent Access (S3 Standard-IA) as its going to be less frequently accessed.

QUESTION 72
A company needs to save the results from a medical trial to an Amazon S3 repository. The repository must allow a few scientists to add new files and must restrict all other users to read-only access. No users can have the ability to modify or delete any files in the repository. The company must keep every file in the repository for a minimum of 1 year after its creation date.

Which solution will meet these requirements?

A. Use S3 Object Lock in governance mode with a legal hold of 1 year
B. Use S3 Object Lock in compliance mode with a retention period of 365 days.
C. Use an IAM role to restrict all users from deleting or changing objects in the S3 bucket Use an S3 bucket policy to only allow the IAM role
D. Configure the S3 bucket to invoke an AWS Lambda function every tune an object is added Configure the function to track the hash of the saved object to that modified objects can be marked accordingly

Answer: B
Explanation:
Compliance mode is more restrictive.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html

QUESTION 73
A large media company hosts a web application on AWS. The company wants to start caching confidential media files so that users around the world will have reliable access to the files. The content is stored in Amazon S3 buckets. The company must deliver the content quickly, regardless of where the requests originate geographically.

Which solution will meet these requirements?

A. Use AWS DataSync to connect the S3 buckets to the web application.
B. Deploy AWS Global Accelerator to connect the S3 buckets to the web application.
C. Deploy Amazon CloudFront to connect the S3 buckets to CloudFront edge servers.
D. Use Amazon Simple Queue Service (Amazon SQS) to connect the S3 buckets to the web application.

Answer: C
Explanation:
CloudFront uses a local cache to provide the response, AWS Global accelerator proxies requests and connects to the application all the time for the response.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html#private-content-granting-permissions-to-oai

QUESTION 74
A company produces batch data that comes from different databases. The company also produces live stream data from network sensors and application APIs. The company needs to consolidate all the data into one place for business analytics. The company needs to process the incoming data and then stage the data in different Amazon S3 buckets. Teams will later run one-time queries and import the data into a business intelligence tool to show key performance indicators (KPIs).

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

A. Use Amazon Athena foe one-time queries.
Use Amazon QuickSight to create dashboards for KPIs.
B. Use Amazon Kinesis Data Analytics for one-time queries.
Use Amazon QuickSight to create dashboards for KPIs.
C. Create custom AWS Lambda functions to move the individual records from me databases to an Amazon Redshift duster.
D. Use an AWS Glue extract transform, and toad (ETL) job to convert the data into JSON format.

Load the data into multiple Amazon OpenSearch Service (Amazon Elasticsearch Service) dusters.

E. Use blueprints in AWS Lake Formation to identify the data that can be ingested into a data lake. Use AWS Glue to crawl the source extract the data and load the data into Amazon S3 in Apache Parquet format.

Answer: AE
Explanation:
https://aws.amazon.com/blogs/big-data/enhance-analytics-with-google-trends-data-using-aws-glue-amazon-athena-and-amazon-quicksight/

QUESTION 75
A gaming company has a web application that displays scores. The application runs on Amazon EC2 instances behind an Application Load Balancer. The application stores data in an Amazon RDS for MySQL database. Users are starting to experience long delays and interruptions that are caused by database read performance. The company wants to improve the user experience while minimizing changes to the application's architecture.

What should a solutions architect do to meet these requirements?

A. Use Amazon ElastiCache in front of the database.
B. Use RDS Proxy between the application and the database.
C. Migrate the application from EC2 instances to AWS Lambda.
D. Migrate the database from Amazon RDS for MySQL to Amazon DynamoDB.

Answer: A
Explanation:
Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases.
https://aws.amazon.com/caching/

QUESTION 76
A business's backup data totals 700 terabytes (TB) and is kept in network attached storage (NAS) at its data center. This backup data must be available in the event of occasional regulatory inquiries and preserved for a period of seven years. The organization has chosen to relocate its backup data from its on-premises data center to Amazon Web Services (AWS). Within one month, the migration must be completed. The company's public internet connection provides 500 Mbps of dedicated capacity for data transport.

What should a solutions architect do to ensure that data is migrated and stored at the LOWEST possible 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 transition 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 77
A company wants to direct its users to a backup static error page if the company's primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53. The domain is pointing to an Application Load Balancer (ALB). The company needs a solution that minimizes changes and infrastructure overhead.

Which solution will meet these requirements?

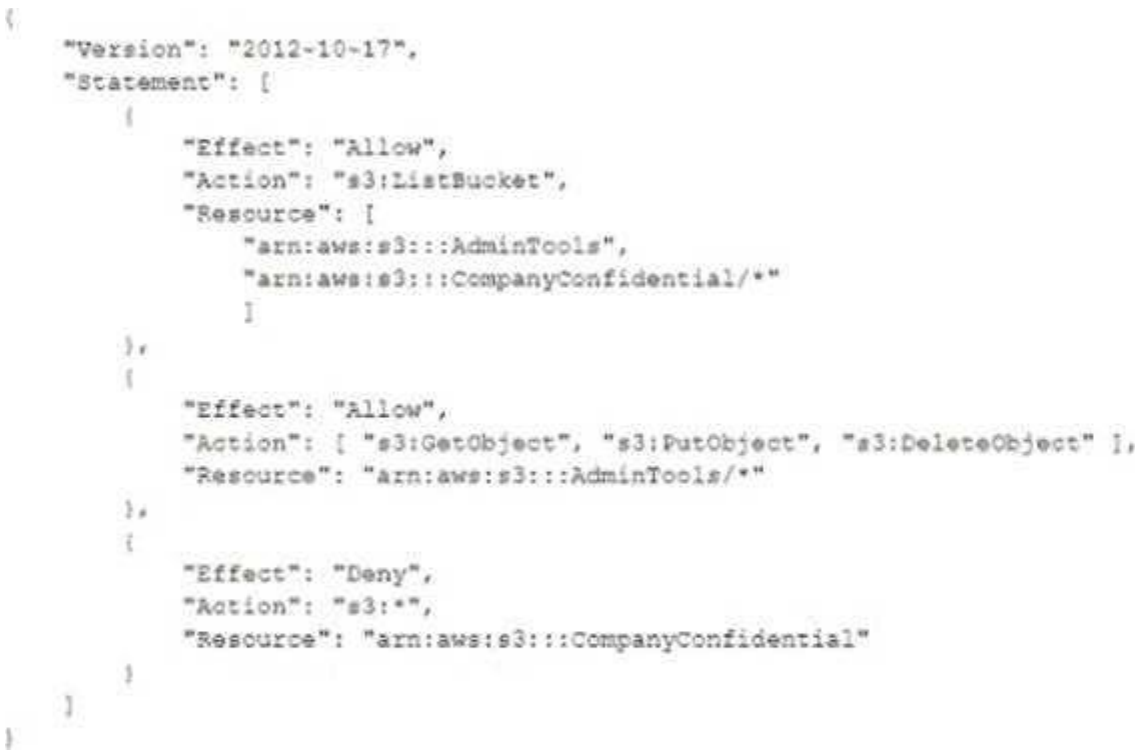
A. Update the Route 53 records to use a latency routing policy.
Add a static error page that is hosted in an Amazon S3 bucket to the records so that the traffic is sent to the most responsive endpoints.
B. Set up a Route 53 active-passive failover configuration.
Direct traffic to a static error page that is hosted in an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
C. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance that hosts a static error page as endpoints.
Configure Route 53 to send requests to the instance only if the health checks fail for the ALB.
D. Update the Route 53 records to use a multivalue answer routing policy.
Create a health check.
Direct traffic to the website if the health check passes.
Direct traffic to a static error page that is hosted in Amazon S3 if the health check does not pass.

Answer: B

QUESTION 78
A corporation has recruited a new cloud engineer who should not have access to the CompanyConfidential Amazon S3 bucket. The cloud engineer must have read and write permissions on an S3 bucket named AdminTools.

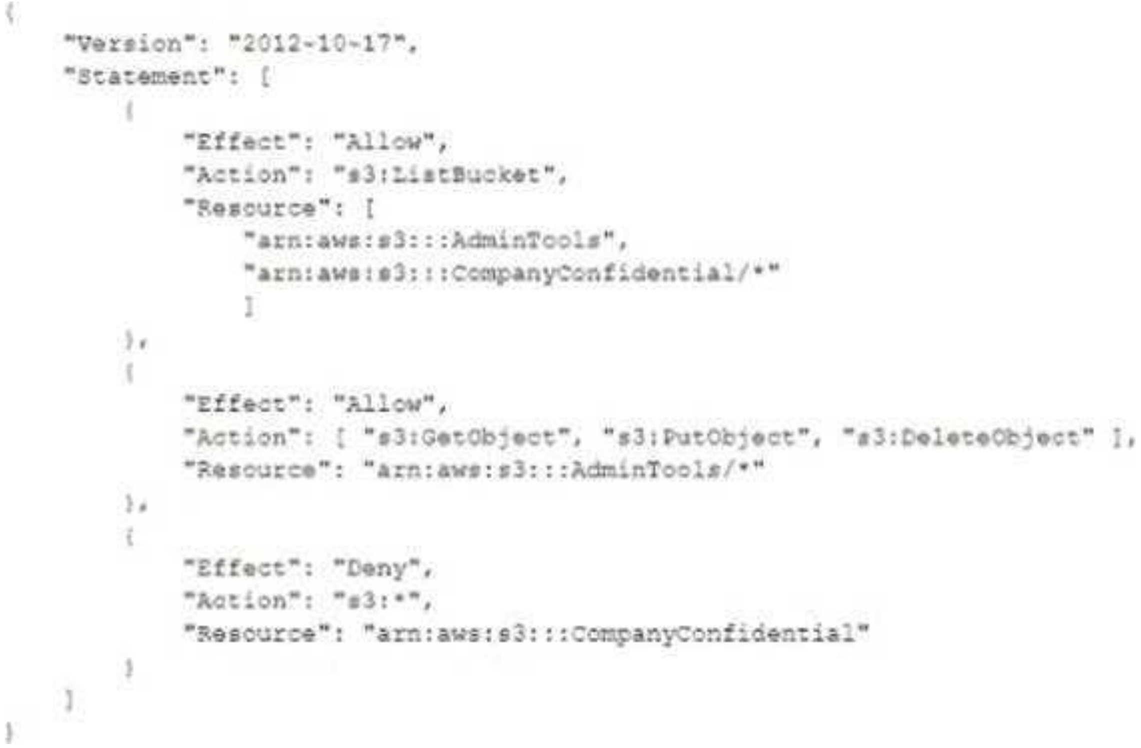
Which IAM policy will satisfy these criteria?

A.



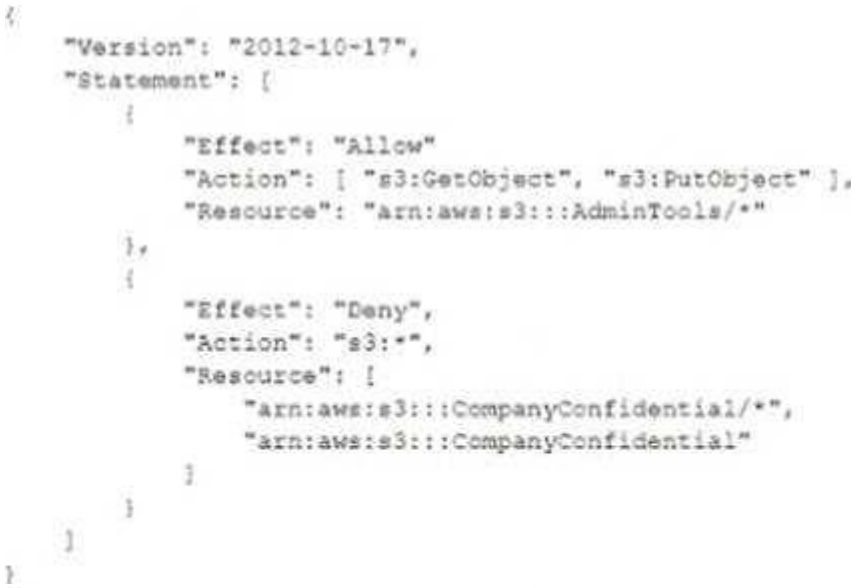
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::AdminTools",
                "arn:aws:s3:::CompanyConfidential/*"
                ]
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::CompanyConfidential"
        }
    ]
}
```

B.



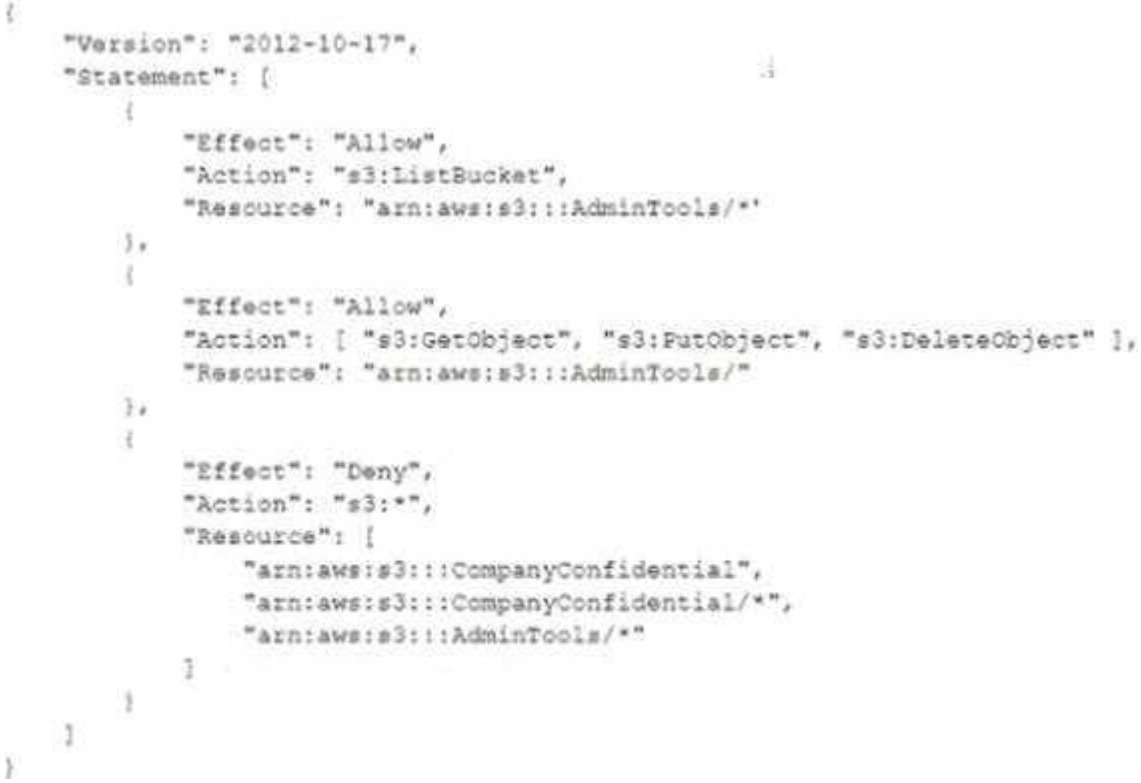
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::AdminTools",
                "arn:aws:s3:::CompanyConfidential/*"
                ]
        },
        {
            "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.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::AdminTools/*'
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential",
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::AdminTools/*"
            ]
        }
    ]
}
```

Answer: A
Explanation:
https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/reference_policies_examples_s3_rw-bucket.html

QUESTION 79
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 steps should the solutions architect do in conjunction to reach this goal? (Choose 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: DE
Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html

QUESTION 80
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
Explanation:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-placementgroup.html
A cluster placement group is a logical grouping of instances within a single Availability Zone that benefit from low network latency, high network throughput.

QUESTION 81
A company wants to use the AWS Cloud to make an existing application highly available and resilient. The current version of the application resides in the company's data center. The application recently experienced data loss after a database server crashed because of an unexpected power outage. The company needs a solution that avoids any single points of failure. The solution must give the application the ability to scale to meet user demand.

Which solution will meet these requirements?

A. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones.
Use an Amazon RDS DB instance in a Multi-AZ configuration.

B. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group in a single Availability Zone.
   Deploy the database on an EC2 instance.
   Enable EC2 Auto Recovery.
C. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones.
   Use an Amazon RDS DB instance with a read replica in a single Availability Zone.
   Promote the read replica to replace the primary DB instance if the primary DB instance fails.
D. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones.
   Deploy the primary and secondary database servers on EC2 instances across multiple Availability Zones.
   Use Amazon Elastic Block Store (Amazon EBS) Multi-Attach to create shared storage between the instances.

Answer: A
Explanation:
To make an existing application highly available and resilient while avoiding any single points of failure and giving the application the ability to scale to meet user demand, the best solution would be to deploy the application servers using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones and use an Amazon RDS DB instance in a Multi-AZ configuration.

By using an Amazon RDS DB instance in a Multi-AZ configuration, the database is automatically replicated across multiple Availability Zones, ensuring that the database is highly available and can withstand the failure of a single Availability Zone. This provides fault tolerance and avoids any single points of failure.

QUESTION 82
A company wants to run a gaming application on Amazon EC2 instances that are part of an Auto Scaling group in the AWS Cloud. The application will transmit data by using UDP packets. The company wants to ensure that the application can scale out and in as traffic increases and decreases. What should a solutions architect do to meet these requirements?

A. Attach a Network Load Balancer to the Auto Scaling group
B. Attach an Application Load Balancer to the Auto Scaling group.
C. Deploy an Amazon Route 53 record set with a weighted policy to route traffic appropriately
D. Deploy a NAT instance that is configured with port forwarding to the EC2 instances in the Auto Scaling group.

Answer: B

QUESTION 83
A solutions architect is designing a customer-facing application for a company. The application's database will have a clearly defined access pattern throughout the year and will have a variable number of reads and writes that depend on the time of year. The company must retain audit records for the database for 7 days. The recovery point objective (RPO) must be less than 5 hours.
Which solution meets these requirements?

A. Use Amazon DynamoDB with auto scaling.
   Use on-demand backups and Amazon DynamoDB Streams.

B. Use Amazon Redshift. Configure concurrency scaling.
Activate audit logging.
Perform database snapshots every 4 hours.
C. Use Amazon RDS with Provisioned IOPS.
Activate the database auditing parameter.
Perform database snapshots every 5 hours.
D. Use Amazon Aurora MySQL with auto scaling.
Activate the database auditing parameter

Answer: B

QUESTION 84
A company hosts a two-tier application on Amazon EC2 instances and Amazon RDS. The application's demand varies based on the time of day. The load is minimal after work hours and on weekends. The EC2 instances run in an EC2 Auto Scaling group that is configured with a minimum of two instances and a maximum of five instances. The application must be available at all times, but the company is concerned about overall cost.

Which solution meets the availability requirement MOST cost-effectively?

A. Use all EC2 Spot Instances.
Stop the RDS database when it is not in use.
B. Purchase EC2 Instance Savings Plans to cover five EC2 instances.
Purchase an RDS Reserved DB Instance
C. Purchase two EC2 Reserved Instances.
Use up to three additional EC2 Spot Instances as needed.
Stop the RDS database when it is not in use.
D. Purchase EC2 Instance Savings Plans to cover two EC2 instances.
Use up to three additional EC2 On-Demand Instances as needed.
Purchase an RDS Reserved DB Instance.

Answer: D

QUESTION 85
A company has an ecommerce checkout workflow that writes an order to a database and calls a service to process the payment. Users are experiencing timeouts during the checkout process. When users resubmit the checkout form, multiple unique orders are created for the same desired transaction.

How should a solutions architect refactor this workflow to prevent the creation of multiple orders?

A. Configure the web application to send an order message to Amazon Kinesis Data Firehose.
Set the payment service to retrieve the message from Kinesis Data Firehose and process the order.
B. Create a rule in AWS CloudTrail to invoke an AWS Lambda function based on the logged application path request.
Use Lambda to query the database, call the payment service, and pass in the order information.
C. Store the order in the database.
Send a message that includes the order number to Amazon Simple Notification Service (Amazon SNS).
Set the payment service to poll Amazon SNS. retrieve the message, and process the order.
D. Store the order in the database.

Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue.
Set the payment service to retrieve the message and process the order.
Delete the message from the queue.

Answer: D
Explanation:
This approach ensures that the order creation and payment processing steps are separate and atomic. By sending the order information to an SQS FIFO queue, the payment service can process the order one at a time and in the order they were received. If the payment service is unable to process an order, it can be retried later, preventing the creation of multiple orders. The deletion of the message from the queue after it is processed will prevent the same message from being processed multiple times.
It's worth noting that FIFO queues guarantee that messages are processed in the order they are received, and prevent duplicates.

QUESTION 86
A company is planning to build a high performance computing (HPC) workload as a service solution that Is hosted on AWS.
A group of 16 AmazonEC2Ltnux Instances requires the lowest possible latency for node-to-node communication.
The instances also need a shared block device volume for high-performing storage.
Which solution will meet these requirements?

A. Use a duster placement group.
Attach a single Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume to all the instances by using Amazon EBS Multi-Attach.
B. Use a cluster placement group.
Create shared 'lie systems across the instances by using Amazon Elastic File System (Amazon EFS).
C. Use a partition placement group.
Create shared tile systems across the instances by using Amazon Elastic File System (Amazon EFS).
D. Use a spread placement group.
Attach a single Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume to all the instances by using Amazon EBS Multi-Attach.

Answer: A

QUESTION 87
A company has an event-driven application that invokes AWS Lambda functions up to 800 times each minute with varying runtimes.
The Lambda functions access data that is stored in an Amazon Aurora MySQL OB cluster.
The company is noticing connection timeouts as user activity increases The database shows no signs of being overloaded. CPU, memory, and disk access metrics are all low.
Which solution will resolve this issue with the LEAST operational overhead?

A. Adjust the size of the Aurora MySQL nodes to handle more connections.
Configure retry logic in the Lambda functions for attempts to connect to the database.
B. Set up Amazon ElastiCache tor Redls to cache commonly read items from the database.
Configure the Lambda functions to connect to ElastiCache for reads.
C. Add an Aurora Replica as a reader node.
Configure the Lambda functions to connect to the reader endpoint of the OB cluster rather than

lo the writer endpoint.

D. Use Amazon ROS Proxy to create a proxy.
Set the DB cluster as the target database.
Configure the Lambda functions lo connect to the proxy rather than to the DB cluster.

Answer: D

QUESTION 88
A company is building a containerized application on premises and decides to move the application to AWS.
The application will have thousands of users soon after li is deployed.
The company Is unsure how to manage the deployment of containers at scale. The company needs to deploy the containerized application in a highly available architecture that minimizes operational overhead.
Which solution will meet these requirements?

A. Store container images In an Amazon Elastic Container Registry (Amazon ECR) repository.
Use an Amazon Elastic Container Service (Amazon ECS) cluster with the AWS Fargate launch type to run the containers.
Use target tracking to scale automatically based on demand.
B. Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository.
Use an Amazon Elastic Container Service (Amazon ECS) cluster with the Amazon EC2 launch type to run the containers.
Use target tracking to scale automatically based on demand.
C. Store container images in a repository that runs on an Amazon EC2 instance.
Run the containers on EC2 instances that are spread across multiple Availability Zones.
Monitor the average CPU utilization in Amazon CloudWatch.
Launch new EC2 instances as needed.
D. Create an Amazon EC2 Amazon Machine Image (AMI) that contains the container image.
Launch EC2 Instances in an Auto Scaling group across multiple Availability Zones.
Use an Amazon CloudWatch alarm to scale out EC2 instances when the average CPU utilization threshold is breached.

Answer: A
Explanation:
AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances. With Fargate, you no longer have to provision, configure, or scale clusters of virtual machines to run containers. This removes the need to choose server types, decide when to scale your clusters, or optimize cluster packing.

QUESTION 89
A company's application Is having performance issues. The application staleful and needs to complete m-memory tasks on Amazon EC2 instances. The company used AWS CloudFormation to deploy infrastructure and used the M5 EC2 Instance family. As traffic increased, the application performance degraded. Users are reporting delays when the users attempt to access the application.
Which solution will resolve these issues in the MOST operationally efficient way?

A. Replace the EC2 Instances with T3 EC2 instances that run in an Auto Scaling group.
Made the changes by using the AWS Management Console.
B. Modify the CloudFormation templates to run the EC2 instances in an Auto Scaling group.
Increase the desired capacity and the maximum capacity of the Auto Scaling group manually when an increase is necessary.

C. Modify the CloudFormation templates.
   Replace the EC2 instances with R5 EC2 instances.
   Use Amazon CloudWatch built-in EC2 memory metrics to track the application performance for future capacity planning.
D. Modify the CloudFormation templates.
   Replace the EC2 instances with R5 EC2 instances.
   Deploy the Amazon CloudWatch agent on the EC2 instances to generate custom application latency metrics for future capacity planning.

Answer: D
Explanation:
EC2 do not provide by default memory metrics to CloudWatch and require the CloudWatch Agent to be installed on the monitored instances.
https://aws.amazon.com/premiumsupport/knowledge-center/cloudwatch-memory-metrics-ec2/

QUESTION 90
An ecommerce company has an order-processing application that uses Amazon API Gateway and an AWS Lambda function.
The application stores data in an Amazon Aurora PostgreSQL database.
During a recent sales event, a sudden surge in customer orders occurred.
Some customers experienced timeouts and the application did not process the orders of those customers.
A solutions architect determined that the CPU utilization and memory utilization were high on the database because of a large number of open connections.
The solutions architect needs to prevent the timeout errors while making the least possible changes to the application.
Which solution will meet these requirements?

A. Configure provisioned concurrency for the Lambda function.
   Modify the database to be a global database in multiple AWS Regions.
B. Use Amazon RDS Proxy to create a proxy for the database.
   Modify the Lambda function to use the RDS Proxy endpoint instead of the database endpoint.
C. Create a read replica for the database in a different AWS Region.
   Use query string parameters in API Gateway to route traffic to the read replica.
D. Migrate the data from Aurora PostgreSQL to Amazon DynamoDB by using AWS Database.
   Migration Service (AWS DMS) Modify the Lambda function to use the OynamoDB table.

Answer: B
Explanation:
Many applications, including those built on modern serverless architectures, can have a large number of open connections to the database server and may open and close database connections at a high rate, exhausting database memory and compute resources. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability.
https://aws.amazon.com/id/rds/proxy/

QUESTION 91
A company runs a global web application on Amazon EC2 instances behind an Application Load Balancer.
The application stores data in Amazon Aurora.
The company needs to create a disaster recovery solution and can tolerate up to 30 minutes of downtime and potential data loss.
The solution does not need to handle the load when the primary infrastructure is healthy.

What should a solutions architect do to meet these requirements?

A. Deploy the application with the required infrastructure elements in place.
Use Amazon Route 53 to configure active-passive failover.
Create an Aurora Replica in a second AWS Region.
B. Host a scaled-down deployment of the application in a second AWS Region.
Use Amazon Route 53 to configure active-active failover.
Create an Aurora Replica in the second Region.
C. Replicate the primary infrastructure in a second AWS Region.
Use Amazon Route 53 to configure active-active failover.
Create an Aurora database that is restored from the latest snapshot.
D. Back up data with AWS Backup.
Use the backup to create the required infrastructure in a second AWS Region.
Use Amazon Route 53 to configure active-passive failover.
Create an Aurora second primary instance in the second Region.

Answer: A
Explanation:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html

QUESTION 92
A company wants to measure the effectiveness of its recent marketing campaigns.
The company performs batch processing on csv files of sales data and stores the results in an Amazon S3 bucket once every hour.
The S3 bipetabytes of objects. The company runs one-time queries in Amazon Athena to determine which products are most popular on a particular date for a particular region Queries sometimes fail or take longer than expected to finish.
Which actions should a solutions architect take to improve the query performance and reliability? (Choose two.)

A. Reduce the S3 object sizes to less than 126 MB
B. Partition the data by date and region in Amazon S3
C. Store the files as large, single objects in Amazon S3.
D. Use Amazon Kinosis Data Analytics to run the Queries as pan of the batch processing operation
E. Use an AWS duo extract, transform, and load (ETL) process to convert the csv files into Apache Parquet format.

Answer: CE

QUESTION 93
A company is running several business applications in three separate VPCs within the us-east-1 Region. The applications must be able to communicate between VPCs. The applications also must be able to consistently send hundreds of gigabytes of data each day to a latency-sensitive application that runs in a single on- premises data center.
A solutions architect needs to design a network connectivity solution that maximizes cost-effectiveness.
Which solution meets these requirements?

A. Configure three AWS Site-to-Site VPN connections from the data center to AWS.
Establish connectivity by configuring one VPN connection for each VPC.
B. Launch a third-party virtual network appliance in each VPC.
Establish an iPsec VPN tunnel between the Data center and each virtual appliance.

C. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1.
   Establish connectivity by configuring each VPC to use one of the Direct Connect connections.
D. Set up one AWS Direct Connect connection from the data center to AWS.
   Create a transit gateway, and attach each VPC to the transit gateway.
   Establish connectivity between the Direct Connect connection and the transit gateway.

Answer: D
Explanation:
https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html

QUESTION 94
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
Explanation:
Priority: Use separate queues to provide prioritization of work.

QUESTION 95
A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon EC2 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
Explanation:
as CloudFront can help provide the best experience for global users. CloudFront integrates seamlessly with ALB and provides and option to use custom DNS and SSL certs.

QUESTION 96
A company has 150 TB of archived image data stored on-premises that needs to be moved 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
Explanation:
eg.6 hrs night
6 hrs*60min/hr=360 min
360 min*60 sec/min=21600 sec
100 Mbps*21600 s=2160000Mb
or 2160 Gb or 2.1 TB can only be done

So, for 150 TB, we can use 2 X Snowball Edge Storage Optimised devices.

Size of Snowball Edge Storage Optimised device=80 TB Size of Snowball Edge Compute Optimised device= 40 TB Size of Snowcone =8 TB
Size of Snowmobile =100 PB (1 PB=1000 TB)

Q: How should I choose between Snowmobile and Snowball?
To migrate large datasets of 10PB or more in a single location, you should use Snowmobile. For datasets less than 10PB or distributed in multiple locations, you should use Snowball. In addition, you should evaluate the amount of available bandwidth in your network backbone. If you have a high speed backbone with hundreds of Gb/s of spare throughput, then you can use Snowmobile to migrate the large datasets all at once. If you have limited bandwidth on your backbone, you should consider using multiple Snowballs to migrate the data incrementally.

QUESTION 97
A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned 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
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/
"Use a multivalue answer routing policy to help distribute DNS responses across multiple resources.
For example, use multivalue answer routing when you want to associate your routing records with a Route 53 health check."
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-multivalue

QUESTION 98
A company wants to use AWS Systems Manager to manage a fleet of Amazon EC2 instances. According to the company's security requirements, no EC2 instances can have internet access. A solutions architect needs to design network connectivity from the EC2 instances to Systems Manager while fulfilling this security obligation.
Which solution will meet these requirements?

A. Deploy the EC2 instances into a private subnet with no route to the internet.
B. Configure an interface VPC endpoint for Systems Manager.
Update routes to use the endpoint.
C. Deploy a NAT gateway into a public subnet.
Configure private subnets with a default route to the NAT gateway.
D. Deploy an internet gateway.
Configure a network ACL to deny traffic to all destinations except Systems Manager.

Answer: B
Explanation:
VPC Peering connections
VPC interface endpoints can be accessed through both intra-Region and inter-Region VPC peering connections.
VPC Gateway Endpoint connections can't be extended out of a VPC. Resources on the other side of a VPC peering connection in your VPC can't use the gateway endpoint to communicate with resources in the gateway endpoint service.
Reference: https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-create-vpc.html

QUESTION 99
A company needs to build a reporting solution on AWS. The solution must support SQL queries that data analysts run on the data.
The data analysts will run lower than 10 total queries each day. The company generates 3 GB of new data daily in an on-premises relational database. This data needs to be transferred to AWS to perform reporting tasks.
What should a solutions architect recommend to meet these requirements at the LOWEST cost?

A. Use AWS Database Migration Service (AWS DMS) to replicate the data from the on-premises database into Amazon S3.
Use Amazon Athena to query the data.
B. Use an Amazon Kinesis Data Firehose delivery stream to deliver the data into an Amazon Elasticsearch Service (Amazon ES) cluster Run the queries in Amazon ES.
C. Export a daily copy of the data from the on-premises database.
Use an AWS Storage Gateway file gateway to store and copy the export into Amazon S3.
Use an Amazon EMR cluster to query the data.
D. Use AWS Database Migration Service (AWS DMS) to replicate the data from the on-premises database and load it into an Amazon Redshift cluster.
Use the Amazon Redshift cluster to query the data.

Answer: D
Explanation:
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.Redshift.html
AWS DMS cannot migrate or replicate changes to a schema with a name that begins with underscore (_). If you have schemas that have a name that begins with an underscore, use mapping transformations to rename the schema on the target.

Amazon Redshift doesn't support VARCHARs larger than 64 KB. LOBs from traditional databases can't be stored in Amazon Redshift.
Applying a DELETE statement to a table with a multi-column primary key is not supported when any of the primary key column names use a reserved word. Go here to see a list of Amazon Redshift reserved words.
You may experience performance issues if your source system performs UPDATE operations on the primary key of a source table. These performance issues occur when applying changes to the target. This is because UPDATE (and DELETE) operations depend on the primary key value to identify the target row. If you update the primary key of a source table, your task log will contain messages like the following:
Update on table 1 changes PK to a PK that was previously updated in the same bulk update.
DMS doesn't support custom DNS names when configuring an endpoint for a Redshift cluster, and you need to use the Amazon provided DNS name. Since the Amazon Redshift cluster must be in the same AWS account and Region as the replication instance, validation fails if you use a custom DNS endpoint.

QUESTION 100
A company wants to monitor its AWS costs for financial review. The cloud operations team is designing an architecture in the AWS Organizations management account to query AWS Cost and Usage Reports for all member accounts.
The team must run this query once a month and provide a detailed analysis of the bill.
Which solution is the MOST scalable and cost-effective way to meet these requirements?

A. Enable Cost and Usage Reports in the management account.
Deliver reports to Amazon Kinesis.
Use Amazon EMR for analysis.
B. Enable Cost and Usage Reports in the management account.
Deliver the reports to Amazon S3.
Use Amazon Athena for analysis.
C. Enable Cost and Usage Reports for member accounts.
Deliver the reports to Amazon S3.
Use Amazon Redshift for analysis.
D. Enable Cost and Usage Reports for member accounts.
Deliver the reports to Amazon Kinesis.
Use Amazon QuickSight for analysis.

Answer: C
Explanation:
https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html
If you are an administrator of an AWS Organizations management account and do not want any of the member accounts in your Organization to set-up a CUR you can do one of the following:
(Recommended) If you've opted into Organizations with all features enabled, you can apply a Service Control Policy (SCP). Note that SCPs only apply to member accounts and if you want to restrict any IAM users associated with the management account from setting up a CUR, you'll need to adjust their specific IAM permissions. SCPs also are not retroactive, so they will not de-activate any CURs a member account may have set-up prior to the SCP being applied.
Submit a customer support case to block access to billing data in the Billing console for member accounts. This is a list of organizations where the payer account prevents member accounts in its organization from viewing billing data on the Bills and Invoices pages. This also prevents those accounts from setting up Cost and Usage Reports. This option is only available for organizations without all features enabled. Please note that if you have already opted into this to prevent member accounts from viewing bills and invoices in the Billing Console, you do not need to request this access again. Those same member accounts will also be prevented from setting up a Cost and Usage Report.

QUESTION 101
A company collects data for temperature, humidity, and atmospheric pressure in cities across multiple continents. The average volume of data that the company collects from each site daily is 500 GB. Each site has a high-speed Internet connection.
The company wants to aggregate the data from all these global sites as quickly as possible in a single Amazon S3 bucket. The solution must minimize operational complexity.
Which solution meets these requirements?

A. Turn on S3 Transfer Acceleration on the destination S3 bucket.
Use multipart uploads to directly upload site data to the destination S3 bucket.
B. Upload the data from each site to an S3 bucket in the closest Region.
Use S3 Cross-Region Replication to copy objects to the destination S3 bucket.
Then remove the data from the origin S3 bucket.
C. Schedule AWS Snowball Edge Storage Optimized device jobs daily to transfer data from each site to the closest Region.
Use S3 Cross-Region Replication to copy objects to the destination S3 bucket.
D. Upload the data from each site to an Amazon EC2 instance in the closest Region.
Store the data in an Amazon Elastic Block Store (Amazon EBS) volume.
At regular intervals, take an EBS snapshot and copy it to the Region that contains the destination S3 bucket.
Restore the EBS volume in that Region.

Answer: A
Explanation:
You might want to use Transfer Acceleration on a bucket for various reasons, including the following:
- You have customers that upload to a centralized bucket from all over the world.
- You transfer gigabytes to terabytes of data on a regular basis across continents.
- You are unable to utilize all of your available bandwidth over the Internet when uploading to Amazon S3.

https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html
https://aws.amazon.com/s3/transfer-acceleration/#:~:text=S3%20Transfer%20Acceleration%20(S3TA)%20reduces,to%20S3%20for%20remote%20applications
"Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects. Customers who have either web or mobile applications with widespread users or applications hosted far away from their S3 bucket can experience long and variable upload and download speeds over the Internet"

https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html
"Improved throughput -You can upload parts in parallel to improve throughput."

QUESTION 102
A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket Queries will be simple and will run on-demand.
A solutions architect needs to perform the analysis with minimal changes to the existing architecture.
What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed

B. Use Amazon CloudWatch Logs to store the logs
Run SQL queries as needed from the Amazon CloudWatch console
C. Use Amazon Athena directly with Amazon S3 to run the queries as needed
D. Use AWS Glue to catalog the logs
Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries as needed

Answer: C
Explanation:
Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds.
https://docs.aws.amazon.com/athena/latest/ug/what-is.html

QUESTION 103
A company uses AWS Organizations to manage multiple AWS accounts for different departments. The management account has an Amazon S3 bucket that contains project reports. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.
Which solution meets these requirements with the LEAST amount of operational overhead?

A. Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.
B. Create an organizational unit (OU) for each department.
Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.
C. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events.
Update the S3 bucket policy accordingly.
D. Tag each user that needs access to the S3 bucket.
Add the aws:PrincipalTag global condition key to the S3 bucket policy.

Answer: A
Explanation:
https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-principals/

The aws:PrincipalOrgID global key provides an alternative to listing all the account IDs for all AWS accounts in an organization.
For example, the following Amazon S3 bucket policy allows members of any account in the XXX organization to add an object into the examtopics bucket.

```
{"Version": "2020-09-10",
"Statement": {
"Sid": "AllowPutObject",
"Effect": "Allow",
"Principal": "*",
"Action": "s3:PutObject",
"Resource": "arn:aws:s3:::examtopics/*",
"Condition": {"StringEquals":
{"aws:PrincipalOrgID":["XXX"]}}}}
```

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html

QUESTION 104

An application runs on an Amazon EC2 instance in a VPC. The application processes logs that are stored in an Amazon S3 bucket. The EC2 instance needs to access the S3 bucket without connectivity to the internet.
Which solution will provide private network connectivity to Amazon S3?

A. Create a gateway VPC endpoint to the S3 bucket.
B. Stream the logs to Amazon CloudWatch Logs. Export the logs to the S3 bucket.
C. Create an instance profile on Amazon EC2 to allow S3 access.
D. Create an Amazon API Gateway API with a private link to access the S3 endpoint.

Answer: A
Explanation:
You can access Amazon S3 from your VPC using gateway VPC endpoints. After you create the gateway endpoint, you can add it as a target in your route table for traffic destined from your VPC to Amazon S3.
You can create a policy that restricts access to specific IP address ranges by using the aws:VpcSourceIp condition key.
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html

QUESTION 105

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 EFS
D. Configure the Application Load Balancer to send the request to both servers.
Return each document from the correct server.

Answer: C
Explanation:
Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your VPC, through the Network File System versions 4.0 and 4.1 (NFSv4) protocol. We recommend using a current generation Linux NFSv4.1 client, such as those found in the latest Amazon Linux, Redhat, and Ubuntu AMIs, in conjunction with the Amazon EFS Mount Helper. For instructions, see Using the amazon-efs-utils Tools.
For a list of Amazon EC2 Linux Amazon Machine Images (AMIs) that support this protocol, see NFS Support. For some AMIs, you'll need to install an NFS client to mount your file system on your Amazon EC2 instance. For instructions, see Installing the NFS Client. You can access your Amazon EFS file system concurrently from multiple NFS clients, so applications that scale beyond a single connection can access a file system. Amazon EC2 instances running in multiple Availability Zones within the same AWS Region can access the file system, so that many users can access and share a common data source.

QUESTION 106
A company uses NFS to store large video files in on-premises network attached storage. Each video file ranges in size from 1 MB to 500 GB. The total storage is 70 TB and is no longer growing. The company decides to migrate the video files to Amazon S3. The company must migrate the video files as soon as possible while using the least possible network bandwidth.
Which solution will meet these requirements?

A. Create an S3 bucket.
Create an IAM role that has permissions to write to the S3 bucket.
Use the AWS CLI to copy all files locally to the S3 bucket.
B. Create an AWS Snowball Edge job.
Receive a Snowball Edge device on premises.
Use the Snowball Edge client to transfer data to the device.
Return the device so that AWS can import the data into Amazon S3.
C. Deploy an S3 File Gateway on premises.
Create a public service endpoint to connect to the S3 File Gateway.
Create an S3 bucket.
Create a new NFS file share on the S3 File Gateway.
Point the new file share to the S3 bucket.
Transfer the data from the existing NFS file share to the S3 File Gateway.
D. Set up an AWS Direct Connect connection between the on-premises network and AWS.
Deploy an S3 File Gateway on premises.
Create a public virtual interlace (VIF) to connect to the S3 File Gateway.
Create an S3 bucket.
Create a new NFS file share on the S3 File Gateway.
Point the new file share to the S3 bucket.
Transfer the data from the existing NFS file share to the S3 File Gateway.

