Q1 A company runs a legacy system on a single m4.2xlarge Amazon EC2 instance with Amazon EBS storage. The EC2 instance runs both the web server and a self-managed Oracle database. A snapshot is made of the EBS volume every 12 hours, and an AMI was created from the fully configured EC2 instance. A recent event that terminated the EC2 instance led to several hours of down time. The application was successfully launched from the AMI, but the age of the EBS snapshot and the repair of the database resulted in the loss of f 8 hours of data. The system was also dot vn for 4 hours while the Systems Operators manually performed these processes. What architectural changes will minimize downtime and reduce the chance of lost data?

B. Run the application on m4.xlarge EC2 instances behind an Elastic Load Balancer Application Load Balancer. Run the EC2 instances in an Auto Scaling group across multiple 4 Availability Zones with a minimum instance count of two. Migrate the database to an Amazon RDS Oracle Multi- AZ DB instance.

run app on m4.xLarge EC2

Q2 A Solutions Architect is working with a company that operates a standard three-tier web application in AWS. The web and application tiers run on Amazon EC2 and the database tier runs or rAmazon RDS. The company is redesigning the web and application tiers to use Amazon 1.API Gateway and AWS Lambda, and the company intends to deploy the new application within 6 months. The IT Manager has asked the Solution 1s Architect to reduce costs in the interim. Which solution will be MOST cost effective while maintaining reliability?

B. Use On-Demand Instances for the web and application tiers, and Reserved Instances for the database tier.

use on-demand instance

Q3 A company uses Amazon S3 to store documents that may only be accessible to an Amazon EC2 instance in a certain virtual private cloud (PC). Thecompany fears that a malicious insider with access to this instance could also set up an EC2 instance in another VPC to access these documents. Which of the following solutions will provide the required protection?

A. Use an S3VPC endpoint and an S3 bucket policy to limit access to this VPC endpoint.

use S3 VPC endpoint

Q4 The Solutions Architect manages a serverless application that consists of multiple API gateways, AWS Lambda functions, Amazon S3 buckets, and Amazon DynamoDB tables. Customers say that a few application components slow while loading dynamic images, and some are timing out with the "504 Gateway Timeout" error . While troubleshooting the scenario, the Solution 1s Architect confirms that DynamoDB monitoring metrics are at acceptable levels. Which of the following steps would be optimal for debugging these application issues? (Choose two.)

B. Parse Amazon CloudWatch Logs to determine processing times for requested images at specified intervals.

D. Parse AWS X-Ray traces and analyze HTTP methods to determine the root cause of the HTTP errors.

parse Amazon CLoudWatch logs

Parse AWS X-ray traces

Q5 A Solutions Architect is designing the storage layer for a recently purchased application. The application will be running on Amazon EC2 instances and has the following layers and requirements:-Data layer.A POSIX file system shared across many systems. -Service layer:Static file content that requires block storage with more than 100k IOPS. Which combination of AWS services will meet these needs? (Choose two.)

C. Data layer-Amazon EFS wxcclosdpasson

E. Service layer-Amazon EC2 Ephemeral Storage

Data layer-Amazon EFS

Service layer-Amazon EC2 Ephemeral Storage

Q6 A company has an application that runs a web service on Amazon EC2 instances and stores jpg images in Amazon S3 The web traffic has a predictable baseline, but often demand spikes unpredictably for short periods of time. The application is loosely coupled and stateless. The jpg images stored in Amazon S3 are accessed frequently for the first 15 to 20 days, they are seldor n accessed thereafter but always need to be : immediately available. The CIO has asked to find ways to reduce costs. Which of the following options will reduce costs? (Choose two.)

A.Purchase Reserved instances for baseline capacity requirements and use On-Demand instances for the demand spikes.

B. Configure a lifecycle policy to move the jpg images on Amazon S3 to S3 IA after 30 days.

purchase Reserved instance

Configure a lifecycle policy to move .jpg images on S3 to S3 IA after30 day

Q7 A hybrid network architecture must be used during a company's multi-year data center migration from multiple private data centers to AWS. The current data centers are linked together with private fiber. Due to unique legacy applications, NAT cannot be used. During the migration period, many applications will need access to other applications in both the data centers and AWS. Which option offers a hybrid network architecture that is secure and highly available, that allows for high bandwidth and a multi-region deployment post-migration?

A. Use an AWS Direct Connect to ex ach data center from different ISPs, and configure routing to failover to the other data center's Direct Connect if one fails. Ensure that no VPC CIDR blocks overlap one another or the on-premises network.

use AWS Direct Connect to each data center from different ISPS

Q8 A company is currently running a production workload on AWS that is very I'O intensive. Its workload consists of a single tier with 10 c4.8xlarge instances, each with 2 TB gp2 vq lumes. The number of processing jobs has recently increased, and latency has increased as well. The team realizes that they are constrained on the IOPS. For the application to perform efficiently, they need to increase the IOPS by 3,000 for each of the instances. Which of the following designs will meet the performance goal MOST cost effectively?

B. Increase the size of the gp2 volumes in each instance to 3 TB.

increase size of gp2 volumes to 3TB

Q9 A company's data center is connected to the AWS Cloud over a minimally used 10-Gbps AWS Direct Connect connection with a private virtual interface to its virtual private cloud (VPC). The company internet connection is 200 Ml pps, and the company has a 150-TB dataset that is created each Friday. The data

must be transferred and available in Amazon S3 on Monday morning. Which is the LEAST expensive way to meet the requirements while allowing for data transfer growth?
D. Create a public virtual interface on a Direct Connect connection, and copy the data to Amazon S3 over the connection.
create a public virtual interface on Direct Connect connection

Q10 A company has created an account for individual Development teams, resulting in a total of 200 accounts. All accounts have a s single virtual private cloud (VPC) in a single region with multiple microservices running in Docker containers that need to communicate with microservices in other accounts. The Security team requirements state that these microservices must not traverse the public internet, and only certain internal services should be allowed to call other individual services. If there is any denied network traffic for a service, the SeCurity team must be notified of any denied requests, including the source IP. How can connectivity be established between services while meeting the security requirements?
D. Create a Network Load Balancer (NLB) for each microservice. Attach the NLB to a PrivateLink endpoint service and whitelist the accounts that will be consuming this service. Create an interface endpoint in the consumer VPC and associate a security group that allows only the security group IDs of the services authorized to call the producer service. On the producer services, create security groups for each mic roservice and allow only the CIDR range the allowed services. Create VPC Flow Logs on each VPC to capture rejected traffic that will be delivered to an Amazon CloudWatch Logs group. Create a Cloud Watch Logs subscription that streams the log data to a security account.
create a NLB for each microservice

Q11 A company runs a dynamic mission-critical web application that has an SLA of 99.99%. Global application users access the application 24/7. The application is currently hosted on premises and routinely fails to meet its SLA, especially when millions of users access the application concurrently. Remote users complain of latency. How should this application be redesigned I to be scalable and allow for automatic failover at the lowest cost?
C. Use Amazon Route 53 latency-based routing to route to the nearest region with health checks. Host the website in Amazon 3 in each region and use Amazon API Gateway with AWS Lambda for the application layer. Use Amazon DynamoDB global tables as the data layer with Amazon DynamoDB Accelerator (DAX) for caching.
use Route 53 latency-based routing

Q12 A company manages more than 200 separate internet-facing web applications. All of the applications are deployed to AWS in 1 single AWS Region The fully qualified domain names (FQDNs) of all of the applications are made available ti trough HTTPS using Application Load BaLancers (ALBs). The ALBs are configured to use put lic SSL/TLS certificates. A Solutions Architect needs to migrate the web applications to a multi- region architecture. All HTTPS services should continue to work without interruption. Which approach meets these requirements?
D. Request certificates for each FQDN in both the primary and secondary AWS Regions using AWS Certificate Manager. Associate the certificates with the corresponding ALBs in each AWS Region.
request cert for each FQDN in both primary and secondary Regions

Q13 An e-commerce company is revamping its IT infrastructure and is planning to use AWS services. The company's CIO has asked a Solutions Architect to design a simple, highly available, and loosely coupled order processing application. The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table. The application has a sporadic traffic pattern and should be able to scale during marketing campaigns to process the orders with minimal delays. Which of the following is the MOST reliable approach to meet the requirements?
B. Receive the orders in an Amazon SQS queue and trigger an AWS Lambda function to process them.
receive orders in SQS queue

Q14 A company has an application written using an in-house software framework. The framework installation takes 30 minutes and is performed with a user data script. Company Developers deploy changes to the application frequently. The framework installation is becoming a bottle neck in this process. Which of the following would speed up this process?
A.Create a pipeline to build a custom AMI with the framework installed and use this AMI as a baseline for application deployments.
create a pipeline to build a custom AMI

Q15 A company wants to ensure that the workloads for each of its business units have complete autonomy and a minimal blast radius in AWS. The Security team must be able to control access to the resources and services in the account to ensure that particular services are t lot used by the business units. How can a Solutions Architect achieve the isolation requirements?
A.Create individual accounts for each business unit and add the account to an OU in AWS Organizations. Modify the OU to ensure that the particular services are blocked. Federate each account with an IdP, and create separate roles for the business units and the Security team.
create individual accounts for each business unit and add it to OU

Q16 A company is migrating a subset of its application APIs from Amazon EC2 instances to run on a serverless infrastructure. The company has set up Amazon API Gateway, AWS Lambda, and Amazon DynamoDB for the new application. The primary responsibility of the Lambda function is to obtain data from a third-party Software as a Service (SaaS) provider. For consistency, the Lambda function is attached to the same virtual private cloud (VPC) as the original EC2 instances. Test users report an inability to use this newly moved functionality, and the company is receiving Sxx errors from API Gateway. Monitoring reports from the SaaS provider shows that the requests never made it to its systems. The company notices that Amazon Cloud Watch Logs are being generated by the Lambda functions. When the same functionality is tested against the EC2 systems, it works as expected. What is causing the issue?
A. Lambda is in a subnet that does not have a NAT gateway attached to it to connect to the SaaS provider.
Lambda does not have NAT gateway

Q17 A Solutions Architect is working with a company that is extremely sensitive to its IT costs and wishes to implement controls that will result in a predictable AWS spend each month. Which co moination of

steps can help the company control and monitor its monthly AWS usage to achieve a cost that is as close as possible to the target amount? (Choose three.)
A. Implement an IAM policy that requires users to specify a workload' tag for cost allocation when launching Amazon EC2 instances.
E. Define workload as a cost allocation tag in the AWS Billing and Cost Management console.
F. Set up AWS Budgets to alert and notify when a given workload is expected to exceed a defined cost.
implement an IAM policy
define “workload” as a cost allocation tag
set up AWS Budgets

Q18 A large global company wants to migrate a stateless mission-critical application to AWS. The application is based on IBM WebSphere (application and integration middleware), IBM MQ (messaging middleware), and IBM DB2 (database software) on a z/ OS operating system. How should the Solutions Architect migrate the application to AWS?
B. Re-host WebSphere-based applications on Amazon EC2 behind a load balancer with Auto Scaling. Re-platform the IBM 1 MQ to an Amazon MQ Re-platform z'OS-based DB2 to Amazon EC2-based DB2.
re-platform OS-based DB2 to Amazon EC2-based DB2

Q19 A media storage application uploads user photos to Amazon S3 for processing. End users are reporting that some uploaded photos are not being processed properly. The Application Developers trace the logs and find that AWS Lambda is experiencing execution issues when thousands of users are on the system simultaneously. Issues are caused by:-Limits around concurrent executions -- The performance of Amazon DynamoDi B when saving data. Which actions can be taken to increase the performance and reliability of the application? (Choose two.)
B. Evaluate and adjust the write capacity units (WCUs) for the DynamoDB tables
D. Configure a dead letter queue that will reprocess failed or timed-out Lambda functions.
Evaluate and adjust WCU for DynamoDB tables
configure a dead letter queue

Q20 A company operates a group of imaging satellites. The satellites stream data to one of the company's ground stations where processing creates about 5 GB of images per minute. This data is added to network-attached storage, where 2 PB of data are already stored. The company runs a website that allows its customers to access and purchase the images over the Internet. This website is a so running in the ground station. Usage analysis shows that customers are most likely to access mages that have been captured in the last 24 It hours. The company would like to migrate the image storage and distribution system to AWS to reduce costs and increase the number of customers that ca in be served. Which AWS architecture and migration strategy will meet these requirements?
A.Use multiple AWS Snowball appliances to migrate the existing imagery to Amazon $3. Create a 1-Gb AWS Direct Connect connection from the ground station to AWS, and upload new data to Amazon S3 through the direct Connect connection. Migrate the data distribution website to Amazon EC2 instances. By using At nazon $3 as an origin, have this website serve the data through Amazon CloudFron t by creating signed URLs.
use multiple AWS Snowball app to migrate to S3. Create 1-Gb Direct Connect connection

Q21 A company ingests and processes streaming market data. The data rate is constant. A nightly process that calculates aggregate statistics is run, and each execution takes about 4 hours to complete. The statistical anal ysis is not mission critical to the business; and previous data poin ts are picked up on the next execution if a particular run fails. The current architecture uses a pool of Amazon EC2 Reserved Instances with 1-year re eservations running full time to ingest and store the streaming data in attached Amazon EBS volumes. On-Demand EC2 instances are launched each night to perform the nightly processing, accessing th le stored data from NFS shares on the ingestion servers, and terminating the nightly processing: servers when complete. The Reserved Instance reservations are expiring, and the company needs to detern nine whether to purchase new reservations or im plement a new design. Which is the most cost-effective design?

B. Update the ingestion process t O use Amazon Kinesis Data Firehose to save a lata to Amazon S3. Use AWS Batch to perfor n nightly processing with a Spot market bid of 50% of the On-Demand price.

AWS batch to perform nightly processing

Q22 A three-tier web application runs on Amazon EC2 instances. Cron daemons are used to trigger scripts that collect the web server, application, and database logs and send them to a centralized location every hour. Occasionally, scaling events or unplanned outages have caused the instances to stop before the latest logs were collected, and the log files were lost. Which of the following options is the MOST reliable way of collecting and preserving the log files?

C. Use the Amazon Cloud Watch Logs agent to stream log messages directly to CloudWatch Logs. Configure the agent with a batch count of 1 to reduce the possibility of log messages being lost in an outage.

use CloudWatch logs agent to stream log messages directly to CloudWatch logs

Q23 A company stores sales transaction data i n Amazon DynamoDB tables. To detect anomalous behaviors and respond quickly, all changes to the items stored in the DynamoDB tables must be logged within 30 minutes. Which solution meets the requirements?

C. Use Amazon DynamoDB Streams to capture and send updates to AWS Lambda. Create a Lambda function to output records t o Amazon Kinesis Data Streams. Analyze any anomalies with Amazon Kinesis Data Analytics. Send SNS notifications when anomalous behaviors are detected.

use DynamoDB Streams to capture and send updates

Q24 A company is running multiple applications on Amazon EC2. Each application is deployed and managed by multiple business units. All applications are deployed on a single AWS account but on different virtual private clouds (VPCS). The company uses a separate VPC in the same account for test and development purposes. Production applications suffered multiple outages when users accidentally terminated and modified resources that belonged to another business unit. A Solutions Architect has been asked to improve the availability of the company applications while allowing the Developers access to the resources they need. Which option meets the requirements with the LEAST disruption?

C. Implement a tagging policy based on business units. Create an IAM policy so that each user can terminate instances belonging to their own business units only.

implement a tagging policy based on business units

Q25 An enterprise runs 103 line-of-business applications on virtual machines in an on-premises data center. Many of the applications are simple PHP, Java, or Ruby web applications, are no longer actively developed, and serve little traffic. Which approach should be used to migra the these applications to AWS with the LOWEST infrastructure costs?
C. Convert each application to a Docker image and deploy to a small Amazon ECS cluster behind an Application Load Balancer.
convert each app to a Docker image

Q26 A Solutions Architect must create a cost-effective backup solution for a company's SOOMB source code repository of proprietary and sensitive applications. The repository runs on Linux and backs up daily to tape. Tape backups are stored for I year. The current solutions are not meeting the company's needs because it is a manual process that is prone to error, expensive to maintain, and does not meet the need for a Recovery Point Objective (RPO) of 1 hour or Recovery Time Objective (RTO) of 2 hours. The new disaster recovery requirement is for backups to be stored offsite and to be able to restore a single file if needed. Which solution meets the customer's needs for TO, RPO, and disaster recovery with the LEAST effort and expense?
B. Configure the local source code repository to synchronize files to an Aws Storage Gateway file Amazon gateway to stc pre backup copies in an Amazon S3 Standard bucket. Enable versioning on the Amazon S3 bucket Create Amazon $3 lifecycle policies to automatically migrate old versions of objects to Amazon S3 Standard 0 Infrequent Access, then Amazon Glacier, then delete backups after 1 year.
configure local source code repository to sync files to AWS Storage Gateway

Q27 A company CFO recently analyzed the company's AWS monthly bill and identified an opportunity to reduce the cost for A VS Elastic Beanstalk environments in use. The CFO has asked a Solutions Architect to design a highly available solution that will spin up an Elastic Beanstalk environment in the morning and terminate it at the end of the day. The solution should be designed with minimal operational overhead and to minimize costs. It should also be able to handle their increased use of Elastic Beanstalk environments among different teams, and must provide a one-stop scheduler solution for all teams to keep the operational costs low. What design will meet these requirements?
B. Develop AWS Lambda functions to start and stop the Elastic Beanstalk environment. Configure a Lambda execution rd ple granting Elastic Beanstalk environment start/ stop permissions, and assign the role to the Lambda function pns. Configure cron expression Amazon Cloud Watch Events rules to trigger the Lambda functions.
Develop Lambda functions to start and stop Elastic Beanstalk

Q28 A company plans to move regulated and security-sensitive businesses to AWS. The Security team is developing a framework to validate the adoption of AWS best practice and industry recognized compliance standards. The AWS Management Console is the preferred method for teams to provision resources. Which strategies should a Solutions Architect use to meet the business requirements and continuously assess ; audit, and monitor the configurations of AWS resources? (Choose two.)
A.Use AWS Config rules to periodically audit changes to AWS resources and monitor the compliance of the configuration. Develop AWS Config custom rules using AWS Lambda to establish a test-driven development approach 1. and further automate the evaluation of configuration changes against the required controls.

C. Use AWS CloudTrail events to assess management activities of all AWS accounts. Ensure that CloudTrail is enabled in all accounts and available AWS services. Enable trails, encrypt CloudTrail event log files with an AWS KMS key, and monitor recorded activities with CloudWatch Logs.
use AWS Config rule to periodically audit changes
use AWS CloudTrail events to assess management activities

Q29 A company is running a high-user-volume media-sharing application on premises. It currently hosts about 400 TB of data with millions of video files. The company is migrating this application to AWS to improve reliability and reduce costs. The Solutions Architecture teat n plans to store the videos in an Amazon S3 bucket and use Amazon CloudF ront to distribute videos to users. The company needs to migrate this application to AWS 10 days with the least amount of downtime possible. The company currently has 1 Gbps connectivity to the Internet with 30 percent free capacity. Which of the following solutions would enable the company to migrate the workload to AWS and meet all of the requirements?
D. Request multiple AWS Snowball devices to be delivered to the data center. Load th re data concurrently into these devices and send it back. Have AWS download that data to the Amazon S3 bucket. Sync the new data that was generated while migration was in flight.
Request multiple AWS Snowball devices

Q30 A company has developed a new billing application that will be released in two weeks. Developers are testing the application in running on 10 EC2 instances managed by an Auto Scaling group in subnet 172.31.0.0124 within VPCA with CIDR block 172.31.0.0/16. The Developers noticed connection timeout errors in the application logs while connecting to an Oracle database running on an Amazon EC2 instance it 1 the same region within VPC B with CIDR block 172.50.0.0716. The IP of the database instance is hard-coded in the aj oplication instances. Which recommendatic pns should a Solutions Architect present to the Developers to solve the problem in a secure way with minimal maintenance and overhead?
C. Create a VPC peering connection between the two VPCs and add a route to the routing table of VPC A that points to the IP address range of 17250.0.016
Create a VPC peering connection between 2 VPCs

Q31 A Solutions Architect has been asked to look at a company's Amazon Redshift cluster, which has quickly become an integral F art of its technology and supports key business processes. The Solutions Arcl hitect is to increase the reliability and availability of the cluster and provide an option is to ensure that if an issue arises, the cluster can either operate or be restored within four hours. Which of the following solution options BEST addresses the business need in the most cost effective manner?
B. Ensure that the Amazon Redshift cluster creation has been template using AwS CloudFormation so it can easily be launched in another Availability Zone and data populated from the automated Redshift back-ups stored in Amazon S3.
ensure Amazon Redshift cluster creation has been template

Q32 A company prefers to limit running Amazon EC "2 instances to those that were launched from AMIs pre- approved by the Information Security department. The Development team has an agile continuous integration and dept oyment process that cannot be stalled by the solution. Which method enforces the required controls with the LEAST impact ot the development process? (Choose two.)

A. Use IAM policies to restrict the ability of users or other automated entities to launch EC2 instances based on a specific set of pre-approved AMIs, such as those tagged in a specific way by Information Security.
D. Use AWS Config rules to spot any launches of EC2 instances based on non-approved AMIs, trigger an AWS Lambda function to automatically terminate the instance, and publish a message to an Amazon SNS topic to inform Information Security that this occurred.
use IAM policies to restrict ability of users
use AWS Config rules to spot any launches of EC2

Q33 A Company has a security event whereby an Amazon S3 bucket with sensitive information was made public. Company policy is to never have public S3 objects, and the Compliance team must be informed immediately wh nen any public objects are identified. How can the presence of a public S3 object be detected, set to trigger alarm notifications, and automatically remediated in the future? (Choose two.)
B. Configure an Amazon CloudWatch Events rule that invokes an AWS Lambda function to secure the S3 bucket.
D. Turn on object-level logging for Amazon S3. Configure a Cloud Watch event to notify by using an SNS topic when a PutObject API call with public-read permission is detected in the AWS CloudTrail logs.
Configure Amazon CloudWatch Events rule
Turn on object-level logging for S3. Configure CloudWatch event

Q34 A company is using a n Amazon CloudFront distribution to distribute both static and dynamic content from a web application running behind an Application Load Balancer. The web application requires user authorization and session tracking for dynamic content. The CloudFr ont distribution has a single cache behavior configured to forward the Authorization, Host, and I User-Agent HTTP whitelist headers and a session cookie to the origin. All other cache behavior settings are set to their default value. A valid ACM certificate is applied to the CloudFront distribution with a matching CNAME in the distribution settings. The ACM certificate is also applied to the HTTPS listener for the application Load Balancer. The CloudFront origin protocol policy is set to HTTPS only. Analysis of the cache statistics report shows that the miss rate for this distribution is very high. What can the Solutions Architect do to improve the cache hit i ate for this distribution without causing the SSL TLS handshake between CloudFront and the Application Load Balancer to fail?
D. Create two cache behaviors for static and dynamic content. Remove the User-Agent HTTP header from the whitelist head lers section on both of the cache behaviors. Remove the session cookie from the whitelist cookies section and the Authorization HTTP header from the whitelist headers section for cache behavior configured for static content.
remove user-agent http…

Q35 An organization has a write-intensive it mobile application that uses Amazon API Gateway, AWS Lambda, and Amazon Dynamodb. The application has scaled well, however, costs have increased exponentially because of higher than anticipated Lambda costs. The application's use is unpredictable, but there has been a steady 20% increase in utilization every month. While monitoring the current Lambda functions, the Solutions 4 Architect notices that the executiontime averages 4.5 minutes. Most of the wait time is the result of a high-later ney network call to a 3TB MySQL database server that is on-

premises. A VPN is used to connect to the VPC, so the Lambda functions have been configured to with a five-minute timeout. How can the Solutions Architect reduce the cost of the current architecture?
D. Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL Enable API caching on API Gateway to reduce the number of Lambda function invocations. Continue to monitor the AWS Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time. Enable Auto Scaling in DynamoDB.
enable auto scaling in dynamodb

Q36 A company runs a video processing platform. Files are uploaded by users who connect to a web server, which stores them on an Amazon EFS share. This web server is running on a single Amazed n EC2 instance. A different group of instances, running in an Auto Scaling group, scans the EFS share directory structure for new files to process and generates new videos (thumbnails, different resolution, compression, etc.) according to the instructions file, which is uploaded along with the video files. A different application running on a group of instances managed by an Auto Scaling group processes the video files and then deletes them from the EFS share. The results are stored in an S3 bucket. Links to the processed video files are emailed to the customer. The company has recently discovered that as they add more instances to the Auto Scaling Group, many files are processed twice, so image processing speed is not improved. The maximum size of these video files is 2GB. What should the Solutions Architect do to improve reliability and reduce the redundant processing of video files?
D. Rewrite the application to run from Amazon S3 and upload the video files to an S3 bucket. Each time a new file is uploaded, trigger an AWS Lambda function to put a mes: sage in an SQS queue containing the link and the instructions. Modify the video processing application to read from the SQS queue and the $3 bucket. Use the queue depth metric to adjust the size of the Auto Scaling group for video processing instances.
put message in SQS queue containing link

Q37 A Solutions Architect must establish a patching Plan for a large mixed fleet of Windows and Linux servers. The patching plan must be implemented securely, be audit ready, and comply with the company's business requirements. Which option will meet these requirements with MINIMAL effort?
B. Use AWS Systems Manager on all instances to manage patching. Test patches outside of production and then deploy du: ring a maintenance window with the appropriate approval.
use Amazon system manager to manage patching

Q38 A Solutions Architect must design a highly available, stateless, REST service. The service will require multiple persistent storage layers for service object meta information and the delivery of a content. Each request needs to be authenticated and securely processed. There is a requirement to keep costs as low as possible? How can these requirements be met?
C. Set up Amazon API Gateway and create the required API resources and methods. Use an Amazon Cognito user pool to control access to the API. Configure the method s to use AWS Lambda proxy integrations ; and process each resource with a unique, AWS Lambda function. Store request meta information in Dynam DB with Auto Scaling and static content in a secured S3 bucket. Generate presigned t IRLs when returning references to content stored in Amazon S3.
setup API GW, use cognito user pool to control access

Q39 A large company experienced a drastic increase in its monthly AWS spend. This is after Developers accidentally launched Amazon EC2 instances in unexpected regions. The company has established practices around least privileges for Developers and controls access to on premises resources using Active Directory groups. The company now wants to control costs by restricting the level of access that Developers have to the AWS Management Console without impacting their productivity. The company would also like to allow Developers to launch Amazon EC2 in only one region, without limiting access to other services in any region. How can this company achieve these new security requirements while minimizing the administrative burden on the Operations team?

D. Set up SAML-based authentication tied to an IAM role that has the PowerUserAccess managed policy attached to it. Attach a customer managed policy that denies access to Amazon EC2 in each region except for the one required.

setup SAML-based authentication, PowerUserAccess managed policy, attach a customer managed policy

Q40 A company is finalizing the architecture for its backup solution fo rapplications running on AWS. All of the applications run on AWS and use at least two Availability Zones in each tier. Company policy requires IT to durably store nightly backups fall its data in at least two locations:production and disaster recovery. The location must be in different geographic regions. The company also needs the backup to be available to restore immediately at the production data center, and within 24 hours at the disaster recovery location. All backup processes must be fully automated. What is the MOST cost- effective backup solution that will meet all requirements?

D. Back up all the data to Amazon S3 in the production region. Set up cross-region replication of this S3 bucket to another region and set up a lifecycle policy in the second region to immediately move this data to Amazon Glacier.

backup all data to S3 in production region

Q41 A company has an existing on-premises three-tier web application. The Linux web servers serve content from a centralized ted file share on a NAS server because the content is refreshed several times a day from various sources. The existing infrastructure is not optimized and the company would like to move to AWS in order to gain the ability to scale resources up and down in response to load. On-premises and AWS resources are connected using AWS Direct Connect. How can the company migrate the web infrastructure to AWS without delaying the content refresh process?

C. Expose an Amazon EFS share to on-premises users to serve as the NAS server. Mount the same EFS share to the web server Amazon EC2 instances to serve the content.

expose EFS share to on-premise user

Q42 A company has multiple AWS accounts hosting IT applications. An Amazon CloudWatch Logs agent is installed on all Amazon EC2 instances. The company wants to aggregate all security events in a centralized AWS account dedicated to log storage. Security Administrators need to perform near-real-time gathering and correlating of events across multiple AWS accounts. Which solution satisfies these requirements?

C. Create Amazon Kinesis Data Streams in the logging account, subscribe the stream to Cloud Watch Logs streams in each application AWS account. configure an Amazon Kinesis Data Firehose delivery stream with the Data Streams as its source, and persist the 1d data in an Amazon S3 bucket inside the logging AWS account.

Amazon kinesis data stream in logging account

Q43 A company has a serverless application comprised of Amazon CloudFront. Amazon API Gateway, and AWS Lambda functions. The current deployment process of the application code is to create a new version number of the Lambda function and run an AWS CLI script to update. If the new function version has errors, another CLI script 1 everts by deploying the previous working version of the function. The company would like to decrease the time to deploy new versions of the application logic provided by the Lambda functions, and also reduce the time to detect and revert when errors are identified. How can this be accomplished?

B. Use AWS SAM and built-in AWS CodeDeploy to deploy the new Lambda version, gradually shift traffic to the new version, and use pre-traffic and post-traffic test functions to verify code. Rollback if Amazon Cloud Watch alarms are triggered.

AWS SAM and built-in AWS CodeDeploy

Q44 A company is running a NET three-tier web application on AWS. The team currently uses XL storage optimized instances to serve the website's image and video files on local instance storage. The company has encountered issues with data loss from replication and instance failures. The Solutions Architect has been asked to redesign this application to improve its reliability while keeping costs low. Which solution will meet these requirements?

B. Implement Auto Scaling with general purpose instance types and an Elastic Load Balancer. Enable an Amazon CloudF ront distribution to Amazon S3 and move images and video files to Amazon 53. Reserve general purpose instances to meet base performance requirements. Use Cost Explorer and AWS Trusted Advisor checks to continue monitoring the environment for future savings.

implement auto scaling

Q45 A company has developed a web application that runs on Amazon EC2 instances in one AWS Region. The company has taken on new business in other countries and must deploy its application into other to meet low-later lcy requirements for its users. The regions can be segregated, and an application running in one region does not need to communicate with instances in other regions. How should the company's Solutions Architect automate the deployment of the application so that it can be MOST efficiently deployed into multiple regions?

D. Write a CloudFormation template describing the application's infrastructure in the Resources section. Use a CloudFor mation stack set from an administrator account to launch stack instances that deploy the application to other regions.

use a CloudFormation stack set from administrator account

Q46 A media company has a 30-TB rd pository of digital news videos. These videos are stored on tape in an on-premises tape library and referenced by a Media Asset Management (MAM) system. The company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature. The company must be able to search based on information in the video, such as objects, scenery items, or people's faces. A catalog is available that contains faces of people who have appeared in the videos that include an image of each person. The company would like to migrate these videos to AWS. The company has a high-speed A WS Direct Connect connection with AWS and would like to move the MAM solution video content directly from its current file system. How can these requirements be met by using the LEAST 'amount of ongoing management overhead and causing MINIMAL disruption to the existing system?"

A.Set up an AWS Storage Gateway, file gateway appliance on premises. Use the MAM solution to extract the videos from the current archive and push them into the file gateway . Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lar nbda function that invokes the Rekognition Javascript SDK to have Rekognition pull the video from the Amazon S3 files backing the file gateway, retrieve the required metadata, and push the metadata into the MAM solution.
aws storage gateway, file gateway appliance on premises .

Q47 A company is planning the migration of several lab environments used for software testing. An assortment of custom tooling is used to manage the test runs for each lab. The labs use immutable infrastructure for the software test runs, and the results are stored in a highly available SQL database cluster. Although completely rewriting the custom tooling is out of scope for the migration project, the company would like to optimize workloads during the migration. Which application migration strategy meets this requirement?
B. Re-platform
re-platform

Q48 A company is implementing a multi-account strategy; however, the Management team has expressed concerns that services like DNS may become overly complex. The company needs a solution that allows private DNS to be shared among virtual private clouds (VPCs) in different accounts. The company will have approximately 50 accounts in total. What solution would create the LEAST complex DNS architecture and ensure that each VPC can resolve all AWS resources?
A.Create a shared services VPC in a central account, and create a VPC peering connection from the shared services VPC to each of the VPCs in the other accounts. Within Amazon Route 53. create a privately hosted zone in the shared services VPC and resource record sets for the domain and subdomains. Programmatically associate other VPCs with the hosted zone.
create shared service VPC in central account, create VPC peering connection from shared services VPC to each of VPCs

Q49 A company has released a new version of a website to target a n audience in Asia and South America. The website's media assets are hosted on Amazon S3 and have an Amazon CloudFront distribution to improve end-user performance. However, users are having a poor login experience the authentication service is only available in the us-east-1 AWS Region. How can the Solutions Architect improve the login experience and maintain high security and performance with minimal management overhead?
C. Use Amazon Lambda Edge attached to the CloudFront viewer request trigger to authenticate and authorize users by maintaining a secure cookie token with a session expiry to improve the user experience in multiple geographies.
use Amazon Lamabda@Edge

Q50 A company has a standard three-tier architecture using two Availability Zones. During the company's off season, users report that the website is not working. The Solutions Architect finds that no changes have been made to the environment recently, the website is reachable, and it is possible to log in. However, when the Solutions Architect selects the "find a store near you' function, the maps provided on the site by a third-party RESTful API call do not work about 50% of the time after refreshing the page. The

outbound API calls are made through Amazon EC2 NAT instances. What is the MOST likely reason for this failure and how can it be mitigated in the future?
D. One of the NAT instances failed. Recommend replacing the EC2 NAT instances with a NAT gateway.
one of NAT instances failed

Q51 A company is migrating to the cloud. It wants to evaluate the configurations of virtual machines in its existing data center environment to ensure that it can size new Amazon EC2 instances accurately. The company wants to collect metrics, such as CPU, memory: and disk utilization, and it needs an inventory of what processes are running on each instance. The company would also like to monitor network connections to map communications between servers. Which would enable the collection of this data MOST cost effectively?
A.Use AWS Application Discovery Service and deploy the data collection agent to each virtual machine in the data center.
use AWS Application Discovery Service and deploy data collection agent

Q52 A company will several AWS accounts is using AWS Organizations and service control policies (SCPs). An Administrator create d the following SCP and has attached it to an organizational unit (OU) that contains AWS account 1111-1111-1111:

Developers working in account 1111-1111 -1111 complain that they cannot create Amazon S3 buckets. How should the Administrator address this problem?
C. Instruct the Developers to add Amazon S3 permissions to their IAM entities.
Instruct the Developers to add S3 permission

Q53 A company that provides wireless services needs a solution to store and analyze log files about user activities. Currently, log files are delivered daily to Amazon Linux on Amazon EC2 instance. A batch script is run once a day to aggregate data used for analysis by a third-party tool. The data pushed to the third-party tool is used to generate a visualization for end users. The batch script is cumbersome to maintain, and it takes several hours to deliver the ever-increasing data volumes to the third-party tool. The company wants to lower costs, and is open to considering a new tool that minimizes development effort and lowers administrative overhead. The company wants to build a more agile solution that can store and pe rform the analysis in near-real time, with minimal overhead. The solution needs to be cost effective and scalable to meet the company's end-user base growth. Which solution meets the company's requirements?
B. Use an Amazon Kinesis agent running on an EC2 instance in an Auto Scaling group to collect and send the data to an Amazon Kinesis Data Firehose delivery stream. The Kinesis Data Firehose delivery stream will deliver the data directly to Amazon ES. Use K ibana to visualize the data.
use Kinesis agent running on EC2 in auto scaling group

Q54 A company wants to move a web application to AWS. The application stores session information locally on each web server, which will make auto scaling difficult. As 1 part of the migration. the application will be rewritten to decouple the session data from the web servers. The company requires low latency, scalability, and availability. Which service will m seet the requirements for storing the session information in the MOST cost effective way?