Answer: B
Explanation:
Option B: As using the least possible network bandwidth.
On a Snowball Edge device you can copy files with a speed of up to 100 Gbps. 70 TB will take around 5600 seconds, so very quickly, less than 2 hours. The downside is that it'll take between 4-6 working days to receive the device and then another 2-3 working days to send it back and for AWS to move the data onto S3 once it reaches them. Total time: 6-9 working days. Bandwidth used: 0.

QUESTION 107
A company has an application that ingests incoming messages. Dozens of other applications and microservices then quickly consume these messages. The number of messages varies drastically and sometimes increases suddenly to 100,000 each second. The company wants to decouple the solution and increase scalability.
Which solution meets these requirements?

A. Persist the messages to Amazon Kinesis Data Analytics.
Configure the consumer applications to read and process the messages.
B. Deploy the ingestion application on Amazon EC2 instances in an Auto Scaling group to scale the number of EC2 instances based on CPU metrics.
C. Write the messages to Amazon Kinesis Data Streams with a single shard.
Use an AWS Lambda function to preprocess messages and store them in Amazon DynamoDB.
Configure the consumer applications to read from DynamoDB to process the messages.
D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SOS) subscriptions.
Configure the consumer applications to process the messages from the queues.

Answer: D
Explanation:
"SNS Standard Topic"
Maximum throughput: Standard topics support a nearly unlimited number of messages per second.
https://aws.amazon.com/sns/features/
"SQS Standard Queue"
Unlimited Throughput: Standard queues support a nearly unlimited number of transactions per second (TPS) per API action.
https://aws.amazon.com/sqs/features/

QUESTION 108
A company is migrating a distributed application to AWS. The application serves variable workloads. The legacy platform consists of a primary server that coordinates jobs across multiple compute nodes. The company wants to modernize the application with a solution that maximizes resiliency and scalability.
How should a solutions architect design the architecture to meet these requirements?

A. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs.
Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group.
Configure EC2 Auto Scaling to use scheduled scaling.
B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs.
Implement the compute nodes with Amazon EC2 Instances that are managed in an Auto Scaling group.
Configure EC2 Auto Scaling based on the size of the queue.
C. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group.
Configure AWS CloudTrail as a destination for the fobs .
Configure EC2 Auto Scaling based on the load on the primary server.
D. implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group.
Configure Amazon EventBridge (Amazon CloudWatch Events) as a destination for the jobs.
Configure EC2 Auto Scaling based on the load on the compute nodes.

Answer: B
Explanation:
Amazon SQS is a fully managed message queue service that enables you to decouple and scale microservices, distributed systems, and serverless applications. By using SQS as the destination for the jobs, you can decouple the primary server from the compute nodes, which will increase resiliency and scalability.
Amazon EC2 Auto Scaling is a service that automatically increases or decreases the number of EC2 instances in your application based on demand. By configuring EC2 Auto Scaling to scale based on the size of the SQS queue, you can ensure that the number of compute nodes is sufficient to handle the workload.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html

QUESTION 109
A company is running an SMB file server in its data center. The file server stores large files that are accessed frequently for the first few days after the files are created. After 7 days the files are

rarely accessed.

The total data size is increasing and is close to the company's total storage capacity. A solutions architect must increase the company's available storage space without losing low-latency access to the most recently accessed files. The solutions architect must also provide file lifecycle management to avoid future storage issues.

Which solution will meet these requirements?

A. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.
B. Create an Amazon S3 File Gateway to extend the company's storage space.
   Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.
C. Create an Amazon FSx for Windows File Server file system to extend the company's storage space.
D. Install a utility on each user's computer to access Amazon S3.
   Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.

Answer: B
Explanation:
Amazon S3 File Gateway offers SMB or NFS-based access to data in Amazon S3 with local caching.
https://docs.aws.amazon.com/filegateway/latest/files3/CreatingAnSMBFileShare.html

QUESTION 110
A company is building an ecommerce web application on AWS. The application sends information about new orders to an Amazon API Gateway REST API to process. The company wants to ensure that orders are processed in the order that they are received.

Which solution will meet these requirements?

A. Use an API Gateway integration to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when the application receives an order.
   Subscribe an AWS Lambda function to the topic to perform processing.
B. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue when the application receives an order.
   Configure the SQS FIFO queue to invoke an AWS Lambda function for processing.
C. Use an API Gateway authorizer to block any requests while the application processes an order.
D. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue when the application receives an order.
   Configure the SQS standard queue to invoke an AWS Lambda function for processing.

Answer: B
Explanation:
SQS FIFO queue guarantees message order.
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html

QUESTION 111
A company has an application that runs on Amazon EC2 instances and uses an Amazon Aurora database. The EC2 instances connect to the database by using user names and passwords that are stored locally in a file. The company wants to minimize the operational overhead of credential management.
What should a solutions architect do to accomplish this goal?

A. Use AWS Secrets Manager.
Turn on automatic rotation.
B. Use AWS Systems Manager Parameter Store.
Turn on automatic rotation.
C. Create an Amazon S3 bucket lo store objects that are encrypted with an AWS Key.
Management Service (AWS KMS) encryption key.
Migrate the credential file to the S3 bucket.
Point the application to the S3 bucket.
D. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume or each EC2 instance.
Attach the new EBS volume to each EC2 instance.
Migrate the credential file to the new EBS volume.
Point the application to the new EBS volume.

Answer: A
Explanation:
AWS Secrets Manager is a secrets management service that helps you protect access to your applications, services, and IT resources. This service enables you to rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.
https://aws.amazon.com/cn/blogs/security/how-to-connect-to-aws-secrets-manager-service-within-a-virtual-private-cloud/
https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/

QUESTION 112
A global company hosts its web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The web application has static data and dynamic data. The company stores its static data in an Amazon S3 bucket. The company wants to improve performance and reduce latency for the static data and dynamic data. The company is using its own domain name registered with Amazon Route 53.
What should a solutions architect do to meet these requirements?

A. Create an Amazon CloudFront distribution that has the S3 bucket and the ALB as origins.
Configure Route 53 to route traffic to the CloudFront distribution.
B. Create an Amazon CloudFront distribution that has the ALB as an origin.
Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint.
Configure Route 53 to route traffic to the CloudFront distribution.
C. Create an Amazon CloudFront distribution that has the S3 bucket as an origin.
Create an AWS Global Accelerator standard accelerator that has the ALB and the CloudFront distribution as endpoints.
Create a custom domain name that points to the accelerator DNS name.
Use the custom domain name as an endpoint for the web application.
D. Create an Amazon CloudFront distribution that has the ALB as an origin.
Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint.
Create two domain names.
Point one domain name to the CloudFront DNS name for dynamic content.
Point the other domain name to the accelerator DNS name for static content.
Use the domain names as endpoints for the web application.

Answer: A
Explanation:
AWS Global Accelerator vs CloudFront
• They both use the AWS global network and its edge locations around the world
• Both services integrate with AWS Shield for DDoS protection.

- CloudFront
- Improves performance for both cacheable content (such as images and videos)
- Dynamic content (such as API acceleration and dynamic site delivery)
- Content is served at the edge
- Global Accelerator
- Improves performance for a wide range of applications over TCP or UDP
- Proxying packets at the edge to applications running in one or more AWS Regions.
- Good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP
- Good for HTTP use cases that require static IP addresses
- Good for HTTP use cases that required deterministic, fast regional failover

QUESTION 113
A company performs monthly maintenance on its AWS infrastructure. During these maintenance activities, the company needs to rotate the credentials tor its Amazon ROS tor MySQL databases across multiple AWS Regions.
Which solution will meet these requirements with the LEAST operational overhead?

A. Store the credentials as secrets in AWS Secrets Manager.
Use multi-Region secret replication for the required Regions.
Configure Secrets Manager to rotate the secrets on a schedule.
B. Store the credentials as secrets in AWS Systems Manager by creating a secure string parameter.
Use multi-Region secret replication for the required Regions.
Configure Systems Manager to rotate the secrets on a schedule.
C. Store the credentials in an Amazon S3 bucket that has server-side encryption (SSE) enabled.
Use Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function to rotate the credentials.
D. Encrypt the credentials as secrets by using AWS Key Management Service (AWS KMS) multi-Region customer managed keys.
Store the secrets in an Amazon DynamoDB global table.
Use an AWS Lambda function to retrieve the secrets from DynamoDB.
Use the RDS API to rotate the secrets.

Answer: A
Explanation:
AWS Secrets Manager meant for storing secrets, Capability to force rotation of secrets every X days, Automate generation of secrets on rotation (uses Lambda), Integration with Amazon RDS (MySQL, PostgreSQL, Aurora).
https://aws.amazon.com/blogs/security/how-to-replicate-secrets-aws-secrets-manager-multiple-regions/

QUESTION 114
A company is planning to run a group of Amazon EC2 instances that connect to an Amazon Aurora database. The company has built an AWS CloudFormation template to deploy the EC2 instances and the Aurora DB cluster. The company wants to allow the instances to authenticate to the database in a secure way. The company does not want to maintain static database credentials.
Which solution meets these requirements with the LEAST operational effort?

A. Create a database user with a user name and password.
Add parameters for the database user name and password to the CloudFormation template.
Pass the parameters to the EC2 instances when the instances are launched.
B. Create a database user with a user name and password.

Store the user name and password in AWS Systems Manager Parameter Store.
Configure the EC2 instances to retrieve the database credentials from Parameter Store.

C. Configure the DB cluster to use IAM database authentication.
Create a database user to use with IAM authentication.
Associate a role with the EC2 instances to allow applications on the instances to access the database.
D. Configure the DB cluster to use IAM database authentication with an IAM user.
Create a database user that has a name that matches the IAM user.
Associate the IAM user with the EC2 instances to allow applications on the instances to access the database.

Answer: A
Explanation:
Finally, you need a way to instruct CloudFormation to complete stack creation only after all the services (such as Apache and MySQL) are running and not after all the stack resources are created. In other words, if you use the template from the earlier section to launch a stack, CloudFormation sets the status of the stack as CREATE_COMPLETE after it successfully creates all the resources. However, if one or more services failed to start, CloudFormation still sets the stack status as CREATE_COMPLETE. To prevent the status from changing to CREATE_COMPLETE until all the services have successfully started, you can add a CreationPolicy attribute to the instance. This attribute puts the instance's status in CREATE_IN_PROGRESS until CloudFormation receives the required number of success signals or the timeout period is exceeded, so you can control when the instance has been successfully created.
Reference:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html

QUESTION 115
A solutions architect is designing a shared storage solution for a web application that is deployed across multiple Availability Zones. The web application runs on
Amazon EC2 instances that are in an Auto Scaling group. The company plans to make frequent changes to the content. The solution must have strong consistency in returning the new content as soon as the changes occur.
Which solutions meet these requirements? (Choose two.)

A. Use AWS Storage Gateway Volume Gateway Internet Small Computer Systems Interface (ISCSI) block storage that is mounted to the individual EC2 instances.
B. Create an Amazon Elastic File System (Amazon EFS) file system.
Mount the EFS file system on the individual EC2 instances.
C. Create a shared Amazon Elastic Block Store (Amazon EBS) volume.
Mount the EBS volume on the individual EC2 instances.
D. Use AWS DataSync to perform continuous synchronization of data between EC2 hosts in the Auto Scaling group.
E. Create an Amazon S3 bucket to store the web content.
Set the metadata for the Cache-Control header to no-cache.
Use Amazon CloudFront to deliver the content.

Answer: AB
Explanation:
Reference:
https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html
https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html
In this example, the EC2 instance in the us-west-2c Availability Zone will pay EC2 data access charges for accessing a mount target in a different Availability Zone. Creating this setup works as

follows:
1. Create your Amazon EC2 resources and launch your Amazon EC2 instance. For more information about Amazon EC2, see Amazon EC2.
2. Create your Amazon EFS file system with One Zone storage.
3. Connect to each of your Amazon EC2 instances, and mount the Amazon EFS file system using the same mount target for each instance.

QUESTION 116
A company that operates a web application on premises is preparing to launch a newer version of the application on AWS. The company needs to route requests to either the AWS-hosted or the on-premises-hosted application based on the URL query string. The on-premises application is not available from the internet, and a VPN connection is established between Amazon VPC and the company's data center. The company wants to use an Application Load Balancer (ALB) for this launch.
Which solution meets these requirements?

A. Use two ALBs: one for on-premises and one for the AWS resource.
Add hosts to each target group of each ALB.
Route with Amazon Route 53 based on the URL query string.
B. Use two ALBs: one for on-premises and one for the AWS resource.
Add hosts to the target group of each ALB.
Create a software router on an EC2 instance based on the URL query string.
C. Use one ALB with two target groups: one for the AWS resource and one for on premises.
Add hosts to each target group of the ALB.
Configure listener rules based on the URL query string.
D. Use one ALB with two AWS Auto Scaling groups: one for the AWS resource and one for on premises.
Add hosts to each Auto Scaling group.
Route with Amazon Route 53 based on the URL query string.

Answer: C
Explanation:
https://aws.amazon.com/blogs/aws/new-advanced-request-routing-for-aws-application-load-balancers/
The host-based routing feature allows you to write rules that use the Host header to route traffic to the desired target group.
Today we are extending and generalizing this feature, giving you the ability to write rules (and route traffic) based on standard and custom HTTP headers and methods, the query string, and the source IP address.

QUESTION 117
A company wants to move from many standalone AWS accounts to a consolidated, multi-account architecture. The company plans to create many new AWS accounts for different business units. The company needs to authenticate access to these AWS accounts by using a centralized corporate directory service
Which combination of actions should a solutions architect recommend to meet these requirements? (Select TWO)

A. Create a new organization in AWS Organizations with all features turned on.
Create the new AWS accounts in the organization.
B. Set up an Amazon Cognito identity pool.
Configure AWS Single Sign-On to accept Amazon Cognito authentication.
C. Configure a service control policy (SCP) to manage the AWS accounts.

Add AWS Single Sign-On to AWS Directory Service.

D. Create a new organization in AWS Organizations.
Configure the organization's authentication mechanism to use AWS Directory Service directly.
E. Set up AWS Single Sign-On (AWS SSO) in the organization.
Configure AWS SSO and integrate it with the company's corporate directory service.

Answer: BC
Explanation:
SCPs affect only IAM users and roles that are managed by accounts that are part of the organization. SCPs don't affect resource-based policies directly. They also don't affect users or roles from accounts outside the organization. For example, consider an Amazon S3 bucket that's owned by account A in an organization. The bucket policy (a resource-based policy) grants access to users from account B outside the organization. Account A has an SCP attached. That SCP doesn't apply to those outside users in account B. The SCP applies only to users that are managed by account A in the organization.

An SCP restricts permissions for IAM users and roles in member accounts, including the member account's root user. Any account has only those permissions permitted by every parent above it. If a permission is blocked at any level above the account, either implicitly (by not being included in an Allow policy statement) or explicitly (by being included in a Deny policy statement), a user or role in the affected account can't use that permission, even if the account administrator attaches the AdministratorAccess IAM policy with */* permissions to the user.

Reference:
https://aws.amazon.com/cognito/
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

QUESTION 118
An entertainment company is using Amazon DynamoDB to store media metadata.
The application is read intensive and experiencing delays.
The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application.
What should a solutions architect recommend to meet this requirement?

A. Use Amazon ElastiCache for Redis
B. Use Amazon DynamoDB Accelerate (DAX)
C. Replicate data by using DynamoDB global tables
D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled

Answer: B
Explanation:
Though DynamoDB offers consistent single-digit-millisecond latency, DynamoDB + DAX takes performance to the next level with response times in microseconds for millions of requests per second for read-heavy workloads. With DAX, your applications remain fast and responsive, even when a popular event or news story drives unprecedented request volumes your way. No tuning required.

QUESTION 119
A company has an application that provides marketing services to stores. The services are based on previous purchases by store customers. The stores upload transaction data to the company through SFTP, and the data is processed and analyzed to generate new marketing offers. Some of the files can exceed 200 GB in size.

Recently, the company discovered that some of the stores have uploaded files that contain personally identifiable information (PII) that should not have been included. The company wants administrators to be alerted if PII is shared again. The company also wants to automate remediation.

What should a solutions architect do to meet these requirements with the LEAST development effort?

A. Use an Amazon S3 bucket as a secure transfer point.
Use Amazon Inspector to scan me objects in the bucket.
If objects contain Pll, trigger an S3 Lifecycle policy to remove the objects that contain Pll.
B. Use an Amazon S3 bucket as a secure transfer point.
Use Amazon Macie to scan the objects in the bucket.
If objects contain Pll, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects mat contain Pll.
C. Implement custom scanning algorithms in an AWS Lambda function.
Trigger the function when objects are loaded into the bucket.
If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
D. Implement custom scanning algorithms in an AWS Lambda function.
Trigger the function when objects are loaded into the bucket.
If objects contain Pll, use Amazon Simple Email Service (Amazon STS) to trigger a notification to the administrators and trigger on S3 Lifecycle policy to remove the objects mot contain PII.

Answer: B
Explanation:
To support integration with other services and systems, Macie publishes findings to Amazon EventBridge as finding events.
https://aws.amazon.com/es/macie/faq/

QUESTION 120
A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

A. Purchase Reserved instances that specify the Region needed
B. Create an On Demand Capacity Reservation that specifies the Region needed
C. Purchase Reserved instances that specify the Region and three Availability Zones needed
D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed

Answer: D
Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html
"When you create a Capacity Reservation, you specify:
The Availability Zone in which to reserve the capacity"

QUESTION 121
A company's website uses an Amazon EC2 instance store for its catalog of items. The company wants to make sure that the catalog is highly available and that the catalog is stored in a durable location.

What should a solutions architect do to meet these requirements?

A. Move the catalog to Amazon ElastiCache for Redis.
B. Deploy a larger EC2 instance with a larger instance store.
C. Move the catalog from the instance store to Amazon S3 Glacier Deep Archive.
D. Move the catalog to an Amazon Elastic File System (Amazon EFS) file system.

Answer: D
Explanation:
Instance store is not durable, if it goes down then instance store data is lost.
EFS is the only option here that will provide high availability and durability, plus it can be accessed by multiple instances at the same time.

QUESTION 122
A company stores call transcript files on a monthly basis. Users access the files randomly within 1 year of the call, but users access the files infrequently after 1 year. The company wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1-year-old as quickly as possible. A delay in retrieving older files is acceptable.

Which solution will meet these requirements MOST cost-effectively?

A. Store individual files with tags in Amazon S3 Glacier Instant Retrieval.
Query the tags to retrieve the files from S3 Glacier Instant Retrieval.
B. Store individual files in Amazon S3 Intelligent-Tiering.
Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year.
Query and retrieve the files that are in Amazon S3 by using Amazon Athena.
Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.
C. Store individual files with tags in Amazon S3 Standard storage.
Store search metadata for each archive in Amazon S3 Standard storage.
Use S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year.
Query and retrieve the files by searching for metadata from Amazon S3.
D. Store individual files in Amazon S3 Standard storage.
Use S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year.
Store search metadata in Amazon RDS. Query the files from Amazon RDS.
Retrieve the files from S3 Glacier Deep Archive.

Answer: B
Explanation:
Users access the files randomly
S3 Intelligent-Tiering is the ideal storage class for data with unknown, changing, or unpredictable access patterns, independent of object size or retention period. You can use S3 Intelligent-Tiering as the default storage class for virtually any workload, especially data lakes, data analytics, new applications, and user-generated content.
https://aws.amazon.com/fr/s3/storage-classes/intelligent-tiering/

QUESTION 123
A company has a production workload that runs on 1,000 Amazon EC2 Linux instances. The workload is powered by third-party software. The company needs to patch the third-party software on all EC2 instances as quickly as possible to remediate a critical security vulnerability.

What should a solutions architect do to meet these requirements?

A. Create an AWS Lambda function to apply the patch to all EC2 instances.
B. Configure AWS Systems Manager Patch Manager to apply the patch to all EC2 instances.
C. Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.
D. Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances.

Answer: D
Explanation:
For Linux-based operating system types that report a severity level for patches, Patch Manager uses the severity level reported by the software publisher for the update notice or individual patch. Patch Manager doesn't derive severity levels from third-party sources, such as the Common Vulnerability Scoring System (CVSS), or from metrics released by the National Vulnerability Database (NVD).
https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html

QUESTION 124
A company is developing an application that provides order shipping statistics for retrieval by a REST API. The company wants to extract the shipping statistics, organize the data into an easy-to-read HTML format, and send the report to several email addresses at the same time every morning.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Configure the application to send the data to Amazon Kinesis Data Firehose.
B. Use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Glue job to query the application's API for the data.
D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.
E. Store the application data in Amazon S3. Create an Amazon Simple Notification Service (Amazon SNS) topic as an S3 event destination to send the report by

Answer: BD
Explanation:
Option B fulfills the email in HTML format requirement (by SES) and D fulfills every morning schedule event requirement (by EventBridge).
https://docs.aws.amazon.com/ses/latest/dg/send-email-formatted.html

QUESTION 125
A company wants to migrate its on-premises application to AWS. The application produces output files that vary in size from tens of gigabytes to hundreds of terabytes The application data must be stored in a standard file system structure. The company wants a solution that scales automatically, is highly available, and requires minimum operational overhead.
Which solution will meet these requirements?

A. Migrate the application to run as containers on Amazon Elastic Container Service (Amazon ECS).
Use Amazon S3 for storage.
B. Migrate the application to run as containers on Amazon Elastic Kubernetes Service (Amazon

EKS).
Use Amazon Elastic Block Store (Amazon EBS) for storage.

C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group.
Use Amazon Elastic File System (Amazon EFS) for storage.

D. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group.
Use Amazon Elastic Block Store (Amazon EBS) for storage.

Answer: C

Explanation:

EFS is a standard file system, it scales automatically and is highly available.

QUESTION 126

A company needs to store its accounting records in Amazon S3. The records must be immediately accessible for 1 year and then must be archived for an additional 9 years. No one at the company, including administrative users and root users, can be able to delete the records during the entire 10-year period. The records must be stored with maximum resiliency.

Which solution will meet these requirements?

A. Store the records in S3 Glacier for the entire 10-year period.
Use an access control policy to deny deletion of the records for a period of 10 years.

B. Store the records by using S3 Intelligent-Tiering.
Use an IAM policy to deny deletion of the records.
After 10 years, change the IAM policy to allow deletion.

C. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year.
Use S3 Object Lock in compliance mode for a period of 10 years.

D. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years.

Answer: C

QUESTION 127

A company runs multiple Windows workloads on AWS. The company's employees use Windows file shares that are hosted on two Amazon EC2 instances. The file shares synchronize data between themselves and maintain duplicate copies. The company wants a highly available and durable storage solution that preserves how users currently access the files.

What should a solutions architect do to meet these requirements?

A. Migrate all the data to Amazon S3.
Set up IAM authentication for users to access files

B. Set up an Amazon S3 File Gateway.
Mount the S3 File Gateway on the existing EC2 Instances.

C. Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration.
Migrate all the data to FSx for Windows File Server.

D. Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration.
Migrate all the data to Amazon EFS.

Answer: C
Explanation:
Windows file shares = Amazon FSx for Windows File Server
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-file-shares.html

QUESTION 128
A solutions architect is developing a multiple-subnet VPC architecture. The solution will consist of six subnets in two Availability Zones. The subnets are defined as public, private and dedicated for databases. Only the Amazon EC2 instances running in the private subnets should be able to access a database.
Which solution meets these requirements?

A. Create a now route table that excludes the route to the public subnets' CIDR blocks.
Associate the route table to the database subnets.
B. Create a security group that denies ingress from the security group used by instances in the public subnets.
Attach the security group to an Amazon RDS DB instance.
C. Create a security group that allows ingress from the security group used by instances in the private subnets.
Attach the security group to an Amazon RDS DB instance.
D. Create a new peering connection between the public subnets and the private subnets.
Create a different peering connection between the private subnets and the database subnets.

Answer: C
Explanation:
Security groups are stateful. All inbound traffic is blocked by default. If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again. You cannot block specific IP address using Security groups (instead use Network Access Control Lists).

"You can specify allow rules, but not deny rules." "When you first create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group."

Source:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#VPCSecurityGroups

QUESTION 129
A company has registered its domain name with Amazon Route 53. The company uses Amazon API Gateway in the ca-central-1 Region as a public interface for its backend microservice APIs. Third-party services consume the APIs securely. The company wants to design its API Gateway URL with the company's domain name and corresponding certificate so that the third-party services can use HTTPS.

Which solution will meet these requirements?

A. Create stage variables in API Gateway with Name="Endpoint-URL" and Value="Company Domain Name" to overwrite the default URL. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).
B. Create Route 53 DNS records with the company's domain name. Point the alias record to the Regional API Gateway stage endpoint. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.
C. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the

company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region. Attach the certificate to the API Gateway endpoint.
Configure Route 53 to route traffic to the API Gateway endpoint.

D. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region. Attach the certificate to the API Gateway APIs.
Create Route 53 DNS records with the company's domain name. Point an A record to the company's domain name.

Answer: C
Explanation:
Regional custom domain names must use an SSL/TLS certificate that's in the same AWS Region as your API.
Edge-optimized custom domain names must use a certificate that's in the following Region: US East (N. Virginia) (us-east-1).
https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-regional-api-custom-domain-create.html

QUESTION 130
A company is running a popular social media website. The website gives users the ability to upload images to share with other users. The company wants to make sure that the images do not contain inappropriate content. The company needs a solution that minimizes development effort. What should a solutions architect do to meet these requirements?

A. Use Amazon Comprehend to detect inappropriate content.
Use human review for low-confidence predictions.

B. Use Amazon Rekognition to detect inappropriate content.
Use human review for low-confidence predictions.

C. Use Amazon SageMaker to detect inappropriate content.
Use ground truth to label low-confidence predictions.

D. Use AWS Fargate to deploy a custom machine learning model to detect inappropriate content.
Use ground truth to label low-confidence predictions.

Answer: B
Explanation:
https://docs.aws.amazon.com/rekognition/latest/dg/moderation.html?pg=ln&sec=ft

QUESTION 131
A company wants to run its critical applications in containers to meet requirements tor scalability and availability The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload.
What should a solutions architect do to meet those requirements?

A. Use Amazon EC2 Instances, and Install Docker on the Instances
B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes
C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate
D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-op6mized Amazon Machine Image (AMI).

Answer: C
Explanation:
AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without having to manage servers. AWS Fargate is compatible with Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).
https://aws.amazon.com/fr/fargate/

QUESTION 132
A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day. What should a solutions architect do to transmit and process the clickstream data?

A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR duster with the data to generate analytics
B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use tor analysis
C. Cache the data to Amazon CloudFron.
Store the data in an Amazon S3 bucket.
When an object is added to the S3 bucket, run an AWS Lambda function to process the data tor analysis.
D. Collect the data from Amazon Kinesis Data Streams.
Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake Load the data in Amazon Redshift for analysis

Answer: D
Explanation:
https://aws.amazon.com/es/blogs/big-data/real-time-analytics-with-amazon-redshift-streaming-ingestion/

QUESTION 133
A company is running a multi-tier ecommerce web application in the AWS Cloud.
The web application is running on Amazon EC2 instances.
The database tier Is on a provisioned Amazon Aurora MySQL DB cluster with a writer and a reader in a Multi-AZ environment.
The new requirement for the database tier is to serve the application to achieve continuous write availability through an Instance failover.
What should a solutions architect do to meet this new requirement?

A. Add a new AWS Region to the DB cluster for multiple writes
B. Add a new reader In the same Availability Zone as the writer.
C. Migrate the database tier to an Aurora multi-master cluster.
D. Migrate the database tier to an Aurora DB cluster with parallel query enabled.

Answer: C
Explanation:
Bring-your-own-shard (BYOS)
A situation where you already have a database schema and associated applications that use sharding. You can transfer such deployments relatively easily to Aurora multi-master clusters. In this case, you can devote your effort to investigating the Aurora benefits such as server consolidation and high availability. You don't need to create new application logic to handle multiple connections for write requests.
Global read-after-write (GRAW)
A setting that introduces synchronization so that any read operations always see the most current

state of the data. By default, the data seen by a read operation in a multi-master cluster is subject to replication lag, typically a few milliseconds. During this brief interval, a query on one DB instance might retrieve stale data if the same data is modified at the same time by a different DB instance. To enable this setting, change aurora_mm_session_consistency_level from its default setting of INSTANCE_RAW to REGIONAL_RAW. Doing so ensures cluster-wide consistency for read operations regardless of the DB instances that perform the reads and writes.
Reference: https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-multi-master.html

QUESTION 134
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
Explanation:
By configuring scheduled scaling, the solutions architect can set the Auto Scaling group to automatically scale up to the desired compute level at a specific time (IAM) when the batch job starts and then automatically scale down after the job is complete. This will allow the desired EC2 capacity to be reached quickly and also help in reducing the cost.

QUESTION 135
A company runs an application in the AWS Cloud and uses Amazon DynamoDB as the database. The company deploys Amazon EC2 instances to a private network to process data from the database.
The company uses two NAT instances to provide connectivity to DynamoDB.
The company wants to retire the NAT instances.
A solutions architect must implement a solution that provides connectivity to DynamoDB and that does not require ongoing management.
What is the MOST cost-effective solution that meets these requirements?

A. Create a gateway VPC endpoint to provide connectivity to DynamoDB
B. Configure a managed NAT gateway to provide connectivity to DynamoDB
C. Establish an AWS Direct Connect connection between the private network and DynamoDB
D. Deploy an AWS PrivateLink endpoint service between the private network and DynamoDB

Answer: A
Explanation:
AWS recommends changing from NAT Gateway to VPC endpoints to access S3 or DynamoDB.
"Determine whether the majority of your NAT gateway charges are from traffic to Amazon Simple Storage Service or Amazon DynamoDB in the same Region. If they are, set up a gateway VPC endpoint. Route traffic to and from the AWS resource through the gateway VPC endpoint, rather than through the NAT gateway. There's no data processing or hourly charges for using gateway VPC endpoints."
https://aws.amazon.com/premiumsupport/knowledge-center/vpc-reduce-nat-gateway-transfer-

costs/

QUESTION 136
A company has an on-premises business application that generates hundreds of files each day. These files are stored on an SMB file share and require a low-latency connection to the application servers.
A new company policy states all application-generated files must be copied to AWS.
There is already a VPN connection to AWS.
The application development team does not have time to make the necessary code modifications to move the application to AWS.
Which service should a solutions architect recommend to allow the application to copy files to AWS?

A. Amazon Elastic File System (Amazon EFS)
B. Amazon FSx for Windows File Server
C. AWS Snowball
D. AWS Storage Gateway

Answer: D
Explanation:
The files will be on the storgare gateway with low latency and copied to AWS as a second copy. FSx in AWS will not provide low latency for the on prem apps over a vpn to the FSx file system.

QUESTION 137
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 SOS) 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: A
Explanation:
You can use AWS Lambda to process event notifications from an Amazon Relational Database Service (Amazon RDS) database. Amazon RDS sends notifications to an Amazon Simple Notification Service (Amazon SNS) topic, which you can configure to invoke a Lambda function. Amazon SNS wraps the message from Amazon RDS in its own event document and sends it to your function.
https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html
https://aws.amazon.com/blogs/compute/messaging-fanout-pattern-for-serverless-architectures-

using-amazon-sns/

QUESTION 138
A company is developing a video conversion application hosted on AWS.
The application will be available in two tiers: a free tier and a paid tier.
Users in the paid tier will have their videos converted first and then the tree 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 file types
C. A single standard Amazon Simple Queue Service (Amazon SQS) queue for all file types
D. Two standard Amazon Simple Queue Service (Amazon SQS) queues with one for the paid tier and one for the free tier

Answer: D
Explanation:
In AWS, the queue service is the Simple Queue Service (SQS). Multiple SQS queues may be prepared to prepare queues for individual priority levels (with a priority queue and a secondary queue). Moreover, you may also use the message Delayed Send function to delay process execution.

QUESTION 139
A company runs an ecommerce application 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 based on CPU utilization metrics. The ecommerce application stores the transaction data in a MySQL 8.0 database that is hosted on a large EC2 instance.

The database's performance degrades quickly as application load increases. The application handles more read requests than write transactions. The company wants a solution that will automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability.

Which solution will meet these requirements?

A. Use Amazon Redshift with a single node for leader and compute functionality.
B. Use Amazon RDS with a Single-AZ deployment.
Configure Amazon RDS to add reader instances in a different Availability Zone.
C. Use Amazon Aurora with a Multi-AZ deployment.
Configure Aurora Auto Scaling with Aurora Replicas.
D. Use Amazon ElastiCache for Memcached with EC2 Spot Instances.

Answer: C
Explanation:
AURORA is 5x performance improvement over MySQL on RDS and handles more read requests than write, maintaining high availability = Multi-AZ deployment

QUESTION 140
A company recently migrated to AWS and wants to implement a solution to protect the traffic that flows in and out of the production VPC. The company had an inspection server in its on-premises data center. The inspection server performed specific operations such as traffic flow inspection

and traffic filtering. The company wants to have the same functionalities in the AWS Cloud.
Which solution will meet these requirements?

A. Use Amazon GuardDuty for traffic inspection and traffic filtering in the production VPC
B. Use Traffic Mirroring to mirror traffic from the production VPC for traffic inspection and filtering.
C. Use AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC.
D. Use AWS Firewall Manager to create the required rules for traffic inspection and traffic filtering for the production VPC.

Answer: C
Explanation:
AWS Network Firewall is a stateful, managed network firewall and intrusion detection and prevention service for your virtual private cloud (VPC) that you created in Amazon Virtual Private Cloud (Amazon VPC). With Network Firewall, you can filter traffic at the perimeter of your VPC. This includes filtering traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect.

QUESTION 141
A company hosts a data lake on AWS. The data lake consists of data in Amazon S3 and Amazon RDS for PostgreSQL. The company needs a reporting solution that provides data visualization and includes all the data sources within the data lake. Only the company's management team should have full access to all the visualizations. The rest of the company should have only limited access.
Which solution will meet these requirements?

A. Create an analysis in Amazon QuickSight.
Connect all the data sources and create new datasets.
Publish dashboards to visualize the data.
Share the dashboards with the appropriate IAM roles.
B. Create an analysis in Amazon OuickSighl.
Connect all the data sources and create new datasets.
Publish dashboards to visualize the data.
Share the dashboards with the appropriate users and groups.
C. Create an AWS Glue table and crawler for the data in Amazon S3.
Create an AWS Glue extract, transform, and load (ETL) job to produce reports.
Publish the reports to Amazon S3.
Use S3 bucket policies to limit access to the reports.
D. Create an AWS Glue table and crawler for the data in Amazon S3.
Use Amazon Athena Federated Query to access data within Amazon RDS for PoslgreSQL.
Generate reports by using Amazon Athena.
Publish the reports to Amazon S3.
Use S3 bucket policies to limit access to the reports.

Answer: B
Explanation:
https://docs.aws.amazon.com/quicksight/latest/user/sharing-a-dashboard.html
https://docs.aws.amazon.com/quicksight/latest/user/share-a-dashboard-grant-access-users.html

QUESTION 142
A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3 bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket.

What should the solutions architect do to meet this requirement?

A. Create an IAM role that grants access to the S3 bucket.
Attach the role to the EC2 instances.
B. Create an IAM policy that grants access to the S3 bucket.
Attach the policy to the EC2 instances.
C. Create an IAM group that grants access to the S3 bucket.
Attach the group to the EC2 instances.
D. Create an IAM user that grants access to the S3 bucket.
Attach the user account to the EC2 instances.

Answer: A
Explanation:
Always remember that you should associate IAM roles to EC2 instances.
https://aws.amazon.com/premiumsupport/knowledge-center/ec2-instance-access-s3-bucket/

QUESTION 143
An application development team is designing a microservice that will convert large images to smaller, compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket.

A solutions architect needs to design a solution that uses durable, stateless components to process the images automatically.

Which combination of actions will meet these requirements? (Choose two.)

A. Create an Amazon Simple Queue Service (Amazon SQS) queue.
Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.
B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source.
When the SQS message is successfully processed, delete the message in the queue
C. Configure the Lambda function to monitor the S3 bucket for new uploads.
When an uploaded image is detected write the file name to a text file in memory and use the text file to keep track of the images that were processed.
D. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue.
When items are added to the queue log the file name in a text file on the EC2 instance and invoke the Lambda function.
E. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket.
When an image is uploaded send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing

Answer: AB

QUESTION 144
A company has a three-tier web application that is deployed on AWS. The web servers are deployed in a public subnet in a VPC. The application servers and database servers are deployed

in private subnets in the same VPC. The company has deployed a third-party virtual firewall appliance from AWS Marketplace in an inspection VPC. The appliance is configured with an IP interface that can accept IP packets.
A solutions architect needs to Integrate the web application with the appliance to inspect all traffic to the application before the traffic teaches the web server.

Which solution will moot these requirements with the LEAST operational overhead?

A. Create a Network Load Balancer the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
B. Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
C. Deploy a transit gateway in the inspection VPC.
Configure route tables to route the incoming pockets through the transit gateway.
D. Deploy a Gateway Load Balancer in the inspection VPC.
Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.

Answer: D
Explanation:
Gateway Load Balancer is a new type of load balancer that operates at layer 3 of the OSI model and is built on Hyperplane, which is capable of handling several thousands of connections per second. Gateway Load Balancer endpoints are configured in spoke VPCs originating or receiving traffic from the Internet. This architecture allows you to perform inline inspection of traffic from multiple spoke VPCs in a simplified and scalable fashion while still centralizing your virtual appliances.
https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-network-traffic-inspection-using-aws-gateway-load-balancer/

QUESTION 145
A company wants to improve its ability to clone large amounts of production data into a test environment in the same AWS Region. The data is stored in Amazon EC2 instances on Amazon Elastic Block Store (Amazon EBS) volumes. Modifications to the cloned data must not affect the production environment. The software that accesses this data requires consistently high I/O performance.

A solutions architect needs to minimize the time that is required to clone the production data into the test environment.

Which solution will meet these requirements?

A. Take EBS snapshots of the production EBS volumes.
Restore the snapshots onto EC2 instance store volumes in the test environment.
B. Configure the production EBS volumes to use the EBS Multi-Attach feature.
Take EBS snapshots of the production EBS volumes.
Attach the production EBS volumes to the EC2 instances in the test environment.
C. Take EBS snapshots of the production EBS volumes.
Create and initialize new EBS volumes.
Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots.
D. Take EBS snapshots of the production EBS volumes.
Turn on the EBS fast snapshot restore feature on the EBS snapshots.
Restore the snapshots into new EBS volumes.
Attach the new EBS volumes to EC2 instances in the test environment.

Answer: D
Explanation:
Amazon EBS fast snapshot restore (FSR) enables you to create a volume from a snapshot that is fully initialized at creation. This eliminates the latency of I/O operations on a block when it is accessed for the first time. Volumes that are created using fast snapshot restore instantly deliver all of their provisioned performance.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-fast-snapshot-restore.html
https://aws.amazon.com/cn/about-aws/whats-new/2020/11/amazon-ebs-fast-snapshot-restore-now-available-us-govcloud-regions/

QUESTION 146
An ecommerce company wants to launch a one-deal-a-day website on AWS. Each day will feature exactly one product on sale for a period of 24 hours. The company wants to be able to handle millions of requests each hour with millisecond latency during peak hours.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon S3 to host the full website in different S3 buckets.
Add Amazon CloudFront distributions.
Set the S3 buckets as origins for the distributions.
Store the order data in Amazon S3.
B. Deploy the full website on Amazon EC2 instances that run in Auto Scaling groups across multiple Availability Zones.
Add an Application Load Balancer (ALB) to distribute the website traffic.
Add another ALB for the backend APIs.
Store the data in Amazon RDS for MySQL.
C. Migrate the full application to run in containers.
Host the containers on Amazon Elastic Kubernetes Service (Amazon EKS).
Use the Kubernetes Cluster Autoscaler to increase and decrease the number of pods to process bursts in traffic.
Store the data in Amazon RDS for MySQL.
D. Use an Amazon S3 bucket to host the website's static content.
Deploy an Amazon CloudFront distribution.
Set the S3 bucket as the origin.
Use Amazon API Gateway and AWS Lambda functions for the backend APIs.
Store the data in Amazon DynamoDB.

Answer: D
Explanation:
All of the components are infinitely scalable dynamoDB, API Gateway, Lambda, and of course s3+cloudfront.

QUESTION 147
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
Explanation:
S3 Intelligent-Tiering -Perfect use case when you don't know the frequency of access or irregular patterns of usage.
Amazon S3 offers a range of storage classes designed for different use cases. These include S3 Standard for general-purpose storage of frequently accessed data; S3 Intelligent-Tiering for data with unknown or changing access patterns; S3 Standard-Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone-IA) for long-lived, but less frequently accessed data; and Amazon S3 Glacier (S3 Glacier) and Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive) for long-term archive and digital preservation. If you have data residency requirements that can't be met by an existing AWS Region, you can use the S3 Outposts storage class to store your S3 data on-premises. Amazon S3 also offers capabilities to manage your data throughout its lifecycle. Once an S3 Lifecycle policy is set, your data will automatically transfer to a different storage class without any changes to your application.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/DataDurability.html

QUESTION 148
A company has an on-premises MySQL database used by the global sales team with infrequent access patterns.
The sales team requires the database to have minimal downtime.
A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.
Which service should a solution architect recommend?

A. Amazon Aurora MySQL
B. Amazon Aurora Serverless for MySQL
C. Amazon Redshift Spectrum
D. Amazon RDS for MySQL

Answer: B
Explanation:
A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future" Serverless sounds right, and it's compatible with MySQL and PostgreSQL.
https://aws.amazon.com/rds/aurora/serverless/

QUESTION 149
A company is building an application on Amazon EC2 instances that generates temporary transactional data.
The application requires access to data storage that can provide configurable and consistent IOPS.

What should a solutions architect recommend?

A. Provision an EC2 instance with a Throughput Optimized HDD (st1) root volume and a Cold HDD (sc1) data volume.
B. Provision an EC2 instance with a Throughput Optimized HDD (st1) volume that will serve as the root and data volume.
C. Provision an EC2 instance with a General Purpose SSD (gp2) root volume and Provisioned IOPS SSD (io1) data volume.