D. Amazon ElastiCache with the Redis engine
Elasticache with redis engine

Q55 A company has an Amazon EC2 deployment that has the following architecture:- An application tier that contains 8 m4.xlarge instances -A Classic Load Balancer Amazon S3 as a persistent data store After one of the EC2 instances fails, t sers report very slow processing of their I equests. A Solutions Architect must recommend design changes to maximize system reliability. The solution must minimize costs. What should the Solution Architect recommend?
C. Replace the application tier with m4. large instances in an Auto Scaling group
replace app tier with m4 large instance

Q56 An on-premises application will be migrated to the cloud. The application consists of a single Elasticsearch virtual machine with data source feeds from local systems that will not be migrated, and a Java web application on Apache Tomcat running on three virtual machines. The Elasticsearch server currently uses 1 TB of storage out of 6 TB available storage, and the web application is updated every 4 months. Multiple 1 lsers access the web application from the Internet. There is a 10Gbit AWS Direct Connect connection established, and the application can be migrated over a scheduled 48- hour change window. Which strategy will have the LEAST impact on the Operations staff after the migration?
D. Create an Amazon ES cluster for Elasticsearch and a public AWS Elastic Beanstalk environment for the web application. Pause the data source feeds, export the Elasticsearch index from on premises, and import into the Amazon ES cluster. Move the data source feeds to the new Amazon ES cluster endpoint and move users to the new web application.
create Amazon ES cluster for ElasticSearch, pause data source feed

Q57 A company's application is increasingly popular and experiencing latency because of high volume reads on the database server. The service has the following properties:-A highly available REST API hosted in one region using Application Load Balancer (ALB) with auto scaling.-A MySQL database hosted on an Amazon EC2 instance in a single Availability Zone. -The company wants to reduce latency, increase in-region database read performance. and have multi-region disaster recovery capabilities that can perform a live recovery automatically without any data or performance loss (HADR). Which deployment strategy will meet these requirements?
A.Use AWS CloudFormation StackSets to deploy the API layer in two regions, Migrate the database to an Amazon Aurora with MySQL database cluster with multiple read replicas in one region and a read replica in a different region than the source database cluster. Use Amazon Route 53 health checks to trigger a DNS failover to the standby region if the health a hecks to the primary load balancer fail. In the event of Route 53 failover, promote the cross-region database replica to be the master and build out new read replicas in the standby region.
use CloudFormation StackSet to deploy API layer, migrate db to aurora

Q58 A company runs a three-tier application in AWS. Users report that the application performance can vary greatly depending on the time of day and functionality being accessed. The application includes the following components: Eight t2. large front-end web servers that serves static content and proxy dynamic content from the application tier. -Four t2. large application servers. -One db.m4. large Amazon RDS MySQL Multi-AZ DE Instance. Operations has determined that the web and application tiers are network constrained. Which of the following should cost effective improve application performance? (Choose two.)

B. Use AWS Auto Scaling and m4. large instances for the web and application tiers D. Create an Amazon CloudFront distribution to cache content
auto scaling & m4 large instances cloudfront distribution to cache content

Q59 An online retailer needs to regularly process large product catalogs, which are handled in batches. These are sent out to b e processed by people using the Amazon Mechanical Turk service, but the retailer has asked its Solutions Architect to design a workflow orchestration system that allows it to handle multiple concurrent Mechanical Turk operations, a leal with the result assessment process, and reprocess failures. Which of the following options gives the retailer the ability to interrogate the state of every workflow with the LEAST amount of
implementation effort?
D. Use Amazon SWF to create a workflow that handles a single batch of catalog records with multiple worker tasks to extract the data, transform it, and send it through Mechar ical Turk. Use Amazon ES and Kibana to visualize AWS Lambda processing logs to see the workflow states.
use Amazon SWF

Q60 An organization has two Amazon EC2 instances:-The first is running an ordering application and an inventory application. The second is running a queuing system. During certain times of the year, several thousand orders are placed per second. Some orders were lost when the queuing system was down. Also, the organization's inventory application has the incorrect quantity of products because some orders vere processed twice. What should be done to ensure that the applications can handle the increasing number of orders?
C. Put the ordering and inventory applications into their own Amazon EC2 instances, and create an Auto Scaling group for each application. Use Amazon SQS standard queues for the incoming orders, and implement idempotency in the inventory application.
use Amazon SQS standard queue for incoming order

Q61 A company is migrating its on-premises build artifact server to an AWS solution. The current system consists of an Apache HTTP server that serves artifacts to clients on the local network, restricted by the perimeter firewall. The artifact consumers are largely build automation scripts that download artifacts via anonymous HTTP: which the company will be unable to modify with in its migration timetable. The company decides to move the solution to Amazon S3 static website hosting . The artifact consumers will be migrated to Amazon EC2 instances located within both public and private subnets in a virtual private cloud (VPC). Which solution will permit the artifact consumers to download artifacts without modifying the existing automation scripts?
B. Create a VPC endpoint and add to the route table associated with subnets containing consumers. Configure the buc! ket policy to allow s3:ListBucket and s3:GetObject actions using the condition and the condition ey aws:source Vpce matching the identification of the VPC StringEquals endpoint.
matching identification of VPC StringEquals endpoint

Q62 A group of research institutions and hospitals are in a partnership to study 2 PBs of genomic data. The institute that owns the data stores it in an Amazon $3 bucket and updates it regularly. The institute would like to give all 1 of the organizations in the partnership read access to the data. All members of the partnership are extremely cost-conscious: and the institute that owns the account with the S3 bucket is

concerned about covering the costs for requests and data transfers from Amazon S3. Which solution allows for secure data sharing without causing the institute that owns the bucket to assume all the costs for S3 requests and data transfers?
B. Ensure that all organizations in the partnership have AWS accounts. Create a bucket policy on the bucket that owns the data. The policy should allow the accounts in the partnership to read l access to the bucket. Enable Requester pays on the bucket. Have the organizat lons use their AWS credentials when accessing the data.
create bucket policy

Q63 A company currently uses a single 1 Gbps AWS Direct Connect connection to establish 1 connectivity between an AWS Region and its data center. The company has five Amazon VPCs, all of which are connected to the data center using the same Direct Connect connection. The Network team is worried about the single point of failure and is interested in improving the redundancy of the connections to AWS while keeping costs to a minimum. Which solution would improve the redundancy of the connection to AWS while meeting the cost requirements?
B. Set up VPN tunnels from the data center to each VPC. Terminate each VPN tunnel at the virtual private gateway (VGW) of the respective VPC and set up BGP for route management.
setup VPN tunnels from dc to each VPC

Q64 A company currently uses Amazon EBS and Amazon RDS for storage purposes. The company intends to use a pilot light approach for disaster recovery in a different AWS Region. The company has an RTO of 6 hours and an RPO of 24 hours. Which solution would achieve the requirements with MINIMAL cost?
Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region. Use Amazon Route 53 with active- passive failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.
Use Lambda to create daily EBS and RDS snapshots. use EC2 with capacity set to 0

Q65 A company needs to cost-effectively persist small data records (up to 1 KiB) for up to 30 days. The data is read rarely. When reading the data, a 5- minute delay is acceptable. Which of the following solutions achieve this goal? (Choose two.)
B Write the records to Amazon Kinesis Data Firehose and configure Kinesis Data Firehose to deliver the data to Amazon S3 after 5 minutes. Set an expiration action at 30 days on the S3 bucket.
D. Write the records to Amazon DynamoDB configured with a Time To Live (TTL) of 30 days. Read data using the GetItem or BatchGetItem call.
write data to kinesis data firehose
write data to dynamodb config

Q66 A Development team is deploying new APIs as serverless applications within a company. The team is currently using the AWS Management Console to provision Amazon API Gateway, AWS Lambda, and Amazon DynamoDB resources. A Solutions Architect has been tasked with automating the future deployments of these serverless APIs. How can this be accomplished?
B. Use the AWS Serverless Application Model to define the resources. Upload a YAML template and application files to the code repository. Use AWS CodePipeline to connect to the code

repository and to create an action to build using AWS CodeBuild. Use the AWS CloudFormation deployment provider in CodePipeline to deploy the solution
use aws serverless application model

Q67 The company Security team queries that all data uploaded into an Amazon S3 bucket must be encrypted. The encryption keys must be highly available and the company must be able to control access on a per-user basis, with different users having access to different encryption keys. Which of the following architectures will meet these requirements? (Choose two.)
B. Use Amazon S3 server-side encryption with AWS KMS-managed keys, create multiple customer master keys, and use key policies to control access to them.
D. Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the keys. Use the Cloud HSM client software to control access to the keys that are generated.
encryption with AWS KMS-managed keys
use cloudHSM client

Q68 A company runs a public-facing application that uses a Java-based web service via a RESTful API. It is hosted on Apache Tomcat on a single server in a data center that runs consistently at 30% CPU utilization. Use of the API is expected to increase by 10 times with a new product launch. The business wants to migrate the application to AWS with no disruption, and needs it to scale to meet demand. The company has already decided to use Amazon Route 53 and CNAME records to redirect traffic. How can these requirements be met with the LEAST amount of effort?
A.Use AWS Elastic Beanstalk to deploy the Java web service and enable Auto Scaling. Then switch the application to use the new web service.
use AWS elastic beanstalk

Q69 A company is using AWS for production and development workloads. Each business unit has its own AWS account for production, and a separate AWS account to develop and deploy its applications. The Information Security department has introduced new security policies that limit access for terminating certain Amazon ECs instances in all accounts to a small group of individuals from the Security team. How can the Solutions Architect meet these requirements?
B. Create a new tag-based IAM policy that allows access to these EC2 instances only for the Security team. Tag the instances appropriately, and apply this policy in each account.
create tag-based IAM policy

Q70 A company is moving a business-critical, multi-tier application to AWS. The architecture consists of a desktop client application and server infrastructure. The server infrastructure resides in an on-premises data center that frequently fails to maintain the application uptime SLA of 99.95%. A Solutions Architect must re-architect the application to ensure that it can meet or exceed the SLA. The application contains a PostgreSQL database running on a single virtual machine. The business logic and presentation layers are load balanced between multiple virtual machines. Remote users complain about slow load times while using this latency-sensitive application. Which of the following will meet the availability requirements with little change to the application while improving user experience and minimizing costs?

B. Migrate the database to an Amazon RDS Aurora PostgreSQL configuration. Host the application and presentation layers in an Auto Scaling configuration on Amazon EC2 instances behind an Application Load Balancer. Use Amazon AppStream 2.0 to improve the user experience.
use Amazon appstream 2.0

Q71 An advisory firm is creating a secure data analytics solution for its regulated financial services users. Users will upload their raw data to an Amazon S3 bucket, where they have PutObject permissions only. Data will be analyzed by applications running on an Amazon EMR cluster launched in a VPC. The firm requires that the environment be isolated from the internet. All data at rest must be encrypted using keys controlled by the firm. Which combination of actions should the Solutions Architect take to meet the user's security requirements? (Choose two.)
A. Launch the Amazon EMR cluster in a private subnet configured to use an AWS KMS CMK for at rest encryption. Configure a gateway VPC endpoint for Amazon S3 and an interface VPC endpoint for AWS KMS. E. Configure the S3 bucket policies to permit access using an aws:source Vpce condition to match the S3 endpoint ID.
an interface VPC endpoint for AWS KMS configure S3 bucket policies

Q72 A company is designing a new highly available web application on AWS. The application requires consistent and reliable connectivity from the application servers in AWS to a backend REST API hosted in the company's on-premises environment. The backend connection between AWS and on- premises will be routed over an AWS Direct Connect connection through a private virtual interface. Amazon Route 53 will be used to manage private DNS records for the application to resolve the IP address on the backend REST API. Which design would provide a reliable connection to the backend API?
B. Install a second Direct Connect connection from a different network carrier and attach it to the same virtual private gateway as the first Direct Connect connection.
install second Direct Connect Connection

Q73 A company has a data center that must be migrated to AWS as quickly as possible. The data center has a 500 Mbps AWS Direct Connect link and a separate, fully available 1 Gbps IS P connection. A Solutions Architect must transfer 20 TB of data from the data center to an Amazon S3 bucket. What is the FASTEST way to transfer the data?
D. Upload the data to the S3 bucket using S3 Transfer Acceleration.
using S3 Transfer Acceleration

Q74 A bank is designing an online customer: service portal where customers can chat w rith customer service agents. The portal is required to maintain a 15-minute RPO or RTO in case of a regional disaster. Banking regulations require that all customer service chat transcripts must be preserved on durable storage for at least 7 years, that conversations must be encrypted in-flight, at ad transcripts must be encrypted at rest. The Da lata Lost Prevention team requires that data at rest must be encrypted using a key that the team contro ls, rotates, and revokes. Which design meets these requirements?
C. The chat application logs each chat message into Amazon CloudWatch Logs. A subscription filter on the Cloud Watch Ld gs group feeds into an Amazon Kinesis Data Firehose which streams the chat messages into an Amazon S3 bucket in the backup region. Separate AWS KMS keys are specified for the CloudWatch Logs group and the Kinesis Data Firehose.
feeds into Amazon kinesis Data Firehose

Q75 A company currently runs a secure application on Amazon EC2 that takes files from on-premises locations through AWS Direct Connect, processes them, and uploads them to a single Amazon S3 bucket. The application uses HTTPS for encryption in transit to Amazon 53, and S3 server side encryption to encrypt at rest. Which of the following changes should the Solutions Architect: recommend to make this solution more secure without impeding application's performance?
D. Add a VPC endpoint. Configure endpoint policies on the VPC endpoint to allow access to the required S3 buckets only. Implement an S3 bucket policy that allows communication from the VPC endpoint only.
allow communication from VPC endpoint only

Q76 As a part of building large applications in the AWS Cloud, the Solutions Architect is required to implement the perimeter security protection. Applications running on AWS have the following endpoints: Application Load Balancer Amazon API Gateway regional endpoint Elastic IP address-based EC2 instances. Amazon S3 hosted websites. Classic Load Balancer The Solutions Architect must design a solution to protect all of the listed web front ends and provide the following security capabilities:Dos protection SQL injection protection IP address whitelist blacklist HTTP flood protection Bad bot scraper protection How should the Solutions Architect design the solution?
C. Deploy Amazon CloudFront in front of all the endpoints. Deploy AWS WAF and AWS Shield Advanced. Add AWS WAF n iles to enforce the company's requirements. Use AWS Lambda to automate and enhance the security posture.
deploy CloudFront, deploy WAF and Shield advanced

Q77 A company has more than 100 AWS accounts, with one VPC per account, that net ed outbound HTTPS connectivity to the 1 internet. The current design contains one NAT gateway per Availability Zone (AZ) in each VPC. To reduce costs and obtain information about outbound traffic, management has asked for a new architecture for internet access. Which solution will meet the current needs, and I continue to grow as new accounts are provisioned, while reducing costs?
D. Create a proxy fleet in a central VPC account. Create an AWS PrivateLink endpoint service in the central VPC. Use Private Link interface for internet connectivity through the proxy fleet.
create a proxy fleet

Q78 A company runs an ecommerce platform with front-end and e-commerce tiers. Bq th tiers run on LAMP stacks with the front- end instances running behind a load balancing appliance that has a virtual offering on AWS. Currently, the Operations team uses SSH to log in to the instances to maintain patches and address other concerns. The platform has recently been the target of multiple attacks, including A DDoS attack. An S(IL injection attack. Several successful dictionary attacks on SSH accounts on the web servers. The company wants to improve the security of the e-commerce platform by migrating to AWS. The company's Solutions Architects have decided to use the following approach: Code review the existing application and fix any SQL injection issues. Migrate the web application to AWS and leverage the latest AWS Linux AMI to address initial security patching. Install AWS Systems Manager to manage patching and allow the system administrators to run commands on all instances, as needed. What additional steps will C address all of other identical attack types while providing high availability and minimizing risk?
B. Disable SSH access to the Amazon EC2 instances. Migrate on-premises MySC to Amazon RDS Multi-AZ. Leverage an Elastic Load Balancer to spread the load and enable AWS Shield Advanced

for protection. Add an Amazon CloudFront distribution in front of the website. Enable AWS WAF on the distribution to manage the rules.
disable ssh access & migrate MySQL to Amazon RDS multi-AZ

Q79 A company has a High Performance Computing (HPC) cluster in its on-premises data center which runs thousands of jobs in parallel for one week every month, processit g petabytes of images. The images are stored a in a network file server, which is replicated to disaster recovery site. The on- premises data center has reached capacity and has started to spread the jobs out over the e course of month in order to better utilize the cluster, causing a delay in the job completion. The company has asked its Solutions Architect to design a cost-effective solution on AWS to scale beyond the current capacity of 5,000 cores and 10 petabytes of data. The solution must require the least amount of management overhead and maintain the current level of durability. Which solution will meet the company's requirements?
C. Store the raw data in Ar nazon S3, and use AWS Batch with Managed Compute Environments to create Spot Fleets. Submit jobs to AWS Batch Job Queues to pull down objects from Amazon $3 pnto Amazon EBS volumes for temp brary storage to be processed, and then write the results back to Amazon S3.
store raw data in S3

Q80 A large company has many business units. Each business unit has multiple AWS accounts for different purposes. The CIO of the company sees that each business unit has data that would be useful to share with other parts of the company in total, there is about 10 PB of data that needs to be shared with users in 1,000 AWS accounts.' The data is proprietary; so some of it should only be available to users with specific job types. Some of the data is used for throughput of intensive workloads, such as simulations. The number of accour its changes frequently because of new initiatives, acquisitions, and divestitures. A Solutions Architect has been asked to design a system that will allow for sharing data for use in AWS with all of the employees in the company. Which approach will allow for secure data sharing in scalable way?
D. Store the data in a series of Amazon S3 buckets. Create an AWS STS token rending machine that is integrated with the e company's identity provider (IdP). When a user logs in, have the token vending machine attach an IAM policy that assumes the role that limits the user's access and or upload only the data the user is authorized to access. Users can get credentials by authenticating to the token vending th rachine's website or API and then use those credentials with an S3 client.
create AWS STS token vending machine

Q81 A company wants to migrate its website from an on-premises data center onto AWS. At the same time, it wants to migrate the website to a containerized microservice-based architecture to improve the availability and cost efficiency. The company's security policy states that privileges and network permissions must be configured according to best practice, using least privilege. A Solutions Architect must create a containerized architecture that meets the security requirements and has deployed the application to an Amazon ECS cluster. What steps are required after the deployment to meet the requirements? (Choose two.)
B. Create tasks using the aws vpc network mode. E. Apply security groups to the tasks; and use IAM roles for tasks to access other resources.
create task using aws vpc network mode use IAM roles for tasks

Q82 A company is migrating its marketing website and content management system from an on premises data center to AWS. The company wants the AWS application to be developed in a VPC with Amazon EC2 instances used for the web servers and an Amazon RDS instance for the database. The company has a runbook document that describes the installation process of the on-premises system. The company would like to base the AWS system on the processes referenced in the runbook document. The runbook document describes the installation and configuration of the operating systems, network settings: the website, and conte: nt management system software on the servers s. After the migration is complete, the company wants to be able to make changes quickly to take advantage of other AWS features. How can the application and environment be deployed and automated in AWS, while allowing for future changes?
D. Write an AWS CloudF ormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Include EC2 user data in the AWS CloudFormation template to install and configure the software.
Include EC2 user data

Q83 A company is adding a new approved external vendor that only supports IPv6 connectivity. The company's backend systems sit in the private subnet of an Amazon VPC. The company uses a NAT gateway to allow these systems to communicate with external vendors over IPv4. Company policy requires systems that communicate with external vendors use a security group that limits access to only approved external vendors. The virtual private cloud (VPC) uses the default network ACL. The Systems Operator successfully assigns IPv6 addresses to each of the backends systems. The Systems Operator also updates the outbound I security group to include the IPv6 CIDR of the external vendor (destination). The systems within the VPC are able to ping one another successfully over IPv6. However, these systems are unable to communicate with the external vendor. What changes are required to enable communication with the external vendor?
D. Create an egress-only internet gateway. Add a route for destination :-/O pointing to the gateway.
create egress-only internet gateway

Q84 A finance company is running its business-critical application on current-generation linux EC2 instances. The application includes a self-managed MySQL database performing heavy 1/O operations. The application is working fine to handle a moderate amount of traffic during the month. However, it slows down during the final three days of each month due to month-end reporting, even though the company is using Elastic Load Balancers and Auto Scaling within its infrastructure to meet the increased demand. Which of the following actions would allow the database to handle the month-end load with the LEAST impact on performance?
B. Performing a one-time migration o f the database cluster to Amazon RDS, and creating several additional read replicas to handle the load during end of month.
perform one-time migration

Q85 A Solutions Architect is designing the storage layer for a data warehousing application. The data files are large, but they have statically placed metadata at the beginning of each file that describes the size and placement of the file's index. The data files are read in by a fleet of Amazon EC2 instances that store the index size, index location, and other category information about the data file in a database. That database is used by Amazon EMR to group files together for deeper analysis. What would be the MOST cost-effective, high availability storage solution for this workflow?
A.Store the data files in Amazon S3 and use Range GET for each file's metadata, then index the relevant data.

store data files in S3

Q86 A company uses an Amazon EMR cluster to process data once a day. The raw data comes from Amazon S3, and the resulting processed data is also stored in Amazon S3. The processing must complete within 4 hours; currently, it only takes 3 hours. However, the processing time is taking 5 to 10 minutes. longer each week due to an increasing volume of raw data. The team is also concerned about rising costs as the compute capacity increases. The EMR cluster is currently running on three m3 xlarge instances (one master and two core nodes). Which of the following solutions will reduce costs related to the increasing compute needs?

B. Add additional task nodes, but use in stance fleets with the master node in on-Demand mode and a mix of On-Demand and Spot Instances for the core and task nodes. Purchase scheduled Reserved Instances for the master node.

purchase a scheduled reserved instance

Q87 A company is building an AWS landing zone and has asked a Solutions Architect to design a multi-account access strategy that will allow hundreds of users to use corporate credentials to access the AWS Console. The company is running a Microsoft Active Directory and users will use an AWS Direct Connect connection to connect to AWS. The company also wants to be able to federate to third-party services and providers, including custom applications. Which solution meets the requirements by using the LEAST amount of management overhead?

B. Create a two-way Forest trust relationship between the on-premises Active Directory and the AWS Directory Service. Set up AWS Single Sign- On with AWS Organizations. Use single sign-on integrations for connections with third-party applications.

create two-way forest trust relationships

Q88 A Solutions Architect is designing a network solution for a company that has applications running in a data center in Northern Virginia. The applications in the company's data server require predictable performance to applications running in a virtual private cloud (V PC) located in us east-1: and a secondary VPC in us- west-2 within the same account. The company d: ata center is collocated in an AWS Direct Connect facility that serves the us- west-1 region. The company has already ordered an AWS Direct Connect connection and a cross-connect has been established. Which solution will meet the requirements at the LOWEST cost?

A.Provision a Direct Connect gateway and attach the virtual private (VGW) for the VPC in us-east-1 and the VGW for the VPC in us-west-2. Create a private VIF on the Direct Connect connection and associate it to the Direct Connect gateway.

provision Direct Connect gateway

Q89 A company has a web service deployed in the following two AWS Regions: us-1 rest-2 and us-estl. Each AWS region runs an identical version of the web service. Amazon Route 53 is used to route customers to the AWS Region that has the lowest latency. The company wants to improve the availability of the web service in case an outage occurs in one of the two AWS Regions. A Solutions Architect has recommended that a Route 53 health check be performed. The health check must detect a specific text on an endpoint. What combination of conditions should the endpoint meet to pass the Route 53 health check? (Choose two.)

C. The endpoint must return an HTTP 2xx or 3xx status code.

D. The specific text string must appear within the first 5,120 bytes of the response.
return 2xx, 3xx status code
text string appear within first 5120 bytes of response

Q90 A company operating a website on AWS requires high levels of scalability, availability and performance. The company is running a Ruby on Rails application on Amazon EC2. It has a data tier on MySQL 5.6 on Amazon EC2 using 16 TB of Amazon EBS storage Amazon Cloud Front is used to cache application content. The Operations team is reporting continuous and unexpected growth of EBS volumes assigned to the MySQL database. The Solutions Architect has been asked to design a highly scalable, highly available, and high-performing solution. Which solution is the MOST cost- effective at scale?
C. Ensure that EC2 instances are right-sized and behind an Elastic Load Balancing load balancer. Implement Auto Scaling with EC2 instances. Ensure that the reserved instances are purchased for fixed capacity and that Auto Scaling instances run on demand. Migrate to an Amazon Aurora MySQL Multi-AZ cluster. Ensure that Multi-AZ architectures are implemented.
ensure EC2 is right-sized. 不要implement storage check

Q91 The Security team needs to provide a team of interns with an AWS environment so they an build the serverless video transcoding application. The project will use Amazon S3, AWS Lambda, Amazon all PI Gateway, Amazon Cognito, Amazon DynamoDB, and Amazon Elastic Transcoder. The interns should be able to create and configure the necessary resources, but they may not have access to create or modify AWS IAM roles. The Solutions Architect creates a policy and attaches it to the interns' group. How should the Security team configure the environment to ensure that the interns are self-sufficient?
A.Create a policy that allows creation of project-related resources only Create roles with required service permissions, which are assumable by the services.
allow creation of project-related resources only & create role with required services permission

Q92 A company is running a commercial Apache Hadoop cluster on Amazon EC2. This s cluster is being used daily to query large files on Amazon S3. The data on Amazon S3 has been curated and does not require any additional transformations steps. The company is using a commerciALBusiness intelligence (BI) tool on Amazon EC2 to run queries against the Hadoop cluster and visualize the data. The company wants to reduce or eliminate the overhead costs associated with managing the Hadoop cluster and the BI tool. The company would like to remove to a more cost- effective solution with minimal effort. The visualization is simple and requires performing some basic aggregation steps only. Which option will meet the company's requirements?
C. Develop a script that uses Amazon Athena to query and analyze the files on Amazon S3. Then use Amazon QuickSight to connect to Athena and perform the visualization.
develop a script that use Amazon Athena to query

Q93 A large multinational company runs a timesheet application on AWS that is used by staff across the world. The application runs on Amazon EC2 instances in an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer, and stores in an Amazon RDS MySQL Multi-AZ database instance. The CFO is concerned about the impact on the business if the application is not available. The application must not be down for more than two hours, but the solution must be as cost-effective as possible. How should the Solutions Architect meet the CFO's requirements while minimizing data loss?

D. Configure a real d replica in another region. Create an A VS CloudFormation template of the application infrastructure. When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance and use the AwS CloudFormation template to create the environment in another region using the promoted Amazon RDS instar ice. Update the DNS record to point to the e other region's ELB.
configure read replica, create cloudformation template

Q94 A development team has created a series of AWS CloudFormation templates to help deploy services. They created a template for a network/virtual private (VPC) stack, a database stack, a bastion host stack, and a web application-specific stack. Each service requires the deployment of at least:A network VPC stack A bastion host stack A web application stack Each template has multiple input parameters that make it difficult to deploy the services individually from the AWS CloudF ormation console. The input parameters from one stack are typically outputs from other stack s. For example, the VPC ID, subnet IDs, and security groups from the network stack may need to be used in the application stack or database stack. Which actions will help reduce the operationALBurden and the number of parameters passed into a service deployment? (Choose two.)
A. Create a new AWS CloudFormation template for each service. After the existing templates to use cross-stack reference to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new stack. Call the newly created service stack from the AWS CloudFormation console to deploy the specified service with a subset of the parameters previously required.
E. Create a new portfolio for the Services in AWS Service Catalog. Create a 1 new AWS CloudFormation template for each service. After the existing templates to use cross-stack references to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new stack. Create a product fc for each application. Add the service template to the product. Add each new product to the portfolio. Deploy the product from the portfolio to deploy the service with the necessary parameters only to s tart the deployment.
create a new AWS CloudFormation template
create a new portfolio, create a new AWS CloudFormation template

Q95 A company has an application behind a load balancer with enough Amazon EC2 instances to satisfy peak demand. Scripts and third-party deployment solutions are used to configure EC2 instances when demand increases or an instance fails. The team must periodically evaluate the utilization of the instance types to ensure that the correct sizes are deployed. How can this workload be optimized to meet these requirements?
D. Deploy the application as a Docker image by using Amazon ECS. Set up Amazon EC2 Auto Scaling and Amazon ECS scaling. Register forAWS Business Support ort and use Trusted Advisor checks to provide suggestions on cost savings
deploy app as a Docker image

Q96 A large global financial services company has multiple business units. The company wants to allow Developers to try new services, but there are multiple compliance requirements for diff erent workloads. The Security team is concerned about the access strategy for or 1-premises and AWS implementations. They would like to enforce governance for AWS services used by business teams for regulatory

workloads, including Payment Card Industry (PCI) requirements. Which solution will address the Security team's concerns and allow the Developers to try new services?
B. Build a multi-account strategy based on business units, environments, and specific regulatory requirements. Implement SAML-based federation across all AWS accounts with an on-premise identity store. Use AWS Organizations and build organizational units (O Us) structure based on regulations and service governance. Implement service control policies across OUs.
build organizational units structure based on regulation

Q97 A company had a tight deadline to migrate its on-premises environment to AWS. It moved over Microsoft SQL Servers and Microsoft Windows Servers using the virtual machine import export service and rebuilt other applicatic pns native to the cloud. The team created both Amazon EC2 databases and used Amazon RDS. Each team in the company was responsible for migrating their applications, and would like suggestion: son reducing its AWS spend. Which steps should a Solutions Architect take to reduce costs?
B. Enable Cost Explorer and AWS Business Support Reserve Amazon EC2 and Amazon RDS DB instances. Use Amazon Cloud Watch and AWS Trusted Advisor for monitoring and to receive cost-savings suggestions. Create a master account under Organizations and have teams join for consolidated billing.
enable cost explorer

Q98 A company wants to replace its call system with a solution built using AWS managed services. The company call center would like the solution to receive calls, create contact flows, and scale to handle growth projections. The call center would also like the solution to use deep learning capabilities to recognize the intent of the call ers and handle basic tasks, reducing the need it to speak an agent. The solution should also be able to query business applications and provide relevant information back to calls as requested. Which services should the Solution Architect use to build this solution? (Choose three.)
B. Amazon Connect to create a cloud-based contact center.
D. AWS Lambda to integrate with internal systems.
E. Amazon Lex to recognize the intent of the caller.
Amazon Connect
Amazon Lambda
Amazon Lex

Q99 A large company is migrating its entire IT portfolio to AWS. Each business unit in the company has a standalone AWS ad count that supports both development and test environments. New accounts to support production workloads will be needed soon. The Finance department requires a centralized method for payment but must maintain visibility into each 1 group's spending to allocate costs." The Security team requires a centralized mechanism to control IAM usage in all the company's accounts. What combination of the following options meet the company's needs with LEAST effort? (Choose two.)
B. Use Aws Organizations to create a new organization from a chosen payer account and define an organizational unit hierarchy. Invite the existing accounts to join the organization and create new accounts using Organizations.
D. Enable all features of WS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts.
use AWS Organizations enable all features from AWS organization

Q100 A company collects a steady stream of 10 million data records from 100,000 sources each day. These records are written to an Amazon RDS MySQL DB. A query must produce the daily average of data sources over the past 30 days. There are twice as many reads as writes. Queries to the collected data are for one source ID at a time. How can the Solutions Architect improve the reliability and cost effectiveness of this solution?

B. Use Aws Organizations to create a new organization from a chosen payer account and define an organizational unit hierarchy. Invite the existing accounts to join the organization and create new accounts using Organizations. D. Enable all features of WS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts. B. Use Amazon DynamoDB with the source ID as the partition key and the timestamp a s the sort key. Use a Time to Live (TTL) to delete data after 30 days.

use Time-to-Live(TTL) to delete data after 30 days

Q101 A company is moving a business-critical application on AWS. It is a traditional three-tier web application using an Oracle database. Data must be encrypted in transit and at rest. The database hosts 12 TB of data. Network connectivity to the source Oracle database over the internal is allowed, and the company wants to reduce the operational costs by using AWS Managed Services where possible. All primary keys only; however, it contains many Binary Large Object (BLOB) fields. It was not possible to use the database's native replication tools because of licensing restrictions. Which database migration solution will result in the LEAST amount of impact to the application's availability?

C. Use AWS DMS to load and replicate the dataset between the on-premises Oracle database and the replication instance hosted on AWS. Provision an Amazon RDS for Oracle instance with Transparent Data Encryption (TDE) enable and configure it as target for the Replication instance. Create a customer-managed AWS KMS master key to set it as the encryption key for the replication instance. The AWS DMS tasks to load the data into the target RDS instance . During the application maintenance window and after the load tasks reach the ongoing replication phase, switch the database connections to the new database.

use AWS DMS to load and replicate dataset

Q102 A company has detected to move some e workloads on AWS to create a grid environment to run market analytics. The grid will consist of many similar instances, spun-up by a job-scheduling function. Each time a large analytics workload is completed, a new VPC is deployed along with a job scheduler and grid nodes. Multiple grids could be running in parallel. Key requirements are :Grid instances must communicate with Amazon S3 retrieve data to be processed. Grid instances must communicate with Amazon DynamoDB to track intermediate data. The job scheduler needs only to communicate with the Amazon EC: API to start new grid nodes. A key requirement is that the environment has no access to the internet, either directly or via the on-premises proxy. However, the application needs to be able to seamlessly communicate to Amazon S3, Amazon Dynan 10DB, and Amazon EC2 API, without the need for reconfiguration for each new deployment. Which of the following should the Solutions Architect to to achieve this target architecture? (Choose three.)

A. Enable VPC endpoints for Amazon S3 and DynamoDB.
E. Enable an interface VPC endpoint for EC2.
F. Configure Amazon S3 endpoint policy to permit access only from the grid nodes.

enable VPC endpoints for S3 and DynamoDB
enable an interface VPC endpoint for EC2
Configure S3 endpoint policy

Q103 An internal security audit of AWS resources within a company found that a number of Amazon EC2 instances running Microsoft Windows workloads were missing several important operating system-level patches. A Solutions Architect has been asked to fix existing patch deficiencies, and to develop a workflow to ensure that future patching requirements are identified and taken care of quickly. The Solutions Architect has decided to use AWS Systems Manager. It is important that EC instance reboots do not occur at the same time on all Windows workloads to meet orginational uptime requirements. Which workflow will meet these requirements in an automated manner?

C. Add a Patch Group tag with a value of either Windows Servers For Windows Server2 to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS- DefaultPatchBaseline with both Windows Servers patch groups. Define two non-overlapping AWS Systems Manager maintenance windows, conduct patching within them, and associate each with a different patch group. Register targets with specific maintenance windows using the Patch Group tags. Assign the AWS-RunPatchBaseline document as a task within each maintenance window.

register target with specific maintenance window using patch group tags

Q104 A company must deploy multiple independent instances of an application. The front-end application is internet accessible. However, corporate policy stipulates that the backends are to be isolated from each other and the internet, yet accessible from a centralized administration server. The application setup should be automated to minimize the opportunity for mistakes as new Instances are deployed. Which option meets the requirements and MINIMIZES costs?

C. Duplicate the application IAM roles and resources in separate accounts by using a single CloudFormati on template. Include VPC peering to connect the VPC of each application instance to a central VPC.

duplicate app IAM roles and resource

Q105 A group of Amazon EC2 instances have been configured as high performance computing (HPC) cluster. The instances are running in a placement group, and are able to communicate with each other at network of up to 20 Gbps. I The cluster needs to communicate with a control EC2 instance outside of the placement group. The control instance has the same instance type and AMI a s the other instances, and is configured with a public IP address. How can the Solutions Architect improve the network speeds between the control instance and the instances in the placement group?

D. Move the control instance inside the placement group.

move control instance inside placement group

Q106 A Solutions Architect has created an AWS Cloudformation template for a three-tier application that contains an Auto Scaling group of Amazon EC2 instances running a custom AMI. The Solutions Architect wants to ensure that future updates to the custom AMI can be deployed to a running stack by first updating the template to refer to the new AMI, and then invoking UpdateStad Ik to replace the EC2 instances with instandes launched from the new AMI. How can updates to the AMI be deployed to meet these requirements?

C. Edit the AWS: AutoScaling: LaunchConfiguration resource in the template, inserting an attribute. UpdatePolicye

inserting an attitude: update policy

Q107 A Solutions Architect is designing a multi-account structure that has 10 existing accounts. The design must meet the following requirements: Consolidate all accounts into one organization. Allow full access to the Amazon EC2 service from the master account and the secondary accounts. Minimize the effort required to add additional secondary accounts. Which combination of steps should be included in the solution? (Choose two.)

A. Create an organization from the master account. Send invitations to the secondary accounts from the master account. Accept the invitations and create an OU.

D. Create a service control policy (SCP) that enables full EC2 access, and attach the policy to the OU.

send invitations to secondary account

create service control policy (SCP)

Q108 AnyCompany has acquired numerous companies over the past few years. The CIO for AnyCompany would like to keep the resources for each acquired company separate. The CIO also would like to enforce a chargeba ck model where each company pays for the A WS services it uses. The Solutions Architect is tasked with designing an AWS architecture that allows Any Company to achieve the following: Implementing a detailed chargeback mechanism to ensure that each company pays for the resources it uses. AnyCompany can pay for AWS services for all its companies through a single invoice. Developers in each acquired company have access to resources in their company only 4. Developers in an acquired company should not be able to affect resources in their company only. A single identity store is used to authenticate Developers across all companies. Which of the following approaches would meet these requirements? (Choose two.)

A. Create an organization from the master account. Send invitations to the secondary accounts from the master account. Accept the invitations and create an OU. D. Create a service control policy (SCP) that enables full EC2 access, and attach the policy to the OU. A. Create a multi-account strategy with an account per company. Use consolidated billing to ensure that AnyCompany needs to pay a single bill only.

D. Create a federated identity store against the company's Active Directory. Create IAM roles with appropriate permissions and set the trust relationships with AWS and the identity store. Use AWS STS to grant users access based on the groups they belong to in the identity store.

use consolidated bill to ensure that any company needs to pay a single bill only

use AWS STS grant user access based on group

Q109 A company deployed a three-tier web application in two regions:us-east-1 and eu-west-1. The application must be active in both regions at the same time. The database tier of the application uses a single Amazon RDS Aurora database globally, with a master in us-east-1 and a read replica in eu- west-1. Both regions are connected by a VP N. The company wants to ensure that the application remains available even in the event of a region-level failure of all of the application's components. It is acceptable for the application to be in read-only mode for up to 1 hour. The company plans to configure two Amazon Route 53 record sets, one for each of the regions. How should the company complete the configuration to meet its requirements while providing the lowest latency for the application end-users? (Choose two.)

C. Use latency-based routing for both record sets. Configure a health check for each region and attach it to the record set for that region.

E. Configure Amazon RDS event notifications to react to the failure of the database in us-east-1 by invoking an AWS Lambda function that promotes the read replica in eu-west-1.

use latency-based routing for both record sets
config RDS event notification to react to failure of DB

Q110 A company runs a Windows Server host in a public subnet that is configured to allow a team of administrators to connect over RDP to troubleshoot issues with hosts in a private subnet. The host must be available at all times outside of a scheduled maintenance window, and needs to receive the latest operating system updates within 3 days of release. What should be done to manage the host with the LEAST amount of administrative effort?
C. Run the host in an Auto Scaling group with a minimum and maximum instance count of 1. Use a hardened machine image from AWS Marketplace. Apply system updates with AWS Systems Manager Patch Manager.
run the host in an auto scaling group

Q111 A company has a large on-premises Apache Hadoop cluster with a 20 PB HDFS database. The cluster is growing every quarter by roughly 200 instances and 1 PB. The company's goals are to enable resiliency for its Hadoop data, limit the impact of losing cluster nodes, and significantly reduce costs. The current cluster runs 24/7 and supports a variety of analysis workloads, including interactive queries and batch processing. Which solution would meet these requirements with the LEAST expense and down time?
A. Use AWS Snowmobile to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially y sized to handle the interactive workload based on historical data from the on-premises cluster. Store the data on EMRFS. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon Cloud Watch I metrics. Create job- specific, optimized clusters for batch workloads that are similarly optimized.
use AWS snowmobile to migrate & EMR(Elastic MapReduce) cluster initially size to handle

Q112 A company is running a large application on-premises. Its technology stack consists of Microsoft NET for the web server platform and Apache Cassandra for the database. The company wants to migrate the application to AWS to improve service reliability. The IT team also wants to reduce the time it spends on capacity management and maintenance of this infrastructure. The I Development team is willing and available to make code changes to support the migration. Which design is the LEAST complex to manage after the migration?
C. Migrate the web servers to an AWS Elastic Beanstalk environment that is running the NET platform in a Multi-AZ Auto Scaling configuration. Migrate the existing Cassandra database to Amazon DynamoDB.
migrate web server to AWS elastic beanstalk environment & Cassandra to Dynamodb

Q113 A company has a requirement that only allows specially hardened AMIs to be launched into public subnets in a VPC, and for the AMIs to be associated with a specific security group. Allowing non-compliant instances to launch into the public subnet could present a significant security risk if they are allowed to operate. A mapping of approved AMIs to subnets to security groups exists in an Amazon DynamoDB table in the same AWS account. The company created an AWS Lambda function that, when invoked, will terminate a given Amazon EC2 instance if the combination of AMI. subnet, and security

group are not approved in the DynamoDB table. What should the Solutions Architect do to MOST quickly mitigate the risk of compliance deviations?
D. Create an Amazon CloudWatch Events rule that matches each time an EC2 instance is launched, and associate it with the Lambda function as the target
Create an CloudWatch events rule , associate it with Lambda function

Q114 A Solutions Architect must migrate an existing on-premises web application with 70 TB of static files supporting a public open-data initiative. The architect wants to upgrade to the latest version of the host operating system as part of the migration effort. Which is the FASTEST and MOST cost- effective way to perform the migration?
C. Re-platform the server to Amazon EC2, and use AWS Snowball to transfer the static data to Amazon S3.
use snowball to transfer

Q115 A company has an application that generates a weather forecast that is updated every 15 minutes with an output resolution of 1 billion unique positions, each approximately 20 bytes in size (20 Gigabytes per forecast). Every hour, the forecast data is globally accessed approximately 5 million times (1.400 requests per second). and up to 10 times i nore during weather events. The forecast data is overwritten every update. Users of the current weather forecast application expect responses to queries to be returned in less than 1 two seconds for each request. Which design meets the required request rate and response time?
A. Store forecast locations in an Amazon ES cluster. Use an Amazon CloudFront distribution targeting an Amazon API Gateway endpoint with AWS Lambda functions responding to queries as the origin. Enable API caching on the API Gateway stage with a cache-control timeout set for 15 minutes.
enable API Caching on API gateway stage

Q116 A company is using AWS C 'loudFormation to deploy its infrastructure. The company is concerned that, if a production CI oudFormation stack is deleted, important data stored in Amazon RDS databases or Amazon EBS volumes might also be deleted. How can the company prevent users from accidentally deleting data in this way?
A.Modify the CloudFormation templates to add a DeletionPolicy attribute to RDS and EBS resources.
modify cloudformation template to add DeletionPolicy

Q117 A company would like to implement a serverless application by using Amazon API Gateway, AWS Lambda a and Amazon DynamoDB. They deployed a proof of concept and stated that the average response time is greater than what their upstream services can accept. Amazon CloudWatch metrics did not indicate any issue: s with DynamoDB but showed that some Lambda functions were hitting their timeout. Which o f the following actions should the Solutions Architect consider to improve performance? (Choose two.)
B. Increase the amount of memory and adjust the timeout on the Lambda function. Complete performance testing to identify the ideal memory and timeout configuration for the Lambda function.

D. Enable API cache on the appropriate stage in Amazon API Gateway, and override the TTL for individual methods that require a lower TTL than the entire stage.
perf testing to identify ideal memory
enable API cache

Q118 A company 1 is using AWS to run an internet-facing production application written in Node.js. The Development team is responsible for pushing new versions of the eir software directly to production. The application software is updated multiple times a day. The team needs guidance from a Solutions Architect to help them deploy the software to the productic pn fleet quickly and with the least amount of disruption to the service. Which option meets these requirements?
C. Use AWS Elastic Beanstalk to host the production application. For software changes, upload the new application version to Elastic Beanstalk to push this to the production fleet using a blue/green deployment method.
use blue/green deployment method

Q119 A company used Amazon EC2 instances to deploy a web fleet to host a blog site. The EC2 instances are behind an Application Load Balancer (ALB) and are configured in an Auto Scaling group. The web application stores all blog content on an Amazon EFS volume. The company recently added a feature for bloggers to add video to their posts, attracting 10 times the previous user traffic. At peak times of day, users 1 eport buffering and timeout issues while attempting to reach the site or watch videos. Which is the MOST cost-efficient and scalable deployment that will resolve the issues for users?
C. Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.
migrate video from EFS to S3

Q120 A company runs its containerized batch jobs on Amazon ECS. The jobs are scheduled by submitting a container image, a task definition, and the relevant data to an Amazon S3 bucket. Container in hages may be unique per job. Running the jobs as quickly as possible is of utmost importance, so submitting jobs artifacts to the S3 bucket triggers the job to run immediately. Sometimes there may no jobs running at all. However, jobs of any size can be submitted with no prior warning to the IT Operations team. Job definitions include CPU and memory resource requirements. What solution will allow the batch jobs to complete as quickly as possible after being scheduled?
C. Schedule the jobs on a n Amazon ECS cluster using the Fargate launch l type. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs.
use fargate launch type, 不需要spot instance

Q121 A company receives clickstream data files to Amazon S3 every five minutes. A Python script runs as a cron job once a day on an Amazon EC2 instance to process each file and load it into a database hosted on Amazon RDS. The cron job takes 15 to 30 minutes to process 24 hours of data. The data consumers ask for the data to be available as soon as possible. Which solution would accomplish the desired outcome?
D. Create an AWS Lambda function that runs when a file is delivered to Amazon S3 using S3 event notifications.
using S3 event notification

Q122 A company that is new to AWS reports it has exhausted its service limits across several accounts that are on the Basic Support plan. The company would like to prevent this from happening in the future. What is the MOST efficient way of monitoring and managing all service limits in the company's accounts?
D. Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked ad counts using AWS Trusted Advisor, and use Amazon SNS for notifications if a limit is close to exceeding the threshold. Ensure that the accounts are using the AWS Business Support plan at a minimum.
use AWS business support plan

Q123 A company needs to run a software package that has a license that must be run on the same physical host for the duration of its use. The software package is only going to be used for 90 days. The company requires patching and restarting g of all instances every 30 days. How can these requirements be met using AWS?
B. Run the instance on a dedicated host with Host Affinity set to Host
host with Host Affinity set to Host

Q124 A company runs an IoT platform on AWS. IoT sensors in various locations send data to the company's Node.js API servers on Amazon EC2 instances running behind an Application Load Balancer. The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume. The number of sensors the company has deployed in the field has increased over time, and is expected to grow significantly. The API servers are consistently overloaded and RDS metrics show high write latency. Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? (Choose two.)
C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data
E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance
leverage kinesis data stream
use dynamodb

Q125 A Solutions Architect is designing a system that will collect and store data from 2,000 internet connected sensors. Each sensor produces 1 KB of data every second. The data must be available for analysis within a few seconds of it being sent to the system and stored for analysis indefinitely. Which is the MOST cost-effective solution for collecting and storing the data?
B. Put each record in Amazon Kinesis Data Streams. Set up Amazon Kinesis Data Firehose to read records from the streat n and group them into objects in Amazon S3. Analyze recent data from Kinesis Data Streams and historical data from Amazon S3.
setup kinesis firehose to read record

Q126 An auction website enables users to bid on collectible items. The auction rules require that each bid is processed only once and in the order it was received. The current implementation is based on a fleet of Amazon EC2 web servers that write bid records into Amazon Kinesis I Data Streams. A single t2. a large instance has a cron job that runs the bid processor. which reads incoming bids from Kinesis Data Streams and processes each bid. The auction site is growing in popularity, but users are complaining that some

bids are not registering. Troubleshooting indicates that the bid processor is too slow during peak demand hd purs, sometimes crashes while processing, and occasionally loses track of which record Is is being processed. What changes should make the bid processing more reliable?
C. Refactor the web application to pd st each incoming bid to an Amazon SQS FIFO queue in place of Kinesis Data Stree ims. Refactor the bid processor to continuously the SQ IS queue. Place the bid processing EC2 instar ice in an Auto Scaling group with a minimum and a maximum size of 1.
post each incoming bid to SQS FIFO queue

Q127 A company has asked a Solutions Architect to design a secure content management solution that can be accessed by API calls by external customer applications. The company requires that a customer administrator must be able to submit an API call and roll back changes to existing files sent to the content management solution, as needed. What is the MOST secure deployment design that meets all solution requirements?
A.Use Amazon S3 for object storage v vith versioning and bucket access logging enabled, and an IAM role and access policy for each customer application. Encrypt objects using SSE-KMS. Develop the content management application to use a separate AWS KMS Key for each customer.
encrypt objects using SSE-KMS

Q128 A company has been using a third-party provider for its content delivery network and recently decided to switch to Amazon CloudFront the Development team wants to maximize performance for the global user base. The company uses a content management system CMS) that serves both static and dynamic content. The CMS is both md an Application Load Balance (ALB) which is set as the default origin for the distribution. Static assets are served from an Amazon S3 bucket. The Origin Access Identity (OAI) was created property S3 bucket policy has been updated to allow the GetObject action from the OAI, but static assets are receiving a 404 error. Which combination of steps should the Solutions Architect take to fix the error? (Select TWO.)
A. Add another origin to the CloudFront distribution for the static assets
D. Add a behavior to the CloudFront distribution for the path pattern and the origin of the static assets
add another origin to cloudfront distribution
add behavior to cloudfront distribution

Q129 A bank is re-architecting its mainframe-based credit card approval processing application to a cloud-native application on the AWS cloud. The new application will receive up to 1,000 requests per second at peak load. There are multiple steps to each transaction. and each step must receive the result of the previous step. The entire request must return an authorization response within less than 2 seconds with zero data loss. Every 1 equest must receive a response. The solution must be Payment Card Industry Data Security Standard (PCI DSS)-compliant. Which option will meet all of the bank's objectives with the LEAST complexity and LOWEST cost while also meeting compliance requirements?
D. Create an Amazon API Gateway to process inbound requests using a series of AWS Lambda processes, each with an Amazon SQS input queue. As each step completes, it writes its result to the next step's queue. The final step returns a JSON object with the approval status. Open a support case to increase the limit for the number of concurrent Lambdas td p allow room for bursts of activity due to the new application.
write result to next step queue

Q130 A Solutions Architect is migrating a 10 TB PostgreSQL database to Amazon RDS for PostgreSQL. The company's internet link is 50 MB with a VPN in the Amazon VPC, and the Solutions Architect: needs to migrate the data and synchronize the changes before the cutover. The cutover must take place within an 8-day period. What is the LEAST complex method of migrating the database securely and reliably?
A.Order an AWS Snowball device and copy the database using the AWS I DMS. When the database is available in Amazon 3 ; use AWS DMS to load it to Amazon RDS, and configure a job to synchronize changes before the cutover.
order SnowBall and copy db using DMS

Q131 A Solutions Architect must update an application environment within AWS Elastic Beanstalk using a blue/ green deployment methodology. The Solutions Architect creates an environment that is identical to the existing application environment and deploys the application to the new environment. What should be done next to complete the update?
B. Select the Swap Environment URLs option
select Swap Environment URLs option

Q132 A company has a legacy application running on servers on premises. To increase the application's reliability, the company wants to gain actionable insights using application logs. A Solutions Architect has been given following requirements for the solution:-Aggregate logs using AWS. -Automate log analysis for errors. -Notify the Operations team when errors go beyond a specified threshold. What solution meets the requirements?
D. Install the Amazon CloudWatch agent on servers, send logs to Amazon CloudWatch Logs and use metric filters to identify errors, create a CloudWatch alarm to notify the Operations team of errors.
install cloudwatch agent on servers, send log to cloudwatch Log

Q133 What combination of steps could a Solutions Architect take to protect a web workload running on Amazon EC2 from DDc S and application layer attacks? (Select two.)
B. Migrate the DNS to Amazon Route 53 and use AWS Shield.
D. Create and use an Amazon CloudFront distribution and configure AWS WAF on it.
migrate DNS to Route 53 and use Amazon shield
use cloudfront distribution and config AWS WAF

Q134 A photo-sharing and publishing company receives 10,000 to 150,000 images daily. The company receives the images from multiple suppliers and users registered with the service. The company is moving to AWS and wants to enrich the existing metadata by adding data using Amazon Rekognition. The following is an example of the additional data:As part of the cloud migration program, the company uploaded existing image : data to Amazon S3 and told users to upload images directly to Amazon S3. What should the Solutions Architect do to support these requirements?
A. Trigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon DynamoDB to store the metadata and Amazon ES to create an index. Use a web front-end to provide search capabilities backed by Amazon ES.
trigger Lambda & use dynamodb to store metadata

Q135 A Solutions Architect is redesigning an image-viewing and messaging platform to be delivered as SaaS. Currently, there is a farm of virtual desktop infrastructure (VDI) that runs a desktop image- viewing application and a desktop messaging application. Both applications use a shared database to manage user accounts and sharing . Users login from a web portal that launches the applications and streams the view of the application on the user's machine. The Development Of operations team wants to move away from using VDI and wants to rewrite the application. What is the MOST cost-effective architecture that offers both security and ease of management?

A. Run a website from an Amazon S3 bucket with a separate S3 bucket for images and messaging data. Call AWS Lambda functions from embedded JavaScript to manage the dynamic content, and use Amazon Cognito for user and sharing management.

call lambda function from embedded JavaScript

Q136 A company is running at 11. application on Amazon EC2 instances in three environments; development, testing, and productic n. The company uses AMIs to deploy the EC2 instances. The company builds the AMIs by using custom deployment scripts and infrastructure orchestration tools for each release in each environment. The company is red ceiving errors in its deployment process. Errors appear during operating system pad kage downloads and during application code installation from a third-party Git hosting service. The company needs deployments to become more reliable across all environments. Which combination of steps will meet these requirements? (Select THREE).

A Mirror the application code to an AWS CodeCommit Git repository.Use the repository to build EC2 AMIs.

C. Produce one EC2 AMI for each release for use across all environments.

E. Replace the custom scripts and tools with AWS CodeBuild. Update the infrastructure deployment process to lse EC2 Image Builder.

mirror code to AWS CodeCommit Git Repo
produce one EC2 AMI for each release
replace with AWS CodeBuild

Q137 A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large, important documents within the application with the following requirements:--The data must be highly durable and available. - The data must always be encrypted at rest and in transit. - The encryption key must be managed by the company and rotated periodically. Which of the following solutions should the Solutions Architect recommend?

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

AWS KMS for object encryption

Q138 A Solutions Architect is designing a highly available and reliable solution for a cluster of Amazon EC2 instances. The Solutions Architect must ensure that any EC2 instance within the cluster recovers automatically after a system failure. The solution must ensure that the recovered instance maintains the same IP address. How can these requirements be met?

D. Create an Amazon Cloud Watch alarm for the StatusCheckFailed System metric, and then configure an EC2 action to recover the instance.

create cloudwatch alarm for StatusCheckFailed_Syatem metrics

Q139 A public retail web application uses an Application Load Balancer (ALB) in front of Amazon EC2 instances running across multiple Availability Zones (AZs) in a Region backed by an Amazon RDS MySQL Multi-AZ deployment. Target group health checks are configured to use HTTP and pointed at the product catalog 1 page. Auto Scaling is configured to maintain the web fleet size based on the ALB health check. Recently, the application experienced an outage. Auto Scaling continuously replaced the instances during the outage. A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load, resulting in severely elevated query response times. Which of the following changes together would remediate these issues while improving monitoring capabilities for the availability and functionality of the entire application stack for future growth? (Select TWO.)

B. Configure the target group health check to point at a simple HTML page instead of a product catalog page and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon Cloud Watch alarms to notify administrators when the site fails.

E. Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySOL instances to reduce the load on the backend database tier.

config target group health check to point at HTML

config ElasticCache cluster

Q140 A company is running an email application across multiple AWS Regions. The company uses Ohio (us-east-2) as the primary Region and Northern Virginia (us-east-1) as the Disaster Recovery (DR) Region. The data is continuously replicated from the primary Region to the I DR Region by a single instance on the public subnet in both Regions. The replication messages between the Regions have a significant backlog during certain times of the day. The backlog clears on its own after a short time. but it affects the application's RPO. Which of the following solutions should help remediate this performance problem? (Select TWO)

B. Have the instance in the primary Region write the data to an Amazon SQS queue in the primary Region instead, and have the instance in the DR Region poll from this queue.

C. Use multiple instances on the primary and DR Regions to send and receive the replication data.

write data to SQS queue in primary region

use multiple instances to send and receive replication data

Q141 A company has implemented AWS Organizations. It has recently set up a number of new accounts and wants to deny access to a specific set of AWS services in these new accounts. How can this be controlled MOST efficiently?

B. Create a service control policy that denies access t o the services. Add all of the new accounts to a single organization unit (OU), and apply the policy to that OU.

add all new accounts to single OU

Q142 A company is planning to migrate an application from on-premises to 4 AWS. The application currently uses an Oracle database and the company can tolerate a brief downtime of 1 hour when performing the switch to the new infrastructure. As part of the migration, the database engine will be changed to MySQL. A Solutions Architect needs to determine which AWS services can be used to

perform the migration while minimizing the amount of work and time required. Which of the following will meet the requirements?
B. Use AWS SCT to generate the schema scripts and apply them on the target prior to migration. Use AWS DMS to begin moving data from the on- premises database to AWS. After the initial copy, continue to use AWS DMS to keep the databases in sync until cutting over to the new database. Use AWS SCT to identify what embedded SQL code in the application can be converted and what has to be done manually.
use AWS SCT to generate schema scripts, use AWS DMS to begin moving data

Q143 A solutions architect must analyze a company's Amazon EC2 Instances and Amazon Elastic Block Store (Amazon EBS) volumes to determine whether the company is using resources efficiently. The company is running several large, high-memory EC2 instances to host database dusters that are deployed in active passive configurations. The utilization of these EC2 instances varies by the applications that use the databases, and the company has not identified a pattern. The solutions ; architect must analyze the environment and take action based on the findings. Which solution meets these requirements MOST cost-effectively?
C. Install the Amazon Cloud Watch agent on each of the EC2 Instances. Turn on AW S Compute Optimizer, and let it run for at least 12 hours.Review the recommendations from Compute Optimizer, and rightsize the EC2 instances as directed
install cloudwatch agent in each of EC2

Q144 Your company has a logging microservice which is used to generate logs when users have entered certain commands in ar lother application. This logging service is implemented via an SQS standard queue that an EC2 instance is listening to. However, you have found that on some occasions, the order of the logs are not maintained. As a result, it becomes harder to use this service to trace users' activities. How should you fix this issue in a simple way?
C. Install the Amazon Cloud Watch agent on each of the EC2 Instances. Turn on AW S Compute Optimizer, and let it run for at least 12 hours.Review the recommendations from Compute Optimizer, and rightsize the EC2 instances as directed B. Delete the existing standard queue and recreate it as a FIFO queue. As a result, the order for the messages to b e received is ensured.
delete existing standard queue and recreate FIFO queue

Q145 A large trading company is using an on-premise system to analyze the trade data. After the trading day closes, the data including the day's transaction costs, execution reporting. and market performance is sent to a Redhat server which runs big data analytics tools for predictions for next day trading. A bash script is used to configure resources and schedule when to run in the data analytics workloads. How should the on-premise system be migrated to AWS with appropriate tools? (Select THREE)
A. Create a S3 bucket to store the trade data that is used for post processing.
C. Use AWS Batch to execute the bash script using a proper job definition.
D. Create EC2 instances with auto-scaling to handle the big data analytics workloads.
create S3 bucket to store data
use AWS Batch to execute bash script
create EC2 with auto scaling

Q146 A large IT company has an on- premise website which provides real-estate information such as renting: house prices and latest news to users. The website has a Java backend and a NoSQL MongoDB database that is used to store subscribers data. You are a cloud analyst and need to migrate the whole application to AWS platform. Your manager requires that a similar structure should be deployed in AWS for high availability. N I oreover, a tracing framework is essential which can red cord data from both the client request and the downstream call to the database in AWS. Which hAWS services should you choose to implement the migration? (Select 3 Options)

A. Deploy an autoscaling group of Java backend servers to provide high availability

C. Create a DynamoDB database to hold subscriber data. Set up an autoscaling policy for the read/write throughput.

D.Use AWS X-Ray SDK to record data about incoming and outgoing requests. View the statistics graph in the X-Ray console.

auto scaling group of Java backend servers

dynamodb to hold subscribers data

use AWS X-Ray sdk to record data about incoming and outgoing request

Q147 You work in a video game company and your team is working on a feature that tells how many times that certain web pages have been viewed or clicked. You also created an AV VS Lambda function to show some key statistics of the data. You tested the Lambda function and it worked perfectly. However, your team lead requires you to show the statistics every day at 8:00AM GMT on a big TV screen so that when employees come into the office every morning, they have a rough idea of how the feature runs. What is the most cost efficient and straightforward way for you to make this happen?

A.Create an AWS CloudWatch Events rule that is scheduled using a cron expression as 00:08 Configure the target as the Lambda function.

using cron expression as 00:08 configure

Q148 A supermarket chain had a big data analysis system deployed in AWS. The system has the raw data such as clickstream or process logs in S3. A m3. large EC2 instance transformed the data to other formats and saved it to another S3 bucket. Amazon Redshift analyzes the data afterwards. Your team is in charge of improving the system using AWS Glue which is a fully managed ETL (extract, transform, and load) service. Which tasks can AWS Glue simplify during re-establishing the big data system? (Select TWO)

A. AWS Glue contains a crawler that connects to the S3 bucket and scans the dataset. Then the service creates metadata tables in the data catalog.

D. AWS Glue has a central metadata repository (data catalog). The data in the catalog is available for analysis immediately.

create metadata table

Glue Has central metadata repository

Q149 An AWS Solutions Architect has noticed that their company is using almost exclusively EBS General Purpose SSD (gp2) volume types for their EBS volumes. They are considering modifying the type of some of these volumes, but it is important that performance is not affected. Which of the following actions could the Solutions Architect consider? (Select TWO)

A. A 50GB gp2 root volume can be modified to an EBS Provisioned IOPS SSD (iol) without stopping the instance.

D. A 1TB gp2 volume that is attached to an instance as a non-root volume can be modified to a Throughput Optimized Hdd (st1) volume without stopping the instance or detaching the volume.
root volume modified to (io1)
non-root volume modified to (st1)

Q150 Which of the following are associated with using the "HLS" method of viewing the Kinesis video stream? (Select TWO)
A. A web application that is able to display the video stream using the third-party player Video.js.
D. Playback video by typing in the HLS streaming session URL in the location bar of the Apple Safari browser for debug purposes.
video.js
playback video by typing in HLS streaming

Q151 A team has just received a task to build an application that needs to recognize faces in streaming videos. They will get the source videos from a third party which uses a container format (M KV). The APP should be able to quickly add ress faces through the video in real time and I save the output in a suitable manner downstream to process. As recommended by the AWS Solutions Architect colleague: they would like to develop the service using AWS Rekognition. Which below options are needed to accomplish the task? Select 3.
B. A Kinesis video stream for sending streaming video to Amazon Rekognition Video. This can be done by using Kinesis u63 dautMedia API in Java SDK. The PutMedia operation writes video data fragments into a Kinesis video stream that Amazon Rekognitic pn Video consumes.
C. An Amazon Rekognition Video stream processor to manage the analysis of the streaming video. It can be used to start, stop, and manage stream processors according to needs.
F. A Kinesis data stream consumer to read the analysis results that Amazon Rekognition Video sends to the Kinesis data stream. It can be an Amazon EC2 instance by adding to one of Amazon Machine Images (AMIs). The consumer can be autoscaled by running it on multiple Amazon EC2 instances under an Auto Scaling group.
rekognition Video stream processor
Kinesis video stream that rekognition video consumes
Kinesis data stream consumer to read

Q152 A large company starts to use A WS organizations with consolidated billing features to manage its separate departments. The AWS operation team has just created 3 OUs (organization unit (3) with 2 AWS accounts each. To be compliant with company-wide security policy, Cloud Trail is required for all AWS accounts which have already been set up. However after some time, there are cases that users in certain OU have turned off the Cloud Trail of their accounts. What is the best way for the AWS operation team to prevent this from happening again?
A.Update the AWS Organizations feature sets to features and then create a Service Control Policies (SCP) to Prevent Users from Disabling AWS CloudTrail. This can be achieved by a deny policy with cloudtrail: StopLogging denied.
update AWS Organization feature sets

Q153 A mobile App developer just made an App in both IOS and Android that has a feature to count step numbers. He has used AWS Cognito to authorize users with a user pool and identity pool to provide

access to AWS DynamoDB tables. The App uses the DynamoDB table to store user subscriber data and number of steps. Now the developer also needs Cognito to it Integrate with Google to provide federated authentication for the mobile application users so that users do not need to remember extra login access. What should the developer do to make this happen for the IOS and Android App?
A. Amazon Cognito Identity pools (federated identities) support user authentication through federated identity providers- including Amazon. Facebook. Google, and SAML identity providers. The developer just needs to set up the federated identities for Google access
amazon cognito identity pools support

Q154 A big company has a service to process gigantic clickstream data sets which are often the result of holiday shopping traffic on a retail website, or sudden dramatic growth on the data network of a media or social networking site. It is becoming more and more expensive to analyze these clickstream datasets for its on-premise infrastructure. As the sample data set keeps growing fewer applications are available to provide a timely response. The service is using a Hadoop cluster with Cascading. How can they migrate the applications to AWS in the best way?
D. Put the source data to a Kinesis strearn and migrate the processing service to an AWS EMR cluster with Cascading. Enable EMR to directly read and query data from Kinesis streams. Write the output to Redshift.
enable EMR to directly read and query data from kinesis stream

Q155 An Artificial Intelligence startup company has used lots of EC2 instances. Some instances use SQL Server databases while the others use Oracle. As the data needs to be kept secure, regular snapshots are required. They want SQL Server EBS volume to take a snapshot every 12 hours. However for Oracle, it only needs a snapshot every day. Which option below is the best one that the company should choose without extra charge?
D. Add different tags for SQL Server and Oracle EBS volumes. In AWS Data Lifecycle Management console, create two management policies based on the tags. Add a 12 hours schedule to SQL Server lifecycle policy and a 24 hours schedule to Oracle lifecycle policy
add different tags for SQL server and oracle EBS

Q156 API gateway and Lambda non-pro zxy integrations have been chosen to implement an application by a software engineer. The application is a data analysis tool that returns some statistical results where the HTTP endpoint is called. The lambda needs to communicate with some back-end data services such as Keen io however there :are chances that error happens such as wror lg data requested, bad communications, etc. The lambda is written using Java and two exceptior Is may be returned which are BadRequestException and InternalErrorException. What should the software engineer do to map these two exceptions in API gateway with proper HTTP return codes? For example, BadRequestException and InternalErrorExcept on are mapped to HTTP return codes 400 and 500 respectively. Select 2
B. Add the corresponding error codes (400 and 500) on the Method Response in API gateway.
D. Add Integration Responses where regular expi ression patterns are set such as BadRequ lest or InternalError. Associate them with HTTP status codes
add error code on Method Response in API
add integration Response

Q157 An IT company owns a web product in AWS that provides discount restaurant information to customers. It has used one S3 Bucket (my_ bucket) to store restaurant data such as pictures, menus, etc. The product is deployed in VPC subnets. The company's Cloud Architect decides t o configure a VPC endpoint for this S3 bucket so that the performance will be enhanced. To be compliant to b security rules, it is required that the new VPC endpoint is only used to communicate with this specific S3 Bucket a and on the other hand, the S3 bucket only allows the read/write operations coming from this VPC endpoint. Which two options should the Cloud Architect choose to meet the security needs?
A. Use a VPC Endpoint policy for Amazon S3 to restrict access to the S3 Bucket 'my _bucket" so that the VPC Endpoint is only allowed to perform S3 actions on "my bucket" dpasson D. For the S3 bucket "my_ bucket", use a S3 bucket policy that denies all actions if the source VPC Endpoint is not equal to the endpoint ID that is created.
restrict access to S3 denies action if src vpc endpoint is no equal to endpoint id

Q158 You work for an ecommerce retailer as an AWS Solutions Architect. Your company is looking to improve customer loyalty programs by partnering with other third-parties to offer a more comprehensive selection of customer rewards. You plan to use Amazon Managed Blockchain to implement a blockchain network that allows your company and third-parties to share and validate rewards information quickly and transparently. How do you add members for this blockchain?
A. When Amazon Managed Blockchain is set up, there is an initial meml per in the AWS account. Then new members can be added in this AWS account without having to send an invitation, or a network invitation can be created for a member in a differ rent AWS account
when Amazon managed blockchain is set up

Q159 A company has deployed an application to multiple environments in AWS, including production and testing. The company has separate accounts for production and testing, and users are allowed to create additional application users for team members or services, as needed. The Security team has asked the Operations team 1 for better isolation between production and testing with centralized controls on security credentials and improved management of permissions between environments. Which of the following options would MOST securely accomplish this goal?
Create a new AWS account to hold user and service accounts, such as an identity account. Create users and groups in the identity account. Create roles with appropriate permissions in the production and testing accounts. Add the identity account to the trust policies for the roles.
create identity account

Q160 The CISO of a large enterprise with multiple IT departments, each with its own AWS account, wants one central place where AWS permissions for users can be managed and users authentication credentials can be synchronized with the company's existing d in-premises solution. Which solution will meet the CISO's requirements?
A. Define AWS IAM roles based on the functional responsibilities of the users in a central account. Create a SAML-based identity management provider. Map users in the on-premises groups to IAM roles. Establish trust relationships between the other accounts and the central account.
define AWS IAM roles based on functional responsibility of uses

Q161 A large company has increased its utilization of AWS over time in an unmanaged way. As such, they have a large number of independent AWS accounts across different business units, projects and

environments. The company has created a Cloud Center of Excellence team, which is responsible for managing all aspects of the AWS Cloud, including their AWS accounts. Which of the following should the Cloud Center of Excellence team do to BEST address their requirements in a centralized way? (Select two.)

D. Set up AWS Organizations. Enable consolidated billing, and link all existing AWS accounts to a master billing account. Tag all AWS resources with details about the business unit, project and environment. Analyze Cost and Usage reports using tools such as Amazon A thena and Amazon QuickSight to collect billing details by business unit.

E. Using a master AWS account, create IAM users within the master account. Define IAM roles in the other AWS accounts: which cover each of the required functions in the accour it. Follow the policy of least privilege in assigning permissions to each role, then enable the . IAM users to assume the roles that they need to use.

set up AWS Organizations

using a master AWS account, create IAM

Q162. To abide by industry regulations, a Solutions Architect must design a solution that will store a company's critical data in multiple public AWS Regions, including in the United States, where the company's headquarters is located. The Solutions Architect is required to provide access to the data stored in AWS to the company's global WAN network. The Security team mandates that no traffic accessing this data should travese the public internet. How should the Solutions Architect design a highly available solution that meets the requirements and is cost-effective?

D. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WANT t o send traffic over a DX connection. Use Direct Connect Gateway to access data in other AWS Regions.

use Direct Connect Gateway to access data

Q163 A company wants to manage the costs associated with a group of 20 applications that are critical, by migrating to AWS. The applications are a mix of Java and Node.js spread across different instance clusters. The company wants to minimize costs while standardizing by using a single deployment methodology. Most of the applications are part of month-end processing routines with a small number of concurrent users, but they are occasionally run at other times. Average application memory consumption is less than 1 GB, though some applications use as much as 2.5 GB of memory during peak processing. The most important application in the group is a billing report written in Java that accesses multiple data sources and often for several hours. Which is the MOST cost-effective solution?

B. Deploy Amazon ECS containers on Amazon EC2 with Auto Scaling configured for memory utilization of 75%. Deploy an ECS task for each application being migrated with ECS task scaling. Monitor services and hosts by using Amazon Cloud Watch

deploy Amazon ESC container on EC2

Q164 A Solutions Architect must build a highly available infrastructure for a popular global video game that runs on a mobile phone platform. The application runs on Amazon EC2 instances behind a 1. Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The database tier is an Amazon RDS MySQL Multi-AZ instance. The entire application stack is deployed in both us-east-1 and eu-central-1. Amazon Route 53 is used to route traffic to the two installations using a latency-based routing policy. A weighted routing policy is configured in Route 53 as a failover to another region in case the installation in a region becomes unresponsive. During the testing of disaster recovery

scenarios, after blocking access to the Amazon RDS MySQL instance in eu-central-1 from all the application instances running in that region. Route 53 does not automatically failover all traffic to us-east-1 Based on this situation. Which changes would allow the infrastructure to failover to us-east-1?(Choose two.)

C. . Set the value of Evaluate Target Health to Yes on the latency alias resources for both eu-central-1 and us-east-1.

D. Write a URL in the application that performs a health check on the database layer. Add it as a health check within the weighted routing policy in both regions.

set value of Evaluate Target Health to YES

write URL in app

Q165 An online e-commerce business is running a workload on AWS. The application architecture includes a web tier, an application tier for business logic, and a database tier for user and transactional data management. The database server has a 100 GB memory requirement. The business requires cost-efficient disaster recovery for the application with an RTO of 5 minutes and an RPO of 1 hour. The business also has a regulation for out-of-region disaster recovery with a minimum distance between the primary and alternate sites of 250 miles. Which of the following option Is can the Solutions Architect design to create a comprehensive solution for this customer that meets the disaster recovery requirements?

C. Use a scaled-down version of the fully functional production environment in the alternate region that includes one instand te of the web server, one instance of the application server, and a replicated instance of the database server in standby mode. Place the web and the application tiers in an Auto Scaling behind a load balancer," which can automatically scale when the load arrives to the application. Use Amazon Route 53 to switch traffic to the alternate region.

use scaled-down version of fully functional production environment

Q166 A company runs a memory-intensive analytics application using on-demand Ar nazon EC2 compute optimized instances. The application is used continuously and application demand doubles during working hours. The application currently scales based on CPU usage. When scaling occurs, a lifecycle hook is used because the instance requires 4 minutes to clean the application state before terminating. Because users reported poor performance during working hours; scheduled scaling activ bns were implemented so additional instances would be added during working hours. The Solutions Architect has been asked to reduce the cost of the application. Which solution is MOST cost-effective?

D. Create a new launch configuration using R5 instances; and update the application AMI to include the Amazon Cloud Watch agent. Change the Auto Scaling policies to scale based on memory utilization. use Reserved Instance: s for the number of instances required after working hours, and use Standard Reserved Instances with On-Demand Instances to cover the increased demand during working hours.

create new launch configuration using R5 instance

Q167 A company wants to follow its website or 1AWS using serverless architecture design patterns for global customers. The company has outlined its requirements as follows:--The website should be responsive. The website should offer minimal latency. - The website should be highly available. -Users should be able to authenticate through social identity providers such as Google e,Facebook, and Amazon. -There should be baseline DDoS protections for spikes in traffic. How can the design requirements be met?