D. Provision an EC2 instance with a General Purpose SSD (gp2) root volume. Configure the application to store its data in an Amazon S3 bucket.

Answer: C
Explanation:
Only gp3, io1, or io2 Volumes have configurable IOPS.
You cannot add HDD in root volume. SSD needs to be selected as root volume and HDD as Data Volume.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes.html

QUESTION 150
A company is hosting 60 TB of production-level data in an Amazon S3 bucket. A solution architect needs to bring that data on premises for quarterly audit requirements. This export of data must be encrypted while in transit. The company has low network bandwidth in place between AWS and its on-premises data center.

What should the solutions architect do to meet these requirements?

A. Deploy AWS Migration Hub with 90-day replication windows for data transfer.
B. Deploy an AWS Storage Gateway volume gateway on AWS. Enable a 90-day replication window to transfer the data.
C. Deploy Amazon Elastic File System (Amazon EFS), with lifecycle policies enabled, on AWS. Use it to transfer the data.
D. Deploy an AWS Snowball device in the on-premises data center after completing an export job request in the AWS Snowball console.

Answer: D
Explanation:
AWS Snowball with the Snowball device has the following features:
80 TB and 50 TB models are available in US Regions; 50 TB model available in all other AWS Regions.
https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html

QUESTION 151
A solutions architect is designing the cloud architecture for a company that needs to host hundreds of machine learning models for its users. During startup, the models need to load up to 10 GB of data from Amazon S3 into memory, but they do not need disk access. Most of the models are used sporadically, but the users expect all of them to be highly available and accessible with low latency.

Which solution meets the requirements and is MOST cost-effective?

A. Deploy models as AWS Lambda functions behind an Amazon API Gateway for each model.
B. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind an Application Load Balancer for each model.
C. Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model.
D. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind a single Application Load Balancer with path-based routing where one path corresponds to each model.

Answer: C
Explanation:

AWS just update Lambda to support 10G memory and helping compute intensive applications like machine learning.
No disk access, lowest cost.
https://aws.amazon.com/about-aws/whats-new/2020/12/aws-lambda-supports-10gb-memory-6-vcpu-cores-lambda-functions/

QUESTION 152
A company is developing an ecommerce application that will consist of a load-balanced front end, a container-based application, and a relational database. A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible.

Which solutions meet these requirements? (Choose two.)

A. Create an Amazon RDS DB instance in Multi-AZ mode.
B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
C. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.
D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

Answer: AD
Explanation:
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html
1. Relational database: RDS
2. Container-based applications: ECS
"Amazon ECS enables you to launch and stop your container-based applications by using simple API calls.
You can also retrieve the state of your cluster from a centralized service and have access to many familiar Amazon EC2 features."
3. Little manual intervention: Fargate
You can run your tasks and services on a serverless infrastructure that is managed by AWS Fargate. Alternatively, for more control over your infrastructure, you can run your tasks and services on a cluster of Amazon EC2 instances that you manage.

QUESTION 153
A company has an ecommerce application that stores data in an on-premises SQL database. The company has decided to migrate this database to AWS. However, as part of the migration, the company wants to find a way to attain sub-millisecond responses to common read requests.

A solutions architect knows that the increase in speed is paramount and that a small percentage of stale data returned in the database reads is acceptable.

What should the solutions architect recommend?

A. Build Amazon RDS read replicas.
B. Build the database as a larger instance type.
C. Build a database cache using Amazon ElastiCache.
D. Build a database cache using Amazon Elasticsearch Service (Amazon ES).

Answer: C
Explanation:

To attain sub-millisecond responses to common read requests.
https://aws.amazon.com/redis/
REDIS (REmote DIctionary Server) delivers sub-millisecond response times enabling millions of requests per second for real-time applications.

QUESTION 154

A company is designing an application where users upload small files into Amazon S3.
After a user uploads a file, the file requires one-time simple processing to transform the data and save the data in JSON format for later analysis.

Each file must be processed as quickly as possible after it is uploaded. Demand will vary.
On some days, users will upload a high number of files. On other days, users will upload a few files or no files.

Which solution meets these requirements with the LEAST operational overhead?

A. Configure Amazon EMR to read text files from Amazon S3.
Run processing scripts to transform the data.
Store the resulting JSON file in an Amazon Aurora DB cluster.

B. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue.
Use Amazon EC2 instances to read from the queue and process the data.
Store the resulting JSON file in Amazon DynamoDB.

C. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue.
Use an AWS Lambda function to read from the queue and process the data.
Store the resulting JSON file in Amazon DynamoDB.

D. Configure Amazon EventBridge (Amazon CloudWatch Events) to send an event to Amazon Kinesis Data Streams when a new file is uploaded.
Use an AWS Lambda function to consume the event from the stream and process the data.
Store the resulting JSON file in Amazon Aurora DB cluster.

Answer: C
Explanation:
Amazon S3 sends event notifications about S3 buckets (for example, object created, object removed, or object restored) to an SNS topic in the same Region.
The SNS topic publishes the event to an SQS queue in the central Region.
The SQS queue is configured as the event source for your Lambda function and buffers the event messages for the Lambda function.
The Lambda function polls the SQS queue for messages and processes the Amazon S3 event notifications according to your application's requirements.

https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/subscribe-a-lambda-function-to-event-notifications-from-s3-buckets-in-different-aws-regions.html

QUESTION 155

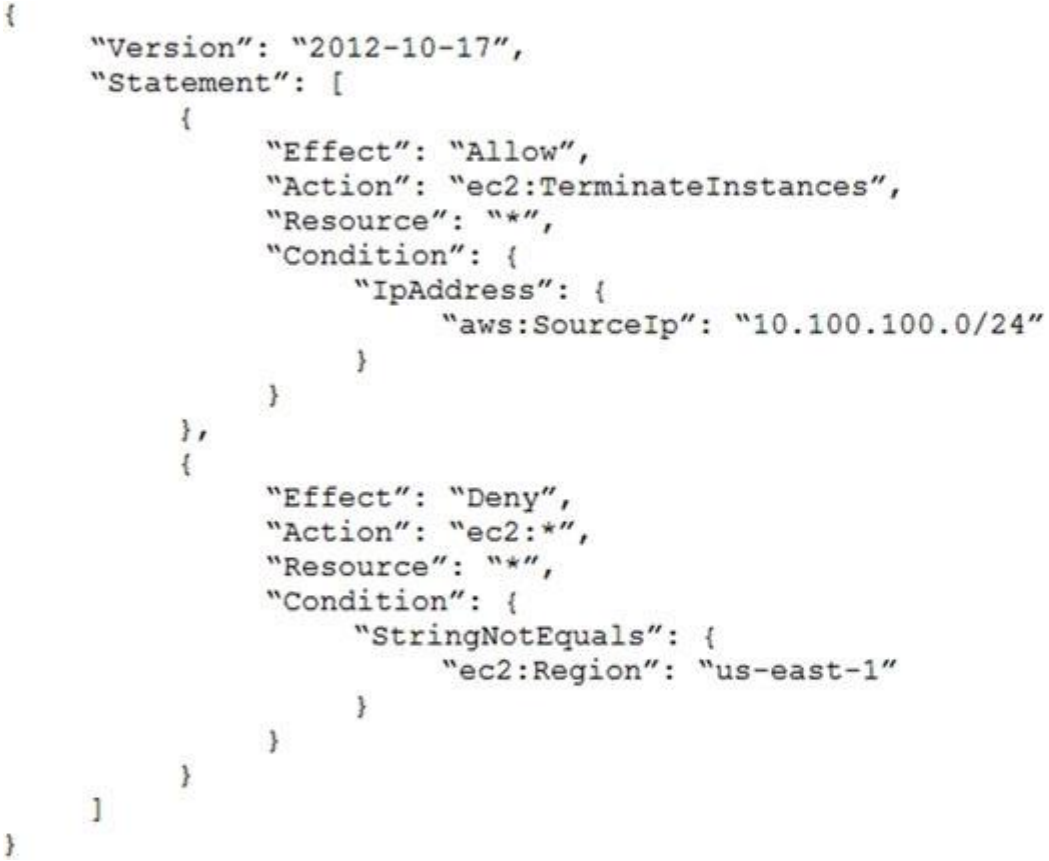
An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic.
A solutions architect needs to optimize 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:
For replication to operate effectively, each read replica should have the same amount of compute and storage resources as the source DB instance.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html

QUESTION 156
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”,
                  “Resource”: “*”,
                  “Condition”: {
                        “IpAddress”: {
                              “aws:SourceIp”: “10.100.100.0/24”
                        }
                  }
            },
            {
                  “Effect”: “Deny”,
                  “Action”: “ec2:*”,
                  “Resource”: “*”,
                  “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 10 100 100 1 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:
As the policy prevents anyone from doing any EC2 action on any region except us-east-1 and allows only users with source ip 10.100.100.0/24 to terminate instances. So user with source ip 10.100.100.254 can terminate instances in us-east-1 region.

QUESTION 157
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 Me share on an AWS Storage Gateway tile 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 is a fully managed file storage service that is designed to be used with Microsoft Windows workloads. It is integrated with Active Directory for access control and is highly available, as it stores data across multiple availability zones. Additionally, FSx can be used to migrate data from on-premises Microsoft Windows file servers to the AWS Cloud. This makes it a good fit for the requirements described in the question.

QUESTION 158
An image-processing company has a web application that users use to upload images. The application uploads the images into an Amazon S3 bucket. The company has set up S3 event notifications to publish the object creation events to an Amazon Simple Queue Service (Amazon SQS) standard queue. The SQS queue serves as the event source for an AWS Lambda function that processes the images and sends the results to users through email.

Users report that they are receiving multiple email messages for every uploaded image. A solutions architect determines that SQS messages are invoking the Lambda function more than once, resulting in multiple email messages.

What should the solutions architect do to resolve this issue with the LEAST operational overhead?

A. Set up long polling in the SQS queue by increasing the ReceiveMessage wait time to 30 seconds.
B. Change the SQS standard queue to an SQS FIFO queue.
Use the message deduplication ID to discard duplicate messages.

C. Increase the visibility timeout in the SQS queue to a value that is greater than the total of the function timeout and the batch window timeout.
D. Modify the Lambda function to delete each message from the SQS queue immediately after the message is read before processing.

Answer: C
Explanation:
Immediately after a message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents other consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The minimum is 0 seconds. The maximum is 12 hours.
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html

QUESTION 159
A company is implementing a shared storage solution for a media application that is hosted in the AWS Cloud.
The company needs the ability to use SMB clients to access data. The solution must he fully managed.
Which AWS solution meets these requirements?

A. Create an AWS Storage Gateway volume gateway.
Create a file share that uses the required client protocol.
Connect the application server to the tile share.
B. Create an AWS Storage Gateway tape gateway.
Configure tapes to use Amazon S3.
Connect the application server lo the tape gateway
C. Create an Amazon EC2 Windows instance.
Install and configure a Windows file share role on the instance.
Connect the application server to the file share.
D. Create an Amazon FSx for Windows File Server tile system.
Attach the fie system to the origin server.
Connect the application server to the tile system

Answer: D
Explanation:
Amazon FSx for Lustre is a fully managed file system that is designed for high-performance workloads, such as gaming applications. It provides a high-performance, scalable, and fully managed file system that is optimized for Lustre clients, and it is fully integrated with Amazon EC2. It is the only option that meets the requirements of being fully managed and able to support Lustre clients.
https://aws.amazon.com/fsx/lustre/

QUESTION 160
A company's containerized application runs on an Amazon EC2 instance. The application needs to download security certificates before it can communicate with other business applications. The company wants a highly secure solution to encrypt and decrypt the certificates in near real time. The solution also needs to store data in highly available storage after the data is encrypted.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create AWS Secrets Manager secrets for encrypted certificates.

Manually update the certificates as needed.
Control access to the data by using fine-grained IAM access.

B. Create an AWS Lambda function that uses the Python cryptography library to receive and perform encryption operations.
Store the function in an Amazon S3 bucket.

C. Create an AWS Key Management Service (AWS KMS) customer managed key.
Allow the EC2 role to use the KMS key for encryption operations.
Store the encrypted data on Amazon S3.

D. Create an AWS Key Management Service (AWS KMS) customer managed key.
Allow the EC2 role to use the KMS key for encryption operations.
Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.

Answer: C
Explanation:
S3 is highly available with LEAST operational overhead.
Amazon S3 provides durability by redundantly storing the data across multiple Availability Zones whereas EBS provides durability by redundantly storing the data in a single Availability Zone.
Both S3 and EBS gives the availability of 99.99%, but the only difference that occurs is that S3 is accessed via the internet using API's and EBS is accessed by the single instance attached to EBS.

QUESTION 161
A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (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 Internet 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 instances, one for each private subnet in each AZ.
Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.

C. Create a second internet gateway on one of the private subnets.
Update the route table for the private subnets that forward non-VPC traffic to the private internet 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
Explanation:
To enable Internet access for the private subnets, the solutions architect should create three NAT gateways, one for each public subnet in each Availability Zone (AZ). NAT gateways allow private instances to initiate outbound traffic to the Internet but do not allow inbound traffic from the Internet to reach the private instances.
The solutions architect should then create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ. This will allow instances in the private subnets to access the Internet through the NAT gateways in the public subnets.

QUESTION 162
A company wants to migrate an on-premises data center to AWS. The data center hosts an SFTP server that stores its data on an NFS-based file system. The server holds 200 GB of data that needs to be transferred. The server must be hosted on an Amazon EC2 instance that uses an Amazon Elastic File System (Amazon EFS) file system.
Which combination of steps should a solutions architect take to automate this task? (Choose two.)

A. Launch the EC2 instance into the same Availability Zone as the EFS file system.
B. Install an AWS DataSync agent in the on-premises data center.
C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance tor the data.
D. Manually use an operating system copy command to push the data to the EC2 instance.
E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.

Answer: AB
Explanation:
A - Makes sense to have the instance in the same AZ the EFS storage is.
B - The DataSync with move the data to the EFS, which already uses the EC2 instance (see the info provided).

QUESTION 163
A company has an AWS Glue extract. transform, and load (ETL) job that runs every day at the same time. The job processes XML data that is in an Amazon S3 bucket. New data is added to the S3 bucket every day. A solutions architect notices that AWS Glue is processing all the data during each run.
What should the solutions architect do to prevent AWS Glue from reprocessing old data?

A. Edit the job to use job bookmarks.
B. Edit the job to delete data after the data is processed
C. Edit the job by setting the NumberOfWorkers field to 1.
D. Use a FindMatches machine learning (ML) transform.

Answer: A
Explanation:
AWS Glue tracks data that has already been processed during a previous run of an ETL job by persisting state information from the job run. This persisted state information is called a job bookmark. Job bookmarks help AWS Glue maintain state information and prevent the reprocessing of old data.
https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html

QUESTION 164
A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website.
Which actions should the solutions architect take to protect the website from such an attack? (Choose two.)

A. Use AWS Shield Advanced to stop the DDoS attack.
B. Configure Amazon GuardDuty to automatically block the attackers.
C. Configure the website to use Amazon CloudFront for both static and dynamic content.

D. Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.
E. Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization

Answer: AC
Explanation:
AWS Shield can handle the DDoS attacks.
Amazon CloudFront supports DDoS protection, integration with Shield, AWS Web Application Firewall.

QUESTION 165
A company is preparing to deploy a new serverless workload.
A solutions architect must use the principle of least privilege to configure permissions that will be used to run an AWS Lambda function.
An Amazon EventBridge (Amazon CloudWatch Events) rule will invoke the function.

Which solution meets these requirements?

A. Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.
B. Add an execution role to the function with lambda:InvokeFunction as the action and Service:amazonaws.com as the principal.
C. Add a resource-based policy to the function with lambda:'* as the action and Service:events.amazonaws.com as the principal.
D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service:events.amazonaws.com as the principal.

Answer: D
Explanation:
The principle of least privilege requires that permissions are granted only to the minimum necessary to perform a task. In this case, the Lambda function needs to be able to be invoked by Amazon EventBridge (Amazon CloudWatch Events). To meet these requirements, you can add a resource-based policy to the function that allows the InvokeFunction action to be performed by the Service: events.amazonaws.com principal. This will allow Amazon EventBridge to invoke the function, but will not grant any additional permissions to the function.
https://docs.aws.amazon.com/eventbridge/latest/userguide/resource-based-policies-eventbridge.html#lambda-permissions

QUESTION 166
A company has an image processing workload running on Amazon Elastic Container Service (Amazon ECS) in two private subnets. Each private subnet uses a NAT instance for internet access. All images are stored in Amazon S3 buckets.
The company is concerned about the data transfer costs between Amazon ECS and Amazon S3.

What should a solutions architect do to reduce costs?

A. Configure a NAT gateway to replace the NAT instances.
B. Configure a gateway endpoint for traffic destined to Amazon S3.
C. Configure an interface endpoint for traffic destined to Amazon S3.
D. Configure Amazon CloudFront for the S3 bucket storing the images.

Answer: B
Explanation:
S3 and Dynamo DB does not support interface endpoints. Both S3 and DynamoDB are routed via Gateway endpoint.
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html
Interface Endpoint only supports services which are integrated with PrivateLink.
https://docs.aws.amazon.com/vpc/latest/userguide/integrated-services-vpce-list.html

QUESTION 167
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: C
Explanation:
As you can see, we have three important memory buffers in this architecture for CDC in AWS DMS. If any of these buffers experience memory pressure, the migration can have performance issues that can potentially cause failures.
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_ReplicationInstance.Types.html

QUESTION 168
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? (Choose 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 169
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: C
Explanation:
The Application uses synchronous transactions each operation is dependent on the previous one. Using asynchronous lambda calls may not work here.

QUESTION 170
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
Explanation:
Question asked is to ensure that all volumes restored are encrypted. So have to be "Enable encryption by default".
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-by-default

QUESTION 171
A company is storing backup files by using Amazon S3 Standard storage. The files are accessed frequently for 1 month. However, the files are not accessed after 1 month. The company must keep the files indefinitely.

Which storage solution will meet these requirements MOST cost-effectively?

A. Configure S3 Intelligent-Tiering to automatically migrate objects.
B. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.
C. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) after 1 month.
D. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 month.

Answer: B
Explanation:
Transition to Glacier deep archive for cost efficiency.

QUESTION 172
A company observes an increase in Amazon EC2 costs in its most recent bill. The billing team notices unwanted vertical scaling of instance types for a couple of EC2 instances. A solutions architect needs to create a graph comparing the last 2 months of EC2 costs and perform an in-depth analysis to identify the root cause of the vertical scaling.
How should the solutions architect generate the information with the LEAST operational overhead?

A. Use AWS Budgets to create a budget report and compare EC2 costs based on instance types
B. Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types
C. Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months
D. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types..

Answer: B
Explanation:
AWS Cost Explorer is a tool that enables you to view and analyze your costs and usage. You can explore your usage and costs using the main graph, the Cost Explorer cost and usage reports, or the Cost Explorer RI reports. You can view data for up to the last 12 months, forecast how much you're likely to spend for the next 12 months, and get recommendations for what Reserved Instances to purchase. You can use Cost Explorer to identify areas that need further inquiry and see trends that you can use to understand your costs.
https://docs.aws.amazon.com/cost-management/latest/userguide/ce-what-is.html

QUESTION 173
A company is designing an application. The application uses an AWS Lambda function to receive information through Amazon API Gateway and to store the information in an Amazon Aurora PostgreSQL database.
During the proof-of-concept stage, the company has to increase the Lambda quotas significantly to handle the high volumes of data that the company needs to load into the database. A solutions architect must recommend a new design to improve scalability and minimize the configuration effort.
Which solution will meet these requirements?

A. Refactor the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances.
Connect the database by using native Java Database Connectivity (JDBC) drivers.
B. Change the platform from Aurora to Amazon DynamoDB.
Provision a DynamoDB Accelerator (DAX) cluster.
Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster.
C. Set up two Lambda functions.
Configure one function to receive the information.
Configure the other function to load the information into the database.
Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS).
D. Set up two Lambda functions. Configure one function to receive the information.
Configure the other function to load the information into the database.
Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

Answer: D
Explanation:
Option D uses SQS, so the 2nd lambda function can go to the queue when responsive to keep with the DB load process.
Usually the app decoupling helps with the performance improvement by distributing load.

QUESTION 174
A company needs to review its AWS Cloud deployment to ensure that its Amazon S3 buckets do not have unauthorized configuration changes.

What should a solutions architect do to accomplish this goal?

A. Turn on AWS Config with the appropriate rules.
B. Turn on AWS Trusted Advisor with the appropriate checks.
C. Turn on Amazon Inspector with the appropriate assessment template.
D. Turn on Amazon S3 server access logging.
Configure Amazon EventBridge (Amazon Cloud Watch Events).

Answer: A
Explanation:
AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.

QUESTION 175
A company is launching a new application and will display application metrics on an Amazon CloudWatch dashboard. The company's product manager needs to access this dashboard periodically. The product manager does not have an AWS account. A solution architect must provide access to the product manager by following the principle of least privilege.
Which solution will meet these requirements?

A. Share the dashboard from the CloudWatch console.
Enter the product manager's email address, and complete the sharing steps.
Provide a shareable link for the dashboard to the product manager.
B. Create an IAM user specifically for the product manager.
Attach the CloudWatch Read Only Access managed policy to the user.
Share the new login credential with the product manager.
Share the browser URL of the correct dashboard with the product manager.

C. Create an IAM user for the company's employees.
   Attach the View Only Access AWS managed policy to the IAM user.
   Share the new login credentials with the product manager.
   Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.
D. Deploy a bastion server in a public subnet.
   When the product manager requires access to the dashboard, start the server and share the RDP credentials.
   On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

Answer: A
Explanation:
Share a single dashboard and designate specific email addresses of the people who can view the dashboard. Each of these users creates their own password that they must enter to view the dashboard.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html

QUESTION 176
A company is migrating applications to AWS. The applications are deployed in different accounts. The company manages the accounts centrally by using AWS Organizations. The company's security team needs a single sign-on (SSO) solution across all the company's accounts.
The company must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory.

Which solution will meet these requirements?

A. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.
   Create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
B. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.
   Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
C. Use AWS Directory Service.
   Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.
D. Deploy an identity provider (IdP) on premises.
   Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

Answer: B
Explanation:
You can configure one and two-way external and forest trust relationships between your AWS Directory Service for Microsoft Active Directory and self-managed (on-premises) directories, as well as between multiple AWS Managed Microsoft AD directories in the AWS cloud. AWS Managed Microsoft AD supports all three trust relationship directions: Incoming, Outgoing and Two-way (Bi-directional).
https://aws.amazon.com/blogs/security/everything-you-wanted-to-know-about-trusts-with-aws-managed-microsoft-ad/

QUESTION 177
A company provides a Voice over Internet Protocol (VoIP) service that uses UDP connections. The service consists of Amazon EC2 instances that run in an Auto Scaling group. The company

has deployments across multiple AWS Regions.

The company needs to route users to the Region with the lowest latency. The company also needs automated failover between Regions.

Which solution will meet these requirements?

A. Deploy a Network Load Balancer (NLB) and an associated target group.
Associate the target group with the Auto Scaling group.
Use the NLB as an AWS Global Accelerator endpoint in each Region.
B. Deploy an Application Load Balancer (ALB) and an associated target group.
Associate the target group with the Auto Scaling group.
Use the ALB as an AWS Global Accelerator endpoint in each Region.
C. Deploy a Network Load Balancer (NLB) and an associated target group.
Associate the target group with the Auto Scaling group.
Create an Amazon Route 53 latency record that points to aliases for each NLB.
Create an Amazon CloudFront distribution that uses the latency record as an origin.
D. Deploy an Application Load Balancer (ALB) and an associated target group.
Associate the target group with the Auto Scaling group.
Create an Amazon Route 53 weighted record that points to aliases for each ALB.
Deploy an Amazon CloudFront distribution that uses the weighted record as an origin.

Answer: A
Explanation:
Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.
https://aws.amazon.com/global-accelerator/faqs/

QUESTION 178
A development team runs monthly resource-intensive tests on its general purpose Amazon RDS for MySQL DB instance with Performance Insights enabled. The testing lasts for 48 hours once a month and is the only process that uses the database. The team wants to reduce the cost of running the tests without reducing the compute and memory attributes of the DB instance.

Which solution meets these requirements MOST cost-effectively?

A. Stop the DB instance when tests are completed.
Restart the DB instance when required.
B. Use an Auto Scaling policy with the DB instance to automatically scale when tests are completed.
C. Create a snapshot when tests are completed.
Terminate the DB instance and restore the snapshot when required.
D. Modify the DB instance to a low-capacity instance when tests are completed.
Modify the DB instance again when required.

Answer: C
Explanation:
It's a DB instance, not an EC2 instance. If the DB instance is stopped, you are still paying for the storage.

QUESTION 179
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 properly 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: A
Explanation:
https://docs.aws.amazon.com/config/latest/developerguide/tagging.html

QUESTION 180
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 Loa d Balancer with an AWS Lambda target that uses the Express js framework.

Answer: B
Explanation:
In Static Websites, Web pages are returned by the server which are prebuilt.
They use simple languages such as HTML, CSS, or JavaScript.
There is no processing of content on the server (according to the user) in Static Websites. Web pages are returned by the server with no change therefore, static Websites are fast.
There is no interaction with databases.
Also, they are less costly as the host does not need to support server-side processing with different languages.
============
In Dynamic Websites, Web pages are returned by the server which are processed during runtime means they are not prebuilt web pages but they are built during runtime according to the user's demand.
These use server-side scripting languages such as PHP, Node.js, ASP.NET and many more supported by the server.
So, they are slower than static websites but updates and interaction with databases are possible.

QUESTION 181
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: C
Explanation:
The destination of your Kinesis Data Firehose delivery stream. Kinesis Data Firehose can send data records to various destinations, including Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon OpenSearch Service, and any HTTP endpoint that is owned by you or any of your third-party service providers. The following are the supported destinations:
* Amazon OpenSearch Service
* Amazon S3
* Datadog
* Dynatrace
* Honeycomb
* HTTP Endpoint
* Logic Monitor
* MongoDB Cloud
* New Relic
* Splunk
* Sumo Logic
https://docs.aws.amazon.com/firehose/latest/dev/create-name.html
https://aws.amazon.com/kinesis/data-streams/
Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.

QUESTION 182
A company hosts its multi-tier applications on AWS. For compliance, governance, auditing, and security, the company must track configuration changes on its AWS resources and record a history of API calls made to these resources.

What should a solutions architect do to meet these requirements?

A. Use AWS CloudTrail to track configuration changes and AWS Config to record API calls
B. Use AWS Config to track configuration changes and AWS CloudTrail to record API calls
C. Use AWS Config to track configuration changes and Amazon CloudWatch to record API calls
D. Use AWS CloudTrail to track configuration changes and Amazon CloudWatch to record API calls

Answer: B

Explanation:
CloudTrail - Track user activity and API call history.
Config - Assess, audits, and evaluates the configuration and relationships of tag resources.

QUESTION 183

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 GuardDuty on the account.
B. Enable Amazon Inspector on the EC2 instances.
C. Enable AWS Shield and assign Amazon Route 53 to it.
D. Enable AWS Shield Advanced and assign the ELB to it.

Answer: D

Explanation:
AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator standard accelerators.
https://aws.amazon.com/shield/faqs/
https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/elastic-load-balancing-bp6.html

QUESTION 184

A company is building an application in the AWS Cloud. The application will store data in Amazon S3 buckets in two AWS Regions. The company must use an AWS Key Management Service (AWS KMS) customer managed key to encrypt all data that is stored in the S3 buckets. The data in both S3 buckets must be encrypted and decrypted with the same KMS key. The data and the key must be stored in each of the two Regions.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create an S3 bucket in each Region.
Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).
Configure replication between the S3 buckets.
B. Create a customer managed multi-Region KMS key.
Create an S3 bucket in each Region.
Configure replication between the S3 buckets.
Configure the application to use the KMS key with client-side encryption.
C. Create a customer managed KMS key and an S3 bucket in each Region.
Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).
Configure replication between the S3 buckets.
D. Create a customer managed KMS key and an S3 bucket in each Region.
Configure the S3 buckets to use server-side encryption with AWS KMS keys (SSE-KMS).
Configure replication between the S3 buckets.

Answer: B

Explanation:
KMS Multi-region keys are required.
https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html

QUESTION 185
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: B
Explanation:
Kinesis data streams consists of shards. The more througput is needed, the more shards you add, the less throughput, the more shards you remove, so it's scalable. Each shard can handle up to 1MB/s of writes.
However Kinesis data streams stores ingested data for only 1 to 7 days so there is a chance of data loss. Additionally,
Kinesis data analytics and kinesis data streams are both for real-time ingestion and analytics.
Firehouse on the other hand is also scalable and processes data in near real time as per the requirement. It also transfers data into Redshift which is a data warehouse so data won't be lost.
Redshift also has a SQL interface for performing queries for data analytics.

QUESTION 186
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 187
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: C
Explanation:
Match deployed capacity to the incoming application load, using scaling policies for both the ECS service and the Auto Scaling group in which the ECS cluster runs. Scaling up cluster instances and service tasks when needed and safely scaling them down when demand subsides, keeps you out of the capacity guessing game. This provides you high availability with lowered costs in the long run.
https://aws.amazon.com/blogs/compute/automatic-scaling-with-amazon-ecs/

QUESTION 188
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 users to an Active 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: D
Explanation:
Before you create an SMB file share, make sure that you configure SMB security settings for your file gateway.
You also configure either Microsoft Active Directory (AD) or guest access for authentication.
https://docs.aws.amazon.com/storagegateway/latest/userguide/CreatingAnSMBFileShare.html

QUESTION 189
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: B
Explanation:
https://cloudonaut.io/getting-started-with-ipv6-on-aws/
First of all, there is no IPv6-only VPC on AWS. A VPC is always IPv4 enabled, but you can optionally enable IPv6 (dual-stack).

QUESTION 190
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 191

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: D
Explanation:
Max instance store possible at this time is 30TB for NVMe which has the higher I/O compared to EBS.
is4gen.8xlarge 4 x 7,500 GB (30 TB) NVMe SSD
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html#instance-store-volumes

QUESTION 192

A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead.

What should a solutions architect do to meet these requirements?

A. Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.
B. Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.
C. Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.
D. Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

Answer: B
Explanation:
Running your Kubernetes and containerized workloads on Amazon EC2 Spot Instances is a great way to save costs. ... AWS makes it easy to run Kubernetes with Amazon Elastic Kubernetes Service (EKS) a managed Kubernetes service to run production-grade workloads on AWS. To cost optimize these workloads, run them on Spot Instances.
https://aws.amazon.com/blogs/compute/cost-optimization-and-resilience-eks-with-spot-instances/

QUESTION 193
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? (Choose 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
Explanation:
A - Aurora supports PostgreSQL.
E - The existing WebApp already run in containers On-Prem and is logical to migrate to a cloud container svc like serverless Fargate on ECS.

QUESTION 194
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 in 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 a target tracking scaling policy, you can increase or decrease the current capacity of the group based on a target value for a specific metric. This policy will help resolve the over-provisioning of your resources. 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 changes in the metric due to a changing load pattern.
https://docs.aws.amazon.com/autoscaling/application/userguide/application-auto-scaling-target-tracking.html

QUESTION 195
A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL.

What should a solutions architect do to meet these requirements?

A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
B. Create an IAM user. Grant the user read permission to objects in the S3 bucket.
Assign the user to CloudFront.
C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution.
Configure the S3 bucket permissions so that only the OAI has read permission.

Answer: D
Explanation:
Create a CloudFront origin access identity (OAI)
https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/

QUESTION 196
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 infrastructure resources, 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 DynamoDB
C. Application Load Balancer with Amazon EC2 Auto Scaling
D. Amazon Route 53 with internal Application Load Balancers

Answer: A
Explanation:
The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

QUESTION 197
A company runs an Oracle database on premises. As part of the company's migration to AWS, the company wants to upgrade the database to the most recent available version. The company also wants to set up disaster recovery (DR) for the database. The company needs to minimize the operational overhead for normal operations and DR setup. The company also needs to maintain access to the database's underlying operating system.

Which solution will meet these requirements?

A. Migrate the Oracle database to an Amazon EC2 instance.
Set up database replication to a different AWS Region.
B. Migrate the Oracle database to Amazon RDS for Oracle.
Activate Cross-Region automated backups to replicate the snapshots to another AWS Region.
C. Migrate the Oracle database to Amazon RDS Custom for Oracle.
Create a read replica for the database in another AWS Region.
D. Migrate the Oracle database to Amazon RDS for Oracle.
Create a standby database in another Availability Zone.

Answer: C
Explanation:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-custom.html
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/working-with-custom-oracle.html

QUESTION 198
A company wants to move its application to a serverless solution. The serverless solution needs to analyze existing and new data by using SQL. The company stores the data in an Amazon S3 bucket. The data requires encryption and must be replicated to a different AWS Region.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create a new S3 bucket. Load the data into the new S3 bucket.
Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region.
Use server-side encryption with AWS KMS multi-Region kays (SSE-KMS).
Use Amazon Athena to query the data.
B. Create a new S3 bucket. Load the data into the new S3 bucket.
Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region.
Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS).
Use Amazon RDS to query the data.
C. Load the data into the existing S3 bucket.
Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region.
Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).
Use Amazon Athena to query the data.
D. Load the data into the existing S3 bucket.
Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region.
Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).
Use Amazon RDS to query the data.

Answer: A
Explanation:
Amazon S3 Bucket Keys reduce the cost of Amazon S3 server-side encryption using AWS Key Management Service (SSE-KMS). This new bucket-level key for SSE can reduce AWS KMS request costs by up to 99 percent by decreasing the request traffic from Amazon S3 to AWS KMS. With a few clicks in the AWS Management Console, and without any changes to your client applications, you can configure your bucket to use an S3 Bucket Key for AWS KMS-based encryption on new objects.
The Existing S3 bucket might have uncrypted data - encryption will apply new data received after the applying of encryption on the new bucket.

QUESTION 199
A company runs workloads on AWS. The company needs to connect to a service from an external provider. The service is hosted in the provider's VPC. According to the company's security team, the connectivity must be private and must be restricted to the target service. The connection must be initiated only from the company's VPC.

Which solution will mast these requirements?

A. Create a VPC peering connection between the company's VPC and the provider's VPC.

Update the route table to connect to the target service.

B. Ask the provider to create a virtual private gateway in its VPC.
Use AWS PrivateLink to connect to the target service.

C. Create a NAT gateway in a public subnet of the company's VPC.
Update the route table to connect to the target service.

D. Ask the provider to create a VPC endpoint for the target service.
Use AWS PrivateLink to connect to the target service.

Answer: D
Explanation:
AWS PrivateLink provides private connectivity between VPCs, AWS services, and your on-premises networks, without exposing your traffic to the public internet. AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify your network architecture.
Interface **VPC endpoints**, powered by AWS PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace.
https://aws.amazon.com/privatelink/

QUESTION 200
A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The on-premises database must remain online and accessible during the migration. The Aurora database must remain synchronized with the on-premises database.

Which combination of actions must a solutions architect take to meet these requirements? (Choose two.)

A. Create an ongoing replication task.
B. Create a database backup of the on-premises database
C. Create an AWS Database Migration Service (AWS DMS) replication server
D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).
E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization

Answer: AC
Explanation:
AWS Database Migration Service (AWS DMS) helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database.
With AWS Database Migration Service, you can also continuously replicate data with low latency from any supported source to any supported target.
https://aws.amazon.com/dms/

QUESTION 201
A company uses AWS Organizations to create dedicated AWS accounts for each business unit to manage each business unit's account independently upon request. The root email recipient missed a notification that was sent to the root user email address of one account. The company wants to ensure that all future notifications are not missed. Future notifications must be limited to account administrators.

Which solution will meet these requirements?

A. Configure the company's email server to forward notification email messages that are sent to the AWS account root user email address to all users in the organization.

B. Configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.
C. Configure all AWS account root user email messages to be sent to one administrator who is responsible for monitoring alerts and forwarding those alerts to the appropriate groups.
D. Configure all existing AWS accounts and all newly created accounts to use the same root user email address.
Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

Answer: B
Explanation:
Use a group email address for the management account's root user
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_email-address

QUESTION 202
A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely. The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework.
Which solution will meet these requirements with the LEAST operational overhead?

A. Use the EC2 serial console to directly access the terminal interface of each instance for administration.
B. Attach the appropriate IAM role to each existing instance and new instance.
Use AWS Systems Manager Session Manager to establish a remote SSH session.
C. Create an administrative SSH key pair.
Load the public key into each EC2 instance.
Deploy a bastion host in a public subnet to provide a tunnel for administration of each instance.
D. Establish an AWS Site-to-Site VPN connection.
Instruct administrators to use their local on-premises machines to connect directly to the instances by using SSH keys across the VPN tunnel.

Answer: B
Explanation:
https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-launch-managed-instance.html

QUESTION 203
A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website.
Which solution meets these requirements MOST cost-effectively?

A. Replicate the S3 bucket that contains the website to all AWS Regions.
Add Route 53 geolocation routing entries.
B. Provision accelerators in AWS Global Accelerator.
Associate the supplied IP addresses with the S3 bucket.
Edit the Route 53 entries to point to the IP addresses of the accelerators.
C. Add an Amazon CloudFront distribution in front of the S3 bucket.

Edit the Route 53 entries to point to the CloudFront distribution.

D. Enable S3 Transfer Acceleration on the bucket.
Edit the Route 53 entries to point to the new endpoint.

Answer: C

QUESTION 204
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 more than 10 million rows. The database has 2 TB of General Purpose SSD storage. There are millions of updates against this data every day through the company's website.
The company has noticed that some insert operations are taking 10 seconds or longer.
The company has determined that the database storage performance is the problem.
Which solution addresses this performance issue?

A. Change the storage type to Provisioned IOPS SSD
B. Change the DB instance to a memory optimized instance class
C. Change the DB instance to a burstable performance instance class
D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Answer: A
Explanation:
Provisioned IOPS volumes are backed by solid-state drives (SSDs) and are the highest performance EBS volumes designed for your critical, I/O intensive database applications. These volumes are ideal for both IOPS-intensive and throughput-intensive workloads that require extremely low latency.
https://aws.amazon.com/ebs/features/

QUESTION 205
A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size.
A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.
The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.

What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts.
Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket.
Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts.
Create a script on the EC2 instances that will store tne alerts in an Amazon S3 bucket.
Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts.
Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon Elasticsearch Service (Amazon ES) duster.
Set up the Amazon ES cluster to take manual snapshots every day and delete data from the duster that is older than 14 days
D. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts

and set the message retention period to 14 days.
Configure consumers to poll the SQS queue check the age of the message and analyze the message data as needed If the message is 14 days old the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue.

Answer: A
Explanation:
Definitely A, it's the most operationally efficient compared to D, which requires a lot of code and infrastructure to maintain. A is mostly managed (firehose is fully managed and S3 lifecycles are also managed).

QUESTION 206
A company's application integrates with multiple software-as-a-service (SaaS) sources for data collection. The company runs Amazon EC2 instances to receive the data and to upload the data to an Amazon S3 bucket for analysis. The same EC2 instance that receives and uploads the data also sends a notification to the user when an upload is complete. The company has noticed slow application performance and wants to improve the performance as much as possible.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an Auto Scaling group so that EC2 instances can scale out.
Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
B. Create an Amazon AppFlow flow to transfer data between each SaaS source and the S3 bucket.
Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for each SaaS source to send output data.
Configure the S3 bucket as the rule's target.
Create a second EventBridge (CloudWatch Events) rule to send events when the upload to the S3 bucket is complete.
Configure an Amazon Simple Notification Service (Amazon SNS) topic as the second rule's target.
D. Create a Docker container to use instead of an EC2 instance. Host the containerized application on Amazon Elastic Container Service (Amazon ECS).
Configure Amazon CloudWatch Container Insights to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

Answer: B
Explanation:
Amazon AppFlow is a fully managed integration service that enables you to securely transfer data between Software-as-a-Service (SaaS) applications like Salesforce, SAP, Zendesk, Slack, and ServiceNow, and AWS services like Amazon S3 and Amazon Redshift, in just a few clicks.
https://aws.amazon.com/appflow/

QUESTION 207
A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC. The EC2 instances run inside several subnets across multiple Availability Zones. The EC2 instances do not communicate with each other. However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway. The company is concerned about data transfer charges.
What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

A. Launch the NAT gateway in each Availability Zone
B. Replace the NAT gateway with a NAT instance
C. Deploy a gateway VPC endpoint for Amazon S3
D. Provision an EC2 Dedicated Host to run the EC2 instances

Answer: C
Explanation:
VPC gateway endpoints allow communication to Amazon S3 and Amazon DynamoDB without incurring data transfer charges within the same Region. On the other hand NAT gateway incurs additional data processing charges.
https://aws.amazon.com/blogs/architecture/overview-of-data-transfer-costs-for-common-architectures/

QUESTION 208
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
Explanation:
Direct connect is a dedicated connection between on-prem and AWS, this is the way to ensure stable network connectivity that will not wax and wane like internet connectivity.

QUESTION 209
A company has an Amazon S3 bucket that contains critical data. The company must protect the data from accidental deletion.
Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Enable versioning on the S3 bucket.
B. Enable MFA Delete on the S3 bucket.
C. Create a bucket policy on the S3 bucket.
D. Enable default encryption on the S3 bucket.
E. Create a lifecycle policy for the objects in the S3 bucket.

Answer: AB
Explanation:
To prevent or mitigate future accidental deletions, consider the following features:
- Enable versioning to keep historical versions of an object.

- Enable Cross-Region Replication of objects.
- Enable MFA delete to require multi-factor authentication (MFA) when deleting an object version.
https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-audit-deleted-missing-objects/

QUESTION 210
A company has a data ingestion workflow that consists the following:

```
- An Amazon Simple Notification Service (Amazon SNS) topic for
notifications about new data deliveries.
- An AWS Lambda function to process the data and record metadata
```

The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job.
Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Choose two.)