C. Use Amazon CloudFront with Amazon S3 for hosting static web resources. Use Amazon Cognito to provide user management authentication functions. Use Amazon API Gateway with AWS Lambda to build an API.
use Amazon cloudfront with S3 for hosting static web resource

Q168 A company is currently using AWS CodeCommit for its source control and AWS CodePipeline for continuous integration. The pipeline has a build stage for building the artifacts which is then staged in an Amazon S3 bucket. THe company has identified various improvement opportunities in the existing process, and a Solutions Architect has been given the following requirement:--Create a new pipeline to support feature development -Support feature development without impacting production applications -Incorporate continuous testing with unit tests -Isolate development and production artifacts -Support the capability to merge tested code into production cod le. How should the Solutions Architect achieve these requirements?
A. Trigger a separate pipe line from CodeCommit feature branches. Use AW 7S CodeBuild for running unit tests. Use CodeBu: ild to stage the artifacts within an S3 bucket in a separate testing account.
Use AWS CodeBuild for running unit tests

Q169 A company runs an ordering system or 1AWS using Amazon SQS and AWS Lambda, with each order received as a JSON 1 message. Recently the company had a marketing event that led to a tenfold increase in orders. With this increase, the following undesired behaviors started in the ordering system:-Lambda failures while processing orders lead to queue backlogs. -The same orders have been processed multiple times. A solutions Architect has been asked to solve the existing issues with the ordering system and add the following resiliency features.-Retain problematic orders for analysis. -Send notification if errors go beyond a threshold value. How should the Solutions Architect meet these requirements?
A.Receive multiple messages with each Lambda invocation, add error handling to message processing code and delete messages after processing. increase the visibility timeout for the messages, create a dead letter queue for messages that could not be processed, create an Amazon or CloudWatch alarm on Lambda errors for notification.
add error handling to message processing code , create dead letter queue

Q170 An organization has recently grown through acquisitions. Two of the purchased companies use the same IP CIDR range. There is a new short-term requirement to allow Any Company A (VPC-A) to communicate with a server that has the IP address 10.0.0.77 in AnyCompany B(VPC-B). AnyCompany A must also communicate with all resources in AnyCompany C (VPC-C). The Network team has created the VPC peer links, but it is having issues with communications between VPC-A and VPC-B. After an investigation, the team believes that the routing tables in the VPC's are incorrect.What configuration will allow AnyCompany A to communicate with Any Company C in addition to the database in Any Company B?
D. On VPC-A, create a static route for the VPC-B CIDR (10.0.77/32) database across VPC peer pCX-AB. Create a statiC route for the VPC-C CIDR on VPC peer pcx-AC. On VPC-B, create a static route for VPC-A CIDR (172.16.0.0124) on peer pcx-AB.On VPC-C create a static route for VPC-A CIDR (172.16.0.01 24) across peer pcx-AC.
on VPC-A,create static route for VPC-B CIDR(10.0.0.77/32)

Q171 A company is planning to set up a REST API application on AWS.The application team wants to set up a new identity store on AWS. The IT team does not want to maintain any infrastructure or servers for this deployment. What is the MOST operationally efficient solution that meets these requirements?
C. Deploy the application as AWS Lambda functions. Set up Amazon API Gateway REST API endpoints for the applic ation.Set up an Amazon Cognito user pool, and configure an Amazon Cognito authorizer
deploy app as Lambda function. set up Cognito user pool

Q172 A retail company is running an application that stores invoice files in Amazon S3 bucket and metadata about the files in an As nazon. The S3 bucket and DynamoDB table are in us-east-1. The company wants to protect itself from data corruption and loss of connectivity to either Region. Which option meets these requirements?
D. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us- east-1. Set up S3 cross-region replication from us-east-1 to eu-west-1.
enable continuous backup, setup S3 cross-region replication

Q173 A company wants to launch an online shopping website in multiple countries and must ensure that customers are protected against potential 'man- in-the-middle' attacks. Which architecture will provide the MOST secure site access?
A.Use Amazon Route 53 for domain registration and DNS services. Enable DNSSEC for all Route 53 requests. use AWS Certificate Manager (ACM) to register TLS/SSL certificates for the shopping website, and use Application Load Balancers configured with those TLS/SSL certificates for the site. Use the Server Name Identification extension in all client requests to the site.
use Route 53 for domain registration and DNS

Q174 A company is creating an account strategy so that they can begin using AWS. The Security team will provide each team with the permissions they need to follow the principle of least privileged access. Teams would like to keep their resources isolated from other groups, and the Finance team would like each team's resource usage separated for billing purposes. Which account creation a process meets these requirements and allows for changes?
D. Create a master account for billing using Organizations: and create each team 's account from that master account. Create a security account for logs and cross-account access. Apply service control policies on each account, and grant the Security team cross-account access to all accounts. Security will create IAM policies for each account to maintain least privilege access.
create master account for billing

Q175 A company has a 24 TB MySQL database in its on-premises data center that grows at the rate of 10 GB per day. The data center is connected to the company's AWS infrastructure with a 50 Mbps VPN connection. The company's migrating the application and workload to AWS The application code is already installed and tested on Amazon EC2. The company now need to migrate the database and wants to go live or tAWS within 3 weeks. Which of the following approaches meets the schedule with LEAST downtime?

C.1. Create a database expd prt locally using database- native tools. 2. Import that into AWS using AWS Snowball. 3. Launch at Amazon RDS Aurora DB instance. 4. Load the d lata in the RDS Aurora DB instance from the e: sport. 5. Set up database replication from the or r-premises database to the RDS Aurora DB instance over the VPN. 6. Change the DNS entry to point to the RDS Aurora DB instance. 7. Stop the replication.
create a db export locally using db-native tools. 不要 take app offline

Q176 A company wants to allow its Marketing team to perform SQL queries on customer records to identify market segments. The data is spread across hundreds of files. The records must be encrypted in transit and at rest. The Team Manager must have the ability to manage users and groups, but no team members should have access to services or 1 esources not required for the SQL queries. Additionally, Administrators need to audit the queries made and receive notifications when a query violates rules defined by the Security team. AWS Organization has been used to create a new accd punt and an AWS IAM user with administrator permissions for the Team Manager. Which design meets these requirements?
B. Apply a service control policy (SCP) that denies access to all services except IAM, Amazon Athena, Amazon S3, and AWS CloudTrail. Store customer record files in Amazon S3 and train users to execute queries using the CL I via Athena. Analyze CloudTrail events to audit and alarm on queries against personal data.
store customer record files in S3 and train uses to execute queries using CLI via Athena

Q177 A Solutions Architect is responsible for redesigning a legacy Java application to improve its availability, data durability, and scalability. Currently, the application runs on a single le high-memory Amazon EC2 instance. It accepts HTTP requests from upstream clients, adds the n to an in-memory queue, and responds with a 200 status. A separate application thread reads items from the queue, processes them. and persists the results to an Amazon RDS MySQL instance. The processing time 1 for each item takes 90 seconds on average. I nost of which is spent waiting on external service calls, but the application is written to process multiple items in parallel. Traffic to this service is unpredictable. During periods of high load. items may sit in the internal queue for over an hour while the application processes the backing. In addition, the current system has issues with availability and data if the single application node fails. Clients that access this service cannot be modified. They expect to receive a response to each HTTP request they send within 10 seconds before they will time out and retry the request. Which approach would improve the availability and durability of the system while decreasing the processing latency and minimizing costs?
B. Create an Amazon API Gateway REST API that uses a service proxy to put items in an Amazon SQS queue. Extract the core processing code from the existing application and update it to pull items from Amazon SQS queue. Extract the core processing code from the existing application and update it to pull items from Amazon SQS ins stead of an in-memory queue. Deploy the new processing application to smaller EC2 instances within an Auto Scaling group that scales dynamically based on the approximate number of messages in the Amazon SQS queue.
put items in Amazon SQS queue

Q178 A solutions architect is designing a disaster recovery solution for a critical workload. The workload stores data in an Amazon S3 bucket that uses server-side encryption and CMK. The company must comply with an RPO of 15 minutes or less for s3 stored objects across different geographic applications in the same AWS acc bunt.Objects stored in Amazon s3 need to be at least 99.99% compliant with RPO requirements In the event of a disaster, the company needs to be at le to recover individual files and

objects in different Regions. The solution should require minimal security changes. Which combination of stops should the solutions architect take? (Select THREE)
A. Use Amazon EventBridge to schedule an AWS Lambda function with an elev: ated IAM role to copy objects to a different S3 bucket every 15 minutes.:
B. Grant additional permissions to the IAM role for the s3GetObjectVersionF prReplication and kms Decrypt, kms Encrypt actions to be able to replicate encrypted objects.
D. In the Destination configuration, add the symmetric AWS KMS CMK and explicitly opt in by enabling replication of encrypted objects using the SourceSolectionCriteria element.
use amazon EventBridge
IAM role for s3 GetObjectVersonForReplication
add symmetric AWS KMS CMK

Q179 A company has a website that enables users to upload videos Company policy states that the uploaded videos must be analyzed for restricted content. An uploaded video is placed in Amazon S3, and a message is pushed to an Amazor 1. SQS queue with the video's location A backend application pulls this location from Amazon SQS and analyzes the video. The video analysis is compute-intensive and occurs sporadically during the day. The website scales with demand The video analysis application runs on a fixed number of instances. Peak demand occurs during the holidays, so the company must add instances to the application during this time. All instances used are currently on-demand Amazon EC2 T2 instances. The company wants to reduce the cost of the current solution. Which of the following solutions is MOST cost-effective?
B. Keep the website on T 2 instances. Determine the minimum number of website instances required during off-peak times and use Reserve ved instances to cover them while using On-Demand Instances to cover peak demand. Use Spot Fleet for the video analysis application comprised of Amazon EC2 C4 and Amazon EC2 C5 Spot Instances.
keep a website on T2 instances. use Spot Fleet for video analysis

Q180 A company has an Amazon VPC that is divided into a public subnet and a private subnet. A web application runs in Amazon VPC, and each subnet has its own NACL. The public subnet has a CIDR of 10.0.0.0.0124. An Application Load Balancer is deployed to the public subnet. The private subnet has a CIDR of 10.0.10/24. Amazon EC2 instances that run a web server on port 80 are launched into the private subnet. Only network traffic that is required for the Application Lq pad Balancer to access the web application can be allowed to travel between the public and private subnets. What collection of rules should be written to ensure that the private subnet's NACL meets the requirement? (Choose two.)
B. An inbound rule for port 80 from source 10.0.0.0124.
E. An outbound rule for ports 1024 through 65535 to destination 10.0.0.0124.
inbound: port 80:ip24
outbound: port:1024:

Q181 A company's CISO has asked a S plutions Architect to re-engineer the company's Current CIVCD practices to make sure 1 patch deployments to its application can happen as quickly a possible with minimal downtime if vulnerabilities are discovered The company must also be able to quickly roll back a change in case of errors. The we b application is deployed in a fleet of Amazon . EC2 instances behind an Application Load balancer. The company is currently using Github to host the application source code and has configured an AWS CodeBuild project to build the application : The company also intends to use

AWS CodePipeline to trigger builds from Github commits using the existing CodeBuild project. What CI/CD configuration meets all of the requirements?
B. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for blue green deployments Monitor the new y deployed code, and if there are any issues, trigger a manual rollback using CodeDeploy.
deploy stage using AWS CodeDeploy config for blue/green

Q182 A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket. The company requires that only authenticated users are allowed to post content." The application generates a presigned URL that is used to upload objects through a browser interface. Most users are reporting slow upload times for objects larger than 100 MB. What can a Solutions Architect do to improve the performance of these uploads while ensuing only authenticated users are allowed to post content?
C. Enable an S3 Transfer Acceleration endpoint on the S3 bucket. Use the endpoint when generating the presigned URL. Have the browser interface upload the objects to this URL using the S3 multipart upload Apl.
enable S3 Transfer Acceleration endpoint

Q183 A company has an application that uses Amazon EC2 instances in an Auto Scaling group. The Quality Assurance(QA) department needs to launch a large number of short-lived environments to test the application. The application environments are currently launched by the Manager of the department using an AWS Cloudformation template. To launch the stack, the Manager uses a role with permission to use Cloudformation.EC 2 and Auto Scaling APIs. The Manager wants to allow testers to launch their own environments. but does not want to grant broad permissions to each user. Which set up would achieve these goals?
B. Create an AWS Service Catalog product from the environment template. Add a launch constraint to the product with the existing role. Give users in the QA department permission to use AWS Service Catalog APIs only. Train users to launch the template from the AWS Service Catalog console.
create AES Service Catalog product from env template

Q184 A financial services company logs personally identifiable information to its application logs stored in Amazon S3. Due to regulatory compliance requirements, the log files must be encrypted at rest. The Security team has mandated that the company's on-premises hardware security modules (HSMI) be used to generate the CMK material. Which steps should the Solution Architect take to meet these requirements?
C. Create a CMK in AWS KMS with no key material and an origin of EXTERNAL. Import the key material generated from the on-premises HSMs into the CMK using the public key and import token provided by AWS. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.
create CMK with no key material

Q185 A company has several teams, and each team has their own Amazon RDS database that totals 100 TB. The company is building a dataquery platform for Business Intelligence analysts to generate a weekly business report. The new system must run ad-hoc SQL queries. What is the MOST cost- effective solution?

D. Use an AWS Glue crawler to crawl all the databases and create tables in the AWS Glue Data Catalog. Use an AWS Glue ETL job to load data from the RDS databases to amazon S3, and use amazon Athena to run the queries.
use AWS Glue crawler

Q186 A company needs to move its on-premises resources to AWS.Th e current environment consists of 100 virtual machines(VMS) with a total of 40 TB of storage. Most of the VMS can be taken offline because they support functions during business hours only, however some are mission critical. so downtime must be-minimized. The Administrator of the on-premises network provisioned 10 Mbps of internet bandwidth for the migration. The on- premises network throughput has reached capacity and would be costly to increase. A Solutions Architect must design a migratic in solution that can be performed within the next 3months Which method would fulfill these requirements?
D. Migrate mission-critical VMs w ith AWS SMS Export the other VMs locally and transfer them to Amazon S3 using AV VS snowball Use VM Import Export to import the VMs into Amazon EC2
migrate mission-critical VMs

Q187 A company has a website that enables users to upload videos. Company policy states the uploaded videos must be analyzed for restricted content. An uploaded video is placed in Amazon S3 and a message is pushed to an Amazon SQS queue with the video location. A backend application pulls this location from Amazon SQS and analyzes the video. The video analysis is compute-intensive and occurs sporadically during the day. The website scales with demand. The video analysis application runs on a fixed number of instances. Peak demand occurs during the holidays , so the company must add instances to the application during this time . All instances used are currently on-demand Amazon 1 EC2 T2 instances. The company want s to reduce the cost of the current solution. Which of the following solutions is MOST cost-effective?
B. Keep the website on T2 instances Determine the minimum number of website instances required during off-peak times and use Reserved Instances to cover them while using On-Demand instances to cover peak demand. Use Spot Fleet for the video analysis application comprised of Amazon EC2 C4 and Amazon EC2 C5 Spot Instances
keep a website on T2 instances. use Spot Fleet for video analysis

Q188 A company's main intranet page has experienced degraded response times as its user base has increased although there are no reports of users seeing error pages. The application uses Amazon DynamoDB in read-only mode. Amazon DynamoDB latency metrics for successful 1 requests have been in a steady state even during times when users have reported degradation. The Development team has correlated the issue to Provisioned Throughput Exceeded exceptions in the application logs when doing Scan and read operations The team also identified an access pattern of steady spikes of read activity on a distributed set of individual data items. The Chief Technology Officer wants to improve the user experience. Which solutions will meet these requirements with the LEAST amount of changes to the application? (Choose two.)
B. Enable DynamoDB Auto Scaling to manage the throughput capacity as table traffic increases. Set the upper and lower limits to control costs and set a target utilization given the peak usage and how quickly the traffic changes.
D. Implement the DynamoDB Accelerator DAX) client and provision a DAX cluster with the appropriate node types to sustain the application load. Tune the item and query cache configuration for an optimal user experience.

enable DynamoDB Auto scaling
implement DynamoDB Accelerator(DAX)

Q189 A company is having issues with a newly deployed serverless infrastructure that uses Amazon API Gateway, Amazon Lambda, and Amazon Dynamodb. In a steady state, the application performs as expected. However, during peak load, tens of thousands of simultaneous invocations are needed and user requests fail multiple times before succeeding. The company has checked the logs for each component, focusing specifically on Amazon Cloudwatch Logs for Lambda. There are no errors logged by the services or applications. What might cause this problem?
C. The throttle limit set on API Gateway is very low. During peak load. the additional requests are not making their way through to lambda.
throttle limit set on API Gateway is low

Q190 A company recently transformed its legacy infrastructure provisioning scripts to AWS Cloudformation templates. The newly developed templates are hosted in the company's private Github repository. Since adopting Cloudforma tion, the company has encountered several issues with updates to the Cloudformation templates, causing failed executions or creating unstable environments Management isconcemed by the increase in errors and has asked a Solutions Architect to design the automated testing of Cloudformation template updates. What should the Solutions Architect do to meet these requirements?
C. Use AWS Codepipeline to create and execute a change set from the Cloud I formation templates stored in the private : Github repository. Configure a CodePipeline action to test the deployment with testing scripts run by AWS Codebuild
config a code pipeline action

Q191 An enterprise company wants to implement cost controls for all its accounts in AWS Organizations, which has full features en abled.The company has mapped organizational units(OUs) to its business units, andit wants to bill these business units for their individual AWS spending. There has been a recent spike in the company's AWS bill, which is generating attention from the Finance team. A Solutions Architect needs to investigate the cause of the spike while designing a solution that will track AWS costs in Organizations and I generate a notification to the required teams if costs from a business unit exceed a specific monetary threshold. Which solution will meet these requirements?
C. Use Cost Explorer to troubleshoot the reason for the additional costs. Create a budget using AWS Budgets with the monetary amount set by the Finance team for each OU by grouping the linked accountsConfigure an Amazon SNS notification to the required teams in the budget.
use Cost Explorer, Create budget using AWS Budgets with monetary amount

Q192 A company provides AWS solutions to its users v TAws Cloudformation templates. Users launch the templates in their accounts to have different solutions provisioned for them. The users want to improve the deployment strategy for solutio pns while retaining the ability to do the following: -Add their own features to a solution for their specific deployments -Run unit tests on their changes - Turn features on and off for their deployments. Automatically update with code changes. -Run security scanning tools for their deployments Which strategies should the Solutions Architect use to meet the requirements?
D. Allow users to download solution code artifacts Use AWS Codecommit and Aws Codepipeline for the CI/CD pipeline Use the AWS Cloud Development Kit constructs for different solution

features, and use the manifest file to turn features on and off. Use AWS Codebuild to run unit tests and security scans, and for deploying and updating a solution with changes
use manifest file to turn features on/off

Q193 A company is operating a large customer service call center, and stores and processes call recordings with a custom application Approximately 2% of the call recordings are transcribed by an offshore team for quality assurance purposes. These recordings take up to 72 hours to be transcribed. The recordings are stored on an NFS share before they are archived at an offsite location after 90 days. The company uses Linux servers fc r processing the call recordings and managing the transcription queue. There is also an application for the quality assurance staff to review and sco re call recordings. The company plans to migrate the system to AWS to reduce storage costs and the time required to transcribe calls. Which set of action ns should be taken to meet the company's objectives?
A.Upload the call recordings to Amazon S3 from the call center. Set up an $3 lifecycle policy to move the call recordings to Amazon S3 Glacier O after 90 days. Use an AWS Lambda trigger to transcribe the callcordings with Amazon Transcribe. Use Amazon S3, Amazon AP Gateway, and Lambda to host the view and scoring application
upload call recordings to S3 from call center, transcribe call recordings with Amazon Mechanical Turk

Q194 A Solutions Architect is building a containerized NET Core application I that will run in AWS Fargate The backend of the application requires Microsoft SQL Server with high availability All tiers of the application must be highly available The credentials used for the connection string to SQL Server should not be stored on disk within the NET Core front-end containers. Which strategies should the Solutions Architect use to meet these requirements'?
B. Create a Multi-az deployment of SQL Server on Amazon RDS. Create a secret in AWS Secrets Manager for the credentials to the RDS database. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading irito the application to construct the connection string Set up the NET Core service in Fargate using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones
create multi-az deployment, create Amazon ECS task execution role

Q195 A company has an internal AWS Elastic Beanstalk worker environment inside a VPC that must access an external payment gateway API available on an HTTPS endpoint on the public internet. Because of security policies, the payment gateways Application team can grant access to only one public IPaddress. Which architecture will set u p an Elastic Beanstalk environment to access the company's application without making multiple changes on the company's end?
A.Configure the Elastic Beanstalk application to place Amazon EC2 instances in a private subnet with an outbound route to a NAT gaay in a public subnet Associate an Elastic IP address to the NA gateway that can be whitelisted on the payment gateway application side.
associate Elastic IP address to NA gateway

Q196 A Solutions Architect is building a solution for updating user metadata that is initiated by web servers. The solution needs to rapidly scale from hundreds to tens of thousands of jobs in less than 30

seconds. The solution must be asynchronous, always avertable and minimize costs. Which strategies should the Solutions Architect use to meet these requirements?
B. Create an AWS Lambda function that will update user metadata. Create an Amazon SQS queue and configure it as ar levent source for the Lambda function. Update the web application to send jobs to the queue.
create Amazon SQS queue and config it as event source

Q197 A company is migrating from on-premises to AWS and has just deployed the first set of applications that run on Linux. The company will continue to maint-pretraffic from the on-premises hosts to AWS The company wants to reduce the cost of the solution andlans to gradually migrate its entire workload to AWS. Which solution will meet these requirements?
A.Establish a VPN connection between on-premises and the VPC. Create IAM roles and permissions to enable AWS Systems Manager Session Manager. Install Systems Manager Agent and enable Systems Manager. Create IAM users and tags based on policy restrictions
establish vpn connection, create IAM roles

Q198 A Solutions Architect needs to design a highly available application that will allow authenticated users to stay connected to the application even when there are underlying failures. Which solution will meet these requirements?
B. Deploy the application on Amazon EC2 instances in an Auto Scaling group Use an internet-facing Application Load Balancer to handle requests. Use Amazon DynamoDB to save the authenticated connection details.
deploy app on EC2 in auto scaling group, use Amazon DynamoDB to save authenticated connection

Q199 A Solutions Architect is designing the data storage and retrieval architecture for a new application that a company will be launching soon. The application is designed to ingest millions of small records per minute from devices all around the world. Each record is less than 4 KB in size and needs to be stored in a durable location where it can be retrieved with low latency. The data is ephemeral and the company is required to store the data for 120 days only, after which the data can be deleted. The Solution Architect calculates that, during the course of a year, the storage requirements would be about 10-15 TB. Which storage strategy is the MOST cost-effective for the design requirements?
B. Design the application to store each incoming record in an Amazon Dynamodb table properly configured for the scale, Congui the Dynamodb Time to Live(TTL) feature to delete records older than 120 days.
store incoming record in Dynamodb

Q200 An enterprise company wants to allow its Developers to purchase third-party software through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled. and has a shared services account in each organization unit (OU) that will be used by Procurement Managers, The Procurement team's policy indicates that Developers should be able to obtain third-party software from an approved list only Private Marketplace in AWS Marketplace to achieve this requirement,The Procurement team wants administration of Private Marketplace to be restricted to a role users, groups, roies, and account administrators in the company should be denied Private Marketplaceadministrative access. What is the MOST efficient way to design an architecture to meet these requirements?

C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization. Add the AWSPrivateMarketp laceAdminFullAccess managed policy to the role. Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.
create IAM role in all shared services accounts

Q201 A company has an internal application running on AWS that is used to track and process shipments in the company's warehouse. Currently, after the system receives an order, it emails the staff the information needed to ship a package. Dnce the package is shipped, the staff replies to the email and the order is marked as shipped. The company wants to stop using email in the application and move to a serverless application model. Which architecture solution meets these requirements?
C. Update the application to store new order information in Amazon Dynamodb When a new order is created, trigger an AWS Step Functions workflow mark the orders as "in progress. 'and print a package label to the warehouse. Once the label has been scanned and fulfilled, the application will trigger an AWS Lambda function that will mark the order as shipped and comp lete the workflow update app to store new order in Dynamodb
update app to store new order in Dynamodb

Q202 A manufacturing company has grown exponentially and has secured funding to improve its IT infrastructure and ecommerce presence. The company's e commerce platform cd insists of :--Static assets primarily comprised of product images stored in Amazon s3 --Amazon in Dynamodb tables that store product information, use r information, and order information --Web servers containing the applications front-end behind Elastic Load BalancersThe company wants to set up a disaster recovery site in a separate Region. Which combination of actions should the solutions Architect take to implement the new design while meeting all the requirements? (Select THREE)
A. Enable Amazon Route 53 health checks to determine if the primary site is down, and route traffic to the disaster recovery site if there is an issue
B. Enable Amazon S3 cross-region replication on the buckets that contain static assets D. Enable Dynamodb global tables to achieve a multi-region table replication enable Route53 health checks enable S3 cross-region replication enable Dynamodb global tables
enable Route53 health checks
enable S3 cross-region replication
enable Dynamodb global tables

Q203 A customer has a website which shows all the deals available across the market. The site experiences a load of 5 large EC2 instances. However, a week before Thanksgiving vacation they encounter a load of almost 20 large instances. The load during that period varies over the day based on the office timings. Which of the below mentioned solutions is cost effective as well as help the website achieve better performance?
A.Setup to run 10 instances during the pre-vacation period and only scale up during the office time by launching 10 more instances using the AutoScaling schedule. setup to run 10 stances
setup to run 10 stances

Q204 A fleet of Amazon ECS instances is used to poll an Amazon sQS queue and update items in an Amazon Dynamodb database Items in the table are not being updated and the SQS queue is filling up 3. Amazon Cloudwatch Logs are showing consistent 400 errors when attempting leg to update the table. The Provisioned write capacity units are appropriately configured, and no throttling is occurring. What is the likely cause of the failure?

D. The ECS task role was modified ECS task role was modified

ECS task role was modified

Q205 A company recently transformed its legacy infrastructure provisioning scripts to AWS Cloudformation templates. The newly developed templates are hosted in the company's private Github repository. Since Adopting CloudFormation, the company has encountered several issues with updates to the CloudFormation templates, causing failed executions or creating unstable environments. Management is concerned by the increase in errors and has asked a Solutions Architect to design the automated testing of Cloudformation template updates. What should the solutions architect do to meet these requirements?

C. Use AWS Codepipeline to create and execute a change set from the Cloud Formation and templates stored in the private Github Repository Configure a Code Pipeline action to test the deployment with testing scripts run by AWS Codebuild use AWS CodePipeline to create/execute change set

use AWS CodePipeline to create/execute change set

Q206 A company is hosting a three-tier web application in an on-premises environment. Due to a recent surgegement has ordered traffic that resulted in downtime and a significant financial impact, the company that the application be moved to Aws, The application is written in NET and has a dependency on aMYSQL database. A Solutions Architect must design a Scalable and highly available solution to meet the demand of 200, OOO daily user. Which steps should the solutions Architect take to design an appropriate solution?

B. Use AWS Cloudformation to launch a stack containing an Application Load Balancer(ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones. The stack should launch a Multi-az deployment of an Amazon Aurora MYSQL DB cluster with a Retain deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB use AWS Cloudformation to launch a stack containing an ALB in front of EC2 Auto Scaling group

use AWS Cloudformation to launch a stack containing an ALB in front of EC2 Auto Scaling group

Q207 A company is migrating its applications on AWS. The applications will be deployed to AWS accounts owned by business units. The company has several teams of Developers who are responsible for the development and maintenance of all applications. The company is expecting rapid growth in the number of users. The company's Chief technology Officer has the following requirements -Developers must launch the AWS infra structure using AWS Cloudformation -Developers must 1 not be able to create resources outside of Cloud Formation - The solution must be able to scale to hundreds of AWS accounts; Which of the following would meet these requirements? (Select Two)

A. Using Cloudformation, create an IAM role that can be assumed by Cloud Formation that has permissions to Create all the resources the company needs , Use Cloudformation stack sets to deploy this template to each AWS Account

C. Using Cloud Formation, create an IAM role that can be assumed by Developers, and lattach policies that allow interaction with and passing a role information Attach an inline policy to deny access all other AWS services Use Cloudformation Stack Sets to deploy this template to each As account
using CloudFormation, create IAM role be assumed by CloudFormation using CloudFormation, create IAM role be assumed by Developers

Q208 During an audit, a Security team discovered that a development team was putting IAM user secret access keys in their code and then committing it to an AWS ode Commit repository. The Security team wants to automatically find and remediate instances of his security Vulnerability Which solution will ensure that the credentials are appropriately secured automatically?
D. Configure a Code Commit trigger to invoke an AWS Lambda function to scan new code submissions for credentials. If credentials are found, disable them in AWS IAM and notify the user. config a Code Commit trigger to invoke Lambda function
config a Code Commit trigger to invoke Lambda function

Q209 A company currently has data hosted in an IBM Db2 database. A web application calls an AP that runs stored procedures on the database to retrieve user information data that i s read-only. This data is historical in nature and changes on a daily basis. When a user logs in to the application's data needs to be retrieved within 3 seconds. Each time a user logs in, the stored procedures run. User s log in several times a day to check stock prices. Running this database has become cost-prohibitive due to Db2 CPU licensing. Performance goals are not being met. Timeouts from Db2 are common due to long- running quenes. Which approach should a Solutions Architect take to migrate this solution to AWS?
B. Use AWS DMS to migrate data to Amazon Dynamodb using a continuous replication task Refactor the API to use the Dynamodb data Implement the refactored API in Amazon API Gateway and enable API use AWS DMS to migrate data to Dynamodb
use AWS DMS to migrate data to Dynamodb

Q210 A Solutions Architect is designing a deployment strategy for an application tier and has the following requirements.-The application code will need a 500 GB static dataset to be pre sent before application startup. -The application tier must be able to scale up and down based on demand with as little startup time as possible. --The Development team should be able to update the code multiple times each day.--Critical operating system(OS)patches must be installed within 48 hours of being released. Which deployment strategy meets these requirements?
A.Use AWS Systems Manager to create a new AMI with the updated OS patches. Update the autoScaling group to use the patched AMI and replace existing unpatched instances, Use Aws CodeDeploy to push the application code to the instances. store the static data in amazon efs use AWS System Manager, user AWS CodeDeploy to push app code
use AWS System Manager, user AWS CodeDeploy to push app code

Q211 A large company with hundreds of AWS accounts has a newly established centralized internal process for purchasing new or modify existing Reserved Instances. This process requires all business units that want to purchase or modify reserved Instances to submit requests to a dedicated team for procurement or execution. Previously business units would directly purchase or modify

ReservedInstances in their own respective AWS accounts autonomously. Which combination of steps should be taken to proactively enforce the new process in the Most secure way possible?
A. Ensure all AWS accounts are part of an AWS Organizations structure operating in all features mode. D. Create an SCP that contains a deny rule to the ec2:PurchaseReserved InstancesOffering and ec2:ModifyReservedInstances actions. Attach the SCP to each organizational unit (OU) of the AWS Organizations structure. operating in all features mode create SCP
operating in all features mode create SCP

Q212 A financial services company is moving to AWS and wants to enable Developers to experiment and innovate while preventing access to production applications. The company has the following requirements:-Production workloads cannot be directly connected to the internet. -All workloads must be restricted to the us-west-2 and eu-central-1 Regions -Notification should be sent when Developer Sandboxes exceed $500 in AWS spending monthly. Which combination of actions needs to be taken to create a multi-account structure that meets the company's requirements? (Select THREE)
B. Create accounts for each production workload within an organization in Aws Organizations. Place the production accounts within an organizational unit(OU). Create an SCP with a deny rule on the attach an internet gateway action Create an SCP with a Deny rule to prevent use of the default VPC. Attach the SCPS to the ou for the production accounts.
C. Create a SCP containing a Deny Effect for cloudfront: * iam:" route53:*, and support: * with a StringNotEquals Condition on an aws RequestedRegion condition key with us-west-2 and eu-central-1 values. Attach the SCP to the organizations root
F. Create accounts for each development workload within an organization in A ws Organizations Place the development accounts within an organizational unit(OU). Create a budget within Aws Budgets for each development account to monitor and report on monthly spending exceeding $500 create a SCP with a deny rule to prevent use of default VPC create a SCP containing a Deny Effect for CloudFront create a budget within AWS Budgets for each development account
create a SCP with a deny rule to prevent use of default VPC
create a SCP containing a Deny Effect for CloudFront
create a budget within AWS Budgets for each development account

Q213 A financial company is using a high-performance compute cluster running on Amazon EC2 instances to perform market simulations A DNS record must be created in an Amazon Route 53 private hosted zone when instances start The DNS record must be removed after instances are terminated. Currently the company uses a combination of Amazon Cloud Watch Events and AWS Lambda to create the DNS record. The solution worked well in testing with small clusters, but in production with clusters containing thousands of instances the company sees the following error in the Lambda logs:-- HTTP 400 error (Bad request). - The response header also includes a status code element with a value of 'Throttling' and a status message element with a value of Rate exceeded. TV Thich combination of steps should the Solutions Architect take to resolve these issues? (Select THREE)
C. Update the Cloudwatch Events rule to trigger on Amazon EC2 " Instance Launch Succ tessful" and "Instance Terminate Successful "events for the auto Scaling group used by the cluster.
D. Configure a Lambda function to retrieve messages from an amazon SQS queue. Modify the Lambda function to retrieve a maximum of 10 messages , then batch the messages by Amazon Route 53 API call type and submit.Delete the messages from the SQS queue after successful API calls.
E. Configure an Amazon S QS standard queue and configure the existing Cloudwatch Events rule to use this queue as a target. Remove the Lambda target from the Cloudwatch Events rule. update

CloudWatch Events rules Configure a Lambda function to retrieve messages from SQS queue Configure SQS standard queue
update CloudWatch Events rules
Configure a Lambda function to retrieve messages from SQS queue
Configure SQS standard queue

Q214 A company uses Amazon S3 to host a web application. Currently, the company uses a continuous integration tool running on an Amazon EC2 instance that builds and deploys the application by uploading it to an S3 bucket. A Solutions Architect needs to enhance the security of the company's platform with the following requirements:-A build process should be run in a separate account from the account hosting the web application. -A build process should have minimal access in the account it operates in. Long-lived credentials should not be used As a start, the Development team created two AWS accounts. one for the application I named web account. and one for the build process named build account. Which solution should the Solutions Architect use to meet the security requirements?
B. In the build account, create a new IAM role which can be assumed by Amazon EC2 only.Attach the role to the EC2 instance running the continuous integration process.Create an IAM policy to allow s3 PutObject calls on the S3 bucket in the web account.In the web account create an $3 bucket policy attached to the $3 bucket that allows the newly. Created IAM role to use s3 PutObject calls. create IAM role to use s3 PutObject calls
create IAM role to use s3 PutObject calls

Q215 A company wants to analyze log data using date ranges with a custom application running on AWS. The application generates about 10 GB of data every day, which is expected to grow . A Solutions Architect is tasked with storing the data in Amazon S3 and using Amazon Athena to analyze the data. Which combination of steps will ensure optimal performance as the data grows?(Select TWO)
C. Store the data in Amazon $3 in a columnar format, such as Apache Parquet or Apache ORC.
E. Store the data using Apache Hive partitioning in Amazo pn S3 using a key that includes a date, such asdt=2019-02
store in columnar format
using Apache Hive partitioning in S3

Q216 A company is refactoring an existing web service that provides read and write access to structured data. The service must respond to short but significant spikes in the system load. The service must be fault tolerant across multiple AWS Regions. Which actions should be taken to meet these requirements?
C. Store the data in an Amazon DynamoDB global table in two Regions using on-demand capacity mode. In both Regions. run the web service as Amazon ECS Fargate tasks in an Auto Scaling ECS service behind an Application Load Balancer (ALB). In Amazon Route 5: 3, configure an alias record in the company's domain and a Route 53 latency- based routing policy r with health checks to distribute traffic between the two ALBs. store data in DynamoDB global table
store data in DynamoDB global table

Q217 A mobile gaming application publishes data continuously to Amazon Kinesis Data Streams. An AWS Lambda function processes records from the data stream and writes to an Amazon DynamoDB table. The DynamoDB table has an auto scaling policy enabled with the target utilization set to 70%. For several minutes at the start and end of each day, there is a spike in traffic that often exceeds five times

the normal load. The company notices the GetRecords.Iteratd prAgeMilliseconds metric of the Kinesis data stream temporarily spikes to over a minute for several minutes. The AWS Lambda function writes Provisioned Throughput Exceeded Exception messages to Amazon CloudWatch Logs during these times, and some records are redirected to the dead letter qu leue. No exceptions are thrown by the Kinesis producer on the gaming application. What change should the company make to resolve this issue?
A.Use Application Auto Scaling to set a scaling schedule to scale out write capacity on the DynamoDB table during predictable load spikes. use application Auto Scaling
use application Auto Scaling

Q218 A company has a single AWS master billing account, which is the root of the AWS Organizations hierarchy. The company has multiple AWS accounts within this hierarchy, all organized into organization units (OUs). More OUS and AWS accounts will continue to be created as other parts of the business migrate applications to AWS. These business units may need to use different AWS services. The Security team is implementing the following requirements for all current and future AWS accounts. -Control policies must be applied across all accounts to prohibit AWS servers. -Exceptions to the control policies are allowed based on valid use cases. Which solution will meet these requirements with minimal optional overhead?
C. Use an SCP in Organization to implement a deny list of AWS services. Apply this SCP at each OU level. Leave the default AWS managed SCP at the root level For any specific executions for an OU, create a new SCP for that OU apply this SCP at each OU level. leave default SCP at root level
apply this SCP at each OU level. leave default SCP at root level

Q219 A retail company has a custom .NET web application running on AWS that uses Microsoft SQL Server for the database. The application servers maintain a user's session locally. Which combination of architecture changes are needed to ensure all tiers of the solution are highly available? (Choose three.)
A. Refactor the application to store the user's session in Amazon ElastiCache. Use Application Load Balancers to distribute the load between application instances.
C. Migrate the database to Amazon RDS for SQL Server. Configure the RDS instance to use a Multi-AZ deployment.
E. Put the application instances in an Auto Scaling group. Configure the Auto Scaling group to create new instances if an instance becomes unhealthy refactor app to store session in Amazon ElastiCache Migrate db to Amazon RDS for SQL server put app instance in Auto Scaling group
refactor app to store session in Amazon ElastiCache
Migrate db to Amazon RDS for SQL server
put app instance in Auto Scaling group

Q220 A retail company processes point-of-sale data on application servers in its data center and writes outputs to an Amazon DynamoDB table. The data center is connected to the company's VPC with an AWS Direct Connect (DX) connection, and the application servers require a consistent network connection at speeds greater than 2 Gbps. The company decides that the DynamoDB table needs to be highly available and fault tolerant. The company policy states that the data should be available across two regions. What changes should the company make to meet these requirements?
A. Establish a second DX connection for redundancy. Use DynamoDB global tables to replicate data to a second Region. Modify the application to fail over to the second Region Use DynamoDB global tables to replicate data to second Region
Use DynamoDB global tables to replicate data to second Region

Q221 An international company has deployed a multi-tier web application that relies on DynamoDB in a single region. For regulatory reasons they need disaster recovery capability in a separate region with a Recovery Time Objective of 2 hours and a Recovery Point Objective of 24 hours. They should synchronize their data on a regular basis and be able to provision the web application rapidly using CloudFormation. The objective is to minimize changes to the existing web application, control the throughput of DynamoDB used for the synchronization of data, and synchronize only the modified elements. Which design would you choose to meet these requirements?

A. Use AWS Data Pipeline to schedule a DynamoDB cross region copy once a day, create a "LastUpdated" attribute in your DynamoDB table that would represent the timestamp of the last update and use it as a filter create “LastUpdated” attribute in DynamoDB table

create “LastUpdated” attribute in DynamoDB table

Q222 Your company currently has a 2-tier web application running in an on-premises data center. You have experienced several infrastructure failures in the past few months resulting in significant financial losses. Your CIO is strongly considering moving the application to AWS. While working on achieving buy-In from the other company executives, he asks you to develop a disaster recovery plan to help improve business continuity in the short term. He specifies a target Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 1 hour or less. He also asks you to implement the solution within 2 weeks. Your database is 200GB in size and you have a 20Mbps Internet connection. How would you do this while minimizing costs?

A.Create an EBS backed private AMI which includes a fresh install of your application. Develop a CloudFormation template which includes your AMI and the required EC2, AutoScaling, and ELB resources to support deploying the application across Multiple-Availability-Zones. Asynchronously replicate transactions from your on-premises database to a database instance in AWS across a secure VPN connection. create EBS backed private AMI, Asynchronously replicate transactions

create EBS backed private AMI, Asynchronously replicate transactions

Q223 During a security audit of a Service team's application, a Solutions Architect discovers that a username and password for an Amazon RDS database and a set of AWS IAM user credentials can be viewed in the AWS Lambda function code. The Lambda function uses the username and password to run queries on the database, and it uses the IAM credentials to cal AWS services in a separate management account. The Solutions Architect concerned that the credentials could grant inappropriate access to anyone who can view the Lambda code. The management account and the Service team's account are in separate AWS Organizations organizational units (OUs). Which combination of changes should the Solutions Architect make to improve the solution's security? (Choose two.)

A. Configure Lambda to assume a role in the management account with appropriate access to AWS

B. Configure Lambda to use the stored database credentials in AWS Secrets Manager and enable automatic rotation. config Lambda to assume a role config Lambda to use stored db credentials

config Lambda to assume a role

config Lambda to use stored db credentials

Q224 Your company runs a customer facing event registration site. This site is built with a 3-tier architecture with web and application tier servers and a MySQL database. The application requires 6 web tier servers and 6 application tier servers for normal operation, but can run on a minimum of 65% server capacity and a single MySQL database. When deploying this application in a region with three availability zones (AZs), which architecture provides high availability?
B. A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 3 AZs with 2 EC2 instances In each AZ inside an Auto Scaling Group behind an ELB, and a Multi-AZ RDS (Relational Database Service) deployment. a web tier deployed across 3 AZs with 2 EC2 instances, Multi-AZ RDS(relational db service)
a web tier deployed across 3 AZs with 2 EC2 instances, Multi-AZ RDS(relational db service)

Q225 An administrator is using Amazon CloudFormation to deploy a three tier web application that consists of a web tier and application tier that will utilize Amazon DynamoDB for storage. When creating the CloudFormation template which of the following would allow the application Instance access to the DynamoDB tables without exposing API credentials?
B. Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and reference the Role in the instance profile property of the application instance. reference role in instance profile property
reference role in instance profile property

Q226 An AWS customer is deploying an application that is composed of an AutoScaling group of EC2 instances. The customers security policy requires that every outbound connection from these instances to any other service within the customers Virtual Private Cloud must be authenticated using a unique X.509 certificate that contains the specific Instance-id. In addition, all X.509 certificates must be signed by the customer's key management service in order to be trusted for authentication. Which of the following configurations will support these requirements?
B. Configure the Auto Scaling group to send an SNS notification of the launch of a new instance to the trusted key management service. Have the key management service generate a signed certificate and send it directly to the newly launched instance. have key management service generate a signed certificate
have key management service generate a signed certificate

Q227 A company has an application that runs on a fleet of Amazon EC2 instances and stores 70 GB of device data for each instance in Amazon S3. Recently, some of the S3 uploads have been failing. At the same time, the company is seeing an unexpected increase in storage data costs. The application code cannot be modified. What is the MOST efficient way to upload the device data to Amazon S3 while managing storage costs?
A.Upload device data using a multipart upload. Use the AWS CLI to list incomplete parts to address the failed S3 uploads. Enable the lifecycle policy for the incomplete multipart uploads on the S3 bucket to delete the old uploads and prevent new failed uploads from accumulating. use AWS CLI to list incomplete parts
use AWS CLI to list incomplete parts

Q228 A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon EC2, Amazon S3, and Amazon DynamoDB. The Developers account resides in a dedicated organizational unit (OU). The Solutions Architect has implemented the following SCP on the Developers account: When this policy is deployed, IAM users in the Developers account are still able to use AWS services that are not listed in the policy. What should the Solutions Architect do to eliminate the Developers' ability to use services outside the scope of this policy?
B. Remove the FullAWSAccess SCP from the Developer account's OU
remove FullAWSAccess SCP

Q229 Your company previously configured a heavily used, dynamically routed VPN connection between your on-premises data center and AWS. You recently provisioned a DirectConnect connection and would like to start using this new connection. After configuring DirectConnect settings in the AWS Console, which of the following options will provide the most seamless transition for your users?
C. Update your VPC route tables to point to the DirectConnect connection, configure your DirectConnect router with the appropriate settings, verify network traffic is leveraging DirectConnect, and then delete the VPN connection. update VPC route tables
update VPC route tables

Q230 Your team has a tomcat-based java application you need to deploy into development, test and production environments. After some research, you opt to use Elastic Beanstalk due to its tight integration with your developer tools and RDS due to its ease of management. Your QA team lead points out that you need to roll a sanitized set of production data into your environment on a nightly basis. Similarly, other software teams in your org want access to that same restored data via their EC2 instances in your VPC. The optimal setup for persistence and security that meets the above requirements would be the following:
D. Create your RDS instance separately and pass its DNS name to your app's DB connection string as an environment variable. Create a security group for client machines and add it as a valid source for DB traffic to the security group of the RDS instance itself. create security group for client machines
create security group for client machines

Q231 You have a periodic image analysis application that gets some files in input, analyzes them and for each file writes some data in output to a text file. The number of files in input per day is high and concentrated in a few hours of the day. Currently you have a server on EC2 with a large EBS volume that hosts the input data and the results. It takes almost 20 hours per day to complete the process. What services could be used to reduce the elaboration time and improve the availability of the solution?
A.S3 to store I/O files, SQS to distribute elaboration commands to a group of hosts working in parallel, Auto Scaling to dynamically size the group of hosts depending on the length of the SQS queue.
S3 to store I/O files ,SQS to distribute elaboration commands

Q232 A company experienced a breach of highly confidential personal information due to permissions issues on an Amazon S3 bucket. The Information Security team has tightened the bucket policy to restrict access. Additionally, to be better prepared for future attacks, these requirements must be met:- Identify remote IP addresses that are accessing the bucket objects. -Receive alerts when the security policy on

the bucket is changed. -Remediate the policy changes automatically. Which strategies should the Solutions Architect use?
B. Use Amazon Athena with S3 access logs to identify remote IP addrésses. Use AWS Config rules with AWS Systems Manager Automation to automatically remediate S3 bucket policy changes. Use Amazon SNS with AWS Config rules for alerts use Amazon Athena
use Amazon Athena

Q233 An organization is planning to host a Wordpress blog as wel a joomla CMS on a single instance launched with VPC. The organization wants to have separate domains for each application and assign them using Route 53. The organization may have about ten instances each with two applications as mentioned above. While launching the instance, the organization configured two separate network interfaces (primary + ENI) and wanted to have two elastic IPs for that instance. It was suggested to use a public IP from AWS instead of an elastic IP as the number of elastic IPs is restricted. What action will you recommend to the organization?
B.I do not agree as it is required to have only an elastic IP since an instance has more than one ENI and AWS does not assign a public IP to an instance with multiple ENIs
I don't agree as it's required to have only an elastic IP

Q234 A Solutions Architect wants to make sure that only AWS users or roles with suitable permissions can access a new Amazon API Gateway endpoint. The Solutions Architect wants an end-to-end view of each request to analyze the latency of the request and create service maps. How can the Solutions Architect design the API Gateway access control and perform request inspections?
A. For the API Gateway method, set the authorization to AWS_IAM. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Enable the API caller to sign requests with AWS Signature when accessing the endpoint. Use AWS X-Ray to trace and analyze user requests to API Gateway.
for API Gateway method, set authorization to AWS_IAM

Q235 A company is running a batch analysis every hour on their main transactional DB. running on an RDS MySQL instance to populate their central Data Warehouse running on Redshift During the execution of the batch their transactional applications are very slow. When the batch completes they need to update the top management dashboard with the new data The dashboard is produced by another system running on-premises that is currently started when a manually-sent email notifies that an update is required The on-premises system cannot be modified because is managed by another team. How would you optimize this scenario to solve performance issues and automate the process as much as possible?
C. Create an RDS Read Replica for the batch analysis and SNS to notify me on-premises system to update the dashboard
create RDS Read replica and SNS to notify me

Q236 A company is building a voting system for a popular TV show, viewers will watch the performances then visit the show's website to vote for their favorite performer. It is expected that in a short period of time after the show has finished the site will receive millions of visitors, the visitors will first login to the site using theirAmazon.com credentials and then submit their vote. After the voting is completed the page will display the vote totals. The company needs to build the site such that it can handle the rapid influx of

traffic while maintaining good performance but also wants to keep costs to a minimum. Which of the design pattern below should they use?
B. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first cal the Login With Amazon service to authenticate the user, the web servers will process the users vote and store the result into an SQS queue using IAM Roles for EC2 Instances to gain permissions to the SQS queue. A set of application servers will then retrieve the items from the queue and store the result into a DynamoDB table.
store result into an SQS queue

Q237 A software as a service (Saas) company offers a cloud solution for document management to private law firms and the public sector. A local government client recently mandated that highly confidential documents cannot be stored outside the country. The company CIO asks a Solutions Architect to ensure the application can adapt to this new requirement. The CIO also wants to have a proper backup plan for these documents, as backups are not currently performed. What solution meets these requirements?
C. Tag documents as either regular or secret in Amazon S3. Create an individual S3 backup bucket in the same AWS account and AWS Region. Use S3 selective cross-region replication based on object tags to move regular documents to an S3 bucket in a different AWS Region. Configure an AWS Lambda function that triggers when new S3 objects are created in the main bucket to replicate only documents tagged as secret into the S3 bucket in the same AWS Region.
config Lambda function that triggers when new S3 are create

Q238 You are developing a new mobile application and are considering storing user preferences in AWS. This would provide a more uniform cross- device experience to users using multiple mobile devices to access the application. The preference data for each user is estimated to be 50KB in size. Additionally, 5 million customers are expected to use the application on a regular basis. The solution needs to be cost-effective, highly-available, scalable and secure. How would you design a solution to meet the above requirements?
D. Setup a DynamoDB table with an item for each user having the necessary attributes to hold the user preferences. The mobile application will query the user preferences directly from the DynamoDB table. Utilize STS, Web Identity Federation, and DynamoDB Fine Grained Access Control to authenticate and authorize access. setup DynamoDB table to hold user preference
setup DynamoDB table to hold user preference

Q239 You want to use AWS CodeDeploy to deploy an application to Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC). What criterion must be met for this to be possible?
C. The AWS CodeDeploy agent installed on the Amazon EC2 instances must be able to access the public AWS CodeDeploy and Amazon S3 service endpoints. access public AWS CodeDeploy and S3 service endpoints
access public AWS CodeDeploy and S3 service endpoints

Q240 While debugging a backend application for an IoT system that supports globally distributed devices, a Solutions Architect notices that stale data is occasionally being sent to user devices. Devices often share data, and stale data does not cause issues in most cases. However, device operations are disrupted when a device reads the stale data after an update. The global system has multiple identical

application stacks deployed in different AWS Regions. If a user device travels out of its home geographic region, it will always connect to the geographically closest AWS Region to write or read data. The same data is available in all supported AWS Regions using an Amazon DynamoDB global table. What change should be made to avoid causing disruptions in device operations?
A.Update the backend to use strongly consistent reads. Update the devices to always write to and read from their home AWS Region. update device to write to and read from home AWS region
update device to write to and read from home AWS region

Q241 A company developed a Java application and deployed it to an Apache Tomcat server that runs on Amazon EC2 instances. The company's Engineering team has implemented AWS CloudFormation and Chef Automate to automate the provisioning of and updates to the infrastructure and configuration of the application in the development, test, and production environments. These implementations have led to significantly improved reliability in releasing changes. The Engineering team reports there are frequent service disruptions due to unexpected errors when updating the application of the Apache Tomcat server. Which solution will increase the reliability of all releases?
A. Implement a blue/green deployment methodology implement blue/green
implement blue/green

Q242 A Developer would like to implement multi-account access for AWS Systems Manager and plans to use two member accounts within their AWS Organization. The Developer has delegated an IAM Role that allows Systems Manager(SSM) Parameter Store and Document resources to be trusted by the member accounts. While testing access from a member account, a user receives"Access Denied" errors when performing any SSM related operations. The Solutions Architect confirms that SSM operations are not denied in any of the Organization's Service Control Policies(SCP). Both member accounts are moved into a test OU which is not associated with any deny SCPs, however the user is still receiving access denied error. What changes should the Solutions Architect make to provide access while maintaining least privileges?
D. Remove both member accounts from the current Organization. Create a new Organization, with the account holding the SSM resources as the new master account and the other account as a member to the new Organization. Create a new SCP which allows SSM operations and specify the ARNs for each SSM Parameter Store andDocument within the new master account
remove both member account, create new SCP which allows SSM operations

Q243 A company is using multiple AWS accounts and has multiple Devops teams running production and non-production workloads in these accounts. The company would like to centrally-restrict access to some of the AWS services that the Devops teams do not use. The company decided to use Aws Organizations and successfully invited all AWS accounts into the Organization. They would like to allow access to services that are currently in-use and deny a few specific services. Also they would like to administer multiple accounts together as a single unit. What combination of steps should the Solutions Architect take to satisfy these requirements?(Select THREE)
C. Review the AWS Trusted Advisor report to determine services recently used
D. Remove the default Fullansaccess Scp
E. Define organizational units(OUS)and place the member accounts in the Ous
review AWS Trusted Advisor report
remove default Fullawsaccess SCP
define organization units(OUS)

Q244 A company hosts a community forum site using an Application Load Balancer(ALB)and a Docker application hosted in an Amazon ECS cluster. The site data is stored in Amazon RDS for MYSQL and the container image is stored in ECR. The company needs to provide their customers with a disaster recovery SLA with an RTO of no more than 24 hours and RPO of no more than 8 hours. Which of the following solutions is the MOST cost- effective way to meet the requirements?

B. Store the Docker image in ECR in two regions. Schedule RDS snapshots every 8 hours with snapshots copied to the secondary region. In the event of a failure, use AWS Cloudformation to deploy the ALB, EC2, ECS and RDS resources in the secondary region, restore from the latest snapshot, and update the DNS record to point to the ALB in the secondary region

store Docker image in ECR in two regions

Q245 A Solutions Architect needs to migrate an on-premises legacy application to AWS. The application runs on two servers behind a load balancer. The application requires a license file that is associated with the MAC address of the server's network adapter. It takes the software vendor 12 hours to send new license files. The application also uses configuration files with a static IP address to access a database server, host names are not supported Siven these requirements, which combination of steps should be taken to enable highly available architecture for the application servers in AWS?(Select TWO)

A. Create a pool of ENIs. Request license files from the vendor for the pool, and store the license files in Amazon S3. Create a bootstrap automation script to download a license file and attach the corresponding ENI to an Amazon EC2 instance

D. Edit the bootstrap automation script to read the database server IP address from the AWS Systems Manager Parameter Store, and inject the value into the local configuration files

create a bootstrap automation script to download a license file

edit bootstrap automation script to read db server IP address

Q246 A company is testing Amazon Elastic File Service(EFS) in its Development VPC, and would like to extend this test on-premises.EFS is running in us- east-1 and the corporate network is currently connected to this Region through a site-to-site VPN. All on-premises computers and servers are required to have all DNS traffic resolved by their on-premises DNS servers. The on-premises users would like to connect to the EFS using a UNS name Instead of an IP address. What collection of steps must be taken to meet this requirement?(Select TWO)

A. Create a new Amazon Route 53 Private Hosted Zone with a domain name of aws cloud. example. com and associate the Development VPC to this zone. Create A CNAME record and point this to the EFS endpoint.

C. Create a conditional forwarder rule in the on-premises DNS servers to forward requests for aws cloud.example. com to the Amazon Route 53 Resolver inbound

create new Route 53 Private Hosted Zone

forward requests to Route 53 Resolver inbound endpoints

Q247 A group of research institutions are partnering to study 2 PB of genomic data that changes regularly. The primary institution that owns the data is storing it in an Amazon S3 bucket in its AWS account. all of the secondary institutions in the partnership have their own AWS accounts and require read access to the data. The institute that owns the data does not want to pay for the data transfer costs

associated with allowing the secondary institutes access to the data. Which of the following solutions will meet the requirements?
B. In the primary account, create an S3 bucket policy to give read access to each secondary account. Enable Requester Pays on the S3 bucket. Have the secondary institutions use their own AWS credentials with read permissions to the S3 bucket, when accessing the data create S3 bucket policy to give read access to each secondary account
create S3 bucket policy to give read access to each secondary account

Q248 A company is planning to deploy a new business analytics application that requires 10.000 hours of compute time each month, The compute resources can have flexible availability ,but must be as cost-effective as possible. The company will also provide a reporting service to distribute analytics reports, which needs to run at all times. How should the Solution Architect design a solution that meets these requirements suff?
C. Deploy the reporting service as a container in Amazon ECS with AWS Fargate as the compute option Deploy the analytics application on a Spot Fleet. Set the analytics application to use a custom metric with Amazon EC2 Auto Scaling applied to the Spot Fleet. deploy analytics app on a Spot Fleet
deploy analytics app on a Spot Fleet

Q249 A utility company wants to collect usage data every 5 minutes from its smart meters to facilitate time-of-use metering. When a meter sends data to AWS, the data is sent to Amazon API Gateway, processed by an AWS Lambda function and stored in an Amazon DynamoDB table. During the pilot phase, the Lambda functions took from 3 to 5 seconds to complete As more smart meters are deployed, the Engineers notice the Lambda functions are taking from 1 to 2 minutes to complete. The functions are also increasing in duration as new types of metrics are collected from the devices. There are many ProvisionedThroughputExceededException errors while performing PUT operations on DynamoDB, and there are also many TooManyRequestsException errors from Lambda. Which combination of changes will resolve these issues? (Choose two.)
A. Increase the write capacity units to the DynamoDB table.
D. Stream the data into an Amazon Kinesis data stream from API Gateway and process the data in batches.
increase write capacity to DynamoDB
stream data into Kinesis data stream

Q250 A company is developing a new service that will be accessed using TCP on a static port. A Solutions Architect must ensure that the service is highly available, has redundancy across Availability Zones, and is accessible using the DNS name my.service.com,which is publicly accessible. The service must use fixed address assignments SO other companies can add the addresses to their allow lists. Assuming that resources are deployed in multiple Availability Zones in a single Region, which solution will meet these requirements?
C. Create Amazon EC2 instances for the service. Create one Elastic IP address for each Availability Zone. Create a Network Load Balancer(NLB)and expose the assigned TCP port. Assign the Elastic IP addresses to the NLB for each Availability Zone. Create a target group and register the EC2 instances with the NLB.Create a new A(alias)record set named my. service.com, and assign the NLB DNS name to the record set. Create EC2 instances for service, Create new A(alias) record set

Create EC2 instances for service, Create new A(alias) record set

Q251 A company is running a web application with On-demand Amazon EC2 instances in Auto Scaling groups that scale dynamically based on custom metrics. After extensive testing, the company determines that the m5.2xlarge instance size is optimal for the workload Application data is stored in db r4.4xlarge Amazon RDS instances that are confirmed to be optimal. The traffic to the web application spikes randomly during the day. What other cost- optimization methods should the company implement to further reduce costs without impacting the reliability of the application?
B. Reserve capacity for the rds database and the minimum number of EC2 instances that are constantly running Reserve capacity for RDS DB
Reserve capacity for RDS DB

Q252 A company with multiple accounts is currently using a configuration that does not meet the following security governance policies:Prevent ingress from port 22 to any Amazon EC2 instance, Require billing and application tags for resources. Encrypt all Amazon EBS volumes.A Solutions Architect wants to provide preventive and detective controls, including notifications about a specific resource, if there are policy deviations. Which solution should the Solutions Architect implement?
B. Use AWS Service Catalog to build a portfolio with products that are in compliance with the governance policies in a central account. Restrict users across all accounts to Aws Service Catalog products. Share a compliant portfolio to other accounts. Use AWS Config managed rules to detect deviations from the policies. Configure an Amazon Cloudwatch Events rule to send a notification when a deviation occurs governance policies in a central account
governance policies in a central account

Q253 A company is using a HTTP webhook from its source control platorm to perform code vulnerability scanning. The vulnerability scanning is done by an application running in Aws Lambda. which is invoked by Amazon Apl Gateway when the webhook is received. The source control platform requires an HTTP 200 response from the webhook destination within 30 seconds. otherwise the webhook is re-sent. Code vulnerability scanning can take up to 10 minutes to complete, depending on the size of the codebase being scanned. The company wants to ensure that only one vulnerability scan is triggered for each webhook. Which solution would achieve the company's requirement?
B. Create a new Lambda function invoked by API Gateway to write the webhook to an Amazon SQS FIFO queue with message deduplication. then return an HTTP 200 response Trigger the code vulnerability scanner from messages in the SQS FIFO queue
write webhook to SQS FIFO queue

Q254 A company has a complex web application that leverages Amazon Cloudfront for global scalability and performance. Over time, users report that the web application is slowing down. The company's operations team reports that the Cloudfront cache hit ratio has been dropping steadily. Thle cache metrics report indicates that query strings on some URLS are inconsistently ordered and are specified sometimes in mixed case letters and sometimes in lowercase letters. Which set of actions should the solutions architect take to increase the cache hit ratio as quickly as possible?
A. Deploy a Lambda@Edge function to sort parameters by name and force them to be lowercase. Select the Cloudfront viewer request trigger to invoke the function
Deploy Lambda@Edge function to sort parameters

Q255 A company has several Amazon EC2 instances to both public and private subnets within a VPC that is not connected to the corporate network. A security group associated with the EC2 instances allows the company to use the Windows remote desktop protocol (RDP) over the internet to access the instances. The security team has noticed connection attempts from unknown sources. The company wants to implement a more secure solution to access the EC2 instances. Which strategy should a solutions architect implement?

B. Deploy AWS Systems Manager Agent on the EC2 instances. Access the EC2 instances using Session Manager restricting access to users with permission.

Deploy AWS Systems Manager Agent on EC2

Q256 A company plans to migrate to AWS. A solutions architect uses AWS Application Discovery Service over the fleet and discovers that there is an Oracle data warehouse and several PostgreSQL databases. Which combination of migration patterns will reduce licensing costs and operational overhead? (Choose two.)

B. Migrate the Oracle data warehouse to Amazon Redshift using AWS SCT and AWS DMS D. Migrate the PostgreSQL databases to Amazon RDS for PostgreSQL using AWS DMS.

Migrate Oracle data warehouse to Redshift

Migrate PostgreSQL to RDS for PostgreSQL

Q257 A company is running a two-tier web application on Amazon EC2. The web tier consists of an Application Load Balancer(ALB) backed by a Auto Scaling group of web server instances spanning multiple Availability Zones. The database tier is using Amazon Aurora MYSQL. The company's security team has deployed AWS WAF and integrated it with the ALB to prevent SQL injection attacks against the application. Recently, a security breach was reported in which the attacker was able to gain access to an individual web server and the company's database from random IP addresses. The security team was eventually able to write a better rule to match the SQL injection technique that the attacker had used. However, this process took about an hour from when the third-party security agent running on theEC2 instances successfully detected the attack. Which strategy allows the security team to protect the database and overall infrastructure?

D. Deploy Amazon Guardduty to analyze VPC Flow Logs. Configure an Amazon Eventbridge rule that triggers an AWS Lambda function upon a Guardduty alert. Configure the Lambda function to automatically block detected attacks by modifying security groups within the VPC Deploy Amazon Guardduty

Deploy Amazon Guardduty

Q258 A company has a mobile app with users in Europe. When the app is used, it downloads a configuration file that is device and app version-specific. The company has the following architecture:-Configuration files are stored in Amazon S3 in the eu-west-1 Region and served to the using Amazon Cloudfront -Lambda@Edge is used to extract the device and version information from the app requests. It then updates the requests to load the correct configuration. The company uses the configuration file load time as a key performance metric, and targets are sponse time of 100 ms or less. The app recently launched in the app-southeast-2 Region, and the latency for requests from users in Australia is significantly above the 100 ms target. A solution architect needs to recommend a solution. Which solution will reduce latency for users in Australia?

C. Configure S3 Transfer Acceleration on the bucket. Add the Transfer Acceleration Edge endpoints for Australia and Europe as Cloudfront origins. Modify Lambda@Edge to update the origin of the request to be the Transfer Acceleration endpoint in the Region that is closest to the user
add Transfer Acceleration Edge endpoints for Australia

Q259 A company operates pipelines across North America and South America. The company assesses pipeline inspection gauges with imagery and ultrasonic sensor data to monitor the condition of its pipelines. The pipelines are in areas with intermittent or unavailable internet connectivity. The imagery data at each site requires terabytes of storage each month. The company wants a solution to collect the data at each site in monthly intervals and to store the data with high durability. The imagery captured must be preprocessed and uploaded to a central location for persistent storage. Which actions should a solutions architect take to meet these requirements?
D. Deploy AWS Iot Greengrass on eligible hardware across the sites. Configure AWS Lambda on the devices for preprocessing. Ship the devices back to the closest AWS Region and store the data in Amazon S3 buckets
Deploy AWS Iot Greengrass, Ship device back to closest AWS region

Q260 A company is using multiple AWS accounts. The DNS records are stored in a private hosted zone for Amazon Route 53 in Account A. The company's applications and databases are running in Account B- A solutions architect will deploy a two-tier application in a new VPC. To simplify the configuration, the db.example.com CNAME record set for the Amazon RDS endpoint was created in a private hosted zone for Amazon Route 53. During deployment the application failed to start. Troubleshooting revealed that db.example. com is not resolvable on the Amazon EC2 instance. The solutions architect confirmed that the record set was created correctly in Route 53. Which combination of steps should the solutions architect take to resolve this issue? (Choose two.)
C. Create an authorization to associate the private hosted zone in Account A with the new VPC in Account B
E. Associate a new VPC in Account B with a hosted zone in Account A. Delete the association authorization in Account A. create authorization to associate private hosted zone Associate a new VPC with hosted zone
create authorization to associate private hosted zone
Associate a new VPC with hosted zone

Q261 A solutions architect is designing a publicly accessible web application that is on an Amazon Cloudfront distribution with an Amazon website endpoint as the origin. When the solution is deployed, the website returns an Error 403:Access Denied message. Which steps should the solutions architect take to correct the issue?(Select TWO)
A. Remove the S3 block public access option from the S3 bucket
B. Remove the requester pays option from the S3 bucket
remove S3 block public access option from S3
remove requester pays option from S3

Q262 A company requires that all internal application connectivity use private IP addresses. To facilitate this policy, a solutions architect has created interface endpoints to connect to AWS public services. Upon

testing, the solutions architect notices that the service names are resolving to public IP addresses, and that internal services cannot connect to the interface endpoints. Which step should the solutions architect take to resolve this issue?
B. Enable the private DNS option on the VPC attributes
enable private DNS option

Q263 An ecommerce company has an order processing application it wants to migrate to AWS. The application has inconsistent data volume patterns, but needs to be available at all times. Orders must be processed as they occur and in the order that they are received. Which set of steps should a solutions architect take to meet these requirements?
C. Use Amazon SQS with FIFO and send orders as they occur. Use Reserved Instances in multiple Availability Zones for processing.
User SQS with FIFO, user reserved Instances

Q264 A company has a web application that allows users to upload short videos. The videos are stored on Amazon EBS volumes and analyzed by custom recognition software for categorization. The website contains static content that has variable traffic with peaks in certain months. The architecture consists of Amazon EC2 instances running in an Auto Scaling group for the web application and EC2 instances running in an Auto Scaling group to process an Amazon SQS- queue. The company wants to re-architect the application to reduce operational overhead using AWS managed services where possible and remove dependencies on third-party software. Which solution meets these requirements?
C. Host the web application in Amazon S3. Store the uploaded videos in Amazon S3. Use S3 event notification to publish events to the SQS queue. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
Host web app in S3

Q265 A solutions architect is designing a web application on AWS that requires 99.99% availability. The application will consist of a three-tier architecture that supports 3000,000 web requests each minute when experiencing peak traffic. The application will use Amazon Route 53 for DNS resolution,Amazon CloudFront as the the content delivery network(CDN), an Elastic Load Balancer for load balancing.Amazon EC2 Auto Scaling groups to scale the application tier,and Amazon Aurora MySQL as the backend database. The backend database load will average 90% reads and 10% writes. The company wants to build a cost-effective solution ,but reliability is critical. Which set of strategies should the solutions architect use?
B. Build the application in a single AWS Region. Deploy the EC2 application layer to three Availability Zones using an Auto Scaling group with a minimum desired capacity sufficient to process 450,000 requests each minute. Use a Multi-AZ Amazon Aurora MYSQL DB cluster with two Aurora Replicas Each Aurora Replica must have enough capacity to support 100% of the peak read queries. support 100% of peak read queries
support 100% of peak read queries

Q266 A company has an on-premises website application that provides real estate information for potential renters and buyers. The website uses a Java backend and a NoSQL MongoDB database to store subscriber data. The company needs to migrate the entire application to AWS with a similar

structure. The application must be deployed for high availability, and the company cannot make changes to the application. Which solution will meet these requirements?
D. Configure Amazon DocumentDB (with MongoDB compatibility) in on-demand capacity mode in multiple Availability Zones as the database for the subscriber data Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application.
config Amazon DocumentDB(with MongoDB compatibility) in on-demand capacity mode

Q267 A video processing company has a fleet of Amazon EC2 Spot Instances. The company uses an Auto Scaling group to launch the EC2 instances. The fleet runs a custom processing service that requires a high amount of CPU for a short amount of time to modify a proprietary video format. The EC2 instances are configured by a user data script that runs the required service at launch and downloads the required video file from Amazon S3. The launch template uses burs table instance types in unlimited mode. The processing of each request takes an average of 20 minutes to complete. A solutions architect must review the existing architecture to determine whether the company is using resources properly. What should the solutions architect recommend to reduce the company's operational costs?
A.Replace the EC2 instances with an Amazon Elastic Transcoder pipeline. Invoke the pipeline by using Amazon S3 Event Notifications. replace EC2 with Amazon Elastic Transcoder pipeline
replace EC2 with Amazon Elastic Transcoder pipeline

Q268 A company plans to refactor a monolithic application into a modern application design deployed on Aws. The CI/CD pipeline needs to be upgraded to support the modern design for the application with the following requirements:-It should allow changes to be released several times every hour -It should be able to rollback the changes as quickly as possible. Which design will meet these requirements?
B. Specify AWS Elastic Beanstalk to stage in a secondary environment as the deployment target for the CLCD pipeline of application. The deploy swap the staging and production environment URLS specify AWS Elastic Beanstalk
specify AWS Elastic Beanstalk

Q269 A solutions architect is migrating an existing workload to AWS Fargate. The task can only run in a private subnet within the VPC where there is no direct connectivity from outside the system to the application. When the Fargate task is launched ,the task fails with the following err:CannotPullcontainererror:API error(500):Get http:/111122223333.dkr.ecr.us-east-1.amazonaws.com/v2/net/http:request canceled while waiting for connection How should the solutions architect correct this error?
B. Ensure the task is set to DISABLED for the auto assign public IP setting when launching the task. Configure a NAT gateway in the public subnet in the VPC to route requests to the internet config a NAT gateway in public subnet in VPC
config a NAT gateway in public subnet in VPC

Q270 A company has a photo sharing social networking application. To provide a consistent experience for users, the company performs some image processing on the photos uploaded by users before publishing on the application. The image processing is implemented using a set of Python libraries. The current architecture is as follows:-The image processing Python code runs in a single Amazon EC2 instance and stores the processed images in an Amazon S3 bucket named ImageBucket. -The front-end application, hosted in another bucket, loads the images from ImageBucket to display to users. With plans

for global expansion, the company wants to implement changes in its existing architecture to be able to scale for increased demand on the application and reduce management complexity as the application scales. Which combination of changes should a solutions architect make? (Choose two.)
B. Use AWS Lambda to run the image processing tasks.
D. Use Amazon CloudFront in front of ImageBucket.
use Lambda to run image processing
use CloudFront in front of ImageBucket

Q271 A company uses AWS Organizations with a single OU named Production to manage multiple accounts. All accounts are members of the Production OU. Administrators use deny list SCPs in the root of the organization to manage access to restricted services. The company recently acquired a new business unit and invited the new unit's existing AWS account to the organization. Once onboarded, the administrators of the new business unit discovered that they are not able to update existing AWS Config rules to meet the company's policies. Which option will allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance?
D. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to allow AWS Config actions. Move the organization's root SCP to the Production OU. Move the new account to the Production OU when adjustments to AWS Config are complete. move organization's root SCP to production OU.
move organization's root SCP to production OU.