A. Configure the Lambda function In multiple Availability Zones.
B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe It to me SNS topic.
C. Increase the CPU and memory that are allocated to the Lambda function.
D. Increase provisioned throughput for the Lambda function.
E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue

Answer: BE
Explanation:
A, C, D options are wrong, since Lambda is fully managed service which provides high availability and scalability by its own.

QUESTION 211
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:
Geographic (Geo) Match Conditions in AWS WAF. This new condition type allows you to use AWS WAF to restrict application access based on the geographic location of your viewers. With geo match conditions you can choose the countries from which AWS WAF should allow access.
https://aws.amazon.com/about-aws/whats-new/2017/10/aws-waf-now-supports-geographic-match/

QUESTION 212

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.

QUESTION 213
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:
CloudFront is a content delivery network (CDN) offered by Amazon Web Services (AWS). It functions as a reverse proxy service that caches web content across AWS's global data centers, improving loading speeds and reducing the strain on origin servers. CloudFront can be used to efficiently deliver large amounts of static or dynamic content anywhere in the world.

QUESTION 214
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
Explanation:
The short name or full Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that grants containers in the task permission to call AWS APIs on your behalf.

QUESTION 215
A solutions architect needs to securely store a database user name and password that an application uses to access an Amazon RDS DB instance. The application that accesses the database runs on an Amazon EC2 instance. The solutions architect wants to create a secure parameter in AWS Systems Manager Parameter Store.
What should the solutions architect do to meet this requirement?

A. Create an IAM role that has read access to the Parameter Store parameter.
Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter.
Assign this IAM role to the EC2 instance.
B. Create an IAM policy that allows read access to the Parameter Store parameter.
Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter.
Assign this IAM policy to the EC2 instance.
C. Create an IAM trust relationship between the Parameter Store parameter and the EC2 instance.
Specify Amazon RDS as a principal in the trust policy.
D. Create an IAM trust relationship between the DB instance and the EC2 instance.
Specify Systems Manager as a principal in the trust policy.

Answer: A
Explanation:
There should be the Decrypt access to KMS.
"If you choose the SecureString parameter type when you create your parameter, Systems Manager uses AWS KMS to encrypt the parameter value."
https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html

QUESTION 216
A company is running a batch application on Amazon EC2 instances.
The application consists of a backend with multiple Amazon RDS databases.
The application is causing a high number of leads on the databases.
A solutions architect must reduce the number of database reads while ensuring high availability.
What should the solutions architect do to meet this requirement?

A. Add Amazon RDS read replicas.
B. Use Amazon ElasbCache for Redls.
C. Use Amazon Route 53 DNS caching.
D. Use Amazon ElastiCache for Memcached.

Answer: B
Explanation:
Use ElastiCache to reduce reading and choose redis to ensure high availability.

QUESTION 217

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) are one type of policy that you can use to manage your organization. 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.
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html.

QUESTION 218
A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application.
What should the solutions architect do to meet this requirement?

A. Add an Amazon Inspector agent to the ALB.
B. Configure Amazon Macie to prevent attacks.
C. Enable AWS Shield Advanced to prevent attacks.
D. Configure Amazon GuardDuty to monitor the ALB.

Answer: C
Explanation:
AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that helps protect web applications running on AWS from DDoS attacks. AWS Shield Advanced is an additional layer of protection that provides enhanced DDoS protection capabilities, including proactive monitoring and automatic inline mitigations, to help protect against even the largest and most sophisticated DDoS attacks. By enabling AWS Shield Advanced, the solutions architect can help protect the application from DDoS attacks and reduce the risk of disruption to the application.

QUESTION 219
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 Instances to handle additional capacity.
D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle

additional capacity.

Answer: D
Explanation:
We recommend that you use On-Demand Instances for applications with short-term, irregular workloads that cannot be interrupted.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-on-demand-instances.html

QUESTION 220
A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAF.
How should the solutions architect comply with these requirements?

A. Configure an S3 bucket policy lo 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
Explanation:
Use an OAI to lockdown CloudFront to S3 origin & enable WAF on CF distribution.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-awswaf.html

QUESTION 221
A company wants to manage Amazon Machine Images (AMIs). The company currently copies AMIs to the same AWS Region where the AMIs were created. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 Createlmage API operation is called within the company's account.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a Createlmage API call is detected.
B. Configure AWS CloudTrail with an Amazon Simple Notification Service (Amazon SNS) notification that occurs when updated logs are sent to Amazon S3.
Use Amazon Athena to create a new table and to query on Createlmage when an API call is detected.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the Createlmage API call. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a Createlmage API call is detected.
D. Configure an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a target for AWS CloudTrail logs.
Create an AWS Lambda function to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic when a Createlmage API call is detected.

Answer: C
Explanation:
To create an EventBridge rule to send a notification when an AMI is created and in the available state.
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html

QUESTION 222
An online retail company has more than 50 million active customers and receives more than 25,000 orders each day. The company collects purchase data for customers and stores this data in Amazon S3. Additional customer data is stored in Amazon RDS. The company wants to make all the data available to various teams so that the teams can perform analytics. The solution must provide the ability to manage fine-grained permissions for the data and must minimize operational overhead.
Which solution will meet these requirements?

A. Migrate the purchase data to write directly to Amazon RDS.
Use RDS access controls to limit access.
B. Schedule an AWS Lambda function to periodically copy data from Amazon RDS to Amazon S3.
Create an AWS Glue crawler.
Use Amazon Athena to query the data.
Use S3 policies to limit access.
C. Create a data lake by using AWS Lake Formation.
Create an AWS Glue JDBC connection to Amazon RDS.
Register (he S3 bucket in Lake Formation.
Use Lake Formation access controls to limit access.
D. Create an Amazon Redshift cluster.
Schedule an AWS Lambda function to periodically copy data from Amazon S3 and Amazon RDS to Amazon Redshift.
Use Amazon Redshift access controls to limit access.

Answer: C
Explanation:
Manage fine-grained access control using AWS Lake Formation.
https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/

QUESTION 223
A company owns an asynchronous API that is used to ingest user 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 Lambda to buffer writes to DynamoDB.
C. Create a secondary index in DynamoDB for the table with the user requests.
D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

Answer: D

Explanation:
because all other options put some more charges to DynamoDB. But the company supplied as much as they can for DynamoDB. And it is async request and we need to have retry mechanism not to lose the customer data.

QUESTION 224
A company needs to move data from an Amazon EC2 instance to an Amazon S3 bucket. The company must ensure that no API calls and no data are routed through public internet routes. Only the EC2 instance can have access to upload data to the S3 bucket.
Which solution will meet these requirements?

A. Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located.
Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
B. Create a gateway VPC endpoint for Amazon S3 in the Availability Zone where the EC2 instance is located.
Attach appropriate security groups to the endpoint.
Attach a resource policy lo the S3 bucket to only allow the EC2 instance's IAM role for access.
C. Run the nslookup tool from inside the EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint.
Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket.
Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
D. Use the AWS provided, publicly available ip-ranges.json tile to obtain the private IP address of the S3 bucket's service API endpoint.
Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket.
Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

Answer: A
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/connect-s3-vpc-endpoint/

QUESTION 225
A gaming company hosts a browser-based application on AWS. The users of the application consume a large number of videos and images that are stored in Amazon S3. This content is the same for all users.
The application has increased in popularity, and millions of users worldwide accessing these media files. The company wants to provide the files to the users while reducing the load on the origin.
Which solution meets these requirements MOST cost-effectively?

A. Deploy an AWS Global Accelerator accelerator in front of the web servers.
B. Deploy an Amazon CloudFront web distribution in front of the S3 bucket.
C. Deploy an Amazon ElastiCache for Redis instance in front of the web servers.
D. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers.

Answer: B
Explanation:
Cloud front is best for content delivery. Global Accelerator is best for non-HTTP (TCP/UDP) cases and supports HTTP cases as well but with static IP (elastic IP) or anycast IP address only.

QUESTION 226
A company has two applications: a sender application that sends messages with payloads to be

processed and a processing application intended to receive the messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1.000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.
Which solution meets these requirements and is the MOST operationally efficient?

A. Set up an Amazon EC2 instance running a Redis database.
Configure both applications to use the instance.
Store, process, and delete the messages, respectively.
B. Use an Amazon Kinesis data stream to receive the messages from the sender application.
Integrate the processing application with the Kinesis Client Library (KCL).
C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue.
Configure a dead-letter queue to collect the messages that failed to process.
D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process.
Integrate the sender application to write to the SNS topic.

Answer: C
Explanation:
Amazon SQS supports dead-letter queues (DLQ), which other queues (source queues) can target for messages that can't be processed (consumed) successfully.
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html

QUESTION 227
A company has an AWS account used for software engineering. The AWS account has access to the company's on-premises data center through a pair of AWS Direct Connect connections. All non-VPC traffic routes to the virtual private gateway.
A development team recently created an AWS Lambda function through the console.
The development team needs to allow the function to access a database that runs in a private subnet in the company's data center.
Which solution will meet these requirements?

A. Configure the Lambda function to run in the VPC with the appropriate security group.
B. Set up a VPN connection from AWS to the data center. Route the traffic from the Lambda function through the VPN.
C. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.
D. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

Answer: C
Explanation:
To connect to another AWS service, you can use VPC endpoints for private communications between your VPC and supported AWS services. An alternative approach is to use a NAT gateway to route outbound traffic to another AWS service.
To give your function access to the internet, route outbound traffic to a NAT gateway in a public subnet. The NAT gateway has a public IP address and can connect to the internet through the VPC's internet gateway.
https://docs.aws.amazon.com/lambda/latest/dg/foundation-networking.html#foundation-nw-connecting

QUESTION 228
A company has a legacy data processing application that runs on Amazon EC2 instances. Data is processed sequentially, but the order of results does not matter. The application uses a monolithic architecture. The only way that the company can scale the application to meet increased demand is to increase the size of the instances.
The company's developers have decided to rewrite the application to use a microservices architecture on Amazon Elastic Container Service (Amazon ECS).
What should a solutions architect recommend for communication between the microservices?

A. Create an Amazon Simple Queue Service (Amazon SQS) queue.
Add code to the data producers, and send data to the queue.
Add code to the data consumers to process data from the queue.
B. Create an Amazon Simple Notification Service (Amazon SNS) topic.
Add code to the data producers, and publish notifications to the topic.
Add code to the data consumers to subscribe to the topic.
C. Create an AWS Lambda function to pass messages.
Add code to the data producers to call the Lambda function with a data object.
Add code to the data consumers to receive a data object that is passed from the Lambda function.
D. Create an Amazon DynamoDB table.
Enable DynamoDB Streams.
Add code to the data producers to insert data into the table.
Add code to the data consumers to use the DynamoDB Streams API to detect new table entries and retrieve the data.

Answer: A
Explanation:
Queue has Limited throughput (300 msg/s without batching, 3000 msg/s with batching whereby up-to 10 msg per batch operation; Msg duplicates not allowed in the queue (exactly-once delivery); Msg order is preserved (FIFO); Queue name must end with .fifo

QUESTION 229
A hospital wants to create digital copies for its large collection of historical written records. The hospital will continue to add hundreds of new documents each day. The hospital's data team will scan the documents and will upload the documents to the AWS Cloud. A solutions architect must implement a solution to analyze the documents, extract the medical information, and store the documents so that an application can run SQL queries on the data. The solution must maximize scalability and operational efficiency.
Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

A. Write the document information to an Amazon EC2 instance that runs a MySQL database.
B. Write the document information to an Amazon S3 bucket.
Use Amazon Athena to query the data.
C. Create an Auto Scaling group of Amazon EC2 instances to run a custom application that processes the scanned files and extracts the medical information.
D. Create an AWS Lambda function that runs when new documents are uploaded.
Use Amazon Rekognition to convert the documents to raw text.
Use Amazon Transcribe Medical to detect and extract relevant medical information from the text.
E. Create an AWS Lambda function that runs when new documents are uploaded.
Use Amazon Textract to convert the documents to raw text.
Use Amazon Comprehend Medical to detect and extract relevant medical information from the

text.

Answer: BE

QUESTION 230
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-lime and on-demand streaming?

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

Answer: A
Explanation:
You can use CloudFront to deliver video on demand (VOD) or live streaming video using any HTTP origin. One way you can set up video workflows in the cloud is by using CloudFront together with AWS Media Services.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html

QUESTION 231
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 and then create a read replica in a separate AWS Region that synchronously replicates the data.
D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Answer: B
Explanation:
Q: What does Amazon RDS manage on my behalf?
Amazon RDS manages the work involved in setting up a relational database: from provisioning the infrastructure capacity you request to installing the database software. Once your database is up and running, Amazon RDS automates common administrative tasks such as performing backups and patching the software that powers your database. With optional Multi-AZ deployments, Amazon RDS also manages synchronous data replication across Availability Zones with automatic failover.
https://aws.amazon.com/rds/faqs/

QUESTION 232

An ecommerce company hosts its analytics application in the AWS Cloud. The application generates about 300 MB of data each month. The data is stored in JSON format. The company is evaluating a disaster recovery solution to back up the data. The data must be accessible in milliseconds if it is needed, and the data must be kept for 30 days.
Which solution meets these requirements MOST cost-effectively?

A. Amazon OpenSearch Service (Amazon Elasticsearch Service)
B. Amazon S3 Glacier
C. Amazon S3 Standard
D. Amazon RDS for PostgreSQL

Answer: C

QUESTION 233
A company has a Windows-based application that must be migrated to AWS. The application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zones.
What should a solutions architect do to meet this requirement?

A. Configure AWS Storage Gateway in volume gateway mode.
Mount the volume to each Windows instance.
B. Configure Amazon FSx for Windows File Server.
Mount the Amazon FSx file system to each Windows instance.
C. Configure a file system by using Amazon Elastic File System (Amazon EFS).
Mount the EFS file system to each Windows instance.
D. Configure an Amazon Elastic Block Store (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: B
Explanation:
Microsoft Windows-based application = shared Windows file system = Amazon FSX for Windows
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonEFS.html

QUESTION 234
A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications.
Which action should the solutions architect take?

A. Configure a CloudFront signed URL.
B. Configure a CloudFront signed cookie.
C. Configure a CloudFront field-level encryption profile.
D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy.

Answer: C
Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html
"With Amazon CloudFront, you can enforce secure end-to-end connections to origin servers by

using HTTPS. Field-level encryption adds an additional layer of security that lets you protect specific data throughout system processing so that only certain applications can see it."

QUESTION 235

A company is planning to move its data to an Amazon S3 bucket. The data must be encrypted when it is stored in the S3 bucket. Additionally, the encryption key must be automatically rotated every year. Which solution will meet these requirements with the LEAST operational overhead?

A. Move the data to the S3 bucket.
Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).
Use the built-in key rotation behavior of SSE-S3 encryption keys.

B. Create an AWS Key Management Service (AWS KMS) customer managed key.
Enable automatic key rotation.
Set the S3 bucket's default encryption behavior to use the customer managed KMS key.
Move the data to the S3 bucket.

C. Create an AWS Key Management Service (AWS KMS) customer managed key.
Set the S3 bucket's default encryption behavior to use the customer managed KMS key.
Move the data to the S3 bucket.
Manually rotate the KMS key every year.

D. Encrypt the data with customer key material before moving the data to the S3 bucket.
Create an AWS Key Management Service (AWS KMS) key without key material.
Import the customer key material into the KMS key.
Enable automatic key rotation.

Answer: B

Explanation:

https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html
Customer managed keys
Automatic key rotation is disabled by default on customer managed keys but authorized users can enable and disable it. When you enable (or re-enable) automatic key rotation, AWS KMS automatically rotates the KMS key one year (approximately 365 days) after the enable date and every year thereafter.

QUESTION 236

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

Explanation:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html
A VPC endpoint for DynamoDB enables Amazon EC2 instances in your VPC to use their private IP addresses to access DynamoDB with no exposure to the public internet. Your EC2 instances do not require public IP addresses, and you don't need an internet gateway, a NAT device, or a virtual private gateway in your VPC. You use endpoint policies to control access to DynamoDB. Traffic between your VPC and the AWS service does not leave the Amazon network.

QUESTION 237
A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions 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 Lambda for tax computations.
C. Create an Application Load Balancer that has two Amazon EC2 instances behind it.
The EC2 instances will compute the tax on the received 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
Explanation:
Lambda server-less is scalable and elastic than EC2 api gateway solution.

QUESTION 238
A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company's HPC workloads run on Linux. Each HPC workflow runs on hundreds of AmazonEC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.
The company seeks a cloud storage solution that permits the copying of on premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files.
Which combination of AWS services meets these requirements?

A. Amazon FSx for Lustre integrated with Amazon S3
B. Amazon FSx for Windows File Server integrated with Amazon S3
C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Answer: A
Explanation:
https://aws.amazon.com/fsx/lustre/
Amazon FSx for Lustre is a fully managed service that provides cost-effective, high-performance, scalable storage for compute workloads. Many workloads such as machine learning, high performance computing (HPC), video rendering, and financial simulations depend on compute instances accessing the same set of data through high-performance shared storage.

QUESTION 239
A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda.
The application's traffic recently spiked due to fraudulent requests from botnets.
Which steps should a solutions architect take to block requests from unauthorized users? (Choose two.)

A. Create a usage plan with an API key that is shared with genuine users only.
B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses.
C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out.
D. Convert the existing public API to a private API.
Update the DNS records to redirect users to the new API endpoint.
E. Create an IAM role for each user attempting to access the API.
A user will assume the role when making the API call.

Answer: AC
Explanation:
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html

QUESTION 240
A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.
What should the solutions architect do to ensure that the architecture supports distributed session data management?

A. Use Amazon ElastiCache to manage and store session data.
B. Use session affinity (sticky sessions) of the ALB to manage session data.
C. Use Session Manager from AWS Systems Manager to manage the session.
D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session

Answer: A
Explanation:
https://aws.amazon.com/vi/caching/session-management/
In order to address scalability and to provide a shared data storage for sessions that can be accessible from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution to for this is to leverage an In-Memory Key/Value store such as Redis and Memcached. ElastiCache offerings for In-Memory key/value stores include ElastiCache for Redis, which can support replication, and ElastiCache for Memcached which does not support replication.

QUESTION 241
A company hosts a marketing website in an on-premises data center. The website consists of static documents and runs on a single server. An administrator updates the website content infrequently and uses an SFTP client to upload new documents.
The company decides to host its website on AWS and to use Amazon CloudFront. The company's solutions architect creates a CloudFront distribution. The solutions architect must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin.
Which solution will meet these requirements?

A. Create a virtual server by using Amazon Lightsail.
Configure the web server in the Lightsail instance.

Upload website content by using an SFTP client.

B. Create an AWS Auto Scaling group for Amazon EC2 instances.
   Use an Application Load Balancer.
   Upload website content by using an SFTP client.
C. Create a private Amazon S3 bucket.
   Use an S3 bucket policy to allow access from a CloudFront origin access identity (OAI).
   Upload website content by using the AWS CLI.
D. Create a public Amazon S3 bucket. Configure AWS Transfer for SFTP.
   Configure the S3 bucket for website hosting.
   Upload website content by using the SFTP client.

Answer: C
Explanation:
AWS transfer is a cost and doesn't mention using CloudFront.
https://aws.amazon.com/aws-transfer-family/pricing/

QUESTION 242
A company is designing a cloud communications platform that is driven by APIs. The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB). The company uses Amazon API Gateway to provide external users with access to the application through APIs. The company wants to protect the platform against web exploits like SQL injection and also wants to detect and mitigate large, sophisticated DDoS attacks.
Which combination of solutions provides the MOST protection? (Choose two.)

A. Use AWS WAF to protect the NLB.
B. Use AWS Shield Advanced with the NLB.
C. Use AWS WAF to protect Amazon API Gateway.
D. Use Amazon GuardDuty with AWS Shield Standard.
E. Use AWS Shield Standard with Amazon API Gateway.

Answer: BC
Explanation:
AWS Shield Advanced - DDos attacks
AWS WAF to protect Amazon API Gateway, because WAF sits before the API Gateway and then comes NLB.

QUESTION 243
A company has a web application that is based on Java and PHP. The company plans to move the application from on premises to AWS. The company needs the ability to test new site features frequently. The company also needs a highly available and managed solution that requires minimum operational overhead.
Which solution will meet these requirements?

A. Create an Amazon S3 bucket.
   Enable static web hosting on the S3 bucket.
   Upload the static content to the S3 bucket.
   Use AWS Lambda to process all dynamic content.
B. Deploy the web application to an AWS Elastic Beanstalk environment.
   Use URL swapping to switch between multiple Elastic Beanstalk environments for feature testing.
C. Deploy the web application lo Amazon EC2 instances that are configured with Java and PHP.
   Use Auto Scaling groups and an Application Load Balancer to manage the website's availability.
D. Containerize the web application.

Deploy the web application to Amazon EC2 instances.
Use the AWS Load Balancer Controller to dynamically route traffic between containers that contain the new site features for testing.

Answer: B
Explanation:
Elastic Beanstalk is a fully managed service that makes it easy to deploy and run applications in the AWS; To enable frequent testing of new site features, you can use URL swapping to switch between multiple Elastic Beanstalk environments.
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html

QUESTION 244
A company has a Microsoft .NET application that runs on an on-premises Windows Server. The application stores data by using an Oracle Database Standard Edition server. The company is planning a migration to AWS and wants to minimize development changes while moving the application. The AWS application environment should be highly available.
Which combination of actions should the company take to meet these requirements? (Choose two.)

A. Refactor the application as serverless with AWS Lambda functions running .NET Core.
B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
C. Replatform the application to run on Amazon EC2 with the Amazon Linux Amazon Machine Image (AMI).
D. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment.
E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

Answer: BE
Explanation:
Company wants to minimize development modifications throughout the process. Option A & C i.e. refactoring or re-platforming options get eliminated. As for option D, oracle to dynamo DB is not possible.

QUESTION 245
A rapidly growing ecommerce company is running its workloads in a single AWS Region. A solutions architect must create a disaster recovery (DR) strategy that includes a different AWS Region. The company wants its database to be up to date in the DR Region with the least possible latency. The remaining infrastructure in the DR Region needs to run at reduced capacity and must be able to scale up if necessary.
Which solution will meet these requirements with the LOWEST recovery time objective (RTO)?

A. Use an Amazon Aurora global database with a pilot light deployment
B. Use an Amazon Aurora global database with a warm standby deployment
C. Use an Amazon RDS Multi-AZ DB instance with a pilot light deployment
D. Use an Amazon RDS Multi-AZ DB instance with a warm standby deployment

Answer: B
Explanation:
In case of disaster, both pilot light and warm standby offer the capability to limit data loss (RPO). Both offer sufficient RTO performance that enables you to limit downtime. Between these two strategies, you have a choice of optimizing for RTO or for cost.

https://aws.amazon.com/es/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/

QUESTION 246
A company's order system sends requests from clients to Amazon EC2 instances. The EC2 instances process the orders and then store the orders in a database on Amazon RDS. Users report that they must reprocess orders when the system fails. The company wants a resilient solution that can process orders automatically if a system outage occurs.
What should a solutions architect do to meet these requirements?

A. Move the EC2 instances into an Auto Scaling group.
Create an Amazon EventBridge (Amazon CloudWatch Events) rule to target an Amazon Elastic Container Service (Amazon ECS) task.
B. Move the EC2 instances into an Auto Scaling group behind an Application Load Balancer (ALB).
Update the order system to send messages to the ALB endpoint.
C. Move the EC2 instances into an Auto Scaling group.
Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue.
Configure the EC2 instances to consume messages from the queue.
D. Create an Amazon Simple Notification Service (Amazon SNS) topic.
Create an AWS Lambda function, and subscribe the function to the SNS topic.
Configure the order system to send messages to the SNS topic.
Send a command to the EC2 instances to process the messages by using AWS Systems Manager Run Command.

Answer: C

QUESTION 247
A company runs an application on a large fleet of Amazon EC2 instances. The application reads and write entries into an Amazon DynamoDB table. The size of the DynamoDB table continuously grows, but the application needs only data from the last 30 days. The company needs a solution that minimizes cost and development effort.
Which solution meets these requirements?

A. Use an AWS CloudFormation template to deploy the complete solution.
Redeploy the CloudFormation stack every 30 days, and delete the original stack.
B. Use an EC2 instance that runs a monitoring application from AWS Marketplace.
Configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp when a new item is created in the table.
Use a script that runs on the EC2 instance to delete items that have a timestamp that is older than 30 days.
C. Configure Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table.
Configure the Lambda function to delete items in the table that are older than 30 days.
D. Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table.
Configure DynamoDB to use the attribute as the TTL attribute.

Answer: D
Explanation:
Amazon DynamoDB Time to Live (TTL) allows you to define a per-item timestamp to determine when an item is no longer needed. Shortly after the date and time of the specified timestamp, DynamoDB deletes the item from your table without consuming any write throughput. TTL is

provided at no extra cost as a means to reduce stored data volumes by retaining only the items that remain current for your workload's needs.
TTL is useful if you store items that lose relevance after a specific time. The following are example TTL use cases:
- Remove user or sensor data after one year of inactivity in an application.
- Archive expired items to an Amazon S3 data lake via Amazon DynamoDB Streams and AWS Lambda.
- Retain sensitive data for a certain amount of time according to contractual or regulatory obligations.

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html

QUESTION 248
A company runs a containerized application on a Kubernetes cluster in an on-premises data center. The company is using a MongoDB database for data storage.
The company wants to migrate some of these environments to AWS, but no code changes or deployment method changes are possible at this time. The company needs a solution that minimizes operational overhead.
Which solution meets these requirements?

A. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes for compute and MongoOB on EC2 for data storage.
B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute and Amazon DynamoDB tor data storage.
C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes for compute and Amazon DynamoDB for data storage.
D. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage.

Answer: D
Explanation:
Amazon DocumentDB (with MongoDB compatibility) is a fast, reliable, and fully managed database service. Amazon DocumentDB makes it easy to set up, operate, and scale MongoDB-compatible databases in the cloud. With Amazon DocumentDB, you can run the same application code and use the same drivers and tools that you use with MongoDB.
https://docs.aws.amazon.com/documentdb/latest/developerguide/what-is.html

QUESTION 249
A company selves a dynamic website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The website needs to support multiple languages to serve customers around the world. The website's architecture is running in the us-west-1 Region and is exhibiting high request latency tor users that are located in other parts of the world. The website needs to serve requests quickly and efficiently regardless of a user's location. However the company does not want to recreate the existing architecture across multiple Regions.
What should a solutions architect do to meet these requirements?

A. Replace the existing architecture with a website that is served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
Set the cache behavior settings to cache based on the Accept-Language request header.
B. Configure an Amazon CloudFront distribution with the ALB as the origin.
Set the cache behavior settings to cache based on the Accept-Language request header.
C. Create an Amazon API Gateway API that is integrated with the ALB.
Configure the API to use the HTTP integration type.

Set up an API Gateway stage to enable the API cache based on the Accept-Language request header.

D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region.
Put all the EC2 instances and the ALB behind an Amazon Route 53 record set with a geotocation routing policy.

Answer: B
Explanation:
Configuring caching based on the language of the viewer.
If you want CloudFront to cache different versions of your objects based on the language specified in the request, configure CloudFront to forward the Accept-Language header to your origin.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html

QUESTION 250
A telemarketing company is designing its customer call center functionality on AWS. The company needs a solution to provides multiples ipsafcar recognition and generates transcript files. The company wants to query the transcript files to analyze the business patterns. The transcript files must be stored for 7 years for auditing policies.
Which solution will meet these requirements?

A. Use Amazon Rekognition for multiple speaker recognition.
Store the transcript files in Amazon S3.
Use machine teaming models for transcript file analysis.
B. Use Amazon Transcribe for multiple speaker recognition.
Use Amazon Athena for transcript file analysts
C. Use Amazon Translate for multiple speaker recognition.
Store the transcript files in Amazon Redshift.
Use SQL queues for transcript file analysis
D. Use Amazon Rekognition for multiple speaker recognition.
Store the transcript files in Amazon S3.
Use Amazon Textract for transcript file analysis.

Answer: B
Explanation:
Amazon Transcribe now supports speaker labeling for streaming transcription. Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for you to convert speech-to-text. In live audio transcription, each stream of audio may contain multiple speakers. Now you can conveniently turn on the ability to label speakers, thus helping to identify who is saying what in the output transcript.
https://aws.amazon.com/about-aws/whats-new/2020/08/amazon-transcribe-supports-speaker-labeling-streaming-transcription/

QUESTION 251
A company stores data in an Amazon Aurora PostgreSQL DB cluster. The company must store all the data for 5 years and must delete all the data after 5 years. The company also must indefinitely keep audit logs of actions that are performed within the database. Currently, the company has automated backups configured for Aurora.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Take a manual snapshot of the DB cluster.
B. Create a lifecycle policy for the automated backups.
C. Configure automated backup retention for 5 years.
D. Configure an Amazon CloudWatch Logs export for the DB cluster.
E. Use AWS Backup to take the backups and to keep the backups for 5 years.

Answer: DE
Explanation:
AWS Backup adds Amazon Aurora database cluster snapshots as its latest protected resource. Starting today, you can use AWS Backup to manage Amazon Aurora database cluster snapshots. AWS Backup can centrally configure backup policies, monitor backup activity, copy a snapshot within and across AWS regions, except for China regions, where snapshots can only be copied from one China region to another.

QUESTION 252
A company has a small Python application that processes JSON documents and outputs the results to an on-premises SQL database. The application runs thousands of times each day. The company wants to move the application to the AWS Cloud. The company needs a highly available solution that maximizes scalability and minimizes operational overhead.

Which solution will meet these requirements?

A. Place the JSON documents in an Amazon S3 bucket.
Run the Python code on multiple Amazon EC2 instances to process the documents.
Store the results in an Amazon Aurora DB cluster.
B. Place the JSON documents in an Amazon S3 bucket.
Create an AWS Lambda function that runs the Python code to process the documents as they arrive in the S3 bucket.
Store the results in an Amazon Aurora DB cluster.
C. Place the JSON documents in an Amazon Elastic Block Store (Amazon EBS) volume.
Use the EBS Multi-Attach feature to attach the volume to multiple Amazon EC2 instances.
Run the Python code on the EC2 instances to process the documents.
Store the results on an Amazon RDS DB instance.
D. Place the JSON documents in an Amazon Simple Queue Service (Amazon SQS) queue as messages.
Deploy the Python code as a container on an Amazon Elastic Container Service (Amazon ECS) cluster that is configured with the Amazon EC2 launch type.
Use the container to process the SQS messages.
Store the results on an Amazon RDS DB instance.

Answer: B
Explanation:
By placing the JSON documents in an S3 bucket, the documents will be stored in a highly durable and scalable object storage service. The use of AWS Lambda allows the company to run their Python code to process the documents as they arrive in the S3 bucket without having to worry about the underlying infrastructure. This also allows for horizontal scalability, as AWS Lambda will automatically scale the number of instances of the function based on the incoming rate of requests. The results can be stored in an Amazon Aurora DB cluster, which is a fully-managed, high-performance database service that is compatible with MySQL and PostgreSQL. This will provide the necessary durability and scalability for the results of the processing.
https://aws.amazon.com/rds/aurora/

QUESTION 253
A company's infrastructure consists of Amazon EC2 instances and an Amazon RDS DB instance in a single AWS Region. The company wants to back up its data in a separate Region.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Backup to copy EC2 backups and RDS backups to the separate Region.
B. Use Amazon Data Lifecycle Manager (Amazon DLM) to copy EC2 backups and RDS backups to the separate Region.
C. Create Amazon Machine Images (AMIs) of the EC2 instances.
Copy the AMIs to the separate Region.
Create a read replica for the RDS DB instance in the separate Region.
D. Create Amazon Elastic Block Store (Amazon EBS) snapshots.
Copy the EBS snapshots to the separate Region.
Create RDS snapshots.
Export the RDS snapshots to Amazon S3.
Configure S3 Cross-Region Replication (CRR) to the separate Region.

Answer: A
Explanation:
Cross-Region backup
Using AWS Backup, you can copy backups to multiple different AWS Regions on demand or automatically as part of a scheduled backup plan. Cross-Region backup is particularly valuable if you have business continuity or compliance requirements to store backups a minimum distance away from your production data.
https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html

QUESTION 254
A company is building a new dynamic ordering website. The company wants to minimize server maintenance and patching. The website must be highly available and must scale read and write capacity as quickly as possible to meet changes in user demand.

Which solution will meet these requirements?

A. Host static content in Amazon S3.
Host dynamic content by using Amazon API Gateway and AWS Lambda.
Use Amazon DynamoDB with on-demand capacity for the database.
Configure Amazon CloudFront to deliver the website content.
B. Host static content in Amazon S3.
Host dynamic content by using Amazon API Gateway and AWS Lambda.
Use Amazon Aurora with Aurora Auto Scaling for the database.
Configure Amazon CloudFront to deliver the website content.
C. Host all the website content on Amazon EC2 instances.
Create an Auto Scaling group to scale the EC2 instances.
Use an Application Load Balancer to distribute traffic.
Use Amazon DynamoDB with provisioned write capacity for the database.
D. Host all the website content on Amazon EC2 instances.
Create an Auto Scaling group to scale the EC2 instances.
Use an Application Load Balancer to distribute traffic.
Use Amazon Aurora with Aurora Auto Scaling for the database.

Answer: A
Explanation:
On-demand mode is a good option if any of the following are true:

You create new tables with unknown workloads.
You have unpredictable application traffic.
You prefer the ease of paying for only what you use.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html

QUESTION 255
A company uses Amazon S3 as its data lake. The company has a new partner that must use SFTP to upload data files. A solutions architect needs to implement a highly available SFTP solution that minimizes operational overhead.

Which solution will meet these requirements?

A. Use AWS Transfer Family to configure an SFTP-enabled server with a publicly accessible endpoint.
Choose the S3 data lake as the destination.
B. Use Amazon S3 File Gateway as an SFTP server.
Expose the S3 File Gateway endpoint URL to the new partner. Share the S3 File Gateway endpoint with the new partner.
C. Launch an Amazon EC2 instance in a private subnet in a VPInstruct the new partner to upload files to the EC2 instance by using a VPN.
Run a cron job script, on the EC2 instance to upload files to the S3 data lake.
D. Launch Amazon EC2 instances in a private subnet in a VPC.
Place a Network Load Balancer (NLB) in front of the EC2 instances.
Create an SFTP listener port for the NLB. Share the NLB hostname with the new partner.
Run a cron job script on the EC2 instances to upload files to the S3 data lake.

Answer: A
Explanation:
AWS Transfer for SFTP, a fully-managed, highly-available SFTP service. You simply create a server, set up user accounts, and associate the server with one or more Amazon Simple Storage Service (Amazon S3) buckets.

QUESTION 256
A company needs to store contract documents. A contract lasts for 5 years. During the 5-year period, the company must ensure that the documents cannot be overwritten or deleted. The company needs to encrypt the documents at rest and rotate the encryption keys automatically every year.

Which combination of steps should a solutions architect take to meet these requirements with the LEAST operational overhead? (Choose two.)

A. Store the documents in Amazon S3.
Use S3 Object Lock in governance mode.
B. Store the documents in Amazon S3.
Use S3 Object Lock in compliance mode.
C. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).
Configure key rotation.
D. Use server-side encryption with AWS Key Management Service (AWS KMS) customer managed keys.
Configure key rotation.
E. Use server-side encryption with AWS Key Management Service (AWS KMS) customer provided

(imported) keys.
Configure key rotation.

Answer: BD

QUESTION 257
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 258
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 259
A company's application is running on Amazon EC2 instances in 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
Explanation:
By default, when you create an AMI from an instance, snapshots are taken of each EBS volume attached to the instance. AMIs can launch with multiple EBS volumes attached, allowing you to replicate both an instance's configuration and the state of all the EBS volumes that are attached to that instance.
https://aws.amazon.com/premiumsupport/knowledge-center/create-ami-ebs-backed/

QUESTION 260
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 261
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 262
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 263
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 264
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 265
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 266
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 267
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 268
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 269
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 270
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 271
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 272
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 273
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
Explanation:
If you are creating a step policy, you can specify the number of seconds that it takes for a newly launched instance to warm up. Until its specified warm-up time has expired, an instance is not counted toward the aggregated metrics of the Auto Scaling group.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html#as-step-scaling-warmup

QUESTION 274
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 275
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 276
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 277
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: 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 278
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 279
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 280
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

Explanation:
Intelligent tearing moves data between storage classes based on its current degree of usage.

QUESTION 281
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: C
Explanation:
The transfer is between EC2 instances and not just between S3 and EC2.
Also, be aware of inter-Availability Zones data transfer charges between Amazon EC2 instances, even within the same region. If possible, the instances in a development or test environment that need to communicate with each other should be co-located within the same Availability Zone to avoid data transfer charges. (This doesn't apply to production workloads which will most likely need to span multiple Availability Zones for high availability.)
https://aws.amazon.com/blogs/mt/using-aws-cost-explorer-to-analyze-data-transfer-costs/

QUESTION 282
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 283
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? (Choose 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 can't let the services in VPC allow access to the bucket .

QUESTION 284
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 12, 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 285
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: A
Explanation:
VPC with public and private subnets (NAT)
The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet. We recommend this scenario if you want to run a public-facing web application, while maintaining back-end servers that aren't publicly accessible. A common example is a multi-tier website, with the web servers in a public subnet and the database servers in a private subnet. You can set up security and routing so that the web servers can communicate with the database servers.
The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet can't. Instead, the instances in the private subnet can access the Internet by using a network address translation (NAT) gateway that resides in the public subnet. The database servers can connect to the Internet for software updates using the NAT gateway, but the Internet cannot establish connections to the database servers.
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

QUESTION 286
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 287
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 288
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 289
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 290
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 291
A solutions 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 solutions 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 WAF 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 them in Amazon S3.
   Create a custom AWS Lambda function that parses the togs looking for a DDoS attack.
   Modify a network ACL to block identified source IP addresses.
D. Enable Amazon GuardDuty and configure findings written to Amazon CloudWatch.
   Create an event with CloudWatch Events for DDoS alerts that triggers Amazon Simple Notification Service (Amazon SNS) .
   Have Amazon 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
Explanation:
AWS WAF is a web application firewall that helps detect and mitigate web application layer DDoS attacks by inspecting traffic inline. Application layer DDoS attacks use well-formed but malicious requests to evade mitigation and consume application resources. You can define custom security rules (also called web ACLs) that contain a set of conditions, rules, and actions to block attacking traffic. After you define web ACLs, you can apply them to CloudFront distributions, and web ACLs are evaluated in the priority order you specified when you configured them. Real-time metrics and sampled web requests are provided for each web ACL.
https://aws.amazon.com/blogs/security/how-to-protect-dynamic-web-applications-against-ddos-attacks-by-using-amazon-cloudfront-and-amazon-route-53/

QUESTION 292
A company is creating a prototype of an ecommerce website on AWS. The website consists of an Application Load Balancer, an Auto Scaling group of Amazon EC2 instances for web servers, and an Amazon RDS for MySQL DB instance that runs with the Single-AZ configuration.
The website is slow to respond during searches of the product catalog. The product catalog is a group of tables in the MySQL database that the company does not update frequently. A solutions architect has determined that the CPU utilization on the DB instance is high when product catalog searches occur.
What should the solutions architect recommend to improve the performance of the website during searches of the product catalog?

A. Migrate the product catalog to an Amazon Redshift database.
   Use the COPY command to load the product catalog tables.
B. Implement an Amazon ElastiCache for Redis cluster to cache the product catalog.
   Use lazy loading to populate the cache.
C. Add an additional scaling policy to the Auto Scaling group to launch additional EC2 instances when database response is slow.
D. Turn on the Multi-AZ configuration for the DB instance.
   Configure the EC2 instances to throttle the product catalog queries that are sent to the database.

Answer: B
Explanation:
Common ElastiCache Use Cases and How ElastiCache Can Help :
Whether serving the latest news, a top-10 leaderboard, a product catalog, or selling tickets to an event, speed is the name of the game. The success of your website and business is greatly affected by the speed at which you deliver content.
https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/elasticache-use-cases.html

QUESTION 293
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 autoscaling:EC2_INSTANCE_LAUNCH events.

Answer: B
Explanation:
Amazon EC2 Auto Scaling supports sending Amazon SNS notifications when the following events occur.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

QUESTION 294
A company is creating an application that runs on containers in a VPC. The application stores and accesses data in an Amazon S3 bucket. During the development phase, the application will store and access 1 TB of data in Amazon S3 each day. The company wants to minimize costs and wants to prevent traffic from traversing the internet whenever possible.
Which solution will meet these requirements?

A. Enable S3 Intelligent-Tiering for the S3 bucket.
B. Enable S3 Transfer Acceleration for the S3 bucket.
C. Create a gateway VPC endpoint for Amazon S3. Associate this endpoint with all route tables in the VPC.
D. Create an interface endpoint for Amazon S3 in the VPC. Associate this endpoint with all route tables in the VPC.

Answer: C

QUESTION 295
A solutions architect is tasked with transferring 750 TB of data from an on-premises network-attached file system located at a branch office Amazon S3 Glacier.
The migration must not saturate the on-premises 1 Mbps internet connection.
Which solution will meet these requirements?

A. Create an AWS site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly. Transfer the files directly by using the AWS CLI.
B. Order 10 AWS Snowball Edge Storage Optimized devices, and select an S3 Glacier vault as the destination.
C. Mount the network-attached file system to an S3 bucket, and copy the files directly.
Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
D. Order 10 AWS Snowball Edge Storage Optimized devices, 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:
To upload existing data to Amazon S3 Glacier (S3 Glacier), you might consider using one of the AWS Snowball device types to import data into Amazon S3, and then move it to the S3 Glacier storage class for archival using lifecycle rules. When you transition Amazon S3 objects to the S3 Glacier storage class, Amazon S3 internally uses S3 Glacier for durable storage at lower cost. Although the objects are stored in S3 Glacier, they remain Amazon S3 objects that you manage in Amazon S3, and you cannot access them directly through S3 Glacier.
https://docs.aws.amazon.com/amazonglacier/latest/dev/uploading-an-archive.html

QUESTION 296
A company's website handles millions of requests each day, and the number of requests continues to increase. A solutions architect needs to improve the response time of the web application. The solutions architect determines that the application needs to decrease latency when retrieving product details from the
Amazon DynamoDB table.
Which solution will meet these requirements with the LEAST amount of operational overhead?

A. Set up a DynamoDB Accelerator (DAX) cluster.
Route all read requests through DAX.
B. Set up Amazon ElastiCache for Redis between the DynamoDB table and the web application.
Route all read requests through Redis.
C. Set up Amazon ElastiCache for Memcached between the DynamoDB table and the web application.
Route all read requests through Memcached.
D. Set up Amazon DynamoDB Streams on the table, and have AWS Lambda read from the table and populate Amazon ElastiCache. Route all read requests through ElastiCache.

Answer: A
Explanation:
Amazon DynamoDB is designed for scale and performance. In most cases, the DynamoDB response times can be measured in single-digit milliseconds. However, there are certain use cases that require response times in microseconds. For these use cases, DynamoDB Accelerator (DAX) delivers fast response times for accessing eventually consistent data.
DAX is a DynamoDB-compatible caching service that enables you to benefit from fast in-memory performance for demanding applications.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.html

QUESTION 297
A media company collects and analyzes user activity data on premises. The company wants to migrate this capability to AWS. The user activity data store will continue to grow and will be petabytes in size. The company needs to build a highly available data ingestion solution that facilitates on-demand analytics of existing data and new data with SQL.
Which solution will meet these requirements with the LEAST operational overhead?

A. Send activity data to an Amazon Kinesis data stream.
Configure the stream to deliver the data to an Amazon S3 bucket.
B. Send activity data to an Amazon Kinesis Data Firehose delivery stream.
Configure the stream to deliver the data to an Amazon Redshift cluster.
C. Place activity data in an Amazon S3 bucket.
Configure Amazon S3 to run an AWS Lambda function on the data as the data arrives in the S3 bucket.
D. Create an ingestion service on Amazon EC2 instances that are spread across multiple Availability

Zones.
Configure the service to forward data to an Amazon RDS Multi-AZ database.

Answer: B
Explanation:
Amazon Kinesis Data Firehose is a data transfer service for loading streaming data into Amazon S3, Splunk, ElasticSearch, and RedShift.
https://www.whizlabs.com/blog/aws-kinesis-data-streams-vs-aws-kinesis-data-firehose/

QUESTION 298
A company is using a centralized AWS account to store log data in various Amazon S3 buckets. A solutions architect needs to ensure that the data is encrypted at rest before the data is uploaded to the S3 buckets. The data also must be encrypted in transit.
Which solution meets these requirements?

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.
B. Use server-side encryption to encrypt the data that is being uploaded to the S3 buckets.
C. Create bucket policies that require the use of server-side encryption with S3 managed encryption keys (SSE-S3) for S3 uploads.
D. Enable the security option to encrypt the S3 buckets through the use of a default AWS Key Management Service (AWS KMS) key.

Answer: A
Explanation:
Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit using Secure Socket Layer/Transport Layer Security (SSL/TLS) or client-side encryption.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html

QUESTION 299
A company has an on-premises business application that generates hundreds of files each day. These files are stored on an SMB file share and require a low- latency connection to the application servers. A new company policy states all application-generated files must be copied to AWS. There is already a VPN connection to AWS.
The application development team does not have time to make the necessary code modifications to move the application to AWS.
Which service should a solutions architect recommend to allow the application to copy files to AWS?

A. Amazon Elastic File System (Amazon EFS)
B. Amazon FSx for Windows File Server
C. AWS Snowball
D. AWS Storage Gateway

Answer: D
Explanation:
The files will be on the storgare gateway with low latency and copied to AWS as a second copy. FSx in AWS will not provide low latency for the on prem apps over a vpn to the FSx file system.

QUESTION 300
A company has an ordering application that stores customer information in Amazon RDS for

MySQL. During regular business hours, employees run one-time queries for reporting purposes. Timeouts are occurring during order processing because the reporting queries are taking a long time to run. The company needs to eliminate the timeouts without preventing employees from performing queries.
What should a solutions architect do to meet these requirements?

A. Create a read replica. Move reporting queries to the read replica.
B. Create a read replica. Distribute the ordering application to the primary DB instance and the read replica.
C. Migrate the ordering application to Amazon DynamoDB with on-demand capacity.
D. Schedule the reporting queries for non-peak hours.

Answer: A
Explanation:
Reporting is OK to run on replicated data with some delay in replication.

QUESTION 301
A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.
Which feature should the solutions architect include in the design to meet this requirement?

A. Read replicas
B. Manual snapshots
C. Automated backups
D. Multi-AZ deployments

Answer: C
Explanation:
RDS creates automated backups of your volume snapshot in which you can recover to a specific point-in-time recovery.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html

QUESTION 302
A company uses Amazon RDS for PostgreSQL databases for its data tier. The company must implement password rotation for the databases.

Which solution meets this requirement with the LEAST operational overhead?

A. Store the password in AWS Secrets Manager.
Enable automatic rotation on the secret.
B. Store the password in AWS Systems Manager Parameter Store.
Enable automatic rotation on the parameter.
C. Store the password in AWS Systems Manager Parameter Store.
Write an AWS Lambda function that rotates the password.
D. Store the password in AWS Key Management Service (AWS KMS).
Enable automatic rotation on the customer master key (CMK).

Answer: A
Explanation:

Only service that rotates credentials automatically is secrets manager.
https://aws.amazon.com/secrets-manager/
https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html (reference note)

QUESTION 303
A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.

A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyze.

Which system architecture should the solutions architect recommend?

A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages. Configure the EC2 instance to save the results to an Amazon S3 bucket.
B. Create an HTTPS endpoint in Amazon API Gateway.
Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.
C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function.
Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.
D. Create a gateway VPC endpoint for Amazon S3.
Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Answer: B
Explanation:
Deploy Amazon API Gateway as an HTTPS endpoint and AWS Lambda to process and save the messages to an Amazon DynamoDB table. This option provides a highly available and scalable solution that can easily handle large amounts of data. It also integrates with other AWS services, making it easier to analyze and visualize the data for the security team.

QUESTION 304
An Amazon EC2 instance is located in a private subnet in a new VPC. This subnet does not have outbound internet access, but the EC2 instance needs the ability to download monthly security updates from an outside vendor.

What should a solutions architect do to meet these requirements?

A. Create an internet gateway, and attach it to the VPC.
Configure the private subnet route table to use the internet gateway as the default route.
B. Create a NAT gateway, and place it in a public subnet.
Configure the private subnet route table to use the NAT gateway as the default route.
C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located.
Configure the private subnet route table to use the NAT instance as the default route.
D. Create an internet gateway, and attach it to the VPC.
Create a NAT instance, and place it in the same subnet where the EC2 instance is located.
Configure the private subnet route table to use the internet gateway as the default route.

Answer: B

Explanation:
This approach will allow the EC2 instance to access the internet and download the monthly security updates while still being located in a private subnet. By creating a NAT gateway and placing it in a public subnet, it will allow the instances in the private subnet to access the internet through the NAT gateway. And then, configure the private subnet route table to use the NAT gateway as the default route. This will ensure that all outbound traffic is directed through the NAT gateway, allowing the EC2 instance to access the internet while still maintaining the security of the private subnet.

QUESTION 305
A company has been running a web application with an Oracle relational database in an on-premises data center for the past 15 years. The company must migrate the database to AWS. The company needs to reduce operational overhead without having to modify the application's code.

Which solution meets these requirements?

A. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon RDS.
B. Use Amazon EC2 instances to migrate and operate the database servers.
C. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon DynamoDB.
D. Use an AWS Snowball Edge Storage Optimized device to migrate the data from Oracle to Amazon Aurora.

Answer: A
Explanation:
DMS can be used for database migration(supports cross database migration too).
RDS supports MySQL, PostgreSQL, Microsoft SQL Server, Oracle.
https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-oracle-database-to-amazon-rds-for-oracle.html

QUESTION 306
A company is running an application on Amazon EC2 instances. Traffic to the workload increases substantially during business hours and decreases afterward. The CPU utilization of an EC2 instance is a strong indicator of end-user demand on the application. The company has configured an Auto Scaling group to have a minimum group size of 2 EC2 instances and a maximum group size of 10 EC2 instances.

The company is concerned that the current scaling policy that is associated with the Auto Scaling group might not be correct. The company must avoid over-provisioning EC2 instances and incurring unnecessary costs.

What should a solutions architect recommend to meet these requirements?

A. Configure Amazon EC2 Auto Scaling to use a scheduled scaling plan and launch an additional 8 EC2 instances during business hours.
B. Configure AWS Auto Scaling to use a scaling plan that enables predictive scaling.
Configure predictive scaling with a scaling mode of forecast and scale, and to enforce the maximum capacity setting during scaling.
C. Configure a step scaling policy to add 4 EC2 instances at 50% CPU utilization and add another 4 EC2 instances at 90% CPU utilization.
Configure scale-in policies to perform the reverse and remove EC2 instances based on the two

values.

D. Configure AWS Auto Scaling to have a desired capacity of 5 EC2 instances, and disable any existing scaling policies.
Monitor the CPU utilization metric for 1 week.
Then create dynamic scaling policies that are based on the observed values.

Answer: B
Explanation:
Predictive Scaling, now natively supported as an EC2 Auto Scaling policy, uses machine learning to schedule the right number of EC2 instances in anticipation of approaching traffic changes. Predictive Scaling predicts future traffic, including regularly-occurring spikes, and provisions the right number of EC2 instances in advance. Predictive Scaling's machine learning algorithms detect changes in daily and weekly patterns, automatically adjusting their forecasts. This removes the need for manual adjustment of Auto Scaling parameters as cyclicality changes over time, making Auto Scaling simpler to configure. Auto Scaling enhanced with Predictive Scaling delivers faster, simpler, and more accurate capacity provisioning resulting in lower cost and more responsive applications.

QUESTION 307
A company wants to use a custom distributed application that calculates various profit and loss scenarios. To achieve this goal, the company needs to provide a network connection between its Amazon EC2 instances. The connection must minimize latency and must maximize throughput

Which solution will meet these requirements?

A. Provision the application to use EC2 Dedicated Hosts of the same instance type.
B. Configure a placement group for EC2 instances that have the same instance type.
C. Use multiple AWS elastic network interfaces and link aggregation.
D. Configure AWS PrivateLink for the EC2 instances.

Answer: B
Explanation:
Cluster placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. They are also recommended when the majority of the network traffic is between the instances in the group. 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.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#placement-groups-cluster

QUESTION 308
A company needs to run a critical application on AWS. The company needs to use Amazon EC2 for the application’s database. The database must be highly available and must fail over automatically if a disruptive event occurs.
Which solution will meet these requirements?

A. Launch two EC2 instances, each in a different Availability Zone in the same AWS Region. Install the database on both EC2 instances. Configure the EC2 instances as a cluster. Set up database replication.
B. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use AWS CloudFormation to automate provisioning of the EC2 instance if a disruptive event occurs.

C. Launch two EC2 instances, each in a different AWS Region. Install the database on both EC2 instances. Set up database replication. Fail over the database to a second Region.
D. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use EC2 automatic recovery to recover the instance if a disruptive event occurs.

Answer: A
Explanation:
Configure the EC2 instances as a cluster) Cluster consist of one or more DB instances and a cluster volume that manages the data for those DB instances. Cluster Volume is a VIRTUAL DATABASE storage volume that spans multiple Availability Zones, with each Availability Zone having a copy of the DB cluster data.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.html

QUESTION 309
A company hosts its application on AWS. The company uses Amazon Cognito to manage users. When users log in to the application, the application fetches required data from Amazon DynamoDB by using a REST API that is hosted in Amazon API Gateway. The company wants an AWS managed solution that will control access to the REST API to reduce development efforts. Which solution will meet these requirements with the LEAST operational overhead?

A. Configure an AWS Lambda function to be an authorizer in API Gateway to validate which user made the request.
B. For each user, create and assign an API key that must be sent with each request. Validate the key by using an AWS Lambda function.
C. Send the user's email address in the header with every request. Invoke an AWS Lambda function to validate that the user with that email address has proper access.
D. Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request.

Answer: D
Explanation:
Use the Amazon Cognito console, CLI/SDK, or API to create a user pool—or use one that's owned by another AWS account.
https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html

QUESTION 310
A company is developing a marketing communications service that targets mobile app users. The company needs to send confirmation messages with Short Message Service (SMS) to its users. The users must be able to reply to the SMS messages. The company must store the responses for a year for analysis.
What should a solutions architect do to meet these requirements?

A. Create an Amazon Connect contact flow to send the SMS messages. Use AWS Lambda to process the responses.
B. Build an Amazon Pinpoint journey. Configure Amazon Pinpoint to send events to an Amazon Kinesis data stream for analysis and archiving.
C. Use Amazon Simple Queue Service (Amazon SQS) to distribute the SMS messages. Use AWS Lambda to process the responses.
D. Create an Amazon Simple Notification Service (Amazon SNS) FIFO topic. Subscribe an Amazon Kinesis data stream to the SNS topic for analysis and archiving.

Answer: B
Explanation:
https://aws.amazon.com/pinpoint/product-details/sms/
Two-Way Messaging:
Receive SMS messages from your customers and reply back to them in a chat-like interactive experience. With Amazon Pinpoint, you can create automatic responses when customers send you messages that contain certain keywords. You can even use Amazon Lex to create conversational bots.
A majority of mobile phone users read incoming SMS messages almost immediately after receiving them. If you need to be able to provide your customers with urgent or important information, SMS messaging may be the right solution for you.
You can use Amazon Pinpoint to create targeted groups of customers, and then send them campaign-based messages. You can also use Amazon Pinpoint to send direct messages, such as appointment confirmations, order updates, and one-time passwords.

QUESTION 311
The customers of a finance company request appointments with financial advisors by sending text messages. A web application that runs on Amazon EC2 instances accepts the appointment requests. The text messages are published to an Amazon Simple Queue Service (Amazon SQS) queue through the web application. Another application that runs on EC2 instances then sends meeting invitations and meeting confirmation email messages to the customers. After successful scheduling, this application stores the meeting information in an Amazon DynamoDB database.
As the company expands, customers report that their meeting invitations are taking longer to arrive.
What should a solutions architect recommend to resolve this issue?

A. Add a DynamoDB Accelerator (DAX) cluster in front of the DynamoDB database.
B. Add an Amazon API Gateway API in front of the web application that accepts the appointment requests.
C. Add an Amazon CloudFront distribution. Set the origin as the web application that accepts the appointment requests.
D. Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

Answer: D
Explanation:
To resolve the issue of longer delivery times for meeting invitations, the solutions architect can recommend adding an Auto Scaling group for the application that sends meeting invitations and configuring the Auto Scaling group to scale based on the depth of the SQS queue. This will allow the application to scale up as the number of appointment requests increases, improving the performance and delivery times of the meeting invitations.

QUESTION 312
A company offers a food delivery service that is growing rapidly. Because of the growth, the company’s order processing system is experiencing scaling problems during peak traffic hours. The current architecture includes the following:

- A group of Amazon EC2 instances that run in an Amazon EC2 Auto Scaling group to collect orders from the application
- Another group of EC2 instances that run in an Amazon EC2 Auto Scaling group to fulfill orders

The order collection process occurs quickly, but the order fulfillment process can take longer.

Data must not be lost because of a scaling event.
A solutions architect must ensure that the order collection process and the order fulfillment process can both scale properly during peak traffic hours. The solution must optimize utilization of the company's AWS resources.
Which solution meets these requirements?

A. Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure each Auto Scaling group's minimum capacity according to peak workload values.
B. Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure a CloudWatch alarm to invoke an Amazon Simple Notification Service (Amazon SNS) topic that creates additional Auto Scaling groups on demand.
C. Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Scale the Auto Scaling groups based on notifications that the queues send.
D. Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Create a metric based on a backlog per instance calculation. Scale the Auto Scaling groups based on this metric.

Answer: D
Explanation:
The number of instances in your Auto Scaling group can be driven by how long it takes to process a message and the acceptable amount of latency (queue delay). The solution is to use a backlog per instance metric with the target value being the acceptable backlog per instance to maintain.

QUESTION 313
A company hosts multiple production applications. One of the applications consists of resources from Amazon EC2, AWS Lambda, Amazon RDS, Amazon Simple Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) across multiple AWS Regions. All company resources are tagged with a tag name of "application" and a value that corresponds to each application. A solutions architect must provide the quickest solution for identifying all of the tagged components.
Which solution meets these requirements?

A. Use AWS CloudTrail to generate a list of resources with the application tag.
B. Use the AWS CLI to query each service across all Regions to report the tagged components.
C. Run a query in Amazon CloudWatch Logs Insights to report on the components with the application tag.
D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag.

Answer: D
Explanation:
https://docs.aws.amazon.com/ARG/latest/userguide/tag-editor.html
Tags are words or phrases that act as metadata that you can use to identify and organize your AWS resources. A resource can have up to 50 user-applied tags. It can also have read-only system tags. Each tag consists of a key and one optional value.

QUESTION 314
A company needs to export its database once a day to Amazon S3 for other teams to access. The exported object size varies between 2 GB and 5 GB. The S3 access pattern for the data is

variable and changes rapidly. The data must be immediately available and must remain accessible for up to 3 months. The company needs the most cost-effective solution that will not increase retrieval time.
Which S3 storage class should the company use to meet these requirements?

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

Answer: A
Explanation:
S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the Infrequent Access tier and after 90 days of no access to the Archive Instant Access tier.

QUESTION 315
A company is developing a new mobile app. The company must implement proper traffic filtering to protect its Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting or SQL injection. The company has minimal infrastructure and operational staff. The company needs to reduce its share of the responsibility in managing, updating, and securing servers for its AWS environment.
What should a solutions architect recommend to meet these requirements?

A. Configure AWS WAF rules and associate them with the ALB.
B. Deploy the application using Amazon S3 with public hosting enabled.
C. Deploy AWS Shield Advanced and add the ALB as a protected resource.
D. Create a new ALB that directs traffic to an Amazon EC2 instance running a third-party firewall, which then passes the traffic to the current ALB.

Answer: A
Explanation:
A solutions architect should recommend option A, which is to configure AWS WAF rules and associate them with the ALB. This will allow the company to apply traffic filtering at the application layer, which is necessary for protecting the ALB against common application-level attacks such as cross-site scripting or SQL injection. AWS WAF is a managed service that makes it easy to protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. The company can easily manage and update the rules to ensure the security of its application.

QUESTION 316
A company's reporting system delivers hundreds of .csv files to an Amazon S3 bucket each day. The company must convert these files to Apache Parquet format and must store the files in a transformed data bucket.
Which solution will meet these requirements with the LEAST development effort?

A. Create an Amazon EMR cluster with Apache Spark installed. Write a Spark application to transform the data. Use EMR File System (EMRFS) to write files to the transformed data bucket.
B. Create an AWS Glue crawler to discover the data. Create an AWS Glue extract, transform, and load (ETL) job to transform the data. Specify the transformed data bucket in the output step.
C. Use AWS Batch to create a job definition with Bash syntax to transform the data and output the data to the transformed data bucket. Use the job definition to submit a job. Specify an array job as

the job type.

D. Create an AWS Lambda function to transform the data and output the data to the transformed data bucket. Configure an event notification for the S3 bucket. Specify the Lambda function as the destination for the event notification.

Answer: B
Explanation:
https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html

QUESTION 317
A company has a serverless website with millions of objects in an Amazon S3 bucket. The company uses the S3 bucket as the origin for an Amazon CloudFront distribution. The company did not set encryption on the S3 bucket before the objects were loaded. A solutions architect needs to enable encryption for all existing objects and for all objects that are added to the S3 bucket in the future.
Which solution will meet these requirements with the LEAST amount of effort?

A. Create a new S3 bucket. Turn on the default encryption settings for the new S3 bucket. Download all existing objects to temporary local storage. Upload the objects to the new S3 bucket.
B. Turn on the default encryption settings for the S3 bucket. Use the S3 Inventory feature to create a .csv file that lists the unencrypted objects. Run an S3 Batch Operations job that uses the copy command to encrypt those objects.
C. Create a new encryption key by using AWS Key Management Service (AWS KMS). Change the settings on the S3 bucket to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Turn on versioning for the S3 bucket.
D. Navigate to Amazon S3 in the AWS Management Console. Browse the S3 bucket's objects. Sort by the encryption field. Select each unencrypted object. Use the Modify button to apply default encryption settings to every unencrypted object in the S3 bucket.

Answer: B
Explanation:
Step 1: S3 inventory to get object list
Step 2 (If needed): Use S3 Select to filter
Step 3: S3 object operations to encrypt the unencrypted objects.
On the going object use default encryption.
https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/

QUESTION 318
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? (Choose 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
Explanation:
To enable the connection to a service running on an instance, the associated network ACL must allow both:
- Inbound traffic on the port that the service is listening on
- Outbound traffic to ephemeral ports
https://aws.amazon.com/premiumsupport/knowledge-center/resolve-connection-sg-acl-inbound/

QUESTION 319
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
Explanation:
API Gateway + Lambda is the perfect solution for modern applications with serverless architecture.

QUESTION 320
A company runs an application on a group of Amazon Linux EC2 instances. For compliance reasons, the company must retain all application log files for 7 years. The log files will be analyzed by a reporting tool that must be able to access all the files concurrently.
Which storage solution meets these requirements MOST cost-effectively?

A. Amazon Elastic Block Store (Amazon EBS)
B. Amazon Elastic File System (Amazon EFS)
C. Amazon EC2 instance store
D. Amazon S3

Answer: D
Explanation:
Amazon S3 - Requests to Amazon S3 can be authenticated or anonymous. Authenticated access requires credentials that AWS can use to authenticate your requests. When making REST API calls directly from your code, you create a signature using valid credentials and include the signature in your request. 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.
Reference:

https://aws.amazon.com/s3/

QUESTION 321
A company has hired an external vendor to perform work in the company's AWS account. The vendor uses an automated tool that is hosted in an AWS account that the vendor owns. The vendor does not have IAM access to the company's AWS account.
How should a solutions architect grant this access to the vendor?

A. Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.
B. Create an IAM user in the company's account with a password that meets the password complexity requirements. Attach the appropriate IAM policies to the user for the permissions that the vendor requires.
C. Create an IAM group in the company's account. Add the tool's IAM user from the vendor account to the group. Attach the appropriate IAM policies to the group for the permissions that the vendor requires.
D. Create a new identity provider by choosing "AWS account" as the provider type in the IAM console. Supply the vendor's AWS account ID and user name. Attach the appropriate IAM policies to the new provider for the permissions that the vendor requires.

Answer: A
Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

QUESTION 322
A company has deployed a Java Spring Boot application as a pod that runs on Amazon Elastic Kubernetes Service (Amazon EKS) in private subnets. The application needs to write data to an Amazon DynamoDB table. A solutions architect must ensure that the application can interact with the DynamoDB table without exposing traffic to the internet.
Which combination of steps should the solutions architect take to accomplish this goal? (Choose two.)

A. Attach an IAM role that has sufficient privileges to the EKS pod.
B. Attach an IAM user that has sufficient privileges to the EKS pod.
C. Allow outbound connectivity to the DynamoDB table through the private subnets' network ACLs.
D. Create a VPC endpoint for DynamoDB.
E. Embed the access keys in the Java Spring Boot code.

Answer: AD
Explanation:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html
https://aws.amazon.com/about-aws/whats-new/2019/09/amazon-eks-adds-support-to-assign-iam-permissions-to-kubernetes-service-accounts/

QUESTION 323
A company recently migrated its web application to AWS by rehosting the application on Amazon EC2 instances in a single AWS Region. The company wants to redesign its application architecture to be highly available and fault tolerant. Traffic must reach all running EC2 instances randomly.
Which combination of steps should the company take to meet these requirements? (Choose two.)

A. Create an Amazon Route 53 failover routing policy.
B. Create an Amazon Route 53 weighted routing policy.
C. Create an Amazon Route 53 multivalue answer routing policy.
D. Launch three EC2 instances: two instances in one Availability Zone and one instance in another Availability Zone.
E. Launch four EC2 instances: two instances in one Availability Zone and two instances in another Availability Zone.

Answer: CE
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/

QUESTION 324
A company collects data from thousands of remote devices by using a RESTful web services application that runs on an Amazon EC2 instance. The EC2 instance receives the raw data, transforms the raw data, and stores all the data in an Amazon S3 bucket. The number of remote devices will increase into the millions soon. The company needs a highly scalable solution that minimizes operational overhead.
Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Use AWS Glue to process the raw data in Amazon S3.
B. Use Amazon Route 53 to route traffic to different EC2 instances.
C. Add more EC2 instances to accommodate the increasing amount of incoming data.
D. Send the raw data to Amazon Simple Queue Service (Amazon SQS). Use EC2 instances to process the data.
E. Use Amazon API Gateway to send the raw data to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to use the data stream as a source to deliver the data to Amazon S3.

Answer: AE
Explanation:
"RESTful web services" => API Gateway.
"EC2 instance receives the raw data, transforms the raw data, and stores all the data in an Amazon S3 bucket" => GLUE with (Extract - Transform - Load)

QUESTION 325
A company needs to retain its AWS CloudTrail logs for 3 years. The company is enforcing CloudTrail across a set of AWS accounts by using AWS Organizations from the parent account. The CloudTrail target S3 bucket is configured with S3 Versioning enabled. An S3 Lifecycle policy is in place to delete current objects after 3 years.
After the fourth year of use of the S3 bucket, the S3 bucket metrics show that the number of objects has continued to rise. However, the number of new CloudTrail logs that are delivered to the S3 bucket has remained consistent.
Which solution will delete objects that are older than 3 years in the MOST cost-effective manner?

A. Configure the organization’s centralized CloudTrail trail to expire objects after 3 years.
B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.
C. Create an AWS Lambda function to enumerate and delete objects from Amazon S3 that are older than 3 years.
D. Configure the parent account as the owner of all objects that are delivered to the S3 bucket.

Answer: B

Explanation:

To delete objects that are older than 3 years in the most cost-effective manner, the company should configure the S3 Lifecycle policy to delete previous versions as well as current versions. This will ensure that all versions of the objects, including the previous versions, are deleted after 3 years.

QUESTION 326

A company has an API that receives real-time data from a fleet of monitoring devices. The API stores this data in an Amazon RDS DB instance for later analysis. The amount of data that the monitoring devices send to the API fluctuates. During periods of heavy traffic, the API often returns timeout errors.

After an inspection of the logs, the company determines that the database is not capable of processing the volume of write traffic that comes from the API. A solutions architect must minimize the number of connections to the database and must ensure that data is not lost during periods of heavy traffic.

Which solution will meet these requirements?

A. Increase the size of the DB instance to an instance type that has more available memory.

B. Modify the DB instance to be a Multi-AZ DB instance. Configure the application to write to all active RDS DB instances.

C. Modify the API to write incoming data to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database.

D. Modify the API to write incoming data to an Amazon Simple Notification Service (Amazon SNS) topic. Use an AWS Lambda function that Amazon SNS invokes to write data from the topic to the database.

Answer: C

Explanation:

Using Amazon SQS will help minimize the number of connections to the database, as the API will write data to a queue instead of directly to the database. Additionally, using an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database will help ensure that data is not lost during periods of heavy traffic, as the queue will serve as a buffer between the API and the database.

QUESTION 327

A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.

Which solution meets these requirements?

A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.

B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.

C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.

D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

Answer: A

Explanation:
https://aws.amazon.com/rds/aurora/serverless/

QUESTION 328
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
Explanation:
If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html#nat-gateway-basics

QUESTION 329
An application runs on an Amazon EC2 instance that has an Elastic IP address in VPC A. The application requires access to a database in VPC B. Both VPCs are in the same AWS account.
Which solution will provide the required access MOST securely?

A. Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.
B. Configure a VPC peering connection between VPC A and VPC B.
C. Make the DB instance publicly accessible. Assign a public IP address to the DB instance.
D. Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new EC2 instance.

Answer: B
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/rds-connectivity-instance-subnet-vpc/

QUESTION 330
A company runs demonstration environments for its customers on Amazon EC2 instances. Each environment is isolated in its own VPC. The company's operations team needs to be notified when RDP or SSH access to an environment has been established.

A. Configure Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected.

B. Configure the EC2 instances with an IAM instance profile that has an IAM role with the AmazonSSMManagedInstanceCore policy attached.
C. Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state.
D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

Answer: C
Explanation:
EC2 Instance State-change Notifications are not the same as RDP or SSH established connection notifications. Use Amazon CloudWatch Logs to monitor SSH access to your Amazon EC2 Linux instances so that you can monitor rejected (or established) SSH connection requests and take action.
https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/

QUESTION 331
A company is building a new web-based customer relationship management application. The application will use several Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS) volumes behind an Application Load Balancer (ALB). The application will also use an Amazon Aurora database. All data for the application must be encrypted at rest and in transit.
Which solution will meet these requirements?

A. Use AWS Key Management Service (AWS KMS) certificates on the ALB to encrypt data in transit. Use AWS Certificate Manager (ACM) to encrypt the EBS volumes and Aurora database storage at rest.
B. Use the AWS root account to log in to the AWS Management Console. Upload the company's encryption certificates. While in the root account, select the option to turn on encryption for all data at rest and in transit for the account.
C. Use AWS Key Management Service (AWS KMS) to encrypt the EBS volumes and Aurora database storage at rest. Attach an AWS Certificate Manager (ACM) certificate to the ALB to encrypt data in transit.
D. Use BitLocker to encrypt all data at rest. Import the company's TLS certificate keys to AWS Key Management Service (AWS KMS) Attach the KMS keys to the ALB to encrypt data in transit.

Answer: C

QUESTION 332
A solutions architect has created a new AWS account and must secure AWS account root user access.
Which combination of actions will accomplish this? (Choose 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 333
A company has a three-tier application for image sharing. The application uses an Amazon EC2 instance for the front-end layer, another EC2 instance for the application layer, and a third EC2 instance for a MySQL database. A solutions architect must design a scalable and highly available solution that requires the least amount of change to the application.
Which solution meets these requirements?

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

Answer: D
Explanation:
for "Highly available": Multi-AZ & for "least amount of changes to the application": Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring

QUESTION 334
A company wants to experiment with individual AWS accounts for its engineer team. The company wants to be notified as soon as the Amazon EC2 instance usage for a given month exceeds a specific threshold for each account.
What should a solutions architect do to meet this requirement MOST cost-effectively?

A. Use Cost Explorer to create a daily report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
B. Use Cost Explorer to create a monthly report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
C. Use AWS Budgets to create a cost budget for each account. Set the period to monthly. Set the scope to EC2 instances. Set an alert threshold for the budget. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.
D. Use AWS Cost and Usage Reports to create a report with hourly granularity. Integrate the report data with Amazon Athena. Use Amazon EventBridge to schedule an Athena query. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.

Answer: C
Explanation:
AWS Budgets allows you to create budgets for your AWS accounts and set alerts when usage exceeds a certain threshold. By creating a budget for each account, specifying the period as monthly and the scope as EC2 instances, you can effectively track the EC2 usage for each account and be notified when a threshold is exceeded. This solution is the most cost-effective option as it does not require additional resources such as Amazon Athena or Amazon EventBridge.
https://aws.amazon.com/getting-started/hands-on/control-your-costs-free-tier-budgets/

QUESTION 335
A solutions architect needs to design a new microservice for a company's application. Clients must be able to call an HTTPS endpoint to reach the microservice. The microservice also must use AWS Identity and Access Management (IAM) to authenticate calls. The solutions architect will write the logic for this microservice by using a single AWS Lambda function that is written in Go 1.x.
Which solution will deploy the function in the MOST operationally efficient way?

A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.
B. Create a Lambda function URL for the function. Specify AWS_IAM as the authentication type.
C. Create an Amazon CloudFront distribution. Deploy the function to Lambda@Edge. Integrate IAM authentication logic into the Lambda@Edge function.
D. Create an Amazon CloudFront distribution. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.

Answer: A

QUESTION 336
A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the 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 Region.

Answer: D
Explanation:
https://aws.amazon.com/directconnect/pricing/
https://aws.amazon.com/blogs/aws/aws-data-transfer-prices-reduced/

QUESTION 337
An online learning company is migrating to the AWS Cloud. The company maintains its student

records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.
Which solution will meet these requirements with the LEAST amount of operational overhead?

A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.
B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.
C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Answer: C
Explanation:
https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/

QUESTION 338
A medical research lab produces data that is related to a new study. The lab wants to make the data available with minimum latency to clinics across the country for their on-premises, file-based applications. The data files are stored in an Amazon S3 bucket that has read-only permissions for each clinic.
What should a solutions architect recommend to meet these requirements?

A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic.
B. Migrate the files to each clinic's on-premises applications by using AWS DataSync for processing.
C. Deploy an AWS Storage Gateway volume gateway as a virtual machine (VM) on premises at each clinic.
D. Attach an Amazon Elastic File System (Amazon EFS) file system to each clinic's on-premises servers.

Answer: A
Explanation:
AWS Storage Gateway is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure. By deploying a file gateway as a virtual machine on each clinic's premises, the medical research lab can provide low-latency access to the data stored in the S3 bucket while maintaining read-only permissions for each clinic. This solution allows the clinics to access the data files directly from their on-premises file-based applications without the need for data transfer or migration.

QUESTION 339
A company is using a content management system that runs on a single Amazon EC2 instance. The EC2 instance contains both the web server and the database software. The company must make its website platform highly available and must enable the website to scale to meet user demand.
What should a solutions architect recommend to meet these requirements?

A. Move the database to Amazon RDS, and enable automatic backups. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer in the Availability Zone, and set the two instances as targets.
B. Migrate the database to an Amazon Aurora instance with a read replica in the same Availability

Zone as the existing EC2 instance. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer, and set the two EC2 instances as targets.

C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.
D. Move the database to a separate EC2 instance, and schedule backups to Amazon S3. Create an Amazon Machine Image (AMI) from the original EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

Answer: C
Explanation:
This approach will provide both high availability and scalability for the website platform. By moving the database to Amazon Aurora with a read replica in another availability zone, it will provide a failover option for the database. The use of an Application Load Balancer and an Auto Scaling group across two availability zones allows for automatic scaling of the website to meet increased user demand. Additionally, creating an AMI from the original EC2 instance allows for easy replication of the instance in case of failure.

QUESTION 340
A company is launching an application on AWS. The application uses an Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group. The instances are in an Auto Scaling group for each environment. The company requires a development environment and a production environment. The production environment will have periods of high traffic.
Which solution will configure the development environment MOST cost-effectively?

A. Reconfigure the target group in the development environment to have only one EC2 instance as a target.
B. Change the ALB balancing algorithm to least outstanding requests.
C. Reduce the size of the EC2 instances in both environments.
D. Reduce the maximum number of EC2 instances in the development environment’s Auto Scaling group.

Answer: D
Explanation:
This option will configure the development environment in the most cost-effective way as it reduces the number of instances running in the development environment and therefore reduces the cost of running the application. The development environment typically requires less resources than the production environment, and it is unlikely that the development environment will have periods of high traffic that would require a large number of instances. By reducing the maximum number of instances in the development environment's Auto Scaling group, the company can save on costs while still maintaining a functional development environment.

QUESTION 341
A company runs a web application on Amazon EC2 instances in multiple Availability Zones. The EC2 instances are in private subnets. A solutions architect implements an internet-facing Application Load Balancer (ALB) and specifies the EC2 instances as the target group. However, the internet traffic is not reaching the EC2 instances.
How should the solutions architect reconfigure the architecture to resolve this issue?

A. Replace the ALB with a Network Load Balancer. Configure a NAT gateway in a public subnet to allow internet traffic.
B. Move the EC2 instances to public subnets. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.
C. Update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.
D. Create public subnets in each Availability Zone. Associate the public subnets with the ALB. Update the route tables for the public subnets with a route to the private subnets.

Answer: D
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/

QUESTION 342
A company has deployed a database in Amazon RDS for MySQL. Due to increased transactions, the database support team is reporting slow reads against the DB instance and recommends adding a read replica.
Which combination of actions should a solutions architect take before implementing this change? (Choose two.)

A. Enable binlog replication on the RDS primary node.
B. Choose a failover priority for the source DB instance.
C. Allow long-running transactions to complete on the source DB instance.
D. Create a global table and specify the AWS Regions where the table will be available.
E. Enable automatic backups on the source instance by setting the backup retention period to a value other than 0.

Answer: CE
Explanation:
An active, long-running transaction can slow the process of creating the read replica. We recommend that you wait for long-running transactions to complete before creating a read replica. If you create multiple read replicas in parallel from the same source DB instance, Amazon RDS takes only one snapshot at the start of the first create action.
When creating a read replica, there are a few things to consider. First, you must enable automatic backups on the source DB instance by setting the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

QUESTION 343
A company runs analytics software on Amazon EC2 instances. The software accepts job requests from users to process data that has been uploaded to Amazon S3. Users report that some submitted data is not being processed Amazon CloudWatch reveals that the EC2 instances have a consistent CPU utilization at or near 100%. The company wants to improve system performance and scale the system based on user load.
What should a solutions architect do to meet these requirements?

A. Create a copy of the instance. Place all instances behind an Application Load Balancer.
B. Create an S3 VPC endpoint for Amazon S3. Update the software to reference the endpoint.
C. Stop the EC2 instances. Modify the instance type to one with a more powerful CPU and more memory. Restart the instances.

D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

Answer: D
Explanation:
By routing incoming requests to Amazon SQS, the company can decouple the job requests from the processing instances. This allows them to scale the number of instances based on the size of the queue, providing more resources when needed. Additionally, using an Auto Scaling group based on the queue size will automatically scale the number of instances up or down depending on the workload. Updating the software to read from the queue will allow it to process the job requests in a more efficient manner, improving the performance of the system.

QUESTION 344
A company is implementing a shared storage solution for a media application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.
Which AWS solution meets these requirements?

A. Create an AWS Storage Gateway volume gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
B. Create an AWS Storage Gateway tape gateway. Configure tapes to use Amazon S3. Connect the application server to the tape gateway.
C. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.

Answer: D
Explanation:
Amazon FSx has native support for Windows file system features and for the industry-standard Server Message Block (SMB) protocol to access file storage over a network.
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html

QUESTION 345
A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.
What should a solutions architect do to meet these requirements when configuring the logs?

A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days
B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

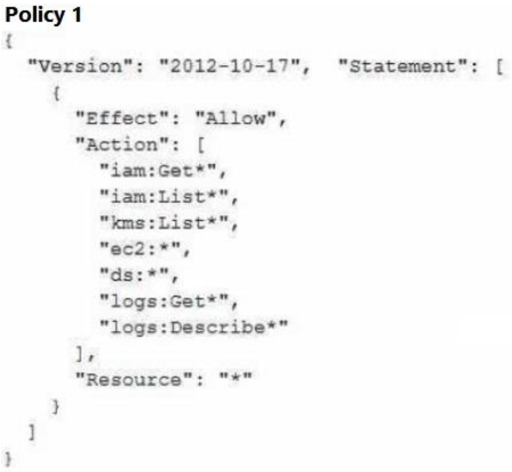
Answer: D
Explanation:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogsConcepts.html

QUESTION 346
A solutions architect needs to design a system to store client case files. The files are core company assets and are important. The number of files will grow over time.
The files must be simultaneously accessible from multiple application servers that run on Amazon EC2 instances. The solution must have built-in redundancy.
Which solution meets these requirements?

A. Amazon Elastic File System (Amazon EFS)
B. Amazon Elastic Block Store (Amazon EBS)
C. Amazon S3 Glacier Deep Archive
D. AWS Backup

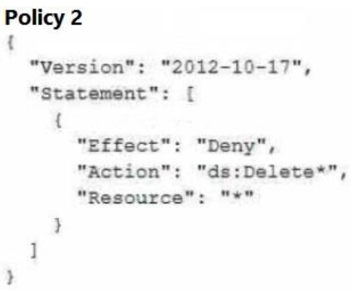
Answer: A
Explanation:
Amazon EFS provides a simple, scalable, fully managed file system that can be simultaneously accessed from multiple EC2 instances and provides built-in redundancy. It is optimized for multiple EC2 instances to access the same files, and it is designed to be highly available, durable, and secure. It can scale up to petabytes of data and can handle thousands of concurrent connections, and is a cost-effective solution for storing and accessing large amounts of data.

QUESTION 347
A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.