Q272 A company has a Microsoft SQL Server database in its data center and plans to migrate data to Amazon Aurora MySQL. The company has already used the AWS Schema Conversion Tool to migrate triggers, stored procedures and other schema objects to Aurora MySQL. The database contains 1 TB of data and grows less than 1 MB per day. The company's data center is connected to AWS through a dedicated 1Gbps AWS Direct Connect connection. The company would like to migrate data to Aurora MySQL and perform reconfigurations with minimal downtime to the applications. Which solution meets the company's requirements?
B. Create an AWS DMS replication instance and task to migrate existing data and ongoing replication from SQL Server to Aurora MySQL. Perform application testing and migrate the data to the new database endpoint. migrate existing data and ongoing replication from SQL server to Aurora MySQL
migrate existing data and ongoing replication from SQL server to Aurora MySQL

Q273 A financial services company receives a regular data feed from its credit card servicing partner. Approximately 5,000 records are sent every 15 minutes in plaintext delivered over HTTPS directly into an Amazon S3 bucket with server-side encryption. This feed contains sensitive credit card primary account number (PAN) data. The company needs to automatically mask the PAN before sending the data to another S3 bucket for additional internal processing. The company also needs to remove and merge specific fields and then transform the record into JSON format Additionally extra feeds are likely to be added in the future so any design needs to be easily expandable. Which solutions will meet these requirements?
C. Create an AWS Glue crawler and custom classifier based on the data feed formats and build a table definition to match Trigger an AWS Lambda function fie delivery to start an AWS Glue ETL job to transform the entire record according to the processing and transformation requirements.

Define the output format as JSON Once complete, have the Etljobsend the results to another S3 bucket for internal processing start AWS Glue ETL job to transform entire record
start AWS Glue ETL job to transform entire record

Q274 A company is manually deploying its application to production and wants to move to a more mature deployment pattern. The company has asked a solutions architect to design a solution that leverages its current Chef tools and knowledge. The application must be deployed to a staging environment for testing and verification before being deployed to production. Any new deployment must be rolled back in 5 minutes if errors are discovered after a deployment. Which AWS service and deployment pattern should the solutions architect use to meet these requirements?
D. Use AWS OpsWorks and deploy the application using a blue/green deployment strategy
using a blue/green

Q275 A solutions architect is implementing federated access to AWS for users of the company's mobile application. Due to regulatory and security requirements, the application must use a custom-built solution for authenticating users and must use AM roles for authorization. Which of the following actions would enable authentication and authorization and satisty the requirements?(Select TWO)
D. Use a custom-built Saml-compatible solution that uses LDAP for authentication and uses a SAML assertion to perform authorization to the LAM identity provider.
E. Use a custom-built Opend Connect-compatible solution for authentication and use Amazon Cognito for authorization
use SAML assertion to perform authorization
use Cognito for authorization

Q276 An online magazine will launch its latest edition this month. This edition will be the first to be distributed globally. The magazine's dynamic website currently uses an Application Load Balancer in front of the web tier, a fleet of Amazon EC2 instances for web and application servers ,and Amazon Aurora MySQL.Portions of the website include static content and almost all traffic is read-only. Which combination of steps should a solutions architect take to reduce system response times for a global audience? (Select TWO)
D. Use an Aurora global database for physical cross-region replication. Use Amazon S3 with cross-region replication for static content and resources. Deploy the web and application tiers in Regions across the world.
E. Introduce Amazon Route 53 with latency-base routing and Amazon Cloudfront distr but ons. Ensure the web and application tiers are each in Auto Scaling groups
use Aurora global db for cross-region replication
introduce Route 53 with latency-based routing

Q277 A company is launching a new web application on Amazon EC2 instances. Development and production workloads exist in separate AWS accounts. According to the company's security requirements, only automated configuration tools are allowed to access the production account. The company's security team wants to receive immediate notification if any manual access to the production AWS account or EC2 instances occurs. Which combination of actions should a solutions architect take in the production account to meet these requirements? (Select THREE.)

C. Deploy EC2 instances in an Auto Scaling group.Configure the launch template to deploy instances without key pairs. Configure Amazon CloudWatch Logs to capture system access logs. Create an Amazon CloudWatch alarm that is based on the logs to detect when a user logs in to an EC2 instance
D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to send a message to the security team when an alarm is activated
E. Turn on AWS CloudTrail logs for all AWS Regions.Configure Amazon CloudWatch alarms to provide an alert when an AwsConsoleSignin event is detected.
deploy EC2 in an Auto Scaling group
Configure Amazon SNS topic to send message
Turn on AWS CloudTrail logs

Q278 A mobile app has become very popular, and usage has gone from a few hundred to millions of users. Users capture and upload images of activities within a city, and provide ratings and recommendations Data access patterns are unpredictable. The current application is hosted on Amazon EC2 instances behind an Application Load Balancer(ALB). The application is experiencing slowdowns and costs are growing rapidly. Which changes should a solutions architect make to the application architecture to control costs and improve performance?
B. Store static content in an Amazon S3 bucket using the Intelligent Tiering storage class. Use an Amazon Cloudfront distribution in front of the S3 bucket and the ALB
store static content in S3 using Intelligent Tiering storage class

Q279 A company wants to Run a serverless application on AWS The company plans to provision its application in Docker containers running n en Amazon ECS cluster The application requires a MYSQL database and the company plans to use Amazon RDS The company has documents that need to be accessed frequently for the first 3 months, and rarely after that The documents must be retained for years. What is the MOST cost effective solution to meet these requirements?
B. Create an ECS cluster using a fleet of Spot Instances, with Spot Instance draining enabled. Provision the database and its read replicas in Amazon RDS using Reserved Instances. Store the documents in a secured Amazon S3 bucket with a lifecycle policy to move the documents that are older than 3 months to Amazon S3 Glacier. then delete the documents from Amazon S3 Glacier that are more than 7 years old
more than 7 years old

Q280 A solutions architect must enable an AWS Cloudhsm M of N access control-also named a quorum authentication mechanism-to allow security officers to make administrative changes to a hardware security module(HSM). The new security policy states that at least three of the five security officers must authorize any administrative changes to CloudHSM. Which well-architected design ensures the security officers can authenticate as a quorum ?
D. Create an Amazon Cognito authenticated Amazon API Gateway API endpoint with an AWS Lambda proxy integration. Allow an officer to create a Cloudhsm quorum token and post it to the API Gateway API after signing in with Amazon Cognito. Configure the Lambda function to perform a signing procedure on the quorum token using the officer's Amazon Cognito IAM role, and store the signed token in Amazon Dynamodb. Once at least three officers have signed the quorum token, allow a POST method to administer Cloudhsm with the signed token
create Cognito authenticated API Gateway

Q281 A company is using an existing orchestration tool to manage thousands of Amazon EC2 instances. A recent penetration test found a vulnerability in the company's software stack. This vulnerability has prompted the company to perform a full evaluation of its current production environment. The analysis determined that the following vulnerabilities exist within the environment:-Operating systems with outdated libraries and known vulnerabilities are being used in production. -Relational databases hosted and managed by the company are running unsupported versions with known vulnerabilities. - Data stored in databases is not encrypted. The solutions architect intends to use AWS Contig to continuously audit and assess the compliance of the company's AWS resource configurations with the company's policies and guidelines. What additional steps will enable the company to secure its environments and track resources while adhering to best practices?

D. Instal the AWS Systems Manager Agent on all existing instances using the company's current orchestration tool. Migrate all relational databases to Amazon RDS and enable AWS KMS encryption. Use Systems Manager Patch Manager to establish a patch baseline and deploy a Systems Manager Maintenance Windows task to execute AWS-RunPatchBaseline using the patch baseline.

migrate all relational db to RDS, execute AWS-RunPatchBaseline

Q282 A company runs a Multi-AZ deployment of Amazon RDS to support a critical business application. The company's infrastructure team wants to be notified whenever an RDS failover event occurs. What should a solutions architect do to meet this requirement?

A.In the RDS console, configure an event subscription. Specify the instance, notification target, and event category.

config an event subscription

Q283 A company has a VPC with two domain controllers running Active Directory in the default configuration. The VPC DHCP options set is configured to use the IP addresses of the two domain controllers. There is a VPC interface endpoint defined; but instances within the VPC are not able to resolve the private endpoint addresses. Which strategies would resolve this issue? (Choose two.)

A. Define an outbound Amazon Route 53 Resolver. Set a conditional forward rule for the Active Directory domain to the Active Directory servers. Update the VPC DHCP options set to AmazonProvidedDNS

B. Update the DNS service on the Active Directory servers to forward all non-authoritative queries to the VPC Resolver.

define outbound Route 53 Resolver

forward all non-authoritative queries to VPC Resolver

Q284 A fitness tracking company serves users around the world , with its primary markets in North America and Asia. The company needs to design an infrastructure for its read-heavy user authorization application with the following requirements -Be resilient to problems with the application in any Regio -Write to a database in a single RegionRead from multiple Regions -Support resilience across application tiers in each Region -Support the relational database semantics reflected in the application Which combination of steps should a solutions architect take?(Select TWO)

C. Use an Amazon Route 53 geolocation routing policy combined with a failover routing policy

E. Set up active-active web and application servers in each Region Deploy an Amazon Aurora global database with clusters in each Region Set up the application to use the in-region Aurora database endpoints. Create snapshots of the web and application servers and store them in an Amazon S3 bucket in both Regions.
use Route 53 geolocation routing policy
deploy Aurora global db with clusters in each Region

Q285 A company is planning on hosting its ecommerce platform on AWS using a multi-tier web application designed for a NoSQL database. The company plans to use the us-west-2 Region as its primary Region. The company wants to ensure that copies of the application and data are available in second Region, us-west-1, for disaster recovery. The company wants to keep the time to fail over as low as possible. Failing back to the primary Region should be possible without administrative interaction after the primary service is restored. Which design should the solutions architect use?
A.Use AWS CloudFormation StackSets to create the stacks in both Regions with Auto Scaling groups for the web and application tiers. Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication. Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us- west-1 in the évent of an outage. Use Amazon DynamoDB global tables for the database tier.
use DynamoDB global tables

Q286 A company wants to host a global web application on AWS. It has the following design requirements: -The access pattern must allow for fetching data from multiple data sources -minimize the cost of API calls -Keep page load times to within 50 ms -Provide user authentication and authorization and manage data access for different user -personas (for example, administrator, manager, or engineer) -use a serverless design Which set of strategies should a solutions architect use?
C. Use Amazon Cloudfront with Amazon S3 to host the web application. Use AWS Appsync to build the application Apls. Use Amazon Cognito groups for each user persona. Authorize data access by leveraging Amazon Cognito groups in AWS AppSync resolvers
use Cognito groups for user persona

Q287 A company's processing team has an AWS account with a production application. The application runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The EC2 instances are hosted in private subnets in a VPC in the eu-west-1 Region. The VPC was assigned the CIDR block of 10.0.0.0/16. The billing team recently created a new AWS account and deployed an application on EC2 instances that are hosted in private subnets in a VPC in the eu-central-1 Region. The new VPC is assigned the CIDR block of 10.0.0.0/16. The processing application needs to securely communicate with the billing application over a proprietary TCP port. What should a solutions architect do to meet this requirement with the LEAST amount of operational effort?
A. In the billing team's account, create a new VPC and subnets in eu-central-1 that use the CIDR block of 192.168.0.0/16. Redeploy the application to the new subnets. Configure a VPC peering connection between the two VPCs.
re-deploy app to new subnets

Q288 A company needs to migrate two individual applications from on premises to AWS:-The first application is a legacy custom application that is hosted on a physical Windows server. The application

source code is no longer available. The application has little documentation, has hard coded operating system configuration settings, and is used by an external third party. -The second application is an IBM Db2 database that is hosted on a single Linux VM that uses network-attached storage (NAS) to store the database data. The company uses this database internally for employee records. The applications are hosted in a data center that the company plans to decommission in 90 days. Where possible, the company must use managed AWS services. Which actions for migration should a solutions architect recommend to meet these requirements? (Select TWO)

A. Migrate the Windows server with the legacy application to Amazon EC2 by using CloudEndure Migration.

D. Migrate the IBM Db2 database data to Amazon RDS for MySQL by using AWS Database Migration Service (AWS DMS) and the AWS Schema Conversion Tool replication agent .

migrate windows server to EC2 by using CloudEndure Migration

migrate IBM DB2 to RDS by using AWS Database Migration Service

Q289 A company hosts an application on Amazon EC2 instance and needs to store files in Amazon S3. The files should never traverse the public internet, and only the application EC2 instances are granted access to a specific Amazon S3 bucket. A solutions architect has created a VPC endpoint for Amazon S3 and connected the endpoint to the application VPC. Which additional steps should the solutions architect take to meet these requirements?

C. Assign an endpoint policy to the VPC endpoint that restricts access to a specific S3 bucket. Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint. Assign an IAM role to the application EC2 instances and only allow access to this role in the S3 bucket's policy.

Assign IAM role to EC2. instance

Q290 A company is migrating its three-tier web application from on-premises to the AWS Cloud. The company has the following requirements for the migration process:-Ingest machine Images from the on-premises environment. -Synchronize changes from the on-promises environment to the AWS environment until the production cutover. -Minimize downtime when executing the Production Cutover -Migrate the virtual machines root volumes and data volumes. Which solution will satisfy these requirements with minimal operational overhead?

A.Use AWS Server Migration Service(SMS)to create and launch a replication job for each tier of the application Launch instances from the AMIs created by AWS MS After initial testing , perform a final replication and create new instances from the updated AMIs.

use AWS SMS(Server Migration Service) to create and launch a replication job

Q291 A Company has an application that sells tickets Online and experiences bursts of demand every 7 days. The application has a stateless presentation layer running on Amazon EC2, an Oracle database to store unstructured data catalog Information, and a backend API layer. The front-end layer uses an Elastic Load Balancer to distribute the load across nine On-demand Instances over three Availability Zones(AZs). The Oracle database is running on **a**

Single EC2 Instance. The company is experiencing performance issues when running more than two Concurrent campaigns. A Solutions architect must design a solution that meets the following requirements -Address Scalability Issues. -Increase the level of concurrency . -Eliminate licensing costs. -Improve reliability Which set of steps should the solutions architect take?

C. Create an Auto Scaling group for the front end with a combination of On-demand and SpotInstances to reduce costs Convert the tables in the Oracle database into Amazon Dynamodb tables
create auto scaling group, convert tables in Oracle into Dynamodb

Q292 A business is operating a distributed application on an Auto Scaling group of Amazon EC2 machines. The program saves massive volumes of data on an Amazon Elastic File System (Amazon EFS) file system and generates fresh data on a monthly basis. The organization needs to back up its data in a secondary AWS Region to use as a fallback in the event of a main Region performance issue. The company's RTO is one hour. A solutions architect must develop a backup plan while keeping the additional expense to a minimum. Which backup method, if any, should the solutions architect propose in order to satisfy these requirements?
A. Create a pipeline in AWS Data Pipeline. Copy the data to an EFS file system in the secondary Region Create a lifecycle policy to move files to the EFS One Zone-Infrequent Access storage class
create pipeline in AWS Data Pipeline

Q293 A company is deploying a public-facing global application on AWS using Amazon Cloudfront. The application communicates with an external system A solutions architect needs to ensure the data is secured during end-to-end transit and at rest Which combination of steps will satisfy these requirements?(Select THREE)
B. Acquire a public certificate from a third-party vendor and deploy it to Cloudfront, an ApplicationLoad Balancer and Amazon EC2 instances
D. Provision Amazon EBS encrypted volumes using AWS KMS
E. Use SSL or encrypt data while communicating with the external system using a VPN
acquire public certificate
provision EBS encrypted volumes
Use SSL

Q294 An enterprise companies data science team wants to provide a safe , cost-effective way to provide easy access to Amazon Sagemaker. The data scientists have limited AWS knowledge and need to be able to launch a Jupyter notebook instance. The notebook instance needs to have a preconfigured AWS KMS key to encrypt data at rest on the machine learning storage volume without exposing the complex setup requirements Which approach will allow the company to set up a self-service mechanism for the data scientists to launch Jupyter notebooks in its. AWS accounts with the LEAST amount of operational overhead?
C. Create an AWS Cloudformation template to launch a Jupyter notebook instance using the AWS:SageMakerc: Notebook Instance resource type with a preconfigured KMS key.Simplify the parameter names , such as the instance size , by mapping them to Small , Large ,and X-large using the Mappings section in Cloudformation. Display the URL to the notebook using the Outputs section , then upload the template into an AWS Service Catalog product in the data scientists portfolio , and share it with the data scientist's LAM role
share it with data scientist’s IAM role

Q295 An enterprise company is building an infrastructure services platform for its users. The company has the following requirements:-Provide least privilege access to users when launching AWS infrastructure so users cannot provision unapproved services. -Use a central account to manage the creation of infrastructure services. -Provide the ability to distribute infrastructure services to multiple accounts in AWS Organizations. -Provide the ability to enforce tags on any infrastructure that is started by users. Which combination of actions using AWS services will meet these requirements?(Choose three.)
B. Develop infrastructure services using AWS Cloud Formation templates. Upload each template as an AWS Service Catalog product to portfolios created in a central AWS account. Share these portfolios with the Organization's structure created for the company.
D. Allow user IAM roles to have ServiceCatalogEndUserAccess permissions only. Use an automation script to import the central portfolios to local AWS accounts, copy the TagOption, assign users access and apply launch constraints.
E. Use the AWS Service Catalog TagOption Library to maintain a list of tags required by the company. Apply the TagOption to AWS Service Catalog products or portfolios.
upload each template as AWS Service Catalog product
allow user IAM roles to have ServiceCatalogEndUserAccess permissions only
use AWS Service Catalog TagOption Library

Q296 A media company has a static web application that is generated programmatically. The company has a build pipeline that generates HTML content that is uploaded to an Amazon S3 bucket served by Amazon Cloudfront. The build pipeline runs inside a Build Account. The S3 bucket and CloudFront distribution are in a Distribution Account. The build pipeline uploads the files to Amazon S3 using an IAM role in the Build Account. The S3 bucket has a bucket policy that only allows Clouderont to read objects using an origin access identity (CAI). During testing , all attempts to access the application using the Cloudfront URL result in an HTTP 403 Access Denied response. What should a solutions architect suggest to the company to allow access to the objects in Amazon S3 through Cloudfront?
A.Modify the S3 upload process in the Build Account to add the bucket-owner-full-control AOL to the objects at upload
add bucket-owner-full-control AOL to object at upload

Q297 A Solutions architect is implementing Infrastructure as code for a two-tier web application in an AWS Cloudformation template. The web frontend application will be deployed on Amazon EC2 instances in an Auto Scaling group. The backend database will be an Amazon RDS for MYSQL DB Instance. The database password will be rotated every 60 days How can the solutions architect MOST securely manage the configuration of the applications database credentials?
B. Create a new AWS Secrets Manager secret resource in the Cloudformation template to be used as the database password. Configure the application to retrieve the password from Secrets Manager when needed Reference the secret resource for the value of the MasterUserPassword property in the AWS RDS:DBInstance resource using a dynamic reference
config app to retrieve password from Secrets Manager

Q298 A weather service provides high-resolution weather maps from a web application hosted on AWS in the eu-west-1 Region The weather maps are updated frequently and stored in Amazon S3 along with static HTML content. The web application is fronted by Amazon Cloudfront: The company recently expanded to serve users in the us-east-1 Region , and these new users report that viewing their

respective weather maps is slow from time to time Which combination of steps will resolve the us-east-1 performance issues?(Select TWO)
B. Create a new S3 bucket in us-east-1 Configure S3 cross-region replication to synchronize from the S3 bucket in eu-west-1
D. Use Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1
create a new S3 bucket in us-east-1.
use S3 bucket in. us-east-1

Q299 A company is using AWS CloudFormation as its deployment tool for all applications. It stages all application binaries and templates within Amazon S3 bucket with versioning enable Developers have access to an Amazon EC2 instance that hosts the integrated development (IDE). The Developers download the application binaries from Amazon S3 to the EC2 instance, make changes, and upload the binaries to an S3 bucket after running the unit locally. The developers want to improve the existing deployment mechanism and implement CI/CD using AWS CodePipeline. The developers have the following requirements:-Use AWS CodeCommit for source control. -Automate unit testing and security scanning. -Alert the Developers when unit tests fail. -Turn application features on and off, and customize deployment dynamically as part of CI/CD. -Have the lead Developer provide approval before deploying an application. Which solution will meet these requirements?
A.Use AWS Code Build to run unit tests and security scans Use an Amazon Eventbridge rule to sendAmazon SNS alerts to the developers when unit tests fail. Write AWS Cloud Development Kit(AWS CDK) constructs for different solution features and use a manifest file to turn features on and off in the AWS CDK application:Use a manual approval stage in the pipeline to allow the lead developer to approve applications
use AWS Code Build to run unit tests

Q300 An ecommerce website running on AWS uses an Amazon RDS for MySQL DB instance with General Purpose SSD storage. The developers chose an appropriate instance type based on demand, and configured 100 GB of storage with a sufficient amount of free space. The website was running smoothly for a few weeks until a marketing campaign launched. On the second day of the campaign, users reported long wait times and time outs. Amazon CloudWatch metrics indicated that both reads and writes to the DB instance were experiencing long response times. The CloudWatch metrics show 40% to 50% CPU and memory utilization, and sufficient free storage space is still available. The application server logs show no evidence of database connectivity issues. What could be the root cause of the issue with the marketing campaign?
A.It exhausted the IO credit balance due to provisioning low disk storage during the setup phase.
It exhausted I/O credit balance

Q301 A company built an ecommerce website on AWS using a three tier web architecture. The application Is Java based and composed of an Amazon Cloudfront distribution , an Apache web server layer of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MYSQL database.Last month, during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts. The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics.Some of the web servers were terminated before logs could be collected and the Aurora metrics were not sufficient for query performance analysis . Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events?(Select THREE)

A. Configure the Aurora MYSQL DB cluster to publish slow query and error logs to Amazon Cloudwatch Logs
B. Implement the AWS X-Ray SDK to trace incoming HTTP requests on the EC2instances and implement tracing of SQL queries with the X Ray SDK for Java
D. Install and configure an Amazon Cloudwatch Logs agent on the EC2 instances to send the Apache logs to Cloudwatch Logs
publish slow query and error logs to CloudWatch logs
implement AWS X-Ray SDK to trace request
install and configure Amazon CLoudwatch logs agent

Q302 A North American company with headquarters on the East Coast is deploying a new web application running on Amazon EC2 in the us-east-1 Region. The application should dynamically scale to meet user demand and maintain resiliency. Additionally, the application must have disaster recovery capabilities in an active-passive configuration with the us-west-1 Region Which steps should a solutions architect take after creating a VPC in the us- east-1 Region?
B. Deploy an Application Load Balancer(ALB) spanning multiple Availability Zones(AZs)to the VPC in the us-east-1 Region Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB Deploy the same solution to the us-west-1 Region. Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions
create Route 53 record set with a failover routing policy

Q303 A company has a web application that uses Amazon API Gateway, AWS Lambda, and Amazon Dynamodb.A recent marketing campaign has increased demand. Monitoring software reports that many requests have significantly longer response times than before the marketing campaign.A solutions architect enabled Amazon Cloudwatch Logs for API Gateway and noticed that errors are occurring on 20% of the requests In Cloudwatch, the Lambda function Throttles metric represents 1% of the requests and the Errors metric represents 10% of the requests. Application logs indicate that . when errors occur , there is a call to Dynamodb. What change should the solutions architect make to improve the current response times as the web application becomes more popular?
B. Implement Dynamodb auto scaling on the table
implement DynamoDB auto scaling on table

Q304 A European online newspaper service hosts its public-facing WordPress site in a collocated data center in London. The current WordPress infrastructure consists of a load balancer, two web servers, and one MySQL database server. A solutions architect is tasked with designing a solution with the following requirements:-Improve the website's performance -Make the web tier scalable and stateless -Improve the database server performance for read-heavy loads -Reduce latency for users across Europe and the US-Design the new architecture with a goal of 99.9% availability Which solution meets these requirements while optimizing operational efficiency?
A. Use an Application Load Balancer (ALB) in front of an Auto Scaling group of WordPress Amazon EC2 instances in one AWS Region and three Availability Zones. Configure an Amazon ElastiCache cluster in front of a Multi-AZ Amazon Aurora MySQL DB cluster. Move the WordPress shared files to Amazon EFS. Configure Amazon CloudFront with the ALB as the origin, and select a price class that includes the US and Europe.
config Amazon ElastiCache in front of Multi-AZ Amazon Aurora MySQL DB

Q305 A solutions architect has implemented a SAML 2.0 federated identity solution with their company's on-premises identity provider (IdP) to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal, access to the AWS environment is granted. However, when test users attempt to authenticate through the federated identity web portal, they are not able to access the AWS environment. Which items should the solutions architect check to ensure identity federation is properly configured? (Choose three.)
B. The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.
D. The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider, the ARN of the IAM role, and the SAML assertion from IdR.
F. The company's IdP defines SAML assertions that properly map users or groups in the company to IAM roles with appropriate permissions.
set SAML provider as principal
web portal calls STS AssumeRoleWithSAML API with ARN of SAML provider
company's idP defines SAML assertion

Q306 A company wants to improve cost awareness for its Amazon EMR platform. The company has allocated budgets for each team's Amazon EMR usage :When a budgetary threshold is reached, a notification should be sent by email to the budget office distribution list. Teams should be able to view their EMR cluster expenses to date.A solutions architect needs to create a solution that ensures this policy is proactively and centrally enforced in a multi-account environment Which combination of steps should the solutions architect take to meet these requirements?(Select Two)
A. Update the AWS Cloudformation template to include the AWS::Budgets::Budget::resource with the Notifications Withsubscribers property
D. Create an AWS Service Catalog portfolio for each team. Add each teams Amazon EMR cluster as an AWS Cloudformation template to their Service Catalog portfolio as a Product
update AWS Cloudformation template
create AWS Service Catalog portfolio

Q307 A company is developing a gene reporting device that will collect genomic information to assist researchers with collecting large samples of data from a diverse population. The device will push 8 KB of genomic data every second to a data platform that will need to process and analyze the data and provide information back to researchers. The data platform must meet the following requirements -Provide near-real-time analytics of the inbound genomic data. -Ensure the data is flexible, parallel, and durable. -Deliver results of processing to a data warehouse Which strategy should a solutions architect use to meet these requirements?
B. Use Amazon Kinesis Data Streams to collect the inbound sensor data , analyze the data with Kinesis clients and save e results to an Amazon Redshift cluster using Amazon EMR
use Kinesis Data Streams to collect inbound sensor data

Q308 A company is using AWS CodePipeline for the CI/CD of an application to an Amazon EC2 Auto Scaling group. All AWS resources are defined in AWS CloudFormation templates. The application artifacts are stored in an Amazon S3 bucket and deployed to the Auto Scaling group using instance user data scripts. As the application has become more complex, recent resource changes in the

CloudFormation templates have caused unplanned downtime.How should a solutions architect improve the CI/CD pipeline to reduce the likelihood that changes in the templates will cause downtime?
B. Implement automated testing using AWS CodeBuild in a test environment. Use CloudFormation change sets to evaluate changes before deployment. Use AWS CodeDeploy to leverage blue/green deployment patterns to allow evaluations and the ability to revert changes, if needed.
implement automated testing using Amazon CodeBuild

Q309 A web application is hosted in a dedicated VPC that is connected to a company's on-premises data center over a Site-to-Site VPN connection. The application is accessible from the company network only. This is a temporary non-production application that is used during business hours. The workload is generally low with occasional surges. The application has an Amazon Aurora MySQL provisioned database cluster on the backend. The VPC has an internet gateway and NAT gateways attached. The web servers are in private subnets in an Auto Scaling group behind an Elastic Load Balancer. The web servers also upload data to an Amazon S3 bucket through the internet. A solutions architect needs to reduce operational costs and simplify the architecture. Which strategy should the solutions architect use?
B. Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only. Detach the internet gateway and remove the NAT gateways from the VPC. Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes.
Detach the internet gateway and remove NAT(network address translation) gateways from VPC

Q310 A company has built a high performance computing (HPC) cluster in AWS for a tightly coupled workload that generates a large number of shared files stored in Amazon EFS. The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1,000 EC2 instances, overall performance was well below expectations. Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? (Choose three.)
A. Ensure the HPC cluster is launched within a single Availability Zone
C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled.
F. Replace Amazon EFS with Amazon FSx for Lustre.
ensure HPC cluster is launched within a single AZ
select EC2 types with an Elastic Fabric Adapter(EFA) enabled
replace Amazon EFS with Amazon FSx for Lustre

Q311 A company built an application based on AWS Lambda deployed in an AWS CloudFormation stack. The last production release of the web application introduced an issue that resulted in an outage lasting several minutes. A solutions architect must adjust the deployment process to support a canary release. Which solution will meet these requirements?
A. Create an alias for every new deployed version of the Lambda function. Use the AWS CLI update-alias command with the routing-config parameter to distribute the load.
use AWS CLI update-alias command

Q312 A company runs a popular public-facing ecommerce website. Its user base is growing quickly from a local market to a national market. The website is hosted in an on-premises data center with web servers

and a MySQL database. The company wants to migrate its workload to AWS. A solutions architect needs to create a solution to:-Improve security -Improve reliability -Improve availability -Reduce latency -Reduce maintenance Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)
A. Use Amazon EC2 instances in two Availability Zones for the web servers in an Auto Scaling group behind an Application Load Balancer.
B. Migrate the database to a Multi-AZ Amazon Aurora MySQL DB cluster.
E. Host static website content in Amazon S3. Use Amazon CloudFront to reduce latency while serving webpages. Use AWS WAF to improve website security
use EC2 in two AZ for web server
migrate db to a Multi-AZ amazon Aurora MySQL DB
use Amazon CouldFront to reduce latency

Q313 A company provides auction services for artwork and has users across North America and Europe. The company hosts its application in Amazon EC2 instances in the us-east-1 Region. Artists upload photos of their work as large-size, high-resolution image files from their mobile phones to a centralized Amazon S3 bucket created in the us-east-1 Region. The users in Europe are reporting slow performance for their image uploads. How can a solutions architect improve the performance of the image upload process?
C. Configure the buckets to use S3 Transfer Acceleration.
config buckets to use S3 Transfer Acceleration

Q314 A company has developed a new release of a popular video game and wants to make it available for public download. The new release package is approximately 5 GB in size. The company provides downloads for existing releases from a Linux-based, publicly facing FTP site hosted in an on- premises data center. The company expects the new release will be downloaded by users worldwide. The company wants a solution that provides improved download performance and low transfer costs, regardless of a user's location. Which solutions will meet these requirements?
C. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Use Amazon CloudFront for the website. Publish the game download URL for users to download the package.
upload game files to S3. use CloudFront for website

Q315 A new startup is running a serverless application using AWS Lambda as the primary source of compute. New versions of the application must be made available to a subset of users before deploying changes to all users. Developers should also have the ability to abort the deployment and have access to an easy rollback mechanism. A solutions architect decides to use AWS CodeDeploy changes when a new version is available. Which CodeDeploy configuration should the solutions architect use?
C. A canary deployment
canary deployment

Q316 A company has developed a custom tool used in its workflow that runs within a Docker container. The company must perform manual steps each time the container code is updated to make the container image available to new workflow executions. The company wants to automate this process to eliminate

manual effort and ensure a new container image is generated every time the tool code is updated. Which combination of actions should a solutions architect take to meet these requirements? (Choose three.)
A. Configure an Amazon ECR repository for the tool. Configure an AWS CodeCommit repository containing code for the tool being deployed to the container image in Amazon ECR
C. Configuration an AWS CodeBuild project that pulls the latest tool container image from Amazon ECR, updates the container with code from the source AWS CodeCommit repository, and pushes the updated container image to Amazon ECR.
F. Configure an AWS CodePipeline pipeline that sources the tool code from the AWS CodeCommit repository and initiates an AWS CodeBuild build.
configure an Amazon ECR repository for tool
configure AWS CodeBuild project
Configure AWS CodePipeline and initiates an AWS CodeBuild build

Q317 A company needs to create a centralized logging architecture for all of its AWS accounts. The architecture should provide near-real-time data analysis for all AWS CloudTrail logs and VPC Flow Logs across all AWS accounts. The company plans to use Amazon Elasticsearch Service (Amazon ES) to perform log analysis in the logging account. Which strategy a solutions architect use to meet these requirements?
B. Configure CloudTrail and VPC Flow Logs to send data to a log group in Amazon CloudWatch account. Configure a CloudWatch subscription filter in each AWS account to send data to Amazon Kinesis Data Firehouse in the logging account. Load data from Kinesis Data Firehouse into Amazon ES in the logging account.
send data to Kinesis Data Firehouse

Q318 A company standardized its method of deploying applications to AWS using AWS CodePipeline and AWS Cloud Formation. The applications are in TypeScript and Python. The company has recently acquired another business that deploys applications to AWS using Python scripts. Developers from the newly acquired company are hesitant to move their applications under Cloud Formation because it would require that they learn a new domain- specific language and eliminate their access to language features, such as looping. How can the acquired applications quickly be brought up to deployment standards while addressing the developers' concerns?
D. Define the AWS resources using TypeScript or Python. Use the AWS Cloud Development Kit (AWS CDK) to create CloudFormation templates from the developers' code, and use the AWS CDK to create CloudFormation stacks. Incorporate the AWS CDK as a CodeBuild job in CodePipeline.
define AWS resources using TypeScript or Python

Q319 A healthcare company runs a production workload on AWS that stores highly sensitive personal information. The security team mandates that, for auditing purposes, any AWS API action using AWS account root user credentials must automatically create a high-priority ticket in the company's ticketing system. The ticketing system has a monthly 3-hour maintenance window when no tickets can be created. To meet security requirements, the company enabled AWS CloudTrail logs and wrote a scheduled AWS Lambda function that uses Amazon Athena to query API actions performed by the root user. The Lambda function submits any actions found to the ticketing system API. During a recent security audit, the security team discovered that several tickets were not created because the ticketing system was unavailable due to planned maintenance. Which combination of steps should a solutions architect take to ensure that the incidents are reported to the ticketing system even during planned maintenance? (Choose two.)

D. Modify the Lambda function to be triggered when there are messages in the Amazon SQS queue and to return successfully when the ticketing system API has processed the request.
E. Create an Amazon EventBridge rule that triggers on all API events where the invoking user identity is root. Configure the EventBridge rule to write the event to an Amazon SQS queue.
modify Lambda to be triggered when messages in SQS queue
create an Amazon EventBridge rule

Q320 A company is running a two-tier web-based application in an on-premises data center. The application user consists of a single server running a stateful application. The application connects to a PostgreSQL database running on a separate server. The application's user base is expected to grow significantly, so the company is migrating the application and database to AWS. The solution will use Amazon Aurora PostgreSQL, Amazon EC2 Auto Scaling, and Elastic Load Balancing. Which solution will provide a consistent user experience that will allow the application and database tiers to scale?
C. Enable Aurora Auto Scaling for Aurora Replicas. Use an Application Load Balancer with the robin routing and sickly sessions enabled.
enable Aurora Auto Scaling for Replicas ,use ALB with robin routing

Q321 A solutions architect is designing a network for a new cloud deployment. Each account will need autonomy to modify route tables and make changes. Centralized and controlled egress internet connectivity is also needed. The cloud footprint is expected to grow to thousands of AWS accounts.Which architecture will meet these requirements?
D. A shared transit gateway to which each VPC will be attached. Outbound internet access will route through a fleet of VPN-attached firewalls.
a shared transit gateway (充当云路由器, 设计大规模网络)

Q322 A solutions architect needs to migrate 50 TB of NFS data to Amazon S3. The files are on several NFS file servers on a corporate network. These are dense file systems containing tens of millions of small files. The system operators have configured the file interface on an AWS Snowball Edge device and are using a shell script to copy data. Developers report that copying the data to the Snowball Edge device is very slow. The solutions architect suspects this may be related to the overhead of encrypting all the small files and transporting them over the network. Which changes can be made to speed up the data transfer?
C. Increase the number of parallel copy jobs to increase the throughput of the Snowball Edge device.
increase num of parallel copy jobs

Q323 A company hosts a blog post application on AWS using Amazon API Gateway, Amazon DynamoDB, and AWS Lambda. The application currently does not use API keys to authorize requests. The API model is as follows: GET/posts/[postid] to get post details GET/users[userid] to get user details GET/comments/[commentid] to get comments details The company has noticed users are actively discussing topics in the comments section, and the company wants to increase user engagement by marking the comments appears in real time. Which design should be used to reduce comment latency and improve user experience?
C. Use AWS AppSync and leverage WebSockets to deliver comments.
use AWS AppSync

Q324 An IoT company has rolled out a fleet of sensors for monitoring temperatures in remote locations. Each device connects to AWS IoT Core and sends a message 30 seconds, updating an Amazon DynamoDB table. A System Administrator uses AWS IoT to verify the devices are still sending messages to AWS IoT Core:the database is not updating. What should a Solutions Architect check to determine why the database is not being updated?
B. Verify that AWS IoT monitoring shows that the appropriate AWS IoT rules are being executed, and that the AWS IoT rules are enabled with the correct rule actions.
verify AWS IoT rules are being executed

Q325 An enterprise company is using a multi-account AWS strategy. There are separate accounts for development staging and production workloads. To control costs and improve governance the following requirements have been defined:-The company must be able to calculate the AWS costs for each project. -The company must be able to calculate the AWS costs for each environment development, staging and production. -Commonly deployed IT services must be centrally managed. -Business units can deploy pre-approved IT services only. -Usage of AWS resources in the development account must be limited. Which combination of actions should be taken to meet these requirements? (Choose three.)
A. Apply environment, cost center, and application name tags to all taggable resources. D. Create a portfolio for each business unit and add products to the portfolios using AWS CloudFormation in AWS Service Catalog.
F. Configure SCPs in AWS Organizations to allow services available using AWS.
Apply environment, cost center, and application name tags to all taggable resources
create a portfolio for each business unit
configure SCPs in AWS Organization

Q326 A company is planning to migrate an existing high performance computing (HPE) solution to the AWS Cloud. The existing solution consists of a 12-node cluster running Linux with high speed interconnectivity developed on a single rack. A solutions architect needs to optimize the performance of the HPE cluster. Which combination of steps will meet these requirements? (Choose two.)
B. Deploy Amazon EC2 instances in a placement group.
C. Use Amazon EC2 instances that support Elastic Fabric Adapter (EFA).
deploy EC2 in a placement group
use EC2 that support Elastic Fabric Adapter

Q327 A company hosts a game player-matching service on a public facing, physical, on-premises instance that all users are able to access over the internet. All traffic to the instance uses UDP. The company wants to migrate the service to AWS and provide a high level of security. A solutions architect needs to design a solution for the player-matching service using AWS. Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)
A. Use a Network Load Balancer (NLB) in front of the player-matching instance. Use a friendly DNS entry in Amazon Route 53 pointing to the NLB's Elastic IP address.
D. Configure a network ACL rule to block all non-UDP traffic. Associate the network ACL with the subnets that hold the load balancer instances.
F. Enable AWS Shield Advanced on all public-facing resources.
use a Network Load Balancer(NLB) in front of player-matching instance
configure a network ACL rule to block all non-UDP traffic

enable AWS Shield Advanced on all public-facing resources

Q328 A company has multiple AWS accounts and manages these accounts which are AWS Organizations. A developer was given IAM user credentials to access AWS resources. The developer should have read-only access to all Amazon S3 buckets in the account. However, when the developer tries to access the S3 buckets from the console, they receive an access denied error message with no bucket listed. A solution architect reviews the permissions and finds that the developer's IAM user is listed as having read-only access to all S3 buckets in the account. Which additional steps should the solutions architect take to troubleshoot the issue? (Choose two.)
C. Check the SCPs set at the organizational units (OUs).
D. Check for the permissions boundaries set for the IAM user.
check SCPs set
check for permission boundaries set

Q329 A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into delays of AWS Billing and Cost Management. There are various accounts associated with AWS Organizations, including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging. Management requires cost center numbers and project ID numbers for all existing and future DynamoDB tables and RDS distances. Which strategy should the solutions architect provide to meet these requirements?
C. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID. Use SCPs to restrict resource creation that do not have the cost center and project ID on the resource.
use SCPs to restrict resource creation

Q330 A company has an application that generates reports and stores them in an Amazon S3 bucket. When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company's security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved. Which set of actions will immediately remediate the security issue without impacting the application's normal workflow?
D. Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcis option to TRUE on the bucket.
use Block Public Access feature in S3

Q331 A company hosts a legacy application that runs on an Amazon EC2 instance inside a VPC without internet access. Users access the application with a desktop program installed on their corporate laptops. Communication between the laptops and the VPC flows through AWS Direct Connect (DX). A new requirement states that all data in transit must be encrypted between users and the VPC. Which strategy should a solutions architect use to maintain consistent network performance while meeting this new requirement?
B. Create a new public virtual interface for the existing DX connection, and create a new VPN that connects to the VPC over the DX public virtual interface.

create a new public virtual interface for existing DX connection

Q332 A company is creating a centralized logging service running on Amazon EC2 that will receive and analyze logs from hundreds of AWS accounts. AWS PrivateLink is being used to provide connectivity between the client services and the logging service. In each AWS account with a client an interface endpoint has been created for the logging service and is available. The logging service running on EC2 instances with a Network Load Balancer (NLB) are deployed in different subnets. The clients are unable to submit logs using the VPC endpoint. Which combination of steps should a solutions architect take to resolve this issue? (Choose two.)
A. Check that the NACL is attached to the logging service subnet to allow communications to and from the NLB subnets. Check that the NACL is attached to the NLB subnet to allow communications to and from the logging service subnets running on EC2 instances.
C. Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the NLB subnets.
找关键字NLB subnets

Q333 A solutions architect needs to define a reference architecture for a solution for three-tier applications with web, application, and NoSQL data layers. The reference architecture must meet the following requirements:-High availability within an AWS Region -Able to fail over in 1 minute to another AWS Region for disaster recovery -Provide the most efficient solution while minimizing the impact on the user experience. Which combination of steps will meet these requirements? (Choose three.)
B. Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region. Set Time to Live (TTL) to 30 seconds.
C. Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.
E. Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources
use an Route 53 failover routing policy for failover
use a global table within Amazon DynamoDB
Implement a hot standby model

Q334 A company runs an application on a fleet of Amazon EC2 instances. The application requires low latency and random access to 100 GB of data. The application must be able to access the data at up to 3.000 IOPS. A Development team has configured the EC2 launch template to provision a 100-GB Provisioned IOPS (PIOPS) Amazon EBS volume with 3 000 IOPS provisioned. A Solutions Architect is tasked with lowering costs without impacting performance and durability. Which action should be taken?
C. Update the EC2 launch template to allocate a new 1-TB EBS General Purpose SSD (gp2) volume.
General Purpose SSD (gp2)

Q335 A company recently transformed its legacy infrastructure provisioning scripts to AWS CloudFormation templates. The newly developed templates are hosted in the company's private GitHub repository. Since adopting CloudFormation, the company has encountered several issues with updates to

the CloudFormation templates, causing execution or creating environments. Management is concerned by the increase in errors and has asked a Solutions
Architect to design the automated testing of CloudFormation template updates. What should the Solution Architect do to meet these requirements?
C. Use AWS CodePipeline to create and execute a change set from the CloudFormation templates stored in the GitHub repository. Configure a CodePipeline action to be deployed with testing scripts run by AWS CodeBuild.
config a CodePipeline action to be deployment

Q336 A company wants to improve cost awareness for its Amazon EMR platform. The company has allocated budgets for each team's Amazon EMR usage. When a budgetary threshold is reached, a notification should be sent by email to the budget office's distribution list. Teams should be able to view their EMR cluster expenses to date. A solutions architect needs to create a solution that ensures the policy is proactively and centrally enforced in a multi- account environment. Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)
A. Update the AWS CloudFormation template to include the AWS: Budgets: Budget: resource with the Notifications WithSubscribers property.
D. Create an AWS Service Catalog portfolio for each team. Add each team's Amazon EMR cluster as an AWS CloudFormation template to their Service Catalog portfolio as a Product.
update CloudFormation template
Create AWS Service Catalog portfolio

Q337 A company is migrating its on-premises systems to AWS. The user environment consists of the following systems:-Windows and Linux virtual machines running on VMware. -Physical servers running Red Hat Enterprise Linux. The company wants to be able to perform the following steps before migrating to AWS:-Identify dependencies between on-premises systems. -Group systems together into applications to build migration plans. -Review performance data using Amazon Athena to ensure that Amazon EC2 instances are right-sized. How can these requirements be met?
D. Install the AWS Application Discovery Service Discovery Agent on the physical on-pre-map servers. Instal the AWS Application Discovery Service Discovery Connector in VMware vCenter. Allow the Discovery Agent to collect data for a period of time.
install AWS App Discovery Service Agent, install AWS app Discovery Service Connector

Q338 A company hosts a web application on AWS in the us-east-1 Region. The application servers are distributed across three Availability Zones behind an Application Load Balancer. The database is hosted in a MYSQL database on an Amazon EC2 instance. A solutions architect needs to design a cross-Region data recovery solution using AWS services with an RTO of less than 5 minutes and an RPO of less than 1 minute. The solutions architect is deploying application servers in us-west- 2, and has configured Amazon Route 53 health checks and DNS failover to us-west-2. Which additional step should the solutions architect take?
B. Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2.
migrate db to Amazon Aurora global db

Q339 A company wants to migrate its on-premises data center to the AWS Cloud. This includes thousands of virtualized Linux and Microsoft Windows servers, SAN storage, Java and PHP applications with MYSQL, and Oracle databases. There are many department services hosted either in the same data center or externally. The technical documentation is incomplete and outdated. A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration. Which tools or services should solutions architect use to plan the cloud migration (Choose three.)
A. AWS Application Discovery Service
D. AWS Cloud Adoption Readness Tool (CART)
F. AWS Migration Hub
AWS Application Discovery Service
AWS Cloud Adoption Readness Tool(CART)
AWS Migration Hub

Q340 A company decided to purchase Amazon EC2 Reserved Instances. A solutions architect is tasked with implementing a solution where only the master account in AWS Organizations is able to purchase the Reserved Instances. Current and future member accounts should be blocked from purchasing Reserved Instances. Which solution will meet these requirements?
A.Create an SCP with the Deny effect on the ec2:PurchaseReservedInstancesOffering action. Attach the SCP to the root of the organization.
attach SCP to root of organization

Q341 A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud. Currently, users upload input files through a web portal. The web server then stores the uploaded files on NAS and messages the processing server over a message queue. Each media file can take up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours. What is the MOST cost-effective migration recommendation?
D. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. Use Amazon EC2 instances in an EC2 Auto Seating group to pull requests from the queue and process the files. Scale the EC2 instances based on the SQS queue length. Store the processed files in an Amazon S3 bucket
Scale EC2 instances based on SQS queue length

Q342 A company has a media catalog with metadata for each item in the catalog. Different types of metadata are extracted from the media items by an application running on AWS Lambda. Metadata is extracted according to a number of rules with the output stored in an Amazon ElastiCache for Redis cluster. The extraction process is done in batches and takes around 40 minutes to complete. The update process is triggered manually whenever the metadata extraction rules change. The company wants to reduce the amount of time it takes to extract metadata from its media catalog. To achieve this, a solutions architect has split the single metadata extraction Lambda function into a Lambda function for each type of metadata. Which additional steps should the solutions architect take to meet the requirements?
A. Create an AWS Step Functions workflow to run the Lambda functions in parallel. Create another Step Functions workflow that retrieves a list of media items and executes a metadata extraction workflow for each one
create AWS Step Functions workflow to run, Create another Step Functions workflow

Q343 An AWS partner company is building a service in AWS Organizations using its organization named org1. This service requires the partner company to have access to AWS resources in a customer account, which is in a separate organization named org2. The company must establish least privilege security access using an API or command line tool to the customer account. What is the MOST secure way to allow org1 to access resources in org2?
D. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN), including the external ID in the IAM role's trust policy, when requesting access to perform the required tasks.
use IAM role's Amazon Resource Name(ARN), including external ID in IAM role's trust policy

Q344 A company's security compliance requirements state that all Amazon EC2 images must be scanned for vulnerabilities and must pass a CVE assessment. A solutions architect is developing a mechanism to create security-approved AMIs that can be used by developers. Any new AMIs should go through an automated assessment process and be marked as approved before developers can use them. The approved images must be scanned every 30 days to ensure compliance. Which combination of steps should the solutions architect take to meet these requirements while following best practices? (Choose two.)
B. Use AWS Lambda to write automatic approval rules. Store the approved AMI list in AWS Systems Manager Parameter Store. Use Amazon EventBridge to trigger an AWS Systems Manager Automation document on all EC2 instances every 30 days
C. Use Amazon Inspector to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned.
use Amazon EventBridge to trigger an AWS Systems Manager Automation document
use Amazon Inspector to run CVE assessment on EC2

Q345 A company is launching a web-based application in multiple regions around the world. The application consists of both static content stored in a private Amazon S3 bucket and dynamic content hosted in Amazon ECS containers content behind an Application Load Balancer (ALB). The company requires that the static and dynamic application content be accessible through Amazon CloudFront only. Which combination of steps should a solutions architect recommend to restrict direct content access to CloudFront? (Choose three.)
A. Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the ALB.
C. Configure CloudFront to add a custom header to origin requests.
F. Create a CloudFront Origin Access Identity (OAI) and add it to the CloudFront distribution. Update the S3 bucket policy to allow access to the OAI only
associate web ACL with the ALB
configure CLoudFront to add a custom header to origin requests
create CloudFront Origin Access Identity(OAI)

Q346 A company has multiple lines of business (LOBs) that roll up to the parent company. The company has asked its solutions architect to develop a solution with the following requirements:-Produce a single AWS invoice for all of the AWS accounts used by its LOBs. -The costs for each LOB account should be broken out on the invoice. -Provide the ability to restrict services and features in the LOB accounts, as defined by the company's governance policy. -Each LOB account should be delegated full administrator

permissions, regardless of the governance policy. Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)
B. Use AWS Organizations to create a single organization in the parent account. Then, invite each LOB's AWS account to pin the organization.
D. Create an SCP that allows only approved services and features, then apply the policy to the LOB accounts.
invite each LOB's AWS account to pin organization
create a SCP that allows only approved service and features

Q347 A solutions architect has been assigned to migrate a 50 TB Oracle data warehouse that contains sales data from on-premises to Amazon Redshift Major updates to the sales data occur on the final calendar day of the month. For the remainder of the month, the data warehouse only receives minor daily updates and is primarily used for reading and reporting. Because of this, the migration process must start on the first day of the month and must be complete before the next set of updates occur. This provides approximately 30 days to complete the migration and ensure that the minor daily changes have been synchronized with the Amazon Redshift data warehouse. Because the migration cannot impact normal business network operations, the bandwidth allocated to the migration for moving data over the internet is 50 Mbps. The company wants to keep data migration costs low. Which steps will allow the solutions architect to perform the migration within the specified timeline?
D. Create an AWS Snowball import job. Configure a server in the company's data center with an extraction agent. Use AWS SCT to manage the extraction agent and convert the Oracle schema to an Amazon Redshift schema. Create a new project in AWS SCT using the registered data extraction agent. Create a local task and an AWS DMS task in AWS SCT with replication of ongoing changes. Copy data to the Snowball device and return the Snowball device to AWS. Allow AWS DMS to copy data from Amazon S3 to Amazon Redshift. Verify that the data migration is complete and perform the cut over to Amazon Redshift.
Create AWS Snowball import job. use AWS SCT(schema conversion tool) to manage extraction agent

Q348 A solutions architect is designing a disaster recovery strategy for a three-tier application. The application has an RTO of 30 minutes and an RPO of 5 minutes for the data tier. The application and web tiers are stateless and leverage a fleet of Amazon EC2 instances. The data tier consists of a 50 TB Amazon Aurora database. Which combination of steps satisfies the RTO and RPO requirements while optimizing costs? (Choose two.)
A. Create daily snapshots of the EC2 instances and replicate the snapshots to another Region.
D. Create a cross-Region Aurora Replica of the database.
Create daily snapshots of EC2 and replicate to another region
Create cross-region Aurora Replica

Q349 A company has a primary Amazon S3 bucket that receives thousands of objects every day. The company needs to replicate these objects into several other S3 buckets from various AWS accounts. A solutions architect is designing a new AWS Lambda function that is triggered when an object is created in the main bucket and replicates the object into the target buckets. The objects do not need to be replicated in real time. There is concern that this function may impact other critical Lambda functions due to Lambda's regional concurrency limit. How can the solutions architect ensure this new Lambda function will not impact other critical Lambda functions?

C. Configure S3 event notifications to add events to an Amazon SQS queue in a separate account. Create the new Lambda function in the same account as the SQS queue and trigger the function when a message arrives in the queue
Configure S3 event notification

Q350 A company wants to run a serverless application on AWS. The company plans to provision its application in Docker containers running in an Amazon ECS cluster. The application requires a MySQL database and the company plans to use Amazon RDS. The company has documents that need to be accessed frequently for the first 3 months, and rarely after that. The document must be retained for 7 years. What is the MOST cost-effective solution to meet these requirements?
B. Create an ECS cluster using a fleet of Spot Instances, with Spot Instance draining enabled. Provision the database and its read replicas in Amazon RDS using Reserved Instances. Store the documents in a secured Amazon S3 bucket with a lifecycle policy to move the documents that are older than 3 months to Amazon S3 Glacier, then delete the documents from Amazon S3 Glacier that are more than 7 years old.
provision db and read replicas in RDS using Reserved instance.

Q351 A media company is serving video files stored in Amazon S3 using Amazon CloudFront. The development team needs access to the logs to diagnose faults and perform service monitoring. The log files from CloudFront may contain sensitive information about users. The company uses a log processing service to remove sensitive information before making the logs available to the development team. The company has the following requirements for the unprocessed logs:-The logs must be encrypted at rest and must be accessible by the log processing service only. -Only the data protection team can control access to the unprocessed log files. -AWS CloudFormation templates must be stored in AWS CodeCommit. -AWS
CodePipeline must be triggered on commit to perform updates made to CloudFormation templates. -CloudFront is already writing the unprocessed logs to an Amazon S3 bucket, and the log processing service is operating against this S3 bucket. Which combination of steps should a solutions architect take 53 to meet the company's requirements? (Choose two.**)**
A. Create an AWS KMS key that allows the AWS Logs Delivery account to generate data keys for encryption Configure S3 default encryption to use server-side encryption with KMS managed keys (SSEKMS) on the log storage bucket using the new KMS key.Modify the KMS key policy to allow the log processing service to perform decrypt operations.
D. Create a new CodeCommit repository for the AWS KMS key template. Create an IAM policy to allow commits to the new repository and attach it to the data protection team's users. Create a new CodePipeline pipeline with a custom IAM role to perform KMS key updates using CloudFormation Modify the KMS key policy to allow the CodePipeline IAM role to modify the key policy.
create AWS KMS key that allows AWS Logs Delivery account to generate data keys for encryption
create a new CodeCommit repository for AWS KMS key template

Q352 A company's service for video game recommendations has just gone viral. The company has new users from all over the world. The website for the service is hosted on a set of Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The website consists of static content with different resources being loaded depending on the device type. Users recently reported that the load

time for the website has increased.Administrators are reporting high loads on the EC2 instances that host the service. Which set actions should a solutions architect take to improve response times?
B. Move content to Amazon S3. Create an Amazon CloudFront distribution to serve content out of the S3 bucket.Use Lambda@Edge to load different resources based on the User-Agent HTTP header.
Use Lambda@Edge to load resources

Q353 A company is planning a large event where a promotional offer will be introduced. The company's website is hosted on AWS and backed by an Amazon RDS for PostgreSQL DB instance. The website explains the promotion and includes a sign-up page that collects user information and preferences. Management expects large and unpredictable volumes of traffic periodically, which will create many database writes. A solutions architect needs to build a solution that does not change the underlying data model and ensures that submissions are not dropped before they are committed to the database. Which solution meets these requirements?
B. Use Amazon SQS to decouple the application and database layers. Configure an AWS Lambda function to write items from the queue into the database.
use Amazon SQS to decouple app

Q354 A team collects and routes behavioral data for an entire company. The company runs a Multi-AZ VPC environment with public subnets, private subnets, and an internet gateway Each public subnet also contains a NAT gateway Most of the company's applications read from and write to Amazon Kinesis Data Streams. Most of the workloads run in private subnets. A solutions architect must review the infrastructure The solutions architect needs to reduce costs and maintain the function of the applications. The solutions architect uses Cost Explorer and notices that the cost in the EC2-Other category is consistently high A further review shows that NatGateway- Bytes charges are increasing the cost in the EC2-Other category. What should the solutions architect do to meet these requirements?
D. Add an interface VPC endpoint for Kinesis Data Streams to the VPC.Ensure that the VPC endpoint policy allows traffic from the applications
ensure VPC endpoint allows traffic from app

Q355 A large financial company is deploying applications that consist of Amazon EC2 and Amazon RDS instances to the AWS Cloud using AWS CloudFormation. The CloudFormation stack has the following stack policy: { "statement" : [{ "Effect" : "Allow", "Action" : ["Update:*"], "Principal": "*", , "Resource" : “*” }] } The company wants to ensure that developers do not lose data by accidentally removing or replacing RDS instances when updating the CloudFormation stack. Developers also still need to be able to modify or remove EC2 instances as needed. How should the company change the stack policy to meet these requirements?
C. Add a second statement that specifies "Effect":"Deny", "Action":["Update:Delete", "Update:Replace"] for all logical RDS resources.
Action: [”Update: Delete, “Update: replace”]

Q356 A company is currently in the design phase of an application that will need an RPO of less than 5 minutes and an RTO of less than 10 minutes. The solutions architecture team is forecasting that the database will store approximately 10 TB of data. As part of the design, they are looking for a database

solution that will provide the company with the ability to fail over to a secondary Region. Which solution will meet these business requirements at the LOWEST cost?
B. Deploy an Amazon RDS instance with a cross-Region read replica in a secondary Region. In the event of a failure, promote the read replica to become the primary.
Deploy RDS instance with cross-Region read replica

Q357 A solutions architect has an operational workload deployed on Amazon EC2 instances in an Auto Scaling group. The VPC architecture spans two Availability Zones (AZ) with a subnet in each that the Auto Scaling group is targeting. The VPC is connected to an on-premises environment and connectivity cannot be interrupted. The maximum size of the Auto Scaling group is 20 instances in service. The VPC IPy4 addressing is as follows:VPC CIDR:10.0.0.0/23 AZ1 subnet CIDR:10.0.0.0/24 AZ2 subnet CIDR:10.0.1.0/24 Since deployment, a third AZ has become available in the Region. The solutions architect wants to adopt the new AZ without adding additional IPv4 address space and without service downtime. Which solution will meet these requirements?
A. Update the Auto Scaling group to use the AZ2 subnet only. Delete and re-create the AZ1 subnet using half the previous address space.Adjust the Auto Scaling group to also use the new AZl subnet. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Remove the current AZ2 subnet. Create a new AZ2 subnet using the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.
update Auto Scaling group to use AZ2 subnet only. Delete and re-create AZ1 subnet using half the previous address space.

Q358 A company is storing data on premises on a Windows file server. The company produces 5 GB of new data daily. The company migrated part of its Windows-based workload to AWS and needs the data to be available on a file system in the cloud. The company already has established an AWS Direct Connect connection between the on-premises network and AWS. Which data migration strategy should the company use?
B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx
use AWS DataSync to schedule to replicate data between file server and Amazon FSx

Q359 A company uses AWS Organizations to manage one parent account and nine member accounts. The number of member accounts is expected to grow as the business grows. A security engineer has requested consolidation of AWS CloudTrail logs into the parent account for compliance purposes. Existing logs currently stored in Amazon S3 buckets in each individual member account should not be lost. Future member accounts should comply with the logging strategy. Which operationally efficient solution meets these requirements?
C. Configure an organization-level CloudTrail in the parent account to deliver log events to a central S3 bucket. Migrate the existing CloudTrail logs from each member account to the central S3 bucket. Delete the existing CloudTrail and log in the member accounts.
delete existing CloudTrail and logs

Q360 A company provides a centralized Amazon EC2 application hosted in a single shared VPC. The centralized application must be accessible from client applications running in the VPCs of other business

units. The centralized application front end is configured with a Network Load Balancer (NLB) for scalability. Up to 10 business unit VPCs will need to be connected to the shared VPC. Some of the business unit VPC CIDR blocks overlap with the shared VPC, and some overlap with each other. Network connectivity to the centralized application in the shared VPC should be allowed from authorized business unit VPCs only. Which network configuration should a solutions architect use to provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC?
B. Create a VPC endpoint service using the centralized application NLB and enable the option to require endpoint acceptance. Create a VPC endpoint in each of the business unit VPCs using the service name of the endpoint service.Accept authorized endpoint requests from the endpoint service console.
Create VPC endpoint service using centralized application NLB

Q361 A company has an on-premises monitoring solution using a PostgreSQL database for persistence of events. The database is unable to scale due to heavy ingestion and it frequently runs out of storage. The company wants to create a hybrid solution and has already set up a VPN connection between its network and AWS. The solution should include the following attributes:-Managed AWS services to minimize operational complexity. -A buffer that automatically scales to match the throughput of data and requires no ongoing administration. -A visualization tool to create dashboards to observe events in near-real time. -Support for semi-structured JSON data and dynamic schemas. Which combination of components will enable the company to create a monitoring solution that will satisfy these requirements? (Choose two.)
A. Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events.
D. Configure Amazon Elasticsearch Service (Amazon ES) to receive events. Use the Kibana endpoint deployed with Amazon ES to create near-real- time visualizations and dashboards
use Kinesis Data Firehose to buffer events
Configure Elasticsearch Service(ES) to receive events

Q362 A life sciences company is using a combination of open source tools to manage data analysis workflows and Docker containers running on servers in its on-premises data center to process genomics data. Sequencing data is generated and stored on a local storage area network (SAN), and then the data is processed. The research and development teams are running into capacity issues and have decided to re-architect their genomics analysis platform on AWS to scale based on workload demands and reduce the turnaround time from weeks to days. The company has a high-speed AWS Direct Connect connection. Sequencers will generate around 200 GB of data for each genome, and individual jobs can take several hours to process the data with ideal compute capacity. The end result will be stored in Amazon S3. The company is expecting 10-15 job requests each day. Which solution meets these requirements?
C. Use AWS DataSync to transfer the sequencing data to Amazon S3.Use S3 events to trigger an AWS Lambda function that starts an AWS Step Functions workflow.Store the Docker images in Amazon Elastic Container Registry (Amazon ECR) and trigger AWS Batch to run the container and process the sequencing data.
use AWS DataSync to transfer sequencing data to S3

Q363 A company has five physical data centers in specific locations around the world. Each data center has hundreds of physical servers with a mix of Windows and Linux-based applications and database

services. Each data center also has an AWS Direct Connect connection of 10 Gbps to AWS with a company-approved VPN solution to ensure that data transfer is secure. The company needs to shut down the existing data centers as quickly as possible and migrate the servers and applications to AWS. Which solution meets these requirements?
C. Instal the CloudEndure Migration agent onto each physical machine. Create a migration blueprint, and start the replication. Once the replication is complete, launch the Amazon EC2 instances in cutover mode.
install CloudEndure Migration agent

Q364 A security engineer determined that an existing application retrieves credentials to an Amazon RDS for MySQL database from an encrypted file in Amazon S3. For the next version of the application, the security engineer wants to implement the following application design changes to improve security:-The database must use strong, randomly generated passwords stored in a secure AWS managed service. -The application resources must be deployed through AWS CloudFormation. -The application must rotate credentials for the database every 90 days. A solutions architect will generate a CloudFormation template to deploy the application. Which resources specified in the CloudFormation template will meet the security engineer's requirements with the LEAST amount of operational overhead?
A. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Specify a Secrets Manager RotationSchedule resource to rotate the database password every 90 days.
specify a Secrets Manger Rotation Schedule resource to rotate db pwd

Q365 A company has a three-tier application running on AWS with a web server, an application server, and an Amazon RDS MySQL DB instance. A solutions architect is designing a disaster recovery (DR) solution with an RPO of 5 minutes. Which solution will meet the company's requirements?
C. Use Amazon EC2 Image Builder to create and copy AMIs of the web and application server to both the primary and DR Regions. Create a cross-Region read replica of the DB instance in the DR Region. In the event of a disaster, promote the read replica to become the master and reprovision the servers with AWS CloudFormation using the AMIs
use amazon EC2 Image Builder to create/ copy AMIs

Q366 A company wants to migrate its corporate data center from on premises to the AWS Cloud. The data center includes physical servers and VMs that use VMware and Hyper-V. An administrator needs to select the correct services to collect data for the initial migration discovery process. The data format should be supported by AWS Migration Hub. The company also needs the ability to generate reports from the data. Which solution meets these requirements?
C. Use the AWS Application Discovery Service agent for data collection on physical servers and Hyper-V. Use the AWS Agentless Discovery Connector for data collection on VMware. Store the collected data in Amazon S3. Query the data with Amazon Athena. Generate reports by using Amazon QuickSight.
generate reports by using Amazon QuickSight

Q367 A company is using Amazon Aurora MySQL for a customer relationship management (CRM) application. The application requires frequent maintenance on the database and the Amazon EC2 instances on which the application runs. For AWS Management Console access, the system

administrators authenticate against AWS Identity and Access Management (IAM) using an internal identity provider. For database access, each system administrator has a user name and password that have previously been configured within the database. A recent security audit revealed that the database passwords are not frequently rotated. The company wants to replace the passwords with temporary credentials using the company's existing AWS access controls. Which set of options will meet the company's requirements?
C. Enable IAM database authentication on the database. Attach an IAM policy to each system administrator's role to map the role to the database user name. Instal the Amazon Aurora SSL certificate bundle to the system administrators' certificate trust store. Use the AWS CLI to generate an authentication token used when connecting to the database.
attach IAM policy to each system administrator's role

Q368 A company's AWS architecture currently uses access keys and secret access keys stored on each instance to access AWS services. Database credentials are hard-coded on each instance. SSH keys for command-line remote access are stored in a secured Amazon S3 bucket. The company has asked its solutions architect to improve the security posture of the architecture without adding operational complexity. Which combination of steps should the solutions architect take to accomplish this? (Choose three.)
A. Use Amazon EC2 instance profiles with an IAM role
C. Use AWS Systems Manager Parameter Store to store database credentials
F. Use AWS Systems Manager Session Manager for remote access
Use EC2 profiles with an IAM role
use AWS Systems manager Parameter Store to store db credential
Use AWS Systems Manager Session Manager for remote access

Q369 A company wants to change its internal cloud billing strategy for each of its business units. Currently, the cloud governance team shares reports for overal cloud spending with the head of each business unit. The company uses AWS Organizations to manage the separate AWS accounts for each business unit. The existing tagging standard in Organizations includes the application, environment, and owner. The cloud governance team wants a centralized solution so each business unit receives monthly reports on its cloud spending. The solution should also send notifications for any cloud spending that exceeds a set threshold. Which solution is the MOST cost-effective way to meet these requirements?
B. Configure AWS Budgets in the organization's master account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization's master account to create monthly reports for each business unit.
config AWS Budgets in organization's master account

Q370 A company is configuring connectivity to a multi-account AWS environment to support application workloads that serve users in a single geographic region. The workloads depend on a highly available, on-premises legacy system deployed across two locations. It is critical for the AWS workloads to maintain connectivity to the legacy system, and a minimum of 5 Gbps of bandwidth is required. All application workloads within AWS must have connectivity with one another. Which solution will meet these requirements?
C. Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from two DX partners for each on-premises location. Create a transit gateway and a DX gateway in a central

network account. Create a transit virtual interface for each DX interface and associate them with the DX gateway. Create a gateway association between the DX gateway and the transit gateway.
Create a transit gateway and Direct Connect(DX) gateway

Q371 A financial company needs to create a separate AWS account for a new digital wallet application. The company uses AWS Organizations to manage its accounts. A solutions architect uses the IAM user Support from the master account to create a new member account with finance1 @example.com as the email address. What should the solutions architect do to create IAM users in the new member account?
A. Sign in to the AWS Management Console with AWS account root user credentials by using the 64-character password from the initial AWS Organizations email sent to financel @example.com. Set up the IAM users as required.
email sent to finance1@example.com

Q372 A company has developed a custom tool used in its workflow that runs within a Docker container. The company must perform manual steps each time the container code is updated to make the container image available to new workflow executions. The company wants to automate this process to eliminate manual effort and ensure a new container image is generated every time the tool code is updated. Which combination of actions should a solutions architect take to meet these requirements? (Select THREE.)
A. Configure an Amazon ECR repository for the tool. Configure an AWS CodeCommit repository containing cod for the tool being deployed to the container image in Amazon ECR
C. Configure an AWS CodeBuild project that pulls the latest tool container image from Amazon ECR, updates the container with code from the source AWS CodeCommit repository, and pushes the updated container image to Amazon ECR.
F. Configure an AWS CodePipeline pipeline that sources the tool code from the AWS CodeCommit repository and initiates an AWS CodeBuild build.
config Amazon ECR repository
config AWS CodeBuild
initiates an AWS CodeBuild build

Q373 A company is migrating its three-tier web application from on-premises to the AWS Cloud. The company has the following requirements for the migration process:-Ingest machine images from the on-premises environment -Synchronize changes from the on-premises environment to the AWS environment until the production cutover -Minimize downtime when executing the production cutover -Migrate the virtual machines' root volumes and data volumes Which solution will satisfy these requirements with minimal operational overhead?
A. Use AWS Server Migration Service (SMS) to create and launch a replication job for each tier of the application. Launch instances from the AMIs created by AWS SMS. After initial testing perform a final replication and create new instances from the updated AMIs
use AWS Server Migration Service(SMS) to create and launch a replication job

Q374 A company has several development teams collaborating on multiple projects. Developers frequently move between projects, and each project requires access to a different set of AWS resources. There are current projects for web mobile, and database development. However, the set of projects may change over time. Developers should have full control over the resources for the project to which they are assigned, and read-only access to resources for all other projects. When developers are assigned to a

different project or new AWS resources are added the company wants to minimize policy maintenance. What type of control policy should a solutions architect recommend?
D. Create a customer managed policy document for each project that requires access to AWS resources. Specify full control of the resources that belong to a project and read-only access for all other resources within the account. Attach the project-specific policy document to an IAM group. Change the group membership when developers change projects. Update the policy document when the set of resources changes
change group membership when developer change projects

Q375 A company uses a load balancer to distribute traffic to Amazon EC2 instances in a single Availability Zone. The company is concerned about security and wants a solutions architect to re-architect the solution to meet the following requirements:-Inbound requests must be filtered for common vulnerability attacks -Rejected requests must be sent to a third-party auditing application -All resources should be highly available Which solution meets these requirements?
D. Configure a Multi-AZ Auto Scaling group using the application's AMI. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target. Create an Amazon Kinesis Data Firehose with a destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the WebACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.
configure a Multi-AZ Auto Scaling group. Create Amazon Kinesis Data Firehose with a destination of third-party auditing app.

Q376 A solutions architect is designing a web application on AWS that requires 99.99% availability. The application will consist of a three-tier architecture that supports 300.000 web requests each minute when experiencing peak traffic. The application will use Amazon Route 53 for DNS resolution. Amazon CloudFront as the content delivery network (CDN), an Elastic Load Balancer far load balancing. Amazon EC2 Auto Scaling groups to scale the application tier, and Amazon Aurora MySQL as the backend database. The backend database load will average 90% reads and 10% writes. The company wants to build a cost-effective solution, but reliability is critical. Which set of strategies should the solutions architect use?
B. Build the application in a single AWS Region. Deploy the EC2 application layer to three Availability Zones using an Auto Scaling group with a minimum desired capacity sufficient to process 450.000 requests each minute. Use a Multi-AZ Amazon Aurora MySQL DB duster with two Au ora Replicas. Each Aurora Replica must have enough capacity to support 100% of the peak read queries.
process 450000 requests each minute

Q377 An online magazine will launch its latest edition this month. This edition will be the first to be distributed globally. The magazine's dynamic website currently uses an Application Load Balance in front of the web tier, a fleet of Amazon EC2 instances for web and application servers, and Amazon Aurora MySQL. Portions of the website include static content and almost all traffic is read-only. The magazine is exporting a significant spike in internet traffic when the new edition is launched. Optimal performance is a top priority for the week following the launch. Which combination of steps should a solutions architect take to reduce system response times for a global audience? (Select three.)
B. Delete existing credit card payment details that have been added to the member accounts.

E. Update any resource-based policies by using the aws: PrincipalOrgId condition key to reference the new organization ID.
F. Delete the OrganizationAccountAccessRole IAM role from each of the member accounts.
delete existing credit card payment details
update resource-based policies
delete OrganizationAccountAccessRole IAM role

Q378 A company has a web-based application deployed in the app-southeast-2 Region behind an Application Load Balancer ALB). AWS Certificate Manager (ACM) has issued a TLS certificate for example.com. This certificate is deployed to the ALB. There is a record set in Amazon Route 53 for example.com associated with the ALB. Due to increased load on the application, the company wants to use Amazon CloudFront. This transition cannot cause application downtime. Which combination of actions can achieve this? (Choose Three.)
C. Create a new ACM certificate in the us-east-1 Region for example.com. Create a CloudFront distribution and use the ACM certificate in the us- east-1 Region. Set origin example.com as the custom origin
D. Update Route 53 for example. com to the alias record of the CloudFront distribution
F. Update the ALB security group to allow access from the CloudFront Edge locations only.
create a CloudFront distribution and use ACM certificate in us-east-1 region
update Route 53 for example.com
update ALB security group

Q379 A company has migrated hundreds of servers from an on-premises data center to Amazon EC2 instances. The company still uses the third-party systems management tools in its data center to manage the EC2 instances. Those tools require that an agent be installed on the EC2 instances. Sometimes the systems management agents fail or do not start automatically, which interferes with the application of patches. The company's DevOps team must be able to apply patches in a timely manner. The team also needs to know if any of the EC2 instances and on-premises servers are failing compliance checks. What is the MOST operationally efficient solution that meets these requirements?
B. Install an Amazon CloudWatch agent on EC2 instances to monitor the status of the third-party systems management agent Configure AWS Systems Manager Run Command to start the systems management agent when the agent is not running
install Amazon CloudWatch agent on EC2

Q380 A solutions architect at a large company needs to set up network security for outbound traffic to the internet from all AWS accounts within an organization in AWS Organizations. The organization has more than 100 AWS accounts, and the accounts route to each other by using a centralized AWS Transit Gateway. Each account has both an internet gateway and a NATgateway for outbound traffic to the internet. The company deploys resources only
Into a single AWS Region. The company needs the ability to add centrally managed rule-based filtering on all outbound traffic to the internet for all AWS accounts in the organization. The peak load of outbound traffic will not exceed 25 Gbps in each Availability Zone. Which solution meets these requirements?
B. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC.Configure a new NAT gateway. Use an AWS Network Firewall firewall for rule-based filtering.Create Network Firewall endpoints In each Availability Zone.Modify all default routes to point to the Network Firewall endpoints

modify routes to point to Network Firewall endpoints

Q381 A company's lease of a colocated storage facility will expire in 90 days. The company wants to move to AWS to avoid signing a contract extension. The company environment consists of 200 virtual machines and a NAS with 40 TB of data. Most of the data is archival, yet instant access is required when data is requested Leadership wants to ensure minimal downtime during the migration. Each virtual machine has a number of customized configurations. The company's existing 1Gbps network connection is mostly idle especially after business hours. Which combination of steps should the company take to migrate to AWS while minimizing downtime and operational impact? (Select TWO)

B. Use AWS SMS to migrate the virtual machines

C. Use AWS Storage Gateway to migrate the data to cloud-native storage

use AWS SMS to migrate vm

use AWS Storage Gateway to migrate data to cloud-native storage

Q382 A company's factory and automation applications are running in a single VPC. More than 20 applications run on a combination of Amazon EC2, Amazon Elastic Container Service (Amazon ECS), and Amazon RDS. The company needs to determine which costs on the monthly AWS bill are attributable to each application or team. The company also must be able to create reports to compare costs from the last 12 months and to help forecast costs for the next 12 months. A solutions architect must recommend an AWS Billing and Cost Management solution that provides these cost reports. Which combination of actions will meet these requirements? (Select THREE.)