Policy 1

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



Policy 2

```
{
  "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
Explanation:
There is an explicit DENY on deleting directories in the second policy. So the only thing that can be deleted is EC2 instances as per the permission in the first policy.

QUESTION 348
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 blocks as the source or destination.
D. Create security group rules using the subnet CIDR blocks as the source or destination.

Answer: B
Explanation:
The ID of a security group (referred to here as the specified security group). For example, the current security group, a security group from the same VPC, or a security group for a peered VPC. This allows traffic based on the private IP addresses of the resources associated with the specified security group. This does not add rules from the specified security group to the current security group.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html

QUESTION 349
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? (Choose 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:
To prevent or mitigate future accidental deletions, consider the following features:
- Enable versioning to keep historical versions of an object.
- Enable cross-region replication of objects.
- Enable MFA Delete to require multi-factor authentication (MFA) when deleting an object version.

QUESTION 350
A company is building a solution that will report Amazon EC2 Auto Scaling events across all the

applications in an AWS account. The company needs to use a serverless solution to store the EC2 Auto Scaling status data in Amazon S3. The company then will use the data in Amazon S3 to provide near-real-time updates in a dashboard. The solution must not affect the speed of EC2 instance launches.
How should the company move the data to Amazon S3 to meet these requirements?

A. Use an Amazon CloudWatch metric stream to send the EC2 Auto Scaling status data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.
B. Launch an Amazon EMR cluster to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.
C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.
D. Use a bootstrap script during the launch of an EC2 instance to install Amazon Kinesis Agent. Configure Kinesis Agent to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

Answer: A
Explanation:
You can use metric streams to continually stream CloudWatch metrics to a destination of your choice, with near-real-time delivery and low latency. One of the use cases is Data Lake: create a metric stream and direct it to an Amazon Kinesis Data Firehose delivery stream that delivers your CloudWatch metrics to a data lake such as Amazon S3.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Metric-Streams.html

QUESTION 351
A company has an application that places hundreds of .csv files into an Amazon S3 bucket every hour. The files are 1 GB in size. Each time a file is uploaded, the company needs to convert the file to Apache Parquet format and place the output file into an S3 bucket.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS Lambda function to download the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Invoke the Lambda function for each S3 PUT event.
B. Create an Apache Spark job to read the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the Spark job.
C. Create an AWS Glue table and an AWS Glue crawler for the S3 bucket where the application places the .csv files. Schedule an AWS Lambda function to periodically use Amazon Athena to query the AWS Glue table, convert the query results into Parquet format, and place the output files into an S3 bucket.
D. Create an AWS Glue extract, transform, and load (ETL) job to convert the .csv files to Parquet format and place the output files into an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the ETL job.

Answer: D
Explanation:
https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html

QUESTION 352
A company is implementing new data retention policies for all databases that run on Amazon RDS DB instances. The company must retain daily backups for a minimum period of 2 years. The backups must be consistent and restorable.

Which solution should a solutions architect recommend to meet these requirements?

A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.
B. Configure a backup window for the RDS DB instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule snapshot deletions.
C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years.
D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target. Configure S3 Lifecycle policies to delete the snapshots after 2 years.

Answer: A

QUESTION 353
A company's compliance team needs to move its file shares to AWS. The shares run on a Windows Server SMB file share. A self-managed on-premises Active Directory controls access to the files and folders.
The company wants to use Amazon FSx for Windows File Server as part of the solution. The company must ensure that the on-premises Active Directory groups restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS. The company has created an FSx for Windows File Server file system.
Which solution will meet these requirements?

A. Create an Active Directory Connector to connect to the Active Directory. Map the Active Directory groups to IAM groups to restrict access.
B. Assign a tag with a Restrict tag key and a Compliance tag value. Map the Active Directory groups to IAM groups to restrict access.
C. Create an IAM service-linked role that is linked directly to FSx for Windows File Server to restrict access.
D. Join the file system to the Active Directory to restrict access.

Answer: D
Explanation:
Joining the FSx for Windows File Server file system to the on-premises Active Directory will allow the company to use the existing Active Directory groups to restrict access to the file shares, folders, and files after the move to AWS. This option allows the company to continue using their existing access controls and management structure, making the transition to AWS more seamless.

QUESTION 354
A company recently announced the deployment of its retail website to a global audience. The website runs on multiple Amazon EC2 instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones.
The company wants to provide its customers with different versions of content based on the devices that the customers use to access the website.
Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)

A. Configure Amazon CloudFront to cache multiple versions of the content.

B. Configure a host header in a Network Load Balancer to forward traffic to different instances.
C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.
D. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up host-based routing to different EC2 instances.
E. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up path-based routing to different EC2 instances.

Answer: AC
Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html
https://docs.aws.amazon.com/lambda/latest/dg/lambda-edge.html

QUESTION 355
A company plans to use Amazon ElastiCache for its multi-tier web application. A solutions architect creates a Cache VPC for the ElastiCache cluster and an App VPC for the application's Amazon EC2 instances. Both VPCs are in the us-east-1 Region.
The solutions architect must implement a solution to provide the application's EC2 instances with access to the ElastiCache cluster.
Which solution will meet these requirements MOST cost-effectively?

A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
B. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
C. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the peering connection's security group to allow inbound connection from the application's security group.
D. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the Transit VPC's security group to allow inbound connection from the application's security group.

Answer: A
Explanation:
Creating a peering connection between the VPCs allows the application's EC2 instances to communicate with the ElastiCache cluster directly and efficiently. This is the most cost-effective solution as it does not involve creating additional resources such as a Transit VPC, and it does not incur additional costs for traffic passing through the Transit VPC. Additionally, it is also more secure as it allows you to configure a more restrictive security group rule to allow inbound connection from only the application's security group.

QUESTION 356
A company is building an application that consists of several microservices. The company has decided to use container technologies to deploy its software on AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.
Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)

A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.

B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.
C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.
D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.
E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Answer: AD
Explanation:
The question repeatedly says managing infrastructure must not be an option so EC2 is off the topic. Also can user fargate with micro services without any issue.
https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/deploy-java-microservices-on-amazon-ecs-using-aws-fargate.html

QUESTION 357
A company has a web application hosted over 10 Amazon EC2 instances with traffic directed by Amazon Route 53. The company occasionally experiences a timeout error when attempting to browse the application. The networking team finds that some DNS queries return IP addresses of unhealthy instances, resulting in the timeout error.
What should a solutions architect implement to overcome these timeout errors?

A. Create a Route 53 simple routing policy record for each EC2 instance. Associate a health check with each record.
B. Create a Route 53 failover routing policy record for each EC2 instance. Associate a health check with each record.
C. Create an Amazon CloudFront distribution with EC2 instances as its origin. Associate a health check with the EC2 instances.
D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.

Answer: D
Explanation:
An Application Load Balancer (ALB) allows you to distribute incoming traffic across multiple backend instances, and can automatically route traffic to healthy instances while removing traffic from unhealthy instances. By using an ALB in front of the EC2 instances and routing traffic to it from Route 53, the load balancer can perform health checks on the instances and only route traffic to healthy instances, which should help to reduce or eliminate timeout errors caused by unhealthy instances.

QUESTION 358
A solutions architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.
Which solution meets these requirements and is MOST secure?

A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
B. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2

instances as the origin.

C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Answer: C
Explanation:
This solution meets the requirements for a highly available application with web, application, and database tiers, as well as providing edge-based content delivery. Additionally, it maximizes security by having the ALB in a private subnet, which limits direct access to the web servers, while still being able to serve traffic over the Internet via the public ALB. This will ensure that the web servers are not exposed to the public Internet, which reduces the attack surface and provides a secure way to access the application.
https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/

QUESTION 359
A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.
Which solution meets these requirements?

A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in-memory cache for DynamoDB hosting the application data.

Answer: A
Explanation:
When you have an Application Load Balancer or Network Load Balancer that includes multiple target groups, Global Accelerator considers the load balancer endpoint to be healthy only if each target group behind the load balancer has at least one healthy target. If any single target group for the load balancer has only unhealthy targets, Global Accelerator considers the endpoint to be unhealthy.
https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-health-check-options.html

QUESTION 360
A company has one million users that use its mobile app. The company must analyze the data usage in near-real time. The company also must encrypt the data in near-real time and must store the data in a centralized location in Apache Parquet format for further processing.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data. Invoke an AWS Lambda function to send the data to the Kinesis Data Analytics application.
B. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data. Invoke an AWS Lambda function to send the data to the EMR cluster.
C. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data.
D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

Answer: D
Explanation:
This solution will meet the requirements with the least operational overhead as it uses Amazon Kinesis Data Firehose, which is a fully managed service that can automatically handle the data collection, data transformation, encryption, and data storage in near-real time. Kinesis Data Firehose can automatically store the data in Amazon S3 in Apache Parquet format for further processing. Additionally, it allows you to create an Amazon Kinesis Data Analytics application to analyze the data in near real-time, with no need to manage any infrastructure or invoke any Lambda function. This way you can process a large amount of data with the least operational overhead.

QUESTION 361
An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.
What should the solutions architect recommend?

A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
B. Load the data into Amazon ElastiCache 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
Explanation:
Creating a read replica of the primary RDS database will offload the read-only SQL queries from the primary database, which will help to improve the performance of the web application. Read replicas are exact copies of the primary database that can be used to handle read-only traffic, which will reduce the load on the primary database and improve the performance of the web application. This solution can be implemented with minimal changes to the existing web application, as the business analysts can continue to run their queries on the read replica without modifying the code.

QUESTION 362
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: C

QUESTION 363
A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application' s data layer that uses Oracle-specific PL/SQL 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 solutions architect do to ensure the system can automatically scale for the increased traffic? (Choose 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 364
A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.

Which storage solution is MOST cost-effective?

A. Use AWS Storage Gateway for files to store and process the video content.
B. Use AWS Storage Gateway for volumes to store and process the video content.
C. Use Amazon EFS for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).
D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing.

Answer: D
Explanation:
A better solution would be to use a transcoding service like Amazon Elastic Transcoder to process the video content directly from Amazon S3. This would eliminate the need for storing the

content on an EBS volume, reduce storage costs, and simplify the architecture by removing the need for managing EBS volumes.

QUESTION 365
A company wants to create an application to store employee data in a hierarchical structured relationship. The company needs a minimum-latency response to high-traffic queries for the employee data and must protect any sensitive data. The company also needs to receive monthly email messages if any financial information is present in the employee data.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Use Amazon Redshift to store the employee data in hierarchies. Unload the data to Amazon S3 every month.
B. Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month.
C. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly events to AWS Lambda.
D. Use Amazon Athena to analyze the employee data in Amazon S3. Integrate Athena with Amazon QuickSight to publish analysis dashboards and share the dashboards with users.
E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

Answer: BE

QUESTION 366
A company has an application that is backed by an Amazon DynamoDB table. The company's compliance requirements specify that database backups must be taken every month, must be available for 6 months, and must be retained for 7 years.

Which solution will meet these requirements?

A. Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years.
B. Create a DynamoDB on-demand backup of the DynamoDB table on the first day of each month. Transition the backup to Amazon S3 Glacier Flexible Retrieval after 6 months. Create an S3 Lifecycle policy to delete backups that are older than 7 years.
C. Use the AWS SDK to develop a script that creates an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the script on the first day of each month. Create a second script that will run on the second day of each month to transition DynamoDB backups that are older than 6 months to cold storage and to delete backups that are older than 7 years.
D. Use the AWS CLI to create an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the command on the first day of each month with a cron expression. Specify in the command to transition the backups to cold storage after 6 months and to delete the backups after 7 years.

Answer: A

QUESTION 367
A company is using Amazon CloudFront with its website. The company has enabled logging on the CloudFront distribution, and logs are saved in one of the company's Amazon S3 buckets. The company needs to perform advanced analyses on the logs and build visualizations.

What should a solutions architect do to meet these requirements?

A. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
B. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.
C. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
D. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.

Answer: B
Explanation:
Quicksite creating data visualizations.
https://docs.aws.amazon.com/quicksight/latest/user/welcome.html

QUESTION 368
A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases.

Which solution meets these requirements?

A. Enable a Multi-AZ deployment for the DB instance.
B. Enable auto scaling for the DB instance in one Availability Zone.
C. Configure the DB instance in one Availability Zone, and create multiple read replicas in a separate Availability Zone.
D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks.

Answer: A
Explanation:
By using Multi-AZ deployment, the company can achieve an RPO of less than 1 second because the standby instance is always in sync with the primary instance, ensuring that data changes are continuously replicated.

QUESTION 369
A company runs a web application that is deployed on Amazon EC2 instances in the private subnet of a VPC. An Application Load Balancer (ALB) that extends across the public subnets directs web traffic to the EC2 instances. The company wants to implement new security measures to restrict inbound traffic from the ALB to the EC2 instances while preventing access from any other source inside or outside the private subnet of the EC2 instances.

Which solution will meet these requirements?

A. Configure a route in a route table to direct traffic from the internet to the private IP addresses of the EC2 instances.

B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB.
C. Move the EC2 instances into the public subnet. Give the EC2 instances a set of Elastic IP addresses.
D. Configure the security group for the ALB to allow any TCP traffic on any port.

Answer: B
Explanation:
This ensures that only the traffic originating from the ALB is allowed access to the EC2 instances in the private subnet, while denying any other traffic from other sources.

QUESTION 370
A research company runs experiments that are powered by a simulation application and a visualization application. The simulation application runs on Linux and outputs intermediate data to an NFS share every 5 minutes. The visualization application is a Windows desktop application that displays the simulation output and requires an SMB file system.

The company maintains two synchronized file systems. This strategy is causing data duplication and inefficient resource usage. The company needs to migrate the applications to AWS without making code changes to either application.

Which solution will meet these requirements?

A. Migrate both applications to AWS Lambda. Create an Amazon S3 bucket to exchange data between the applications.
B. Migrate both applications to Amazon Elastic Container Service (Amazon ECS). Configure Amazon FSx File Gateway for storage.
C. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon Simple Queue Service (Amazon SQS) to exchange data between the applications.
D. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon FSx for NetApp ONTAP for storage.

Answer: D
Explanation:
Amazon FSx for NetApp ONTAP is a fully-managed shared storage service built on NetApp's popular ONTAP file system. Amazon FSx for NetApp ONTAP provides the popular features, performance, and APIs of ONTAP file systems with the agility, scalability, and simplicity of a fully managed AWS service, making it easier for customers to migrate on-premises applications that rely on NAS appliances to AWS. FSx for ONTAP file systems are similar to on-premises NetApp clusters. Within each file system that you create, you also create one or more storage virtual machines (SVMs). These are isolated file servers each with their own endpoints for NFS, SMB, and management access, as well as authentication (for both administration and end-user data access). In turn, each SVM has one or more volumes which store your data.
https://aws.amazon.com/de/blogs/storage/getting-started-cloud-file-storage-with-amazon-fsx-for-netapp-ontap-using-netapp-management-tools/

QUESTION 371
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 efficient 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 372
A company hosts its static website by using Amazon S3. The company wants to add a contact form to its webpage. The contact form will have dynamic server-side components for users to input their name, email address, phone number, and user message. The company anticipates that there will be fewer than 100 site visits each month.

Which solution will meet these requirements MOST cost-effectively?

A. Host a dynamic contact form page in Amazon Elastic Container Service (Amazon ECS). Set up Amazon Simple Email Service (Amazon SES) to connect to any third-party email provider.
B. Create an Amazon API Gateway endpoint with an AWS Lambda backend that makes a call to Amazon Simple Email Service (Amazon SES).
C. Convert the static webpage to dynamic by deploying Amazon Lightsail. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.
D. Create a t2.micro Amazon EC2 instance. Deploy a LAMP (Linux, Apache, MySQL, PHP/Perl/Python) stack to host the webpage. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.

Answer: B
Explanation:
https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/

QUESTION 373
A company has a static website that is hosted on Amazon CloudFront in front of Amazon S3. The static website uses a database backend. The company notices that the website does not reflect updates that have been made in the website's Git repository. The company checks the continuous integration and continuous delivery (CI/CD) pipeline between the Git repository and Amazon S3. The company verifies that the webhooks are configured properly and that the CI/CD pipeline is sending messages that indicate successful deployments.

A solutions architect needs to implement a solution that displays the updates on the website.

Which solution will meet these requirements?

A. Add an Application Load Balancer.
B. Add Amazon ElastiCache for Redis or Memcached to the database layer of the web application.
C. Invalidate the CloudFront cache.
D. Use AWS Certificate Manager (ACM) to validate the website's SSL certificate.

Answer: C
Explanation:
Invalidate the CloudFront cache: The solutions architect should invalidate the CloudFront cache to ensure that the latest version of the website is being served to users.

QUESTION 374
A company wants to migrate a Windows-based application from on premises to the AWS Cloud. The application has three tiers: an application tier, a business tier, and a database tier with Microsoft SQL Server. The company wants to use specific features of SQL Server such as native backups and Data Quality Services. The company also needs to share files for processing between the tiers.

How should a solutions architect design the architecture to meet these requirements?

A. Host all three tiers on Amazon EC2 instances. Use Amazon FSx File Gateway for file sharing between the tiers.
B. Host all three tiers on Amazon EC2 instances. Use Amazon FSx for Windows File Server for file sharing between the tiers.
C. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use Amazon Elastic File System (Amazon EFS) for file sharing between the tiers.
D. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume for file sharing between the tiers.

Answer: B
Explanation:
Data Quality Services: If this feature is critical to your workload, consider choosing Amazon RDS Custom or Amazon EC2.
https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-sql-server/comparison.html

QUESTION 375
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. The company must not make any changes to the application.

What should a solutions architect do to meet these requirements?

A. Create an Amazon S3 Standard bucket with access to the web servers.
B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.
D. Configure a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume to all web servers.

Answer: C
Explanation:
Create an Amazon Elastic File System (Amazon EFS) file system.
Mount the EFS file system on all web servers.
To meet the requirements of providing a shared file store for Linux-based web servers without making changes to the application, using an Amazon EFS file system is the best solution.
Amazon EFS is a managed NFS file system service that provides shared access to files across multiple Linux-based instances, which makes it suitable for this use case.
Amazon S3 is not ideal for this scenario since it is an object storage service and not a file system, and it requires additional tools or libraries to mount the S3 bucket as a file system.
Amazon CloudFront can be used to improve content delivery performance but is not necessary for this requirement.

Additionally, Amazon EBS volumes can only be mounted to one instance at a time, so it is not suitable for sharing files across multiple instances.

QUESTION 376
A company has an AWS Lambda function that needs read access to an Amazon S3 bucket that is located in the same AWS account.

Which solution will meet these requirements in the MOST secure manner?

A. Apply an S3 bucket policy that grants read access to the S3 bucket.
B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket.
C. Embed an access key and a secret key in the Lambda function's code to grant the required IAM permissions for read access to the S3 bucket.
D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets in the account.

Answer: B
Explanation:
This is the most secure and recommended way to provide an AWS Lambda function with access to an S3 bucket. It involves creating an IAM role that the Lambda function assumes, and attaching an IAM policy to the role that grants the necessary permissions to read from the S3 bucket.
https://docs.aws.amazon.com/lambda/latest/dg/lambda-permissions.html

QUESTION 377
A company hosts a web application on multiple Amazon EC2 instances. The EC2 instances are in an Auto Scaling group that scales in response to user demand. The company wants to optimize cost savings without making a long-term commitment.

Which EC2 instance purchasing option should a solutions architect recommend to meet these requirements?

A. Dedicated Instances only
B. On-Demand Instances only
C. A mix of On-Demand Instances and Spot Instances
D. A mix of On-Demand Instances and Reserved Instances

Answer: C
Explanation:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-mixed-instances-groups.html

QUESTION 378
A media company uses Amazon CloudFront for its publicly available streaming video content. The company wants to secure the video content that is hosted in Amazon S3 by controlling who has access. Some of the company's users are using a custom HTTP client that does not support cookies. Some of the company's users are unable to change the hardcoded URLs that they are using for access.

Which services or methods will meet these requirements with the LEAST impact to the users? (Choose two.)

A. Signed cookies
B. Signed URLs
C. AWS AppSync
D. JSON Web Token (JWT)
E. AWS Secrets Manager

Answer: AB
Explanation:
Signed URLs are URLs that grant temporary access to an S3 object. They include a signature that verifies the authenticity of the request, as well as an expiration date that limits the time during which the URL is valid. This solution will work for users who are using custom HTTP clients that do not support cookies.
Signed cookies are similar to signed URLs, but they use cookies to grant temporary access to S3 objects. This solution will work for users who are unable to change the hardcoded URLs that they are using for access.
https://aws.amazon.com/blogs/media/secure-content-using-cloudfront-functions/

QUESTION 379
A company is preparing a new data platform that will ingest real-time streaming data from multiple sources. The company needs to transform the data before writing the data to Amazon S3. The company needs the ability to use SQL to query the transformed data.

Which solutions will meet these requirements? (Choose two.)

A. Use Amazon Kinesis Data Streams to stream the data. Use Amazon Kinesis Data Analytics to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
B. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use AWS Glue to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
C. Use AWS Database Migration Service (AWS DMS) to ingest the data. Use Amazon EMR to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
D. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use Amazon Kinesis Data Analytics to transform the data and to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.
E. Use Amazon Kinesis Data Streams to stream the data. Use AWS Glue to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.

Answer: AB

QUESTION 380
A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.

Which solution meets these requirements?

A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.

B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.
D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

Answer: D
Explanation:
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 381
An application that is hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Traffic must not traverse the internet.

How should a solutions architect configure access to meet these requirements?

A. Create a private hosted zone by using Amazon Route 53.
B. Set up a gateway VPC endpoint for Amazon S3 in the VPC.
C. Configure the EC2 instances to use a NAT gateway to access the S3 bucket.
D. Establish an AWS Site-to-Site VPN connection between the VPC and the S3 bucket.

Answer: B

QUESTION 382
An ecommerce company stores terabytes of customer data in the AWS Cloud. The data contains personally identifiable information (PII). The company wants to use the data in three applications. Only one of the applications needs to process the PII. The PII must be removed before the other two applications process the data.

Which solution will meet these requirements with the LEAST operational overhead?

A. Store the data in an Amazon DynamoDB table. Create a proxy application layer to intercept and process the data that each application requests.
B. Store the data in an Amazon S3 bucket. Process and transform the data by using S3 Object Lambda before returning the data to the requesting application.
C. Process the data and store the transformed data in three separate Amazon S3 buckets so that each application has its own custom dataset. Point each application to its respective S3 bucket.
D. Process the data and store the transformed data in three separate Amazon DynamoDB tables so that each application has its own custom dataset. Point each application to its respective DynamoDB table.

Answer: B
Explanation:
Amazon S3 Object Lambda allows you to add custom code to S3 GET requests, which means that you can modify the data before it is returned to the requesting application. In this case, you

can use S3 Object Lambda to remove the PII before the data is returned to the two applications that do not need to process PII. This approach has the least operational overhead because it does not require creating separate datasets or proxy application layers, and it allows you to maintain a single copy of the data in an S3 bucket.
https://aws.amazon.com/ko/blogs/korea/introducing-amazon-s3-object-lambda-use-your-code-to-process-data-as-it-is-being-retrieved-from-s3/

QUESTION 383
A development team has launched a new application that is hosted on Amazon EC2 instances inside a development VPC. A solutions architect needs to create a new VPC in the same account. The new VPC will be peered with the development VPC. The VPC CIDR block for the development VPC is 192.168.0.0/24. The solutions architect needs to create a CIDR block for the new VPC. The CIDR block must be valid for a VPC peering connection to the development VPC.

What is the SMALLEST CIDR block that meets these requirements?

A. 10.0.1.0/32
B. 192.168.0.0/24
C. 192.168.1.0/32
D. 10.0.1.0/24

Answer: D
Explanation:
The allowed block size is between a /28 netmask and /16 netmask.
The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.
https://docs.aws.amazon.com/vpc/latest/userguide/configure-your-vpc.html

QUESTION 384
A company deploys an application on five Amazon EC2 instances. An Application Load Balancer (ALB) distributes traffic to the instances by using a target group. The average CPU usage on each of the instances is below 10% most of the time, with occasional surges to 65%.

A solutions architect needs to implement a solution to automate the scalability of the application. The solution must optimize the cost of the architecture and must ensure that the application has enough CPU resources when surges occur.

Which solution will meet these requirements?

A. Create an Amazon CloudWatch alarm that enters the ALARM state when the CPUUtilization metric is less than 20%. Create an AWS Lambda function that the CloudWatch alarm invokes to terminate one of the EC2 instances in the ALB target group.
B. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set a target tracking scaling policy that is based on the ASGAverageCPUUtilization metric. Set the minimum instances to 2, the desired capacity to 3, the maximum instances to 6, and the target value to 50%. Add the EC2 instances to the Auto Scaling group.
C. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set the minimum instances to 2, the desired capacity to 3, and the maximum instances to 6. Add the EC2 instances to the Auto Scaling group.
D. Create two Amazon CloudWatch alarms. Configure the first CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is below 20%. Configure the second CloudWatch alarm to enter the ALARM state when the average CPUUtilization matric is above 50%. Configure the alarms to publish to an Amazon Simple Notification Service (Amazon SNS)

topic to send an email message. After receiving the message, log in to decrease or increase the number of EC2 instances that are running.

Answer: B
Explanation:
It allows for automatic scaling based on the average CPU utilization of the EC2 instances in the target group. With the use of a target tracking scaling policy based on the ASGAverageCPUUtilization metric, the EC2 Auto Scaling group can ensure that the target value of 50% is maintained while scaling the number of instances in the group up or down as needed. This will help ensure that the application has enough CPU resources during surges without overprovisioning, thus optimizing the cost of the architecture.

QUESTION 385
A company is running a critical business application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances run in an Auto Scaling group and access an Amazon RDS DB instance.

The design did not pass an operational review because the EC2 instances and the DB instance are all located in a single Availability Zone. A solutions architect must update the design to use a second Availability Zone.

Which solution will make the application highly available?

A. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
B. Provision two subnets that extend across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
C. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.
D. Provision a subnet that extends across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.

Answer: C
Explanation:
A subnet must reside within a single Availability Zone.
https://aws.amazon.com/vpc/faqs/#:~:text=Can%20a%20subnet%20span%20Availability,within%20a%20single%20Availability%20Zone.

QUESTION 386
A research laboratory needs to process approximately 8 TB of data. The laboratory requires sub-millisecond latencies and a minimum throughput of 6 GBps for the storage subsystem. Hundreds of Amazon EC2 instances that run Amazon Linux will distribute and process the data.

Which solution will meet the performance requirements?

A. Create an Amazon FSx for NetApp ONTAP file system. Sat each volume' tiering policy to ALL. Import the raw data into the file system. Mount the fila system on the EC2 instances.
B. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to

Amazon S3. Mount the file system on the EC2 instances.

C. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent HDD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
D. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to NONE. Import the raw data into the file system. Mount the file system on the EC2 instances.

Answer: B
Explanation:
Create an Amazon S3 bucket to store the raw data Create an Amazon FSx for Lustre file system that uses persistent SSD storage Select the option to import data from and export data to Amazon S3 Mount the file system on the EC2 instances. Amazon FSx for Lustre uses SSD storage for sub-millisecond latencies and up to 6 GBps throughput, and can import data from and export data to Amazon S3. Additionally, the option to select persistent SSD storage will ensure that the data is stored on the disk and not lost if the file system is stopped.

QUESTION 387
A company needs to migrate a legacy application from an on-premises data center to the AWS Cloud because of hardware capacity constraints. The application runs 24 hours a day, 7 days a week. The application's database storage continues to grow over time.

What should a solutions architect do to meet these requirements MOST cost-effectively?

A. Migrate the application layer to Amazon EC2 Spot Instances. Migrate the data storage layer to Amazon S3.
B. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon RDS On-Demand Instances.
C. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon Aurora Reserved Instances.
D. Migrate the application layer to Amazon EC2 On-Demand Instances. Migrate the data storage layer to Amazon RDS Reserved Instances.

Answer: C
Explanation:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.AuroraMySQL.html

QUESTION 388
A university research laboratory needs to migrate 30 TB of data from an on-premises Windows file server to Amazon FSx for Windows File Server. The laboratory has a 1 Gbps network link that many other departments in the university share.

The laboratory wants to implement a data migration service that will maximize the performance of the data transfer. However, the laboratory needs to be able to control the amount of bandwidth that the service uses to minimize the impact on other departments. The data migration must take place within the next 5 days.

Which AWS solution will meet these requirements?

A. AWS Snowcone
B. Amazon FSx File Gateway
C. AWS DataSync
D. AWS Transfer Family

Answer: C
Explanation:
DataSync can be used to migrate data between on-premises Windows file servers and Amazon FSx for Windows File Server with its compatibility for Windows file systems.
The laboratory needs to migrate a large amount of data (30 TB) within a relatively short timeframe (5 days) and limit the impact on other departments' network traffic. Therefore, AWS DataSync can meet these requirements by providing fast and efficient data transfer with network throttling capability to control bandwidth usage.
https://docs.aws.amazon.com/datasync/latest/userguide/configure-bandwidth.html

QUESTION 389
A company wants to create a mobile app that allows users to stream slow-motion video clips on their mobile devices. Currently, the app captures video clips and uploads the video clips in raw format into an Amazon S3 bucket. The app retrieves these video clips directly from the S3 bucket. However, the videos are large in their raw format.

Users are experiencing issues with buffering and playback on mobile devices. The company wants to implement solutions to maximize the performance and scalability of the app while minimizing operational overhead.

Which combination of solutions will meet these requirements? (Choose two.)

A. Deploy Amazon CloudFront for content delivery and caching.
B. Use AWS DataSync to replicate the video files across AW'S Regions in other S3 buckets.
C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.
D. Deploy an Auto Sealing group of Amazon EC2 instances in Local Zones for content delivery and caching.
E. Deploy an Auto Scaling group of Amazon EC2 instances to convert the video files to more appropriate formats.

Answer: AC
Explanation:
https://aws.amazon.com/elastictranscoder/

QUESTION 390
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

Explanation:
https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto-scaling.html

QUESTION 391
A company recently created a disaster recovery site in a different AWS Region. The company needs to transfer large amounts of data back and forth between NFS file systems in the two Regions on a periodic basis.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS DataSync.
B. Use AWS Snowball devices.
C. Set up an SFTP server on Amazon EC2.
D. Use AWS Database Migration Service (AWS DMS).

Answer: A
Explanation:
AWS DataSync is a fully managed data transfer service that simplifies moving large amounts of data between on-premises storage systems and AWS services. It can also transfer data between different AWS services, including different AWS Regions. DataSync provides a simple, scalable, and automated solution to transfer data, and it minimizes the operational overhead because it is fully managed by AWS.

QUESTION 392
A company uses Amazon API Gateway to run a private gateway with two REST APIs in the same VPC. The BuyStock RESTful web service calls the CheckFunds RESTful web service to ensure that enough funds are available before a stock can be purchased. The company has noticed in the VPC flow logs that the BuyStock RESTful web service calls the CheckFunds RESTful web service over the internet instead of through the VPC. A solutions architect must implement a solution so that the APIs communicate through the VPC.

Which solution will meet these requirements with the FEWEST changes to the code?

A. Add an X-API-Key header in the HTTP header for authorization.
B. Use an interface endpoint.
C. Use a gateway endpoint.
D. Add an Amazon Simple Queue Service (Amazon SQS) queue between the two REST APIs.

Answer: B
Explanation:
An interface endpoint is a horizontally scaled, redundant VPC endpoint that provides private connectivity to a service. It is an elastic network interface with a private IP address that serves as an entry point for traffic destined to the AWS service. Interface endpoints are used to connect VPCs with AWS services.
https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html

QUESTION 393
A company wants to run an in-memory database for a latency-sensitive application that runs on Amazon EC2 instances. The application processes more than 100,000 transactions each minute and requires high network throughput. A solutions architect needs to provide a cost-effective network design that minimizes data transfer charges.

Which solution meets these requirements?

A. Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances.
B. Launch all EC2 instances in different Availability Zones within the same AWS Region. Specify a placement group with partition strategy when launching EC2 instances.
C. Deploy an Auto Scaling group to launch EC2 instances in different Availability Zones based on a network utilization target.
D. Deploy an Auto Scaling group with a step scaling policy to launch EC2 instances in different Availability Zones.

Answer: A
Explanation:
To achieve low latency, high throughput, and cost-effectiveness, the optimal solution is to launch EC2 instances as a placement group with the cluster strategy within the same Availability Zone.

QUESTION 394
A company that primarily runs its application servers on premises has decided to migrate to AWS. The company wants to minimize its need to scale its Internet Small Computer Systems Interface (iSCSI) storage on premises. The company wants only its recently accessed data to remain stored locally.

Which AWS solution should the company use to meet these requirements?

A. Amazon S3 File Gateway
B. AWS Storage Gateway Tape Gateway
C. AWS Storage Gateway Volume Gateway stored volumes
D. AWS Storage Gateway Volume Gateway cached volumes

Answer: D
Explanation:
AWS Storage Gateway Volume Gateway provides two configurations for connecting to iSCSI storage, namely, stored volumes and cached volumes. The stored volume configuration stores the entire data set on-premises and asynchronously backs up the data to AWS. The cached volume configuration stores recently accessed data on-premises, and the remaining data is stored in Amazon S3.
Since the company wants only its recently accessed data to remain stored locally, the cached volume configuration would be the most appropriate. It allows the company to keep frequently accessed data on-premises and reduce the need for scaling its iSCSI storage while still providing access to all data through the AWS cloud. This configuration also provides low-latency access to frequently accessed data and cost-effective off-site backups for less frequently accessed data.
https://docs.amazonaws.cn/en_us/storagegateway/latest/vgw/StorageGatewayConcepts.html#storage-gateway-cached-concepts

QUESTION 395
A company has multiple AWS accounts that use consolidated billing. The company runs several active high performance Amazon RDS for Oracle On-Demand DB instances for 90 days. The company's finance team has access to AWS Trusted Advisor in the consolidated billing account and all other AWS accounts.

The finance team needs to use the appropriate AWS account to access the Trusted Advisor check recommendations for RDS. The finance team must review the appropriate Trusted Advisor check to reduce RDS costs.

Which combination of steps should the finance team take to meet these requirements? (Choose two.)

A. Use the Trusted Advisor recommendations from the account where the RDS instances are running.
B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time.
C. Review the Trusted Advisor check for Amazon RDS Reserved Instance Optimization.
D. Review the Trusted Advisor check for Amazon RDS Idle DB Instances.
E. Review the Trusted Advisor check for Amazon Redshift Reserved Node Optimization.

Answer: BD
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/trusted-advisor-cost-optimization/

QUESTION 396
A solutions architect needs to optimize storage costs. The solutions architect must identify any Amazon S3 buckets that are no longer being accessed or are rarely accessed.

Which solution will accomplish this goal with the LEAST operational overhead?

A. Analyze bucket access patterns by using the S3 Storage Lens dashboard for advanced activity metrics.
B. Analyze bucket access patterns by using the S3 dashboard in the AWS Management Console.
C. Turn on the Amazon CloudWatch BucketSizeBytes metric for buckets. Analyze bucket access patterns by using the metrics data with Amazon Athena.
D. Turn on AWS CloudTrail for S3 object monitoring. Analyze bucket access patterns by using CloudTrail logs that are integrated with Amazon CloudWatch Logs.

Answer: A
Explanation:
S3 Storage Lens is a fully managed S3 storage analytics solution that provides a comprehensive view of object storage usage, activity trends, and recommendations to optimize costs. Storage Lens allows you to analyze object access patterns across all of your S3 buckets and generate detailed metrics and reports.
https://aws.amazon.com/blogs/aws/s3-storage-lens/

QUESTION 397
A company sells datasets to customers who do research in artificial intelligence and machine learning (AI/ML). The datasets are large, formatted files that are stored in an Amazon S3 bucket in the us-east-1 Region. The company hosts a web application that the customers use to purchase access to a given dataset. The web application is deployed on multiple Amazon EC2 instances behind an Application Load Balancer. After a purchase is made, customers receive an S3 signed URL that allows access to the files.

The customers are distributed across North America and Europe. The company wants to reduce the cost that is associated with data transfers and wants to maintain or improve performance.

What should a solutions architect do to meet these requirements?

A. Configure S3 Transfer Acceleration on the existing S3 bucket. Direct customer requests to the S3 Transfer Acceleration endpoint. Continue to use S3 signed URLs for access control.
B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin. Direct customer requests to the CloudFront URL. Switch to CloudFront signed URLs for access control.
C. Set up a second S3 bucket in the eu-central-1 Region with S3 Cross-Region Replication between the buckets. Direct customer requests to the closest Region. Continue to use S3 signed URLs for access control.
D. Modify the web application to enable streaming of the datasets to end users. Configure the web application to read the data from the existing S3 bucket. Implement access control directly in the application.

Answer: B
Explanation:
To reduce the cost associated with data transfers and maintain or improve performance, a solutions architect should use Amazon CloudFront, a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.
Deploying a CloudFront distribution with the existing S3 bucket as the origin will allow the company to serve the data to customers from edge locations that are closer to them, reducing data transfer costs and improving performance.
Directing customer requests to the CloudFront URL and switching to CloudFront signed URLs for access control will enable customers to access the data securely and efficiently.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html

QUESTION 398
A company is using AWS to design a web application that will process 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 get lost. The solution must maximize operational efficiency and must minimize maintenance.

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 use the Kinesis Client Library (KCL) to pool messages from its own data stream.
B. Create an AWS Lambda function and an Amazon Simple Notification Service (Amazon SNS) topic for each quote type. Subscribe the Lambda function to its associated SNS topic. Configure the application to publish requests for quotes to the appropriate SNS topic.
C. Create a single Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon Simple Queue Service (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 use 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 OpenSearch Service cluster. Configure the application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from OpenSearch Service and process them accordingly.

Answer: C
Explanation:
Quote types need to be separated: SNS message filtering can be used to publish messages to the appropriate SQS queue based on the quote type, ensuring that quotes are separated by type.
Quotes must be responded to within 24 hours and must not get lost: SQS provides reliable and scalable queuing for messages, ensuring that quotes will not get lost and can be processed in a

timely manner. Additionally, each backend application server can use its own SQS queue, ensuring that quotes are processed efficiently without any delay.
Operational efficiency and minimizing maintenance: Using a single SNS topic and multiple SQS queues is a scalable and cost-effective approach, which can help to maximize operational efficiency and minimize maintenance. Additionally, SNS and SQS are fully managed services, which means that the company will not need to worry about maintenance tasks such as software updates, hardware upgrades, or scaling the infrastructure.
https://aws.amazon.com/getting-started/hands-on/filter-messages-published-to-topics/

QUESTION 399
A company has an application that runs on several Amazon EC2 instances. Each EC2 instance has multiple Amazon Elastic Block Store (Amazon EBS) data volumes attached to it. The application's EC2 instance configuration and data need to be backed up nightly. The application also needs to be recoverable in a different AWS Region.

Which solution will meet these requirements in the MOST operationally efficient way?

A. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Region.
B. Create a backup plan by using AWS Backup to perform nightly backups. Copy the backups to another Region. Add the application's EC2 instances as resources.
C. Create a backup plan by using AWS Backup to perform nightly backups. Copy the backups to another Region. Add the application's EBS volumes as resources.
D. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Availability Zone.

Answer: B
Explanation:
https://aws.amazon.com/vi/blogs/aws/aws-backup-ec2-instances-efs-single-file-restore-and-cross-region-backup/
When you back up an EC2 instance, AWS Backup will protect all EBS volumes attached to the instance, and it will attach them to an AMI that stores all parameters from the original EC2 instance except for two.

QUESTION 400
A company is building a mobile app on AWS. The company wants to expand its reach to millions of users. The company needs to build a platform so that authorized users can watch the company's content on their mobile devices.

What should a solutions architect recommend to meet these requirements?

A. Publish content to a public Amazon S3 bucket. Use AWS Key Management Service (AWS KMS) keys to stream content.
B. Set up IPsec VPN between the mobile app and the AWS environment to stream content.
C. Use Amazon CloudFront. Provide signed URLs to stream content.
D. Set up AWS Client VPN between the mobile app and the AWS environment to stream content.

Answer: C
Explanation:
Amazon CloudFront is a content delivery network (CDN) that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. CloudFront supports signed URLs that provide authorized access to your content. This feature allows the company to control who can access their content and for how long, providing a secure

and scalable solution for millions of users.
https://www.amazonaws.cn/en/cloudfront/

QUESTION 401
A company hosts a three-tier web application that includes a PostgreSQL database The database stores the metadata from documents The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month The documents are stored in Amazon S3 The documents are usually written only once, but they are updated frequency The reporting process takes a few hours with the use of relational queries The reporting process must not affect any document modifications or the addition of new documents.
What are the MOST operationally efficient solutions that meet these requirements? (Choose two.)

A. Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica Scale the read replica to generate the reports.
B. Set up a new Amazon RDS for PostgreSQL Reserved Instance and an On-Demand read replica Scale the read replica to generate the reports.
C. Set up a new Amazon Aurora PostgreSQL DB cluster that includes a Reserved Instance and an Aurora Replica issue queries to the Aurora Replica to generate the reports.
D. Set up a new Amazon RDS for PostgreSQL Multi-AZ Reserved Instance Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node.
E. Set up a new Amazon DynamoDB table to store the documents Use a fixed write capacity to support new document entries Automatically scale the read capacity to support the reports.

Answer: BC

QUESTION 402
A company experienced a breach that affected several applications in its on-premises data center. The attacker took advantage of vulnerabilities in the custom applications that were running on the servers. The company is now migrating its applications to run on Amazon EC2 instances. The company wants to implement a solution that actively scans for vulnerabilities on the EC2 instances and sends a report that details the findings.

Which solution will meet these requirements?

A. Deploy AWS Shield to scan the EC2 instances for vulnerabilities. Create an AWS Lambda function to log any findings to AWS CloudTrail.
B. Deploy Amazon Macie and AWS Lambda functions to scan the EC2 instances for vulnerabilities. Log any findings to AWS CloudTrail.
C. Turn on Amazon GuardDuty. Deploy the GuardDuty agents to the EC2 instances. Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings.
D. Turn on Amazon Inspector. Deploy the Amazon Inspector agent to the EC2 instances. Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings.

Answer: D
Explanation:
Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.
https://aws.amazon.com/inspector/features/?nc=sn&loc=2

QUESTION 403
A company uses an Amazon EC2 instance to run a script to poll for and process messages in an Amazon Simple Queue Service (Amazon SQS) queue. The company wants to reduce operational costs while maintaining its ability to process a growing number of messages that are added to the queue.

What should a solutions architect recommend to meet these requirements?

A. Increase the size of the EC2 instance to process messages faster.
B. Use Amazon EventBridge to turn off the EC2 instance when the instance is underutilized.
C. Migrate the script on the EC2 instance to an AWS Lambda function with the appropriate runtime.
D. Use AWS Systems Manager Run Command to run the script on demand.

Answer: C
Explanation:
By migrating the script to AWS Lambda, the company can take advantage of the auto-scaling feature of the service. AWS Lambda will automatically scale resources to match the size of the workload. This means that the company will not have to worry about provisioning or managing instances as the number of messages increases, resulting in lower operational costs.

QUESTION 404
A company uses a legacy application to produce data in CSV format. The legacy application stores the output data in Amazon S3. The company is deploying a new commercial off-the-shelf (COTS) application that can perform complex SQL queries to analyze data that is stored in Amazon Redshift and Amazon S3 only. However, the COTS application cannot process the .csv files that the legacy application produces.

The company cannot update the legacy application to produce data in another format. The company needs to implement a solution so that the COTS application can use the data that the legacy application produces.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS Glue extract, transform, and load (ETL) job that runs on a schedule. Configure the ETL job to process the .csv files and store the processed data in Amazon Redshift.
B. Develop a Python script that runs on Amazon EC2 instances to convert the .csv files to .sql files. Invoke the Python script on a cron schedule to store the output files in Amazon S3.
C. Create an AWS Lambda function and an Amazon DynamoDB table. Use an S3 event to invoke the Lambda function. Configure the Lambda function to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in the DynamoDB table.
D. Use Amazon EventBridge to launch an Amazon EMR cluster on a weekly schedule. Configure the EMR cluster to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in an Amazon Redshift table.

Answer: A
Explanation:
https://docs.aws.amazon.com/glue/latest/dg/aws-glue-programming-etl-format-csv-home.html

QUESTION 405
A company recently migrated its entire IT environment to the AWS Cloud. The company discovers that users are provisioning oversized Amazon EC2 instances and modifying security group rules without using the appropriate change control process. A solutions architect must

devise a strategy to track and audit these inventory and configuration changes.

Which actions should the solutions architect take to meet these requirements? (Choose two.)

A. Enable AWS CloudTrail and use it for auditing.
B. Use data lifecycle policies for the Amazon EC2 instances.
C. Enable AWS Trusted Advisor and reference the security dashboard.
D. Enable AWS Config and create rules for auditing and compliance purposes.
E. Restore previous resource configurations with an AWS CloudFormation template.

Answer: AD

QUESTION 406
A company has hundreds of Amazon EC2 Linux-based instances in the AWS Cloud. Systems administrators have used shared SSH keys to manage the instances. After a recent audit, the company's security team is mandating the removal of all shared keys. A solutions architect must design a solution that provides secure access to the EC2 instances.

Which solution will meet this requirement with the LEAST amount of administrative overhead?

A. Use AWS Systems Manager Session Manager to connect to the EC2 instances.
B. Use AWS Security Token Service (AWS STS) to generate one-time SSH keys on demand.
C. Allow shared SSH access to a set of bastion instances. Configure all other instances to allow only SSH access from the bastion instances.
D. Use an Amazon Cognito custom authorizer to authenticate users. Invoke an AWS Lambda function to generate a temporary SSH key.

Answer: A
Explanation:
AWS Systems Manager Session Manager provides secure and auditable instance management without the need for any inbound connections or open ports. It allows you to manage your instances through an interactive one-click browser-based shell or through the AWS CLI. This means that you don't have to manage any SSH keys, and you don't have to worry about securing access to your instances as access is controlled through IAM policies.

QUESTION 407
A company is building a data analysis platform on AWS by using AWS Lake Formation. The platform will ingest data from different sources such as Amazon S3 and Amazon RDS. The company needs a secure solution to prevent access to portions of the data that contain sensitive information.

A. Create an IAM role that includes permissions to access Lake Formation tables.
B. Create data filters to implement row-level security and cell-level security.
C. Create an AWS Lambda function that removes sensitive information before Lake Formation ingests re data.
D. Create an AWS Lambda function that perodically Queries and removes sensitive information from Lake Formation tables.

Answer: A

QUESTION 408

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
Explanation:
To ensure that all objects uploaded to an Amazon S3 bucket are encrypted, the solutions architect should update the bucket policy to deny any PutObject requests that do not have an x-amz-server-side-encryption header set. This will prevent any objects from being uploaded to the bucket unless they are encrypted using server-side encryption.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/amazon-s3-policy-keys.html

QUESTION 409
A solutions architect is designing a multi-tier application for a company. The application's users upload images from a mobile device. The application generates a thumbnail of each image and returns a message to the user to confirm that the image was uploaded successfully.

The thumbnail generation can take up to 60 seconds, but the company wants to provide a faster response time to its users to notify them that the original image was received. The solutions architect must design the application to asynchronously dispatch requests to the different application tiers.

What should the solutions architect do to meet these requirements?

A. Write a custom AWS Lambda function to generate the thumbnail and alert the user. Use the image upload process as an event source to invoke the Lambda function.
B. Create an AWS Step Functions workflow. Configure Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete.
C. Create an Amazon Simple Queue Service (Amazon SQS) message queue. As images are uploaded, place a message on the SQS queue for thumbnail generation. Alert the user through an application message that the image was received.
D. Create Amazon Simple Notification Service (Amazon SNS) notification topics and subscriptions. Use one subscription with the application to generate the thumbnail after the image upload is complete. Use a second subscription to message the user's mobile app by way of a push notification after thumbnail generation is complete.

Answer: C

QUESTION 410
A solution architect needs to assign a new microsoft for a company's application. Clients must be able to call an HTTPS endpoint to reach the micoservice. The microservice also must use AWS identity and Access Management (IAM) to authentication calls. The soltions architect will write the logic for this microservice by using a single AWS Lambda function that is written in Go 1.x.
Which solution will deploy the function in the in the MOST operationally efficient way?

A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.
B. Create a Lambda function URL for the function. Specify AWS_IAM as the authentication type.
C. Create an Amazon CloudFront distribution. Deploy the function to Lambda@Edge. Integrate IAM authentication logic into the Lambda@Edge function.
D. Create an Amazon CloudFront distribuion. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.

Answer: A

QUESTION 411
A company wants to implement a disaster recovery plan for its primary on-premises file storage volume. The file storage volume is mounted from an Internet Small Computer Systems Interface (iSCSI) device on a local storage server. The file storage volume holds hundreds of terabytes (TB) of data.

The company wants to ensure that end users retain immediate access to all file types from the on-premises systems without experiencing latency.

Which solution will meet these requirements with the LEAST amount of change to the company's existing infrastructure?

A. Provision an Amazon S3 File Gateway as a virtual machine (VM) that is hosted on premises. Set the local cache to 10 TB. Modify existing applications to access the files through the NFS protocol. To recover from a disaster, provision an Amazon EC2 instance and mount the S3 bucket that contains the files.
B. Provision an AWS Storage Gateway tape gateway. Use a data backup solution to back up all existing data to a virtual tape library. Configure the data backup solution to run nightly after the initial backup is complete. To recover from a disaster, provision an Amazon EC2 instance and restore the data to an Amazon Elastic Block Store (Amazon EBS) volume from the volumes in the virtual tape library.
C. Provision an AWS Storage Gateway Volume Gateway cached volume. Set the local cache to 10 TB. Mount the Volume Gateway cached volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.
D. Provision an AWS Storage Gateway Volume Gateway stored volume with the same amount of disk space as the existing file storage volume. Mount the Volume Gateway stored volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

Answer: D

QUESTION 412
A company is hosting a web application from an Amazon S3 bucket. The application uses Amazon Cognito as an identity provider to authenticate users and return a JSON Web Token (JWT) that provides access to protected resources that are stored in another S3 bucket.

Upon deployment of the application, users report errors and are unable to access the protected content. A solutions architect must resolve this issue by providing proper permissions so that users can access the protected content.

Which solution meets these requirements?

A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content.
B. Update the S3 ACL to allow the application to access the protected content.
C. Redeploy the application to Amazon S3 to prevent eventually consistent reads in the S3 bucket from affecting the ability of users to access the protected content.
D. Update the Amazon Cognito pool to use custom attribute mappings within the identity pool and grant users the proper permissions to access the protected content.

Answer: A
Explanation:
https://docs.aws.amazon.com/cognito/latest/developerguide/tutorial-create-identity-pool.html
You have to create an custom role such as read-only.

QUESTION 413
An image hosting company uploads its large assets to Amazon S3 Standard buckets. The company uses multipart upload in parallel by using S3 APIs and overwrites if the same object is uploaded again. For the first 30 days after upload, the objects will be accessed frequently. The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent. The company must optimize its S3 storage costs while maintaining high availability and resiliency of stored assets.

Which combination of actions should a solutions architect recommend to meet these requirements? (Choose two.)

A. Move assets to S3 Intelligent-Tiering after 30 days.
B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.
C. Configure an S3 Lifecycle policy to clean up expired object delete markers.
D. Move assets to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
E. Move assets to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Answer: AB
Explanation:
S3 Intelligent-Tiering - Data with unknown, changing, or unpredictable access patterns and moves objects that have not been accessed in 30 consecutive days to the Infrequent Access tier.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html

QUESTION 414
A solutions architect must secure a VPC network that hosts Amazon EC2 instances. The EC2 instances contain highly sensitive data and run in a private subnet. According to company policy, the EC2 instances that run in the VPC can access only approved third-party software repositories on the internet for software product updates that use the third party's URL. Other internet traffic must be blocked.

Which solution meets these requirements?

A. Update the route table for the private subnet to route the outbound traffic to an AWS Network Firewall firewall. Configure domain list rule groups.
B. Set up an AWS WAF web ACL. Create a custom set of rules that filter traffic requests based on source and destination IP address range sets.

C. Implement strict inbound security group rules. Configure an outbound rule that allows traffic only to the authorized software repositories on the internet by specifying the URLs.
D. Configure an Application Load Balancer (ALB) in front of the EC2 instances. Direct all outbound traffic to the ALB. Use a URL-based rule listener in the ALB's target group for outbound access to the internet.

Answer: A
Explanation:
Send the outbound connection from EC2 to Network Firewall. In Network Firewall, create stateful outbound rules to allow certain domains for software patch download and deny all other domains.
https://docs.aws.amazon.com/network-firewall/latest/developerguide/suricata-examples.html#suricata-example-domain-filtering

QUESTION 415
A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.

The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products.

What should a solutions architect recommend to ensure that all the requests are processed successfully?

A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.
B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.
C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.
D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances.

Answer: D
Explanation:
Static content can include images and style sheets that are the same across all users and are best cached at the edges of the content distribution network (CDN). Dynamic content includes information that changes frequently or is personalized based on user preferences, behavior, location or other factors - all content is sales requests.

QUESTION 416
A security audit reveals that Amazon EC2 instances are not being patched regularly. A solutions architect needs to provide a solution that will run regular security scans across a large fleet of EC2 instances. The solution should also patch the EC2 instances on a regular schedule and provide a report of each instance's patch status.

Which solution will meet these requirements?

A. Set up Amazon Macie to scan the EC2 instances for software vulnerabilities. Set up a cron job on each EC2 instance to patch the instance on a regular schedule.

B. Turn on Amazon GuardDuty in the account. Configure GuardDuty to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Session Manager to patch the EC2 instances on a regular schedule.
C. Set up Amazon Detective to scan the EC2 instances for software vulnerabilities. Set up an Amazon EventBridge scheduled rule to patch the EC2 instances on a regular schedule.
D. Turn on Amazon Inspector in the account. Configure Amazon Inspector to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Patch Manager to patch the EC2 instances on a regular schedule.

Answer: D
Explanation:
Amazon Inspector is a security assessment service that helps improve the security and compliance of applications deployed on Amazon Web Services (AWS). It automatically assesses applications for vulnerabilities or deviations from best practices. Amazon Inspector can be used to identify security issues and recommend fixes for them. It is an ideal solution for running regular security scans across a large fleet of EC2 instances.
AWS Systems Manager Patch Manager is a service that helps you automate the process of patching Windows and Linux instances. It provides a simple, automated way to patch your instances with the latest security patches and updates. Patch Manager helps you maintain compliance with security policies and regulations by providing detailed reports on the patch status of your instances.

QUESTION 417
A company is planning to store data on Amazon RDS DB instances. The company must encrypt the data at rest.

What should a solutions architect do to meet this requirement?

A. Create a key in AWS Key Management Service (AWS KMS). Enable encryption for the DB instances.
B. Create an encryption key. Store the key in AWS Secrets Manager. Use the key to encrypt the DB instances.
C. Generate a certificate in AWS Certificate Manager (ACM). Enable SSL/TLS on the DB instances by using the certificate.
D. Generate a certificate in AWS Identity and Access Management (IAM). Enable SSL/TLS on the DB instances by using the certificate.

Answer: A
Explanation:
To encrypt data at rest in Amazon RDS, you can use the encryption feature of Amazon RDS, which uses AWS Key Management Service (AWS KMS). With this feature, Amazon RDS encrypts each database instance with a unique key. This key is stored securely by AWS KMS. You can manage your own keys or use the default AWS-managed keys. When you enable encryption for a DB instance, Amazon RDS encrypts the underlying storage, including the automated backups, read replicas, and snapshots.

QUESTION 418
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
Explanation:
AWS Snowball is a secure data transport solution that accelerates moving large amounts of data into and out of the AWS cloud. It can move up to 80 TB of data at a time, and provides a network bandwidth of up to 50 Mbps, so it is well-suited for the task. Additionally, it is secure and easy to use, making it the ideal solution for this migration.
https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html

QUESTION 419
A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded securely to the employees' devices.
The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.
Which solution will meet these requirements?

A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.
B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.
C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS IAM Identity Center (AWS Single Sign-On).

Answer: B
Explanation:
It provides a secure way for employees to access confidential and sensitive files from anywhere using AWS Client VPN. The Amazon FSx for Windows File Server file system is designed to provide native support for Windows file system features such as NTFS permissions, Active Directory integration, and Distributed File System (DFS). This means that the company can continue to use their on-premises Active Directory to manage user access to files.

QUESTION 420
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 runs. 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:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html

QUESTION 421
A company wants to give a customer the ability to use on-premises Microsoft Active Directory to download files that are stored in Amazon S3. The customer's application uses an SFTP client to download the files.

Which solution will meet these requirements with the LEAST operational overhead and no changes to the customer's application?

A. Set up AWS Transfer Family with SFTP for Amazon S3. Configure integrated Active Directory authentication.
B. Set up AWS Database Migration Service (AWS DMS) to synchronize the on-premises client with Amazon S3. Configure integrated Active Directory authentication.
C. Set up AWS DataSync to synchronize between the on-premises location and the S3 location by using AWS IAM Identity Center (AWS Single Sign-On).
D. Set up a Windows Amazon EC2 instance with SFTP to connect the on-premises client with Amazon S3. Integrate AWS Identity and Access Management (IAM).

Answer: A
Explanation:
https://docs.aws.amazon.com/transfer/latest/userguide/directory-services-users.html

QUESTION 422
A company is experiencing sudden increases in demand. The company needs to provision large Amazon EC2 instances from an Amazon Machine Image (AMI). The instances will run in an Auto Scaling group. The company needs a solution that provides minimum initialization latency to meet the demand.

Which solution meets these requirements?

A. Use the aws ec2 register-image command to create an AMI from a snapshot. Use AWS Step Functions to replace the AMI in the Auto Scaling group.
B. Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot. Provision an AMI by using the snapshot. Replace the AMI in the Auto Scaling group with the new AMI.
C. Enable AMI creation and define lifecycle rules in Amazon Data Lifecycle Manager (Amazon DLM). Create an AWS Lambda function that modifies the AMI in the Auto Scaling group.
D. Use Amazon EventBridge to invoke AWS Backup lifecycle policies that provision AMIs. Configure Auto Scaling group capacity limits as an event source in EventBridge.

Answer: B
Explanation:
Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows you to quickly create a new Amazon Machine Image (AMI) from a snapshot, which can help reduce the initialization latency when provisioning new instances. Once the AMI is provisioned, you can replace the AMI in the Auto Scaling group with the new AMI. This will ensure that new instances are launched from the updated AMI and are able to meet the increased demand quickly.

QUESTION 423
A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days.

What should a solutions architect do to meet this requirement with the LEAST operational effort?

A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days.
B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.
C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file. Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file.
D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials. Download the file to the application regularly to ensure that the correct credentials are used. Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket.

Answer: A
Explanation:
To implement password rotation lifecycles, use AWS Secrets Manager. You can rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle using Secrets Manager.
https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/

QUESTION 424
A company has deployed a web application on AWS. The company hosts the backend database on Amazon RDS for MySQL with a primary DB instance and five read replicas to support scaling needs. The read replicas must lag no more than 1 second behind the primary DB instance. The database routinely runs scheduled stored procedures.

As traffic on the website increases, the replicas experience additional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutions architect must minimize changes to the application code and must minimize ongoing operational overhead.

Which solution will meet these requirements?

A. Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the stored procedures with Aurora MySQL native functions.
B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the application to check the cache before the application queries the database. Replace the stored procedures with AWS Lambda functions.

C. Migrate the database to a MySQL database that runs on Amazon EC2 instances. Choose large, compute optimized EC2 instances for all replica nodes. Maintain the stored procedures on the EC2 instances.
D. Migrate the database to Amazon DynamoDB. Provision a large number of read capacity units (RCUs) to support the required throughput, and configure on-demand capacity scaling. Replace the stored procedures with DynamoDB streams.

Answer: A
Explanation:
You can scale reads for your Amazon RDS for PostgreSQL DB instance by adding read replicas to the instance. As with other Amazon RDS database engines, RDS for PostgreSQL uses the native replication mechanisms of PostgreSQL to keep read replicas up to date with changes on the source DB. For general information about read replicas and Amazon RDS, see Working with read replicas.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PostgreSQL.Replication.ReadReplicas.html

QUESTION 425
A solutions architect must create a disaster recovery (DR) plan for a high-volume software as a service (SaaS) platform. All data for the platform is stored in an Amazon Aurora MySQL DB cluster.
The DR plan must replicate data to a secondary AWS Region.
Which solution will meet these requirements MOST cost-effectively?

A. Use MySQL binary log replication to an Aurora cluster in the secondary Region. Provision one DB instance for the Aurora cluster in the secondary Region.
B. Set up an Aurora global database for the DB cluster. When setup is complete, remove the DB instance from the secondary Region.
C. Use AWS Database Migration Service (AWS DMS) to continuously replicate data to an Aurora cluster in the secondary Region. Remove the DB instance from the secondary Region.
D. Set up an Aurora global database for the DB cluster. Specify a minimum of one DB instance in the secondary Region.

Answer: D
Explanation:
An Aurora DB cluster can contain up to 15 Aurora Replicas. The Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans WITHIN an AWS Region.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html
You can replicate data across multiple Regions by using an Aurora global database.

QUESTION 426
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) 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: C
Explanation:
https://ws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/

QUESTION 427
A media company hosts its website on AWS. The website application's architecture includes a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) and a database that is hosted on Amazon Aurora. The company's cybersecurity team reports that the application is vulnerable to SQL injection.

How should the company resolve this issue?

A. Use AWS WAF in front of the ALB. Associate the appropriate web ACLs with AWS WAF.
B. Create an ALB listener rule to reply to SQL injections with a fixed response.
C. Subscribe to AWS Shield Advanced to block all SQL injection attempts automatically.
D. Set up Amazon Inspector to block all SQL injection attempts automatically.

Answer: A
Explanation:
Protect against SQL injection and cross-site scripting
To protect your applications against SQL injection and cross-site scripting (XSS) attacks, use the built-in SQL injection and cross-site scripting engines. Remember that attacks can be performed on different parts of the HTTP request, such as the HTTP header, query string, or URI. Configure the AWS WAF rules to inspect different parts of the HTTP request against the built-in mitigation engines.

QUESTION 428
A company has an Amazon S3 data lake that is governed by AWS Lake Formation. The company wants to create a visualization in Amazon QuickSight by joining the data in the data lake with operational data that is stored in an Amazon Aurora MySQL database. The company wants to enforce column-level authorization so that the company's marketing team can access only a subset of columns in the database.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon EMR to ingest the data directly from the database to the QuickSight SPICE engine. Include only the required columns.
B. Use AWS Glue Studio to ingest the data from the database to the S3 data lake. Attach an IAM policy to the QuickSight users to enforce column-level access control. Use Amazon S3 as the data source in QuickSight.
C. Use AWS Glue Elastic Views to create a materialized view for the database in Amazon S3. Create an S3 bucket policy to enforce column-level access control for the QuickSight users. Use

Amazon S3 as the data source in QuickSight.

D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake. Use Lake Formation to enforce column-level access control for the QuickSight users. Use Amazon Athena as the data source in QuickSight.

Answer: D
Explanation:
This solution leverages AWS Lake Formation to ingest data from the Aurora MySQL database into the S3 data lake, while enforcing column-level access control for QuickSight users. Lake Formation can be used to create and manage the data lake's metadata and enforce security and governance policies, including column-level access control. This solution then uses Amazon Athena as the data source in QuickSight to query the data in the S3 data lake. This solution minimizes operational overhead by leveraging AWS services to manage and secure the data, and by using a standard query service (Amazon Athena) to provide a SQL interface to the data.
https://aws.amazon.com/blogs/big-data/enforce-column-level-authorization-with-amazon-quicksight-and-aws-lake-formation/

QUESTION 429
A transaction processing company has weekly scripted batch jobs that run on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group. The number of transactions can vary, but the baseline CPU utilization that is noted on each run is at least 60%. The company needs to provision the capacity 30 minutes before the jobs run.

Currently, engineers complete this task by manually modifying the Auto Scaling group parameters. The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts. The company needs an automated way to modify the Auto Scaling group's desired capacity.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create a dynamic scaling policy for the Auto Scaling group. Configure the policy to scale based on the CPU utilization metric. Set the target value for the metric to 60%.
B. Create a scheduled scaling policy for the Auto Scaling group. Set the appropriate desired capacity, minimum capacity, and maximum capacity. Set the recurrence to weekly. Set the start time to 30 minutes before the batch jobs run.
C. Create a predictive scaling policy for the Auto Scaling group. Configure the policy to scale based on forecast. Set the scaling metric to CPU utilization. Set the target value for the metric to 60%. In the policy, set the instances to pre-launch 30 minutes before the jobs run.
D. Create an Amazon EventBridge event to invoke an AWS Lambda function when the CPU utilization metric value for the Auto Scaling group reaches 60%. Configure the Lambda function to increase the Auto Scaling group's desired capacity and maximum capacity by 20%.

Answer: C
Explanation:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html

QUESTION 430
A solutions architect is designing a company's disaster recovery (DR) architecture. The company has a MySQL database that runs on an Amazon EC2 instance in a private subnet with scheduled backup. The DR design needs to include multiple AWS Regions.

Which solution will meet these requirements with the LEAST operational overhead?

A. Migrate the MySQL database to multiple EC2 instances. Configure a standby EC2 instance in the DR Region. Turn on replication.
B. Migrate the MySQL database to Amazon RDS. Use a Multi-AZ deployment. Turn on read replication for the primary DB instance in the different Availability Zones.
C. Migrate the MySQL database to an Amazon Aurora global database. Host the primary DB cluster in the primary Region. Host the secondary DB cluster in the DR Region.
D. Store the scheduled backup of the MySQL database in an Amazon S3 bucket that is configured for S3 Cross-Region Replication (CRR). Use the data backup to restore the database in the DR Region.

Answer: C
Explanation:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html

QUESTION 431
A company has a Java application that uses Amazon Simple Queue Service (Amazon SQS) to parse messages. The application cannot parse messages that are larger than 256 KB in size. The company wants to implement a solution to give the application the ability to parse messages as large as 50 MB.

Which solution will meet these requirements with the FEWEST changes to the code?

A. Use the Amazon SQS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.
B. Use Amazon EventBridge to post large messages from the application instead of Amazon SQS.
C. Change the limit in Amazon SQS to handle messages that are larger than 256 KB.
D. Store messages that are larger than 256 KB in Amazon Elastic File System (Amazon EFS). Configure Amazon SQS to reference this location in the messages.

Answer: A
Explanation:
To send messages larger than 256 KiB, you can use the Amazon SQS Extended Client Library for Java. This library allows you to send an Amazon SQS message that contains a reference to a message payload in Amazon S3. The maximum payload size is 2 GB.
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/quotas-messages.html

QUESTION 432
A company wants to restrict access to the content of one of its main web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture and an authentication solution for fewer than 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as the company's user base grows while providing the lowest login latency possible.

Which solution will meet these requirements MOST cost-effectively?

A. Use Amazon Cognito for authentication. Use Lambda@Edge for authorization. Use Amazon CloudFront to serve the web application globally.
B. Use AWS Directory Service for Microsoft Active Directory for authentication. Use AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.
C. Use Amazon Cognito for authentication. Use AWS Lambda for authorization. Use Amazon S3

Transfer Acceleration to serve the web application globally.

D. Use AWS Directory Service for Microsoft Active Directory for authentication. Use Lambda@Edge for authorization. Use AWS Elastic Beanstalk to serve the web application globally.

Answer: A

Explanation:

Amazon CloudFront is a global content delivery network (CDN) service that can securely deliver web content, videos, and APIs at scale. It integrates with Cognito for authentication and with Lambda@Edge for authorization, making it an ideal choice for serving web content globally. Lambda@Edge is a service that lets you run AWS Lambda functions globally closer to users, providing lower latency and faster response times. It can also handle authorization logic at the edge to secure content in CloudFront. For this scenario, Lambda@Edge can provide authorization for the web application while leveraging the low-latency benefit of running at the edge.

QUESTION 433

A company has an aging network-attached storage (NAS) array in its data center. The NAS array presents SMB shares and NFS shares to client workstations. The company does not want to purchase a new NAS array. The company also does not want to incur the cost of renewing the NAS array's support contract. Some of the data is accessed frequently, but much of the data is inactive.

A solutions architect needs to implement a solution that migrates the data to Amazon S3, uses S3 Lifecycle policies, and maintains the same look and feel for the client workstations. The solutions architect has identified AWS Storage Gateway as part of the solution.

Which type of storage gateway should the solutions architect provision to meet these requirements?

A. Volume Gateway
B. Tape Gateway
C. Amazon FSx File Gateway
D. Amazon S3 File Gateway

Answer: D

Explanation:

Amazon S3 File Gateway provides a file interface to objects stored in S3. It can be used for a file-based interface with S3, which allows the company to migrate their NAS array data to S3 while maintaining the same look and feel for client workstations. Amazon S3 File Gateway supports SMB and NFS protocols, which will allow clients to continue to access the data using these protocols. Additionally, Amazon S3 Lifecycle policies can be used to automate the movement of data to lower-cost storage tiers, reducing the storage cost of inactive data.
https://aws.amazon.com/about-aws/whats-new/2018/06/aws-storage-gateway-adds-smb-support-to-store-objects-in-amazon-s3/

QUESTION 434

A company has an application that is running on Amazon EC2 instances. A solutions architect has standardized the company on a particular instance family and various instance sizes based on the current needs of the company.

The company wants to maximize cost savings for the application over the next 3 years. The company needs to be able to change the instance family and sizes in the next 6 months based on application popularity and usage.

Which solution will meet these requirements MOST cost-effectively?

A. Compute Savings Plan
B. EC2 Instance Savings Plan
C. Zonal Reserved Instances
D. Standard Reserved Instances

Answer: A
Explanation:
Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, Region, OS or tenancy, and also apply to Fargate or Lambda usage.
EC2 Instance Savings Plans provide the lowest prices, offering savings up to 72% in exchange for commitment to usage of individual instance families in a Region
https://aws.amazon.com/savingsplans/compute-pricing/

QUESTION 435
A company collects data from a large number of participants who use wearable devices. The company stores the data in an Amazon DynamoDB table and uses applications to analyze the data. The data workload is constant and predictable. The company wants to stay at or below its forecasted budget for DynamoDB.

Which solution will meet these requirements MOST cost-effectively?

A. Use provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA). Reserve capacity for the forecasted workload.
B. Use provisioned mode. Specify the read capacity units (RCUs) and write capacity units (WCUs).
C. Use on-demand mode. Set the read capacity units (RCUs) and write capacity units (WCUs) high enough to accommodate changes in the workload.
D. Use on-demand mode. Specify the read capacity units (RCUs) and write capacity units (WCUs) with reserved capacity.

Answer: B
Explanation:
"The data workload is constant and predictable."
https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html
"With provisioned capacity you pay for the provision of read and write capacity units for your DynamoDB tables. Whereas with DynamoDB on-demand you pay per request for the data reads and writes that your application performs on your tables."

QUESTION 436
A company stores confidential data in an Amazon Aurora PostgreSQL database in the ap-southeast-3 Region. The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The company was recently acquired and must securely share a backup of the database with the acquiring company's AWS account in ap-southeast-3.

What should a solutions architect do to meet these requirements?

A. Create a database snapshot. Copy the snapshot to a new unencrypted snapshot. Share the new snapshot with the acquiring company's AWS account.
B. Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy.

Share the snapshot with the acquiring company's AWS account.

C. Create a database snapshot that uses a different AWS managed KMS key. Add the acquiring company's AWS account to the KMS key alias. Share the snapshot with the acquiring company's AWS account.

D. Create a database snapshot. Download the database snapshot. Upload the database snapshot to an Amazon S3 bucket. Update the S3 bucket policy to allow access from the acquiring company's AWS account.

Answer: B
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/

QUESTION 437
A company uses a 100 GB Amazon RDS for Microsoft SQL Server Single-AZ DB instance in the us-east-1 Region to store customer transactions. The company needs high availability and automatic recovery for the DB instance.

The company must also run reports on the RDS database several times a year. The report process causes transactions to take longer than usual to post to the customers' accounts. The company needs a solution that will improve the performance of the report process.

Which combination of steps will meet these requirements? (Choose two.)

A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment.
B. Take a snapshot of the current DB instance. Restore the snapshot to a new RDS deployment in another Availability Zone.
C. Create a read replica of the DB instance in a different Availability Zone. Point all requests for reports to the read replica.
D. Migrate the database to RDS Custom.
E. Use RDS Proxy to limit reporting requests to the maintenance window.

Answer: AC

QUESTION 438
A company is moving its data management application to AWS. The company wants to transition to an event-driven architecture. The architecture needs to be more distributed and to use serverless concepts while performing the different aspects of the workflow. The company also wants to minimize operational overhead.

Which solution will meet these requirements?

A. Build out the workflow in AWS Glue. Use AWS Glue to invoke AWS Lambda functions to process the workflow steps.
B. Build out the workflow in AWS Step Functions. Deploy the application on Amazon EC2 instances. Use Step Functions to invoke the workflow steps on the EC2 instances.
C. Build out the workflow in Amazon EventBridge. Use EventBridge to invoke AWS Lambda functions on a schedule to process the workflow steps.
D. Build out the workflow in AWS Step Functions. Use Step Functions to create a state machine. Use the state machine to invoke AWS Lambda functions to process the workflow steps.

Answer: D
Explanation:

AWS Step functions is serverless Visual workflows for distributed applications。
https://aws.amazon.com/step-functions/

QUESTION 439
A company is designing the network for an online multi-player game. The game uses the UDP networking protocol and will be deployed in eight AWS Regions. The network architecture needs to minimize latency and packet loss to give end users a high-quality gaming experience.

Which solution will meet these requirements?

A. Setup a transit gateway in each Region. Create inter-Region peering attachments between each transit gateway.
B. Set up AWS Global Accelerator with UDP listeners and endpoint groups in each Region.
C. Set up Amazon CloudFront with UDP turned on. Configure an origin in each Region.
D. Set up a VPC peering mesh between each Region. Turn on UDP for each VPC.

Answer: B
Explanation:
Global Accelerator supports the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), making it an excellent choice for an online multi-player game using UDP networking protocol. By setting up Global Accelerator with UDP listeners and endpoint groups in each Region, the network architecture can minimize latency and packet loss, giving end users a high-quality gaming experience.

QUESTION 440
A company hosts a three-tier web application on Amazon EC2 instances in a single Availability Zone. The web application uses a self-managed MySQL database that is hosted on an EC2 instance to store data in an Amazon Elastic Block Store (Amazon EBS) volume. The MySQL database currently uses a 1 TB Provisioned IOPS SSD (io2) EBS volume. The company expects traffic of 1,000 IOPS for both reads and writes at peak traffic.

The company wants to minimize any disruptions, stabilize performance, and reduce costs while retaining the capacity for double the IOPS. The company wants to move the database tier to a fully managed solution that is highly available and fault tolerant.

Which solution will meet these requirements MOST cost-effectively?

A. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with an io2 Block Express EBS volume.
B. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with a General Purpose SSD (gp2) EBS volume.
C. Use Amazon S3 Intelligent-Tiering access tiers.
D. Use two large EC2 instances to host the database in active-passive mode.

Answer: B
Explanation:
RDS does not support IO2 or IO2express . GP2 can do the required IOPS.
RDS supported Storage >
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html
GP2 max IOPS >
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose.html#gp2-performance

QUESTION 441
A company hosts a serverless application on AWS. The application uses Amazon API Gateway, AWS Lambda, and an Amazon RDS for PostgreSQL database. The company notices an increase in application errors that result from database connection timeouts during times of peak traffic or unpredictable traffic. The company needs a solution that reduces the application failures with the least amount of change to the code.

What should a solutions architect do to meet these requirements?

A. Reduce the Lambda concurrency rate.
B. Enable RDS Proxy on the RDS DB instance.
C. Resize the RDS DB instance class to accept more connections.
D. Migrate the database to Amazon DynamoDB with on-demand scaling.

Answer: B
Explanation:
https://aws.amazon.com/rds/proxy/

QUESTION 442
A company is migrating an old application to AWS. The application runs a batch job every hour and is CPU intensive. The batch job takes 15 minutes on average with an on-premises server. The server has 64 virtual CPU (vCPU) and 512 GiB of memory.

Which solution will run the batch job within 15 minutes with the LEAST operational overhead?

A. Use AWS Lambda with functional scaling.
B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.
C. Use Amazon Lightsail with AWS Auto Scaling.
D. Use AWS Batch on Amazon EC2.

Answer: D
Explanation:
AWS Batch is a fully-managed service that can launch and manage the compute resources needed to execute batch jobs. It can scale the compute environment based on the size and timing of the batch jobs.

QUESTION 443
A company stores its data objects in Amazon S3 Standard storage. A solutions architect has found that 75% of the data is rarely accessed after 30 days. The company needs all the data to remain immediately accessible with the same high availability and resiliency, but the company wants to minimize storage costs.

Which storage solution will meet these requirements?

A. Move the data objects to S3 Glacier Deep Archive after 30 days.
B. Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
C. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
D. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately.

Answer: B

Explanation:
Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days - will meet the requirements of keeping the data immediately accessible with high availability and resiliency, while minimizing storage costs. S3 Standard-IA is designed for infrequently accessed data, and it provides a lower storage cost than S3 Standard, while still offering the same low latency, high throughput, and high durability as S3 Standard.

QUESTION 444
A company has a three-tier application 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. The application tier makes calls to a database.

What should a solutions architect do to improve the security of the data in transit?

A. Configure a TLS listener. Deploy the server certificate on the NLB.
B. Configure AWS Shield Advanced. Enable AWS WAF on the NLB.
C. Change the load balancer to an Application Load Balancer (ALB). Enable AWS WAF on the ALB.
D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances by using AWS Key Management Service (AWS KMS).

Answer: A
Explanation:
Network Load Balancers now support TLS protocol. With this launch, you can now offload resource intensive decryption/encryption from your application servers to a high throughput, and low latency Network Load Balancer. Network Load Balancer is now able to terminate TLS traffic and set up connections with your targets either over TCP or TLS protocol.
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html
https://exampleloadbalancer.com/nlbtls_demo.html

QUESTION 445
A social media company runs its application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. The application has more than a billion images stored in an Amazon S3 bucket and processes thousands of images each second. The company wants to resize the images dynamically and serve appropriate formats to clients.

Which solution will meet these requirements with the LEAST operational overhead?

A. Install an external image management library on an EC2 instance. Use the image management library to process the images.
B. Create a CloudFront origin request policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.
C. Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.
D. Create a CloudFront response headers policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

Answer: C
Explanation:
https://aws.amazon.com/cn/blogs/networking-and-content-delivery/resizing-images-with-amazon-cloudfront-lambdaedge-aws-cdn-blog/

QUESTION 446
A hospital needs to store patient records in an Amazon S3 bucket. The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest. The compliance team must administer the encryption key for data at rest.

Which solution will meet these requirements?

A. Create a public SSL/TLS certificate in AWS Certificate Manager (ACM). Associate the certificate with Amazon S3. Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
B. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with S3 managed encryption keys (SSE-S3). Assign the compliance team to manage the SSE-S3 keys.
C. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
D. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Use Amazon Macie to protect the sensitive data that is stored in Amazon S3. Assign the compliance team to manage Macie.

Answer: C
Explanation:
It allows the compliance team to manage the KMS keys used for server-side encryption, thereby providing the necessary control over the encryption keys. Additionally, the use of the "aws:SecureTransport" condition on the bucket policy ensures that all connections to the S3 bucket are encrypted in transit.

QUESTION 447
A data analytics company wants to migrate its batch processing system to AWS. The company receives thousands of small data files periodically during the day through FTP. A on-premises batch job processes the data files overnight. However, the batch job takes hours to finish running. The company wants the AWS solution to process incoming data files are possible with minimal changes to the FTP clients that send the files. The solution must delete the incoming data files the files have been processed successfully. Processing for each file needs to take 3-8 minutes. Which solution will meet these requirements in the MOST operationally efficient way?

A. Use an Amazon EC2 instance that runs an FTP server to store incoming files as objects in Amazon S3 Glacier Flexible Retrieval. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the objects nightly from S3 Glacier Flexible Retrieval. Delete the objects after the job has processed the objects.
B. Use an Amazon EC2 instance that runs an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the process the files nightly from the EBS volume. Delete the files after the job has processed the files.
C. Use AWS Transfer Family to create an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use an Amazon S3 event notification when each files arrives to invoke the job in AWS Batch. Delete the files after the job has processed the files.
D. Use AWS Transfer Family to create an FTP server to store incoming files in Amazon S3 Standard. Create an AWS Lambda function to process the files and delete the files after they are processed.use an S3 event notification to invoke the lambda function when the files arrive.

Answer: C

QUESTION 448
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. The company must not make any changes to the application.

What should a solutions architect do to meet these requirements?

A. Create an Amazon S3 Standard bucket with access to the web servers.
B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.
D. Configure a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume to all web servers.

Answer: C

QUESTION 449
A company wants to migrate a Windows-based application from on premises to the AWS Cloud. The application has three tiers, a business tier, and a database tier with Microsoft SQL Server. The company wants to use specific features of SQL Server such as native backups and Data Quality Services. The company also needs to share files for process between the tiers.

How should a solution architect design the architecture to meet these requirements?

A. Host all three on Amazon instances. Use Mmazon FSx File Gateway for file sharing between tiers.
B. Host all three on Amazon EC2 instances. Use Amazon FSx for Windows file sharing between the tiers.
C. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use Amazon Elastic File system (Amazon EFS) for file sharing between the tiers.
D. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume for file sharing between the tiers.

Answer: B
Explanation:
Data Quality Services: If this feature is critical to your workload, consider choosing Amazon RDS Custom or Amazon EC2.
https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-sql-server/comparison.html

QUESTION 450
A company uses Amazon EC2 instances and AWS Lambda functions to run its application. The company has VPCs with public subnets and private subnets in its AWS account. The EC2 instances run in a private subnet in one of the VPCs. The Lambda functions need direct network access to the EC2 instances for the application to work.

The application will run for at least 1 year. The company expects the number of Lambda functions that the application uses to increase during that time. The company wants to maximize its savings on all application resources and to keep network latency between the services low.

Which solution will meet these requirements?

A. Purchase on an EC2 instance Savings Plan. Optimize the Lambda functions duration and memory usage and the number of invocations. Connect the Lambda functions to the private subnet that contains the EC2 instances.
B. Purchase on an EC2 instance Savings Plan. Optimize the Lambda functions duration and memory usage and the number of invocation, and the amount of data that is transfered. Connect the Lambda functions to a public subnet in the same VPC where the EC2 instances run.
C. Purchase a Compute Savings Plan. Optimize the Lambda functions duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda function to the Private subnet that contains the EC2 instances.
D. Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Keep the Lambda functions in the Lambda service VPC.

Answer: C
Explanation:
By purchasing a Compute Savings Plan, the company can save on the costs of running both EC2 instances and Lambda functions. The Lambda functions can be connected to the private subnet that contains the EC2 instances through a VPC endpoint for AWS services or a VPC peering connection. This provides direct network access to the EC2 instances while keeping the traffic within the private network, which helps to minimize network latency.

Optimizing the Lambda functions' duration, memory usage, number of invocations, and amount of data transferred can help to further minimize costs and improve performance. Additionally, using a private subnet helps to ensure that the EC2 instances are not directly accessible from the public internet, which is a security best practice.

QUESTION 451
A company is building a mobile app on AWS. The company wants to expand its reach to millions of users. The company needs to build a platform so that authorized users can watch the company's content on their mobile devices.

What should a solutions architect recommend to meet these requirements?

A. Publish content to a public Amazon S3 bucket. Use AWS Key Management Service (AWS KMS) keys to stream content.
B. Set up IPsec VPN between the mobile app and the AWS environment to stream content.
C. Use Amazon CloudFront Provide signed URLs to stream content.
D. Set up AWS Client VPN between the mobile app and the AWS environment to stream content.

Answer: C
Explanation:
Amazon CloudFront is a content delivery network (CDN) that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. CloudFront supports signed URLs that provide authorized access to your content. This feature allows the company to control who can access their content and for how long, providing a secure and scalable solution for millions of users.
https://www.amazonaws.cn/en/cloudfront/

QUESTION 452

A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.

The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products.

What should a solutions architect recommend to ensure that all the requests are processed successfully?

A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.
B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.
C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.
D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SOS) queue to receive requests from the website for later processing by the EC2 instances.

Answer: D
Explanation:
Static content can include images and style sheets that are the same across all users and are best cached at the edges of the content distribution network (CDN). Dynamic content includes information that changes frequently or is personalized based on user preferences, behavior, location or other factors - all content is sales requests.

QUESTION 453
A company's web application consists of an Amazon API Gateway API in front of an AWS Lambda function and an Amazon DynamoDB database. The Lambda function handles the business logic, and the DynamoDB table hosts the data. The application uses Amazon Cognito user pools to identify the individual users of the application. A solutions architect needs to update the application so that only users who have a subscription can access premium content.

Which solution will meet this requirement with the LEAST operational overhead?

A. Enable API caching and throttling on the API Gateway API.
B. Set up AWS WAF on the API Gateway API Create a rule to filter users who have a subscription.
C. Apply fine-grained IAM permissions to the premium content in the DynamoDB table.
D. Implement API usage plans and API keys to limit the access of users who do not have a subscription.

Answer: D
Explanation:
To meet the requirement with the least operational overhead, you can implement API usage plans and API keys to limit the access of users who do not have a subscription. This way, you can control access to your API Gateway APIs by requiring clients to submit valid API keys with requests. You can associate usage plans with API keys to configure throttling and quota limits on individual client accounts.
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html

QUESTION 454
A company's application runs on AWS. The application stores large documents in an Amazon S3 bucket that uses the S3 Standard-infrequent Access (S3 Standerd-IA) storage class. The company will continue paying to store the data but wants to save on its total S3 costs. The company wants authorized external users to have the ability to access the documents in milliseconds.

Which solution will meet these requirements MOST cost-effectively?

A. Configure the S3 bucket to be a Requester Pays bucket.
B. Change the storage tier to S3 Standard for all existing and future objects.
C. Turn on S3 Transfer Acceleration tor the S3 Docket.
D. Use Amazon CloudFront to handle all the requests to the S3 bucket.

Answer: D

QUESTION 455
A company recently created a disaster recovery site in a different AWS Region. The company needs to transfer large amounts of data back and forth between NFS file systems in the two Regions on a periodic basis.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS DataSync.
B. Use AWS Snowball devices
C. Set up an SFTP server on Amazon EC2
D. Use AWS Database Migration Service (AWS DMS)

Answer: A
Explanation:
AWS DataSync is a fully managed data transfer service that simplifies moving large amounts of data between on-premises storage systems and AWS services. It can also transfer data between different AWS services, including different AWS Regions. DataSync provides a simple, scalable, and automated solution to transfer data, and it minimizes the operational overhead because it is fully managed by AWS.

QUESTION 456
A company has an On-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.

Which solution meets these requirements?

A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software application on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.

D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage software application on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

Answer: D
Explanation:
https://docs.aws.amazon.com/storagegateway/latest/vgw/WhatIsStorageGateway.html

QUESTION 457
A company runs an application on Amazon EC2 instances. The company needs to implement a disaster recovery (DR) solution for the application. The DR solution needs to have a recovery time objective (RTO) of less than 4 hours. The DR solution also needs to use the fewest possible AWS resources during normal operations.

Which solution will meet these requirements in the MOST operationally efficient way?

A. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS Lambda and custom scripts.
B. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation.
C. Launch EC2 instances in a secondary AWS Region. Keep the EC2 instances in the secondary Region active at all times.
D. Launch EC2 instances in a secondary Availability Zone. Keep the EC2 instances in the secondary Availability Zone active at all times.

Answer: B
Explanation:
Option B would be the most operationally efficient solution for implementing a DR solution for the application, meeting the requirement of an RTO of less than 4 hours and using the fewest possible AWS resources during normal operations.
By creating Amazon Machine Images (AMIs) to back up the EC2 instances and copying them to a secondary AWS Region, the company can ensure that they have a reliable backup in the event of a disaster. By using AWS CloudFormation to automate infrastructure deployment in the secondary Region, the company can minimize the amount of time and effort required to set up the DR solution.

QUESTION 458
A company hosts a multiplayer gaming application on AWS. The company wants the application to read data with sub-millisecond latency and run one-time queries on historical data.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon RDS for data that is frequently accessed. Run a periodic custom script to export the data to an Amazon S3 bucket.
B. Store the data directly in an Amazon S3 bucket. Implement an S3 Lifecycle policy to move older data to S3 Glacier Deep Archive for long-term storage. Run one-time queries on the data in Amazon S3 by using Amazon Athena
C. Use Amazon DynamoDB with DynamoDB Accelerator (DAX) for data that is frequently accessed. Export the data to an Amazon S3 bucket by using DynamoDB table export. Run one-time queries on the data in Amazon S3 by using Amazon Athena.

D. Use Amazon DynamoDB for data that is frequently accessed. Turn on streaming to Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to read the data from Kinesis Data Streams. Store the records in an Amazon S3 bucket.

Answer: C
Explanation:
DynamoDB supports some of the world's largest scale applications by providing consistent, single-digit millisecond response times at any scale. You can build applications with virtually unlimited throughput and storage.
https://aws.amazon.com/dynamodb/dax/?nc1=h_ls

QUESTION 459
A company has a regional subscription-based streaming service that runs in a single AWS Region. The architecture consists of web servers and application servers on Amazon EC2 instances. The EC2 instances are in Auto Scaling groups behind Elastic Load Balancers. The architecture includes an Amazon Aurora database cluster that extends across multiple Availability Zones.

The company wants to expand globally and to ensure that its application has minimal downtime.

A. Extend the Auto Scaling groups for the web tier and the application tier to deploy instances in Availability Zones in a second Region. Use an Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
B. Deploy the web tier and the application tier to a second Region. Add an Aurora PostgreSQL cross-Region Aurara Replica in the second Region. Use Amazon Route 53 health checks with a failovers routing policy to the second Region, Promote the secondary to primary as needed.
C. Deploy the web tier and the applicatin tier to a second Region. Create an Aurora PostSQL database in the second Region. Use AWS Database Migration Service (AWS DMS) to replicate the primary database to the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
D. Deploy the web tier and the application tier to a second Region. Use an Amazon Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.

Answer: A

QUESTION 460
A company wants to configure its Amazon CloudFront distribution to use SSL/TLS certificates. The company does not want to use the default domain name for the distribution. Instead, the company wants to use a different domain name for the distribution.

Which solution will deploy the certificate with icurring any additional costs?

A. Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the us-east-1 Region.
B. Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the us-west-1 Region.
C. Request an Amazon issued public certificate from AWS Certificate Manager (ACU) in the us-east-1 Region.
D. Request an Amazon issued public certificate from AWS Certificate Manager (ACU) in the us-

west-1 Regon.

Answer: B

QUESTION 461
A solutions architect is designing a company’s disaster recovery (DR) architecture. The company has a MySQL database that runs on an Amazon EC2 instance in a private subnet with scheduled backup. The DR design needs to include multiple AWS Regions.

Which solution will meet these requirements with the LEAST operational overhead?

A. Migrate the MySQL database to multiple EC2 instances. Configure a standby EC2 instance in the DR Region Turn on replication.
B. Migrate the MySQL database to Amazon RDS. Use a Multi-AZ deployment. Turn on read replication for the primary DB instance in the different Availability Zones.
C. Migrate the MySQL database to an Amazon Aurora global database. Host the primary DB cluster in the primary Region. Host the secondary DB cluster in the DR Region.
D. Store the schedule backup of the MySQL database in an Amazon S3 bucket that is configured for S3 Cross-Region Replication (CRR). Use the data backup to restore the database in the DR Region.

Answer: C
Explanation:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html

QUESTION 462
A rapidly growing global ecommerce company is hosting its web application on AWS. The web application includes static content and dynamic content. The website stores online transaction processing (OLTP) data in an Amazon RDS database. The website's users are experiencing slow page loads.

Which combination of actions should a solutions architect take to resolve this issue? (Choose two.)

A. Configure an Amazon Redshift cluster.
B. Set up an Amazon CloudFront distribution
C. Host the dynamic web content in Amazon S3
D. Create a read replica for the RDS DB instance.
E. Configure a Multi-AZ deployment for the RDS DB instance

Answer: BD

QUESTION 463
A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods tor IAM 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 IAM 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
Explanation:
To accomplish this, the solutions architect should set an overall password policy for the entire AWS account. This policy will apply to all IAM users in the account, including new users.

QUESTION 464
A company wants to deploy a new public web application on AWS. The application includes a web server tier that uses Amazon EC2 instances. The application also includes a database tier that uses an Amazon RDS for MySQL DB instance.

The application must be secure and accessible for global customers that have dynamic IP addresses.

How should a solutions architect configure the security groups to meet these requirements?

A. Configure the security group tor the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.
B. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance lo allow inbound traffic on port 3306 from the security group of the web servers.
C. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the IP addresses of the customers.
D. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0.0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from 0.0.0.0/0.

Answer: A

QUESTION 465
A company is planning to migrate a commercial off-the-shelf application from is on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year.

Which Amazon EC2 pricing option is the MOST cost-effective?

A. Dedicated Reserved Hosts
B. Dedicated On-Demand Hosts
C. Dedicated Reserved Instances
D. Dedicated On-Demand Instances

Answer: A
Explanation:
Dedicated Host Reservations provide a billing discount compared to running On-Demand Dedicated Hosts. Reservations are available in three payment options.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-hosts-overview.html

QUESTION 466
An ecommerce company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier web application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead.

What should a solutions architect do to meet these requirements?

A. Create a separate application tier using EC2 instances dedicated to email processing.
B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).
C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).
D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

Answer: B
Explanation:
Amazon SES is a cost-effective and scalable email service that enables businesses to send and receive email using their own email addresses and domains. Configuring the web instance to send email through Amazon SES is a simple and effective solution that can reduce the time spent resolving complex email delivery issues and minimize operational overhead.

QUESTION 467
A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.

The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs, security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

A. Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.
B. Add a route in the VPC route table to allow traffic between the web tier’s EC2 instances and the database tier.
C. Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs and configure VPC peering.
D. Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tier's security group.

Answer: D
Explanation:
By default, all inbound traffic to an RDS instance is blocked. Therefore, an inbound rule needs to be added to the security group of the RDS instance to allow traffic from the security group of the web tier's EC2 instances.

QUESTION 468

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 for MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation DB instance with 2,000 GB of storage in a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. The database performance affects the application during periods of high demand.

A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance always degrades when the number of read and write IOPS is higher than 20,000.

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 gp3 volume.
C. Replace the volume with a Provisioned IOPS SSD (Io2) volume.
D. Replace the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes.

Answer: D
Explanation:
To improve the application performance, you can replace the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes. This will increase the number of IOPS available to the database and improve performance.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

QUESTION 469
A company is deploying a new application on Amazon EC2 instances. The application writes data to Amazon Elastic Block Store (Amazon EBS) volumes. The company needs to ensure that all data that is written to the EBS volumes is encrypted at rest.

Which solution will meet this requirement?

A. Create an IAM role that specifies EBS encryption. Attach the role to the EC2 instances.
B. Create the EBS volumes as encrypted volumes. Attach the EBS volumes to the EC2 instances.
C. Create an EC2 instance tag that has a key of Encrypt and a value of True. Tag all instances that require encryption at the ESS level.
D. Create an AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account Ensure that the key policy is active.

Answer: B

QUESTION 470
A company is moving its data management application to AWS. The company wants to transition to an event-driven architecture. The architecture needs to be more distributed and to use serverless concepts while performing the different aspects of the workflow. The company also wants to minimize operational overhead.

Which solution will meet these requirements?

A. Build out the workflow in AWS Glue. Use AWS Glue to invoke AWS Lambda functions to process the workflow slaps.
B. Build out the workflow in AWS Step Functions. Deploy the application on Amazon EC2 Instances. Use Step Functions to invoke the workflow steps on the EC2 instances.

C. Build out the workflow in Amazon EventBridge. Use EventBridge to invoke AWS Lambda functions on a schedule to process the workflow steps.
D. Build out the workflow in AWS Step Functions. Use Step Functions to create a state machine. Use the state machine to invoke AWS Lambda functions to process the workflow steps.

Answer: D
Explanation:
Step 3: Create a State Machine
Use the Step Functions console to create a state machine that invokes the Lambda function that you created earlier in Step 1.
https://docs.aws.amazon.com/step-functions/latest/dg/tutorial-creating-lambda-state-machine.html
In Step Functions, a workflow is called a state machine, which is a series of event-driven steps. Each step in a workflow is called a state.

QUESTION 471
An image-hosting company stores its objects in Amazon S3 buckets. The company wants to avoid accidental exposure of the objects in the S3 buckets to the public. All S3 objects in the entire AWS account need to remain private.

Which solution will meal these requirements?

A. Use Amazon GuardDuty to monitor S3 bucket policies. Create an automatic remediation action rule that uses an AWS Lambda function to remediate any change that makes the objects public.
B. Use AWS Trusted Advisor to find publicly accessible S3 Dockets. Configure email notifications In Trusted Advisor when a change is detected manually change the S3 bucket policy if it allows public access.
C. Use AWS Resource Access Manager to find publicly accessible S3 buckets. Use Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function when a change it detected. Deploy a Lambda function that programmatically remediates the change.
D. Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting. Apply tie SCP to tie account.

Answer: D

QUESTION 472
A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.
A solutions architect must design a solution to protect the application from this type of attack.

Which solution meats these requirements with the LEAST operational overhead?

A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.
B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.
C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached.
D. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway

Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

Answer: B
Explanation:
A rate-based rule in AWS WAF allows the security team to configure thresholds that trigger rate-based rules, which enable AWS WAF to track the rate of requests for a specified time period and then block them automatically when the threshold is exceeded. This provides the ability to prevent HTTP flood attacks with minimal operational overhead.
https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html

QUESTION 473
A payment processing company records all voice communication with its customers and stores the audio files in an Amazon S3 bucket. The company needs to capture the text from the audio files. The company must remove from the text any personally identifiable information (Pll) that belongs to customers.

What should a solutions architect do to meet these requirements?

A. Process the audio files by using Amazon Kinesis Video Streams. Use an AWS Lambda function to scan for known Pll patterns.
B. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start an Amazon Textract task to analyze the call recordings.
C. Configure an Amazon Transcribe transcription job with Pll redaction turned on. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start the transcription job. Store the output in a separate S3 bucket.
D. Create an Amazon Connect contact flow that ingests the audio files with transcription turned on. Embed an AWS Lambda function to scan for known Pll patterns. Use Amazon EventBridge (Amazon CloudWatch Events) to start the contact flow when an audio file is uploaded to the S3 bucket.

Answer: C

QUESTION 474
A company is migrating its on-premises workload to the AWS Cloud. The company already uses several Amazon EC2 instances and Amazon RDS DB instances. The company wants a solution that automatically starts and stops the EC2 instances and D6 instances outside of business hours. The solution must minimize cost and infrastructure maintenance.

Which solution will meet these requirement?

A. Scale the EC2 instances by using elastic resize Scale the DB instances to zero outside of business hours.
B. Explore AWS Marketplace for partner solutions that will automatically start and stop the EC2 Instances and OB instances on a schedule.
C. Launch another EC2 instance. Configure a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule.
D. Create an AWS Lambda function that will start and stop the EC2 instances and DB instances. Configure Amazon EventBridge to invoke the Lambda function on a schedule.

Answer: D
Explanation:

The most efficient solution for automatically starting and stopping EC2 instances and DB instances on a schedule while minimizing cost and infrastructure maintenance is to create an AWS Lambda function and configure Amazon EventBridge to invoke the function on a schedule.

QUESTION 475
A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). All ecommerce data is stored in an Amazon RDS for ManaDB Multi-AZ DB instance. The company wants to optimize customer session management during transactions. The application must store session data durably.

Which solutions will meet these requirements? (Choose two.)

A. Turn on the sticky sessions feature (session affinity) on the ALB
B. Use an Amazon DynamoDB table to store customer session information
C. Deploy an Amazon Cognito user pool to manage user session information
D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information
E. Use AWS Systems Manager Application Manager in the application to manage user session information

Answer: AD
Explanation:
https://aws.amazon.com/caching/session-management/

QUESTION 476
An ecommerce company needs to run a scheduled daily job to aggregate and filter sales records for analytics. The company stores the sales records in an Amazon S3 bucket. Each object can be up to 10 GB in size. Based on the number of sales events, the job can take up to an hour to complete. The CPU and memory usage of the job are constant and are known in advance.

A solutions architect needs to minimize the amount of operational effort that is needed for the job to run.

Which solution meets these requirements?

A. Create an AWS Lambda function that has an Amazon EventBridge notification. Schedule the EventBridge event to run once a day.
B. Create an AWS Lambda function. Create an Amazon API Gateway HTTP API, and integrate the API with the function. Create an Amazon EventBridge scheduled avert that calls the API and invokes the function.
C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.
D. Create an Amazon Elastic Container Service (Amazon ECS) duster with an Amazon EC2 launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge scheduled event that launches an ECS task on the duster to run the job.

Answer: C

QUESTION 477
A solutions 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 solutions architect has proposed migrating the MS web servers to Amazon EC2 instances in multiple Availability Zones that are connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances.
Which replacement to the on-premises file share is MOST resilient and durable?

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

Answer: C
Explanation:
Amazon FSx makes it easy and cost effective to launch, run, and scale feature-rich, high-performance file systems in the cloud.

QUESTION 478
A company wants to restrict access to the content of one of its man web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture end an authentication solution for fewer tian 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as to company's user base grows while providing lowest login latency possible.

A. Use Amazon Cognito tor authentication. Use Lambda#Edge tor authorization. Use Amazon CloudFront 10 serve the web application globally.
B. Use AWS Directory Service for Microsoft Active Directory tor authentication. Use AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.
C. Usa Amazon Cognito for authentication. Use AWS Lambda tor authorization. Use Amazon S3 Transfer Acceleration 10 serve the web application globally.
D. Use AWS Directory Service for Microsoft Active Directory for authentication. Use Lambda@Edge for authorization. Use AWS Elastic Beanstalk to serve the web application.

Answer: A

QUESTION 479
An ecommerce company is building a distributed application that involves several serverless functions and AWS services to complete order-processing tasks. These tasks require manual approvals as part of the workflow. A solutions architect needs to design an architecture for the order-processing application. The solution must be able to combine multiple AWS Lambda functions into responsive serverless applications. The solution also must orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Step Functions to build the application.
B. Integrate all the application components in an AWS Glue job
C. Use Amazon Simple Queue Service (Amazon SQS) to build the application
D. Use AWS Lambda functions and Amazon EventBridge (Amazon CloudWatch Events) events to build the application

Answer: A

Explanation:
AWS Step Functions is a fully managed service that makes it easy to build applications by coordinating the components of distributed applications and microservices using visual workflows. With Step Functions, you can combine multiple AWS Lambda functions into responsive serverless applications and orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers. Step Functions also allows for manual approvals as part of the workflow. This solution meets all the requirements with the least operational overhead.

QUESTION 480
A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States. Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.

What should a solutions architect do to meet these requirements?

A. A Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs. and use it as an origin for an Amazon CloudFront distribution Provide access to the application by using a CNAME that points to the CloudFront DNS.
D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53 create a latency-based record that points to the three ALBs and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.v

Answer: A
Explanation:
Q: How is AWS Global Accelerator different from Amazon CloudFront?
A: AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

QUESTION 481
A company runs an application on Amazon EC2 Linux instances across multiple Availability Zones. The application needs a storage layer that is highly available and Portable Operating System Interface (POSIX)-compliant. The storage layer must provide maximum data durability and must be shareable across the EC2 instances. The data in the storage layer will be accessed frequently for the first 30 days and will be accessed infrequently after that time.

Which solution will meet these requirements MOST cost-effectively?

A. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Glacier.
B. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Standard-Infrequent Access (EF3 Standard-IA).
C. Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a Lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access (EFS Standard-IA).
D. Use the Amazon Elastic File System (Amazon EFS) One Zone storage class. Create a Lifecycle management policy to move infrequently accessed data to EFS One Zone-Infrequent Access (EFS One Zone-IA).

Answer: C
Explanation:
https://aws.amazon.com/efs/features/infrequent-access/

QUESTION 482
A company wants to migrate its 1 PB on-premises image repository to AWS. The images will be used by a serverless web application. Images stored in the repository are rarely accessed, but they must be immediately available Additionally, the images must be encrypted at rest and protected from accidental deletion.

Which solution meets these requirements?

A. Implement client-side encryption and store the images in an Amazon S3 Glacier vault. Set a vault lock to prevent accidental deletion.
B. Store the images in an Amazon S3 bucket in the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Enable versioning default encryption and MFA Delete on the S3 bucket.
C. Store the images in an Amazon FSx for Windows File Server file share. Configure the Amazon FSx file share to use an AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the images in the file share. Use NTFS permission sets on the images to prevent accidental deletion.
D. Store the images in an Amazon Elastic File System (Amazon EFS) file share in the Infrequent Access storage class. Configure the EFS file share to use an AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the images in the file share. Use NFS permission sets on the images to prevent accidental deletion.

Answer: B

QUESTION 483
A company runs an application that receives data from thousands of geographically dispersed remote devices that use UDP. The application processes the data immediately and sends a message back to the device if necessary. No data is stored.

The company needs a solution that minimizes latency for the data transmission from the devices. The solution also must provide rapid failover to another AWS Region.

Which solution will meet these requirements?

A. Configure an Amazon Route 53 failover routing policy. Create a Network Load Balancer (NLB) in each of the two Regions. Configure the NLB to invoke an AWS Lambda function to process the data.

B. Use AWS Global Accelerator. Create a Network Load Balancer (NLB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the NLProcess the data in Amazon ECS.
C. Use AWS Global Accelerator Create an Application Load Balancer (ALB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB Process the data in Amazon ECS.
D. Configure an Amazon Route 53 failover routing policy. Create an Application Load Balancer (ALB) in each of the two Regions. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB Process the data in Amazon ECS.

Answer: B
Explanation:
Geographically dispersed (related to UDP) - Global Accelerator - multiple entrances worldwide to the AWS network to provide better transfer rates.
UDP - NLB (Network Load Balancer).

QUESTION 484
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 ElasticCache to cache the large database.
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
Explanation:
Key term is identical datasets from the database it means caching can solve this issue by cached in frequently used dataset from DB.

QUESTION 485
A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SOS) and Amazon Simple Notification Service (Amazon SNS) in the architecture. A solutions architect is reviewing the infrastructure design Data must be encrypted at test and in transit. Only authorized personnel of the hospital should be able to access the data.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

A. Turn on server-side encryption on the SQS components. Update tie default key policy to restrict key usage to a set of authorized principals.
B. Turn on server-side encryption on the SNS components by using an AWS Key Management

Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals.

C. Turn on encryption on the SNS components. Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic pokey to allow only encrypted connections over TLS.

D. Turn on server-side encryption on the SOS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key pokey to restrict key usage to a set of authorized principals. Set a condition in the queue pokey to allow only encrypted connections over TLS.

E. Turn on server-side encryption on the SOS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM pokey to restrict key usage to a set of authorized principals. Set a condition in the queue pokey to allow only encrypted connections over TLS.

Answer: BD
Explanation:
For a customer managed KMS key, you must configure the key policy to add permissions for each queue producer and consumer.
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-key-management.html

QUESTION 486
A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers 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 solutions architect use to meet these requirements?

A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and 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 for the MySQL servers and allow port 3306 from the web servers security group.

D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

Answer: C
Explanation:
Load balancer is public facing accepting all traffic coming towards the VPC (0.0.0.0/0). The web server needs to trust traffic originating from the ALB. The DB will only trust traffic originating from the Web server on port 3306 for Mysql.

QUESTION 487
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: C

QUESTION 488
A solutions architect is designing a two-tiered architecture that includes a public subnet and a database subnet. The web servers in the public subnet must be open to the internet on port 443. The Amazon RDS for MySQL DB instance in the database subnet must be accessible only to the web servers on port 3306.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

A. Create a network ACL for the public subnet. Add a rule to deny outbound traffic to 0.0.0.0/0 on port.
B. Create a security group for the DB instance. Add a rule to allow traffic from the public subnet CIDR block on port 3306.
C. Create a security group for the web servers in the public subnet. Add a rule to allow traffic from 0.0.0.0/0 on port 443.
D. Create a security group for the DB instance. Add a rule to allow traffic from the web servers' security group on port 3306.
E. Create a security group for the DB instance. Add a rule to deny all traffic except traffic from the web servers' security group on port 3306.

Answer: CD

QUESTION 489
A company has an application that collects data from loT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Date Firehose. The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models.

Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.

Which storage solution meets these requirements MOST cost-effectively?

A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.
C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

Answer: D

QUESTION 490

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 run a script remotely on all EC2 instances to send data to the audit system.
B. Use EC2 Auto Scaling lifecycle hooks to run 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 run a custom script through user data to send data to the audit system when instances are launched and terminated.
D. Run a custom script on the instance operating system to send data to the audit system. Configure the script to be invoked by the EC2 Auto Scaling group when the instance starts and is terminated.

Answer: B
Explanation:
Amazon EC2 Auto Scaling offers the ability to add lifecycle hooks to your Auto Scaling groups. These hooks let you create solutions that are aware of events in the Auto Scaling instance lifecycle, and then perform a custom action on instances when the corresponding lifecycle event occurs.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html

QUESTION 491

A company has launched an Amazon RDS for MySQL DB instance. Most of the connections to the database come from serverless applications. Application traffic to the database changes significantly at random intervals. At limes of high demand, users report that their applications experience database connection rejection errors.

Which solution will resolve this issue with the LEAST operational overhead?

A. Create a proxy in RDS Proxy. Configure the users' applications to use the DB instance through RDS Proxy.
B. Deploy Amazon ElastCache for Memcached between the users' application and the DB instance.
C. Migrate the DB instance to a different instance class that has higher I/O capacity. Configure the users' applications to use the new DB instance.
D. Configure Multi-AZ for the DB instance. Configure the users' application to switch between the DB instances.

Answer: A
Explanation:
Many applications, including those built on modern serverless architectures, can have a large number of open connections to the database server and may open and close database connections at a high rate, exhausting database memory and compute resources. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability.
https://aws.amazon.com/pt/rds/proxy/

QUESTION 492
A solutions architect is designing the architecture for a software demonstration environment. The environment will run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The system will experience significant increases in traffic during working hours but Is not required to operate on weekends.

Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Choose two.)

A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate.
B. Use AWS Auto Scaling to scale the capacity of the VPC internet gateway.
C. Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions.
D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization.
E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.

Answer: DE

QUESTION 493
A company has deployed a serverless application that invokes an AWS Lambda function when new documents are uploaded to an Amazon S3 bucket. The application uses the Lambda function to process the documents. After a recent marketing campaign, the company noticed that the application did not process many of the documents.

What should a solutions architect do to improve the architecture of this application?

A. Set the Lambda function's runtime timeout value to 15 minutes.
B. Configure an S3 bucket replication policy. Stage the documents m the S3 bucket for later processing.
C. Deploy an additional Lambda function Load balance the processing of the documents across the two Lambda functions.
D. Create an Amazon Simple Queue Service (Amazon SOS) queue. Send the requests to the queue. Configure the queue as an event source for Lambda.

Answer: D
Explanation:
To improve the architecture of this application, the best solution would be to use Amazon Simple Queue Service (Amazon SQS) to buffer the requests and decouple the S3 bucket from the Lambda function. This will ensure that the documents are not lost and can be processed at a later time if the Lambda function is not available.

This will ensure that the documents are not lost and can be processed at a later time if the Lambda function is not available. By using Amazon SQS, the architecture is decoupled and the Lambda function can process the documents in a scalable and fault-tolerant manner.

QUESTION 494
A developer has an application that uses an AWS Lambda function to upload files to Amazon S3 and needs the required permissions to perform the task. The developer already has an IAM user with valid IAM credentials required for Amazon S3.

What should a solutions architect do to grant the permissions?

A. Add required IAM permissions in the resource policy of the Lambda function.
B. Create a signed request using the existing IAM credentials in the Lambda function
C. Create a new IAM user and use the existing IAM credentials in the Lambda function.
D. Create an IAM execution role with the required permissions and attach the IAM rote to the Lambda function.

Answer: D
Explanation:
To grant the necessary permissions to an AWS Lambda function to upload files to Amazon S3, a solutions architect should create an IAM execution role with the required permissions and attach the IAM role to the Lambda function. This approach follows the principle of least privilege and ensures that the Lambda function can only access the resources it needs to perform its specific task.

QUESTION 495
A company has a large dataset for its online advertising business stored in an Amazon RDS for MySQL DB instance in a single Availability Zone. The company wants business reporting queries to run without impacting the write operations to the production DB instance.

Which solution meets these requirements?

A. Deploy RDS read replicas to process the business reporting queries.
B. Scale out the DB instance horizontally by placing it behind an Elastic Load Balancer.
C. Scale up the DB instance to a larger instance type to handle write operations and queries.
D. Deploy the OB distance in multiple Availability Zones to process the business reporting queries.

Answer: A

QUESTION 496
A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store is data and wants to build a new service that sends an alert to the managers of four Internal teams every time a new weather event is recorded. The company does not want true new service to affect the performance of the current application.

What should a solutions architect do to meet these requirement with the LEAST amount of operational overhead?

A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a mingle Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SOS) queue to which the teams can subscribe.

Answer: C
Explanation:

The best solution to meet these requirements with the least amount of operational overhead is to enable Amazon DynamoDB Streams on the table and use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe. This solution requires minimal configuration and infrastructure setup, and Amazon DynamoDB Streams provide a low-latency way to capture changes to the DynamoDB table. The triggers automatically capture the changes and publish them to the SNS topic, which notifies the internal teams.

QUESTION 497

A company is developing a real-time multiplayer game that uses UDP for communications between the 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 solutions 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 Aurora Global Database for data storage.
D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

Answer: B
Explanation:
A Network Load Balancer can handle UDP traffic, and Amazon DynamoDB on-demand can provide automatic scaling without intervention.

QUESTION 498

A company needs to create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to host a digital media streaming application. The EKS cluster will use a managed node group that is backed by Amazon Elastic Block Store (Amazon EBS) volumes for storage. The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service (AWS KMS).

Which combination of actions will meet this requirement with the LEAST operational overhead? (Choose two.)

A. Use a Kubernetes plugin that uses the customer managed key to perform data encryption.
B. After creation of the EKS cluster, locate the EBS volumes. Enable encryption by using the customer managed key.
C. Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.
D. Create the EKS cluster. Create an IAM role that has a policy that grants permission to the customer managed key. Associate the role with the EKS cluster.
E. Store the customer managed key as a Kubernetes secret in the EKS cluster. Use the customer managed key to encrypt the EBS volumes.

Answer: CD

QUESTION 499

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
Explanation:
Amazon RDS for MySQL is a fully-managed relational database service that makes it easy to set up, operate, and scale MySQL deployments in the cloud. Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora (MySQL-compatible edition), where the database will automatically start up, shut down, and scale capacity up or down based on your application's needs. It is a simple, cost-effective option for infrequent, intermittent, or unpredictable workloads.

QUESTION 500
A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent. Otherwise, the payments might be processed incorrectly.

Which actions should a solutions architect take to meet this requirement? (Choose two.)

A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key
B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.
C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key.
D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue. Set the message attribute to use the payment ID.
E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

Answer: BE

QUESTION 501
An IAM user made several configuration changes to AWS resources in their company's account during a production deployment last week. A solutions architect learned that a couple of security group rules are not configured as desired. The solutions architect wants to confirm which IAM user was responsible for making changes.

Which service should the solutions architect use to find the desired information?

A. Amazon GuardDuty
B. Amazon Inspector
C. AWS CloudTrail
D. AWS Config

Answer: C
Explanation:
The best option is to use AWS CloudTrail to find the desired information. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS account activities. CloudTrail can be used to log all changes made to resources in an AWS account, including changes made by IAM users, EC2 instances, AWS management console, and other AWS services. By using CloudTrail, the solutions architect can identify the IAM user who made the configuration changes to the security group rules.

QUESTION 502
A company runs a public three-Tier web application in a VPC. The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet. The company needs a managed solution that minimizes operational maintenance.

Which solution meets these requirements?

A. Provision a NAT instance in a public subnet. Modify each private subnets route table with a default route that points to the NAT instance.
B. Provision a NAT instance in a private subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
C. Provision a NAT gateway in a public subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.
D. Provision a NAT gateway in a private subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.

Answer: C
Explanation:
As the company needs a managed solution that minimizes operational maintenance - NAT Gateway is a public subnet is the answer.

QUESTION 503
A company needs to transfer 600 TB of data from its on-premises network-attached storage (NAS) system to the AWS Cloud. The data transfer must be complete within 2 weeks. The data is sensitive and must be encrypted in transit. The company's internet connection can support an upload speed of 100 Mbps.

Which solution meets these requirements MOST cost-effectively?

A. Use Amazon S3 multi-part upload functionality to transfer the fees over HTTPS.
B. Create a VPN connection between the on-premises NAS system and the nearest AWS Region. Transfer the data over the VPN connection.
C. Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.
D. Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.

Answer: C
Explanation:
The best option is to use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices and use the devices to transfer the data to Amazon S3. Snowball

Edge is a petabyte-scale data transfer device that can help transfer large amounts of data securely and quickly. Using Snowball Edge can be the most cost-effective solution for transferring large amounts of data over long distances and can help meet the requirement of transferring 600 TB of data within two weeks.

QUESTION 504
A company needs a backup strategy for its three-tier stateless web application. The web application runs on Amazon EC2 instances in an Auto Scaling group with a dynamic scaling policy that is configured to respond to scaling events. The database tier runs on Amazon RDS for PostgreSQL. The web application does not require temporary local storage on the EC2 instances. The company's recovery point objective (RPO) is 2 hours.

The backup strategy must maximize scalability and optimize resource utilization for this environment.

Which solution will meet these requirements?

A. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances and database every 2 hours to meet the RPO.
B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS to meet the RPO.
C. Retain the latest Amazon Machine Images (AMIs) of the web and application tiers. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.
D. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances every 2 hours. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.

Answer: C
Explanation:
The web application does not require temporary local storage on the EC2 instances => No EBS snapshot is required, retaining the latest AMI is enough.

QUESTION 505
A company needs to ingest and handle large amounts of streaming data that its application generates. The application runs on Amazon EC2 instances and sends data to Amazon Kinesis Data Streams, which is configured with default settings. Every other day, the application consumes the data and writes the data to an Amazon S3 bucket for business intelligence (BI) processing. The company observes that Amazon S3 is not receiving all the data that the application sends to Kinesis Data Streams.

What should a solutions architect do to resolve this issue?

A. Update the Kinesis Data Streams default settings by modifying the data retention period.
B. Update the application to use the Kinesis Producer Library (KPL) lo send the data to Kinesis Data Streams.
C. Update the number of Kinesis shards lo handle the throughput of me data that is sent to Kinesis Data Streams.
D. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.

Answer: A
Explanation:
https://docs.aws.amazon.com/streams/latest/dev/kinesis-extended-retention.html

The question mentioned Kinesis data stream default settings and "every other day". After 24hrs, the data isn't in the Data stream if the default settings is not modified to store data more than 24hrs.

QUESTION 506
A company has migrated an application to Amazon EC2 Linux instances. One of these EC2 instances runs several 1-hour tasks on a schedule. These tasks were written by different teams and have no common programming language. The company is concerned about performance and scalability while these tasks run on a single instance. A solutions architect needs to implement a solution to resolve these concerns.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Batch to run the tasks as jobs. Schedule the jobs by using Amazon EventBridge (Amazon CloudWatch Events).
B. Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs.
C. Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events).
D. Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create an Auto Scaling group with the AMI to run multiple copies of the instance.

Answer: A
Explanation:
Lambda functions are short lived; the Lambda max timeout is 900 seconds (15 minutes). This can be difficult to manage and can cause issues in production applications. We'll take a look at AWS Lambda timeout limits, timeout errors, monitoring timeout errors, and how to apply best practices to handle them effectively.

QUESTION 507
A company wants to migrate an Oracle database to AWS. The database consists of a single table that contains millions of geographic information systems (GIS) images that are high resolution and are identified by a geographic code. When a natural disaster occurs tens of thousands of images get updated every few minutes. Each geographic code has a single image or row that is associated with it. The company wants a solution that is highly available and scalable during such events.

Which solution meets these requirements MOST cost-effectively?

A. Store the images and geographic codes in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.
B. Store the images in Amazon S3 buckets. Use Amazon DynamoDB with the geographic code as the key and the image S3 URL as the value.
C. Store the images and geographic codes in an Amazon DynamoDB table. Configure DynamoDB Accelerator (DAX) during times of high load.
D. Store the images in Amazon S3 buckets Store geographic codes and image S3 URLs in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.

Answer: B

QUESTION 508

A company has implemented a self-managed DNS service on AWS. The solution consists of the following:

```
- Amazon EC2 instances in different AWS Regions
- Endpoints of a standard accelerator in AWS Global Accelerator
```

The company wants to protect the solution against DDoS attacks.

What should a solutions architect do to meet this requirement?

A. Subscribe to AWS Shield Advanced. Add the accelerator as a resource to protect.
B. Subscribe to AWS Shield Advanced. Add the EC2 instances as resources to protect.
C. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the accelerator.
D. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the EC2 instances.

Answer: A
Explanation:
AWS Shield is a managed service that provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service. AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53.

QUESTION 509
A gaming company is moving its public scoreboard from a data center to the AWS Cloud. The company uses Amazon EC2 Windows Server instances behind an Application Load Balancer to host its dynamic application. The company needs a highly available storage solution for the application. The application consists of static files and dynamic server-side code.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge.
B. Store the static files on Amazon S3. Use Amazon ElastiCache to cache objects at the edge.
C. Store the server-side code on Amazon Elastic File System (Amazon EFS). Mount the EFS volume on each EC2 instance to share the files.
D. Store the server-side code on Amazon FSx for Windows File Server. Mount the FSx for Windows File Server volume on each EC2 instance to share the files.
E. Store the server-side code on a General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on each EC2 instance to share the files.

Answer: AD
Explanation:
https://www.techtarget.com/searchaws/tip/Amazon-FSx-vs-EFS-Compare-the-AWS-file-services
FSx is built for high performance and submillisecond latency using solid-state drive storage volumes. This design enables users to select storage capacity and latency independently. Thus, even a subterabyte file system can have 256 Mbps or higher throughput and support volumes up to 64 TB.

QUESTION 510
A company is migrating an old application to AWS. The application runs a batch job every hour and is CPU intensive. The batch job takes 15 minutes on average with an on-premises server. The server has 64 virtual CPU (vCPU) and 512 GiB of memory.

Which solution will run the batch job within 15 minutes with the LEAST operational overhead?

A. Use AWS Lambda with functional scaling
B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate
C. Use Amazon Lightsail with AWS Auto Scaling
D. Use AWS Batch on Amazon EC2

Answer: D
Explanation:
Use AWS Batch on Amazon EC2. AWS Batch is a fully managed batch processing service that can be used to easily run batch jobs on Amazon EC2 instances. It can scale the number of instances to match the workload, allowing the batch job to be completed in the desired time frame with minimal operational overhead.

QUESTION 511
A company hosts a frontend application that uses an Amazon API Gateway API backend that is integrated with AWS Lambda. When the API receives requests, the Lambda function loads many libraries. Then the Lambda function connects to an Amazon RDS database, processes the data, and returns the data to the frontend application. The company wants to ensure that response latency is as low as possible for all its users with the fewest number of changes to the company's operations.

Which solution will meet these requirements?

A. Establish a connection between the frontend application and the database to make queries faster by bypassing the API.
B. Configure provisioned concurrency for the Lambda function that handles the requests.
C. Cache the results of the queries in Amazon S3 for faster retrieval of similar datasets.
D. Increase the size of the database to increase the number of connections Lambda can establish at one time.

Answer: B
Explanation:
Configure provisioned concurrency for the Lambda function that handles the requests. Provisioned concurrency allows you to set the amount of compute resources that are available to the Lambda function, so that it can handle more requests at once and reduce latency. Caching the results of the queries in Amazon S3 could also help to reduce latency, but it would not be as effective as setting up provisioned concurrency. Increasing the size of the database would not help to reduce latency, as this would not increase the number of connections the Lambda function could establish, and establishing a direct connection between the frontend application and the database would bypass the API, which would not be the best solution either.

QUESTION 512
A company is building a game system that needs to send unique events to separate leaderboard, matchmaking, and authentication services concurrently. The company needs an AWS event-driven system that guarantees the order of the events.

Which solution will meet these requirements?

A. Amazon EventBridge event bus
B. Amazon Simple Notification Service (Amazon SNS) FIFO topics
C. Amazon Simple Notification Service (Amazon SNS) standard topics
D. Amazon Simple Queue Service (Amazon SQS) FIFO queues

Answer: B

QUESTION 513
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
Explanation:
Key term is identical datasets from the database it means caching can solve this issue by cached in frequently used dataset from DB.

QUESTION 514
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? (Choose two.)

A. Have the deployment engineer use AWS account root 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 AdministratorAccess 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 that IAM role.

Answer: DE

QUESTION 515
A company is implementing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use Lustre clients to access data. The solution

must be fully managed.

Which solution meets these requirements?

A. Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.
B. Create an AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
C. Create an Amazon Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Answer: D

QUESTION 516
A company has a business system that generates hundreds of reports each day. The business system saves the reports to a network share in CSV format. The company needs to store this data in the AWS Cloud in near-real time for analysis.

Which solution will meet these requirements with the LEAST administrative overhead?

A. Use AWS DataSync to transfer the files to Amazon S3. Create a scheduled task that runs at the end of each day.
B. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.
C. Use AWS DataSync to transfer the files to Amazon S3. Create an application that uses the DataSync API in the automation workflow.
D. Deploy an AWS Transfer for SFTP endpoint. Create a script that checks for new files on the network share and uploads the new files by using SFTP.

Answer: B
Explanation:
https://aws.amazon.com/storagegateway/file/?nc1=h_ls

QUESTION 517
A company is storing petabytes of data in Amazon S3 Standard. The data is stored in multiple S3 buckets and is accessed with varying frequency. The company does not know access patterns for all the data. The company needs to implement a solution for each S3 bucket to optimize the cost of S3 usage.

Which solution will meet these requirements with the MOST operational efficiency?

A. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.
B. Use the S3 storage class analysis tool to determine the correct tier for each object in the S3 bucket. Move each object to the identified storage tier.
C. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Glacier Instant Retrieval.
D. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: A
Explanation:
https://aws.amazon.com/s3/storage-classes/intelligent-tiering/

QUESTION 518
A solutions architect needs to allow team members to access Amazon S3 buckets in two different AWS accounts: a development account and a production account. The team currently has access to S3 buckets in the development account by using unique IAM users that are assigned to an IAM group that has appropriate permissions in the account.

The solutions architect has created an IAM role in the production account. The role has a policy that grants access to an S3 bucket in the production account.

Which solution will meet these requirements while complying with the principle of least privilege?

A. Attach the Administrator Access policy to the development account users.
B. Add the development account as a principal in the trust policy of the role in the production account.
C. Turn off the S3 Block Public Access feature on the S3 bucket in the production account.
D. Create a user in the production account with unique credentials for each team member.

Answer: B
Explanation:
By adding the development account as a principal in the trust policy of the IAM role in the production account, you are allowing users from the development account to assume the role in the production account. This allows the team members to access the S3 bucket in the production account without granting them unnecessary privileges.

About Lead2pass.com