A. Activate the user-defined cost allocation tags that represent the application and the team.

C. Create a cost category for each application in Billing and Cost Management.

F. Enable Cost Explorer.

activate user-defined cost allocation tags

create cost category

enable cost explorer

Q383 A solutions architect has been assigned to migrate a 50 TB Oracle data warehouse that contains sales data from on-premises to Amazon Redshift Major updates to the sales data occur on the final calendar day of the month. For the remainder of the month the data warehouse only receives minor daily updates and is primarily used for reading and reporting. Because of this the migration process must start on the first day of the month and must be
complete before the next set of updates occur. This provides approximately 30 days to complete the migration and ensure that the minor daily changes have been synchronized with the Amazon Redshift data warehouse. Because the migration cannot impact normal business network operations the bandwidth allocated to the migration for moving data over the internet is 50 Mbps. The company wants to keep data migration costs low. Which steps will allow the solutions architect to perform the migration within the specified timeline?

D. Create an AWS Snowball import job Configure a server in the company's data center with an extraction agent Use AWS SCT to manage the extraction agent and convert the Oracle schema to an Amazon Redshift schema. Create a new project in AWS SCT using the registered data extraction agent Create a local task and an AWS DMS task in AWS SCT with replication of ongoing changes Copy data to the Snowball device and return the Snowball device to AWS Allow AWS DMS to copy data from Amazon S3 to Amazon Redshift Verify that the data migration is complete and perform the cut over to Amazon Redshift

use AWS SCT to manage

Q384 A company operates pipelines across North America and South America. The company assesses pipeline inspection gauges with imagery and ultrasonic sensor data to monitor the condition of its pipelines. The pipelines are in areas with intermittent or unavailable internet connectivity. The imager data at each site requires terabytes of storage each month. The company wants a solution to collect the data at each site in monthly intervals and to store the data with high durability. The imagery captured must be preprocessed and uploaded to a central location for persistent Storage. Which actions should a solutions architect take to meet these requirements?

D. Deploy AWS IoT Greengrass n eligible hardware across the sites. Configure AWS Lambda on the devices for preprocessing. Ship the devices back to the closest AWS Region and store the data in Amazon S3 buckets

deploy AWS IoT Greengrass, ship device back to closest Region

Q385 A solutions architect is troubleshooting an application that runs on Amazon EC2 instances. The EC2 instance runs in an Auto Scaling group. The application needs to access user data in an Amazon DynamoDB table that has fixed provisioned capacity. To match the increased workload, the solutions architect recently doubled the maximum size of the Auto Scaling group. New, when many instances launch at the same time, some application components are throttled when the component scans the DynamoDB table. The Auto Scaling group terminates the falling instances and starts new instances until all applications are running. A solution architect must implement a solution to mitigate the throttling issue in the MOST cost- effective manner. Which solution will meet these requirements?

D. Add DynamoDB Accelerator (DAX) to the table.

add DynamoDB Accelerator(DAX) to table

Q386 A large company runs workloads in VPCs that are deployed on AWS accounts. Each VPC consists of public subnets and private subnets that span across multiple Availability Zones NAT gateway are deployed in the public subnets and allow outbound connectivity to the internet from the private subnets. A solution architect is working on a hub-and-spoke design. All private subnets in the spoke VPCs must route traffic to the internal through an address VPC. The solutions architect has deployed a NAT gateway in an egress VPC in a central AWS account. Which set of additional steps should the solution architect take to meet these requirements?

B. Create a transit gateway and share it with the existing AWS accounts. Attach existing VPCs to the transit gateway. Configure routing to allow access to the internet.

create transit gateway and share it with existing account

Q387 A large company has a business-critical application that runs in a single AWS Region. The application consists of multiple Amazon EC2 instances and an amazon RDS Multi-AZ DB instance. The EC2 instances run in an Amazon EC2 Scaling group across multiple Availability Zones. A solution architect is implementing a disaster recovery (DR) plan for the application. The solution architect has created a pilot light application deployments in a new Region, which Is referred to as the RD Region. The DR environment has an Auto Scaling group with a single EC2 instance and a read replica of the RDS DB instance. The solution architect must automate a failover from the primary application environment to the pilot light environment in the DR Region. Which solution meets the requirements with the MOST operational efficiency?

D. publish an application available metric to Amazon CloudWatch in the DR Region from the application environment in the primary Region. Create a CloudWatch alarm in the DR Region that is invoked when the application availability metric steps are being delivered. Configure the CloudWatch alarm to send a notification to an Amazon Simple and to add EC2 instances to the Auto Scaling group.
add EC2 instances to Auto Scaling group

Q388 A developer reports receiving an Error 403:Access Denied message when they try to download an object from an Amazon S3 bucket. The S3 bucket is accessed using an S3 endpoint inside a VPC, and is encrypted with an AWS KMS key. A solution architect has verified that the developer is assuming the correct IAM role in the account that allows the object to be downloaded. The S3 bucket policy and the NACL are also valid. Which additional step should the solutions architect take to troubleshoot this issue?
B. Verify that the IAM role has permission to decrypt the referenced KMS key.
verify that IAM role has permission to decrypt referenced KMS key

Q389 A company is migrating its data from an on-premises Oracle relational database server to an Amazon Aurora PostgresQL DB cluster. The new database implementation must have at least one standby DB instance in a geographically separate location. In the event that the primary DB instance fails, the standby DB instance must be automatically promoted to the primary DB instance. Both the RTO and RPO are 5 minutes. Which solution will meet these requirements?
D. Turn on the Aurora global database feature. Define a secondary AWS Region .
turn on Aurora global db feature

Q390 A company is running a containerized application in the AWS Cloud. The application is running by using Amazon Elastic Container Service (Amazon ECS) on a set Amazon EC2 instance. The EC2 instances run in an Auto Scaling group. The company uses Amazon Elastic Container Registry (Amazon ECRJ to store its container images. When a new image version is uploaded, the new image version receives a unique tag. The company needs a solution that inspects new image versions for common vulnerabilities and exposures. The solution must automatically delete new image tags that have Critical or High severity findings. The solution also must notify the development team when such a deletion occurs. Which solution meets these requirements'?
A. Configure scan on push on the repository. Use Amazon EventBndge (Amazon Cloud Watch Events) to invoke an AWS Step Functions state machine when a scan is complete for images that have Critical or High severity findings. Use the Step Functions state machine to delete the image tag for those images and to notify the development team through Amazon Simple Notification Service (Amazon SNS)
use Amazon EventBridge(CloudWatch Events) to invoke AWS Step Functions state machine

Q391 A travel company built a web application that uses Amazon Simple Email Service (Amazon SES) to send email notifications to users. The company needs to enable logging to help troubleshoot email delivery issues. The company also needs the ability to do searches that are based on recipient, subject, and time sent. Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)
A. Create an Amazon SES configuration set with Amazon Kinesis Data Firehose as the destination. Choose to send logs to an Amazon S3 bucket.

C. Use Amazon Athena to query the logs in the Amazon S3 bucket for recipient, subject, and time sent.
create Amazon SES configuration set
Use Amazon Athena to query logs in S3 bucket

Q392 A startup company recently migrated a large ecommerce website to AWS The website has experienced a 70% increase in sales. Software engineers are using a private GitHub repository to manage code. The development team is using Jenkins for builds and unit testing. The engineers need to receive notifications for bad builds and zero downtime during deployments. The engineers also need to ensure any changes to production are seamless for users and can be rolled back in the event of a major issue. The software engineers have decided to use AWS CodePipeline to manage their build and deployment process. Which solution will meet these requirements?
B. Use GitHub webhooks to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS Code Build to conduct unit testing. Deploy in a blue/green deployment using AWS CodeDeploy.
use Jenkins plugin for AWS Code Build to conduct unit testing. Deploy in blue/green deployment

Q393 A company has developed a mobile game. The backend for the game runs on several virtual machines located in an on-premises data center. The business logic is exposed using a REST API with multiple functions. Player session data is stored file storage. Backend services use different API keys for throttling and to distinguish between live and test traffic. The load on the game backend varies throughout the day During peak hours, the server capacity is not sufficient. There are also latency issues when fetching player sessions data. Management has asked a solutions architect to present a cloud architecture that can handle the games varying load and provide low-latency data access. The API model should not be changed. Which solution meets these requirements?
C. Implement the REST API using Amazon API Gateway Run the business logic in AWS Lambda Store player session data in Amazon DynamoDB with on-demand capacity
implement REST API using API Gateway

Q394 A company uses Amazon S3 to host a web application. Currently, the company uses a continuous integration tool running on an Amazon EC2 instance that builds and deploys the application by uploading it to an S3 bucket. A Solutions Architect needs to enhance the security of the company's platform with the following requirements:-A build process should be run in a separate account from the account hosting the web application. -A build process should have minimal access in the account it operates in. Long-lived credentials should not be used. As a start the Development team created two AWS accounts:one for the application named web account, and one for the build process named build account. Which solution should the Solutions Architect use to meet the security requirements?
B. In the build account, create a new IAM role which can be assumed by Amazon EC2 only. Attach the role to the EC2 instance running the continuous integration process Create an IAM policy to allow s3 PutObject calls on the S3 bucket in the web account. In the web account create an S3 bucket policy attached to the S3 bucket that allows the newly createdIAM role to use s3 PutObject calls.
create a new IAM role which can be assumed by EC2 only. allows newly createdIAM role to use S3 PutObject calls

Q395 A large company will be migrating to AWS. The company has 20 business units and anticipates another 10 coming online in the future. Each business unit will need its own IP range and will operate in its own AWS account. There will be a lot of communication between business units with very large data transfers. The company wants to make sure that the proposed solution will minimize data transfer costs and reduce complexity. How should a solutions architect design the network to meet these requirements?
B. Create a transit gateway in a networking account. Share the transit gateway with each business unit's AWS account. Attach the VPC in each account to the transit gateway.
Create transit gateway in networking account

Q396 A company hosts a web application on AWS that uses Amazon RDS for MySQL Multi-AZ DB instances. Usage of the web application has increased recently. Users have indicated that dynamic reports in the application load slowly. Which configuration change will improve application performance while ensuring the database is highly available for data operations?
A. Add a read replica and configure the application to direct read requests to it
add a read replica

Q397 A company is using AWS Organizations to manage multiple accounts. Due to regulatory requirements the company wants to restrict specific member accounts to certain AWS Regions where they are permitted to deploy resources. The resources in the accounts must be tagged enforced based on a group standard and centrally managed with minimal configuration. What should a solutions architect do to meet these requirements?
D. Associate the specific member accounts with a new OU Apply a tag policy and an SCP using conditions to limit Regions
associate account with a new OU

Q398 A company has an application that sends newsletters through email to users. The application runs on two Amazon EC2 instances in a VPC. The first EC2 instance contains the email application that sends email directly to users. The second EC2 instance contains a MySQL database that is heavily dependent upon relational data Each EC instance is controlled by its own Auto Scaling group with a minimum and maximum of one instance Management wants improved application reliability and support for personalized email. Which set of steps should a solutions architect take to meet these requirements?
D. Migrate the database to an Amazon RDS MySQL Multi-AZ DB instance Reconfigure the email application to use Amazon Pinpoint to send email
migrate db to Amazon RDS MySQL

Q399 A company operates an on-premises software-as-a-service (SaaS) solution that ingests several files daily. The company provides multiple public SFTP endpoints to its customers to facilitate the file transfers. The customers add the SFTP endpoint IP addresses to their firewall allow list for outbound traffic. Changes to the SFTP endpoint IP addresses are not permitted. The company wants to migrate the SaaS solution to AWS and decrease the operational overhead of the file transfer service. Which solution meets these requirements?
A. Register the customer-owned block of iP addresses in the company's AWS account Create Elastic IP addresses from the address pool and assign them to an AWS Transfer for SFTP endpoint Use AWS Transfer to store the files of Amazon S3.
assign IP to AWS Transfer for SFTP endpoint

Q400 A multimedia company with a single AWS account is launching an application for a global user base. The application storage and bandwidth requirements are unpredictable. The application will use Amazon EC2 instances behind an Application Load Balancer as the web tier and will use Amazon DynamoDB as the database tier. The environment for the application must meet the following requirements -Low latency when accessed from any part of the world -WebSocket support -End-to-end encryption -Protection against the latest security threats -Managed layer 7 DDoS protection Which actions should the solutions architect take to meet these requirements? (Select TWO)

A. Use Amazon Route 53 and Amazon CloudFront for content distribution Use Amazon S3 to store static content

C. Use AWS WAF with AWS Shield Advanced to protect the application

use Route53 and CloudFront for content distribution

User AWS WAF with Shield Advanced to protect app

Q401 A company wants to refactor its retail ordering web application that currently has a load-balanced Amazon EC2 instance fleet for web hosting database API services and business logic. The company needs to create a decoupled, scalable architecture with a mechanism for retaining failed orders while also minimizing operational costs. Which solution will meet these requirements?

C. Use Amazon S3 for web hosting with AWS AppSync for database API services Use Amazon Simple Queue Service (Amazon SQS) for order queuing Use AWS Lambda for business logic with an Amazon SQS dead-letter queue for retaining failed orders Amazon SQS dead-letter queue for retaining failed orders

Amazon SQS dead-letter queue for retaining failed orders

Q402 A large payroll company recently merged with a small staffing company. The unified company now has multiple business units, each with its own existing AWS account. A solutions architect must ensure that the company can centrally manage the billing and access policies for all the AWS accounts. The solutions architect configures AWS Organizations by sending an invitation to all member accounts of the company from a centralized management account. What should the solutions architect do next to meet these requirements?

C. Create the OrganizationAccountAccessRole IAM role in each member account. Grant permission to the management account to assume the IAM role. create OrganizationAccountAccessRole IAM role in each member account

create OrganizationAccountAccessRole IAM role in each member account

Q403 A company operates quick-service restaurants. The restaurants follow a predictable model with high sales traffic for 4 hours daily. Sales traffic is lower outside of those peak hours. -The point of sale and management platform is deployed in the AWS Cloud and has a backend that is based on Amazon DynamoDB. -The database table uses provisioned throughput mode with 100,000 RCUs and 80,000 WCUs to match known peak resource consumption. -The company wants to reduce Its DynamoDB cost and minimize the operational overhead for the IT staff. Which solution meets these requirements MOST cost-effectively?

C. Enable DynamoDB auto scaling for the table

Enable DynamoDB auto scaling for table

Q404 A financial services company loaded millions of historical stock trades into an Amazon DynamoDB table. The table uses on-demand capacity mode Once each day at midnight. a few million new records are loaded into the table Application road activity against the table happens in bursts throughout the day. and a limited set of keys are repeatedly looked up. The company needs to notice costs associated with DynamoDB. Which strategy should a solutions architect recommend to meet this requirement?
D. Deploy DynamoDB Accelerator (DAX). Use provisioned capacity mode. Configure DynamoDB auto scaling.
use provisioned capacity mode

Q405 A company has a project that is launching Amazon EC2 instances that arc larger than required. The project's account cannot be part of the company's organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT. The company wants to allow only the launch of t3.small EC2 instances by developers in the project's account. These EC2 instances must be restricted to the us-east-2 Region. What should a solutions architect do to meet these requirements?
D. Create an IAM policy that allows the launch of only t3.small EC2 instances in us-east-2. Attach the policy to the roles and groups that the developers use in the proofs account
create an IAM policy

Q406 A company is running a workload that consists of thousands of Amazon EC2 instances. The workload is running in a VPC that contains several public subnets and private subnets. The public subnets have a route for 0 0.0 0/0 to an existing internet gateway. The private subnets have a route for 0.0.0.0/0 to an existing NAT gateway. A solutions architect needs to migrate the entire fleet of EC2 instances to use IPv6. The EC2 instances that are in private subnets must not be accessible from the public internet. What should the solutions architect do to meet these requirements?
C. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets Create an egress-only internet gateway Update the VPC route tables for all private subnets, and add a route for :/0 to the egress-only internet gateway.
create egress-only internet gateway

Q407 A company is developing and hosting several projects in the AWS Cloud. The projects are developed across multiple AWS accounts under the same organization in AWS Organizations. The company requires the cost for cloud infrastructure to be allocated to the owning project. The team responsible for all of the AWS accounts has discovered that several Amazon EC2 instances are lacking the Project tag used for cost allocation. Which actions should a solutions architect take to resolve the problem and prevent it from happening in the future? (Select THREE)
A. Create an AWS Config rule in each account to find resources with missing tags
B. Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing
E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag
create AWS Config rule
Create SCP in the organization
Create AWS Config aggregator

Q408 A company has a serverless application that is deployed on AWS. The application uses an Amazon API Gateway REST API and AWS Lambda to receive and process requests from other applications within the company's on-premises network. The application uses a preshared API key as the authentication method. A recent security review showed that the application was accessible from anywhere on the internet. The company's security policy states that requests can be accepted only from the company's on-premises network. What should a solutions architect recommend to meet this requirement?

C. Create a resource policy with a statement to deny the execute-api:Invoke action if the aws:SourceIp attribute is not from within the company's public IP address range Attach that resource policy to the API Gateway API Redeploy the API

Create resource policy

Q409 A company wants to retire its Oracle Solans NFS storage arrays. The company requires rapid data migration over its internet network connection to a combination of destinations for Amazon S3, Amazon Elastic File System (Amazon EFS), and Amazon FSx for Windows File Server. The company also requires a full initial copy, as well as incremental transfers of changes until the retirement of the storage arrays. All data must be encrypted and checked for integrity. What should a solutions architect recommend to meet these requirements?

B. Configure AWS DataSync, Configure the DataSync agent and deploy it to the local network Create a transfer task and start the transfer

Configure AWS DataSync

Q410 A company has many AWS accounts and uses AWS Organizations to manage all of them. A solutions architect must implement a solution that the company can use to share a common network across multiple accounts. The company's infrastructure team has a dedicated infrastructure account that has a VPC. The infrastructure team must use this account to manage the network Individual accounts cannot have the ability to manage their own networks. However, individual accounts must be able to create AWS resources within subnets. Which combination of actions should the solutions architect perform to meet these requirements? (Select TWO)

B. Enable resource sharing from the AWS Organizations management account

D. Create a resource share in AWS Resource Access Manager in the infrastructure account Select the specific AWS Organizations OU that will use the shared network Select each subnet to associate with the resource share

enable resource sharing

select each subnet to associate with resource share

Q411 A research company is running daily simulations in the AWS Cloud to meet high demand. The simulations run on several hundred Amazon EC2 instances that are based on Amazon Linux 2 Occasionally, a simulation gets stuck and requires a cloud operations engineer to solve the problem by connecting to an EC2 instance through SSH. Company policy states that no EC2 instance can use the same SSH key and that all connections must be logged in AWS CloudTrail. How can a solutions architect meet these requirements?

D. Set up AWS Secrets Manager to store the EC2 SSH key Create a new AWS Lambda function to create a new SSH key and to cal AWS Systems Manager Session Manager to set the SSH key on the EC2 instance Configure Secrets Manager to use the Lambda function for automatic rotation once daily Instruct the engineers to fetch the SSH key from Secrets Manager when they connect through any SSH client

launch new EC2 without setting up any SSH key

Q412 A large company is running a popular web application. The application runs on several Amazon EC2 Linux instances in an Auto Scaling group in a private subnet. An Application Load Balancer is targeting the instances in the Auto Scaling group in the private subnet. AWS Systems Manager Session Manager is configured, and AWS Systems Manager Agent is running on all the EC2 instances. The company recently released a new version of the application Some EC2 instances are now being marked as unhealthy and are being terminated. As a result, the application is running at reduced capacity. A solutions architect tries to determine the root cause by analyzing Amazon CloudWatch logs that are collected from the application, but the logs are Inconclusive. How should the solutions architect gain access to an EC2 instance to troubleshoot the issue?
D. Suspend the Auto Scaling group's Terminate process Use Session Manager to log in to an instance that is marked as unhealthy.
Suspend Autoscaling group's Terminate process

Q413 A company has an on-premises Microsoft SQL Server database that writes a nightly 200 GB export to a local drive. The company wants to move the backups to more robust cloud storage on Amazon S3. The company has set up a 10 Gbps AWS Direct Connect connection between the on-premises data center and AWS. Which solution meets these requirements Most cost effectively?
A.Create a new S3 bucket Deploy an AWS Storage Gateway file gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share.
Deploy AWS Storage Gateway file gateway

Q414 A company Is serving files to its customers through an SFTP server that Is accessible over the internet. The SFTP server Is running on a single Amazon EC2 instance with an Elastic IP address attached Customers connect to the SFTP server through its Elastic IP address and use SSH for authentication. The EC2 instance also has an attached security group that allows access from all customer IP addresses. A solutions architect must implement a solution to improve availability, minimize the complexity of infrastructure management and minimize the disruption to customers who access files. The solution must not change the way customers connect. Which solution will meet these requirements?
B. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting.Create an AWS Transfer Family server. Configure the Transfer Family server with a VPC-hosted internet-facing endpoint. Associate the SFTP Elastic IP address with the new endpoint.Attach the security group with customer IP addresses to the new endpoint.Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket
Configure Transfer Family server with a VPC-hosted internet-facing endpoint

Q415 A company that provisions job boards for a seasonal workforce is seeing an increase in traffic and usage. The backend services run on a pair of Amazon EC2 instances behind an Application Load Balancer with Amazon DynamoDB as the datastore Application read and write traffic is slow during peak seasons. Which option provides a scalable application architecture to handle peak seasons with the LEAST development effort?
C. Use Auto Scaling groups for the backend services Use DynamoDB auto scaling
use DynamoDB auto scaling

Q416 A company is hosting a single-page web application in the AWS Cloud. The company is using Amazon CloudFront to reach its goal audience. The CloudFront distribution has an Amazon S3 bucket that is configured as its origin. The static files for the web application are stored in this S3 bucket. The company has used a simple routing policy to configure an Amazon Route 53. A record. The record points to the CloudFront distribution. The company wants to use a canary deployment release strategy for new versions of the application. What should a solutions architect recommend to meet these requirements?
A. Create a second CloudFront distribution for the new version of the application. Update the Route 53 record to use a weighted routing policy.
Create a second CloudFront distribution

Q417 A company manages an on-premises data ingestion application that receives metrics from IoT devices in JSON format. The data is collected, transformed and stored in a data warehouse for analysis. The current infrastructure has severe performance issues at peak loads due to insufficient compute capacity causing some of the data ingestion to be dropped. The company wants to migrate the application to AWS. The solution must support its current analytics tool that connects to the data warehouse with a Java Database Connectivity (JDBC) driver. The company requires a resilient and cost-effective solution that will address the performance issues. Which solution will meet these requirements?
C. Re-architect the application Load the data into Amazon S3 Use AWS Glue to transform the data Store the table schema in an AWS Glue Data Catalog Use Amazon Athena to query the data
use Amazon Athena to query data

Q418 A company wants to migrate an application to Amazon EC2 from VMware Infrastructure that runs in an on-premises data center. A solutions architect must preserve the software and configuration settings during the migration. What should the solutions architect do to meet these requirements?
B. Use the VMware vSphere client to export the application as an image in Open Visualization Format (OVF) format. Create an Amazon S3 bucket to store the image in the destination AWS Region. Create and apply an IAM role for VM Import. Use the AWS CLI to run the EC2 import command.
use VMware vSphere client to export app as an image in OVF format

Q419 A company hosts a photography website on AWS that has global visitors. The website has experienced steady increases in traffic during the last 12 months, and users have reported a delay in displaying images. The company wants to configure Amazon CloudFront to deliver photos to visitors with minimal latency. Which actions will achieve this goal? (Select TWO.)
B. Set the Minimum TTL and Maximum TTL to a high value in the CloudFront distribution. D. Set up additional origin servers that are geographically closer to the requesters. Configure latency-based routing in Amazon Route 53.
set Minimum TTL and Maximum TTL to a high value
set up additional origin servers that are geographically closer to requester

Q420 A company is building an image service on the web that will allow users to upload and search random photos. At peak usage, up to 10,000 users worldwide will upload their images. The service will

then overlay text on the uploaded images, which will then be published on the company website.Which design should a solutions architect implement?
C. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to the Amazon Simple Queue Service (Amazon SQS) queue. Create a fleet of Amazon EC2 instances to pull messages from the SQS queue to process the images and place them in another S3 bucket. Use Amazon CloudWatch metrics for queue depth to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the S3 bucket that contains the processed images.
configure S3 event notification to send message to Amazon SQS queue

Q421 A company manages hundreds of AWS accounts centrally in an organization in AWS Organizations. The company recently started to allow product teams to create and manage their own S3 access points in their accounts. The S3 access points can be accessed only within VPCs, not on the internet. What is the MOST operationally efficient way to enforce this requirement?
B. Create an SCP at the root level in the organization to deny the s3: CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
Create an SCP at the root level

Q422 A company that tracks medical devices in hospitals wants to migrate its existing storage solution to the AWS Cloud. The company equips all of its devices with sensors that collect location and usage information. This sensor data is sent in unpredictable patterns with large spikes. The data is stored in a MySQL database running on premises at each hospital. The company wants the cloud storage solution to scale with usage. The company's analytics team uses the sensor data to calculate usage by device type and hospital. The team needs to keep analysis tools running locally while fetching data from the cloud. The team also needs to use existing Java applications and SQL queries with as few changes as possible. How should a solutions architect meet these requirements while ensuring the sensor data is secure?
C. Store the data in an Amazon Aurora Serverless database. Serve the data through the Aurora Data API using an IAM user authorized with AWS Identity and Access Management (IAM) and the AWS Secrets Manager ARN.
server data through Aurora Data API

Q423 A company has multiple AWS accounts as part of an organization created with AWS Organizations. Each account has a VPC in the us-east-2 Region and is used for either production or development workloads Amazon EC2 instances across production accounts need to communicate with each other and EC2 instances across development accounts need to communicate with each other but production and development instances should not be able to communicate with each other. To facilitate connectivity, the company created a common network account. The company used AWS Transit Gateway to create a transit gateway in the us-east-2 Region in the network account and shared the transit gateway with the entire organization by using AWS Resource Access Manager Network administrators then attached VPCs in each account to the transit gateway after which the EC2 instances were able to communicate across the account. However production and development accounts were also able to communicate with one another. Which set of steps should a solutions architect take to ensure production traffic and development traffic are completely isolated?
C. Create separate route tables for production and development traffic Delete each account's association and route propagation to the default AWS Transit Gateway route table Attach

development VPCs to the development AWS Transit Gateway route table and production VPCs to the production route table and enable automatic route propagation on each attachment
create separate route tables for production and development traffic

Q424 A solutions architect is designing a solution that consists of a fleet of Amazon EC2 Reserved Instances (RIs) in an Auto Scaling group that will grow over time as usage increases. The solution needs to maintain 80% RI coverage to maintain cost control with an alert to the DevOps team using an email distribution list when coverage drops below 30%. The solution must also include the ability to generate a report to easily track and manage coverage. The company has a policy that allows only one workload for each AWS account. Which set of steps should the solutions architect take to create the report and alert the DevOps team?
B. Create an Amazon Simple Notification Service (Amazon SNS1 topic and subscribe the DevOps email distribution list Use the Cost Explorer console to configure the report for RI utilization set the utilization target to 30% and link to the SNS topic created in the alert configuration
set utilization target to 30%

Q425 A company built an application based on AWS Lambda deployed in an AWS Cloud Formation stack. The last production release of the web application introduced an issue that resulted in an outage lasting several minutes. A solutions architect must adjust the deployment process to support a canary release. Which solution will meet these requirements?
A. Create an alias for every new deployed version of the Lambda function. Use the AWS CLI update-alias command with the routing-config parameter to distribute the load
create an alias for every new deployed version of Lambda function

Q426 A company hosts a large on-premises MySQL database at its main office that supports an issue tracking system used by employees around the world. The company already uses AWS for some workloads and has created an Amazon Route 53 entry for the database endpoint that points to the on-premises database. Management is concerned about the database being a single point of failure and wants a solutions architect to migrate the database to AWS without any data loss or downtime. Which set of actions should the solutions architect implement?
C. Create an Amazon Aurora DB cluster Use AWS Database Migration Service (AWS DMS) to do a full load with continuous replication from the on-premises database to Aurora When the migration is complete update the Route 53 entry for the database to point to the Aurora cluster endpoint and shut down the on-premises database
use AWS DMS to do a full load with continuous replication

Q427 A company has many services running in its on-premises data center. The data center is connected to AWS using AWS Direct Connect (DX) and an iPSec VPN The service data is sensitive and connectivity cannot traverse the internet. The company wants to expand into a new market segment and begin offering its services to other companies that are using AWS. Which solution will meet these requirements?
A. Create a VPC Endpoint Service that accepts TCP traffic host it behind a Network Load Balancer and make the service available over DX
Create VPC Endpoint service that accepts TCP traffic

Q428 A company maintains a restaurant review website. The website is a single-page application where files are stored on Amazon S3 and delivered using Amazon CloudFront. The company receives several fake postings every day that are manually removed. The security team has identified that most of the fake posts are from Dots with IP addresses that have a bad reputation within the same global region. The team needs to create a solution to help restrict the bots from accessing the website. Which strategy should a solutions architect use?

B. Associate an AWS WAF web ACL with the CloudFront distribution Select the managed Amazon IP reputation rule group for the web ACL with a deny action

select managed Amazon IP reputation rule group for web ACL

Q429 A company has application services that have been containerized and deployed on multiple Amazon EC2 instances with public IPs. An Apache Kafka cluster has been deployed to the EC2 instances. A PostgreSQL database has been migrated to Amazon RDS for PostgreSQL The company expects a significant increase of orders on its platform when a new version of its flagship product is released. What changes to the current architecture will reduce operational overhead and support the product release?

D. Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate and enable auto scaling behind an Application Load Balancer. Create additional read replicas for the DB instance. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.

deploy app on Amazon Elastic Kubernetes service(EKS)

Q430 A company is running a line-of-business (LOB) application on AWS to support its users. The application runs in one VPC, with a backup copy in a second VPC in a different AWS Region for disaster recovery. The company has a single AWS Direct Connect connection between its on-premises network and AWS. The connection terminates at a Direct Connect gateway. All access to the application must originate from the company's on-premises network, and traffic must be encrypted in transit through the use of IPsec. The company is routing traffic through a VPN tunnel over the Direct Connect connection to provide the required encryption. A business continuity audit determines that the Direct Connect connection represents a potential single point of failure for access to the application. The company needs to remediate this issue as quickly as possible. Which approach will meet these requirements?

C. Create a transit gateway. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Configure an AWS Site-to-Site VPN connection, and terminate it at the transit gateway.

Configure Site-to-Site VPN and terminate it at transit gateway

Q431 An online retail company hosts its stateful web-based application and MySQL database in an on-premises data center on a single server. The company wants to increase its customer base by conducting more marketing campaigns and promotions. In preparation, the company wants to migrate its application and database to AWS to increase the reliability of its architecture. Which solution should provide the HIGHEST level of reliability?

B. Migrate the database to Amazon Aurora MySQL. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in an Amazon ElastiCache for Redis replication group.

migrate db to Amazon Aurora MySQL

Q432 A startup company hosts a fleet of Amazon EC2 instances in private subnets using the latest Amazon Linux 2 AMI. The company's engineers rely heavily on SSH access to the instances for troubleshooting. The company's existing architecture includes the following:-A VPC with private and public subnets, and a NAT gateway -Site-to-Site VPN for connectivity with the on-premises environment -EC2 security groups with direct SSH access from the on-premises environment The company needs to increase security controls around SSH access and provide auditing of commands executed by the engineers. Which strategy should a solutions architect use?

D. Create an IAM role with the AmazonSSM Managed InstanceCore managed policy attached Attach the IAM role to all the EC2 instances Remove all security group rules attached to the C2 instances that allow inbound TCP on port 22. Have the engineers install the AWS Systems Manager Session Manager plugin for their devices and remotely access the instances by using the start-session API call from Systems Manager

Create IAM role with Amazon SSM

Q433 A company is building a sensor data collection pipeline in which thousands of sensors write data to an Amazon Simple Queue Service (Amazon SQS) queue every minute. The queue is processed by an AWS Lambda function that extracts a standard set of metrics from the sensor data. The company wants to send the data to Amazon CloudWatch. The solution should allow for viewing individual and aggregate sensor metrics and interactively querying the sensor log data using CloudWatch Logs Insights. What is the MOST cost-effective solution that meets these requirements?

A. Write the processed data to CloudWatch Logs in the CloudWatch embedded metric format

write processed data to CloudWatch Logs in CloudWatch embedded metric format

Q434 A company is creating a REST API to share information with six of Its partners based in the United States. The company has created an Amazon API Gateway Regional endpoint. Each of the six partners will access the API once per day to post daily sales figures. After Initial deployment the company observes 1,000 requests per second originating from 500 different IP addresses around the world. The company believes this traffic is originating from a botnet and wants to secure its API while minimizing cost. Which approach should the company take to secure its API?

D. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners Associate the web ACL with the API Create a usage plan with a request limit and associate it with the API Create an API key and add it to Hie usage plan.

Create a usage plan with a request limit

Q435 An education company Is running a web application used by college students around the world. The application runs in an Amazon Elastic Container Service (Amazon ECS) cluster in an Auto Scaling group behind an Application Load Balancer (ALB). A system administrator detects a weekly spike In the number of failed login attempts which overwhelm the application's authentication service. All the tailed login attempts originate from about 500 different IP addresses that change each week. A solutions architect must prevent the tailed login attempts from overwhelming the authentication service. Which solution meets these requirements with the MOST operational efficiency?

B. Create an AWS WAF web ACL with a rate-based rule and set the rule action to Block Connect the web ACL to the ALB

Create AWS WAF web ACL with rate-based rule

Q436 A company's site reliability engineer is performing a review of Amazon FSx for Windows File Server deployments within an account that the company acquired. Company policy states that all Amazon FSx file systems must be configured to be highly available across Availability Zones. During the review, the site reliability engineer discovers that one of the Amazon FSx file systems used a deployment type of Single-AZ 2. A solutions architect needs to minimize downtime while aligning this Amazon FSx file system with company policy. What should the solutions architect do to meet these requirements?
B. Create a new Amazon FSx file system with a deployment type of Multi-AZ. Use AWS DataSync to transfer data to the new Amazon FSx file system. Point users to the new location.
Use AWS DataSync to transfer data to new Amazon FSx file system

Q437 A company has several applications running in an on-premises data center. The data center runs a mix of Windows and Linux VMs managed by VMware vCenter. A solution architect needs to create a plan to migrate the application to AWS. However, the solution architect discovers that the documentation for the applications is not up to date and that there are no complete infrastructure diagrams. The company's developers lack time to discuss their applications and current usage with the solutions architect. What should the solutions architect do to gather the required information?
C. Install the AWS Application Discovery Service on each of the VMs to collect the configuration and utilization data.
install AWS Application Discovery Service

Q438 A company wants to use Amazon WorkSpaces in combination with the client devices to replace aging desktops. Employees use the desktops to access applications that work with clinical trial data. Corporate security policy states that access to the applications must be restricted to only company branch office locations. The company is considering adding an additional branch in the next 6 months. Which solution meets these requirements with the
Most operational efficiency?
C. USE AWS Certificate Manager (ACM) to issue trusted device certificates to the machine deployed in the branch office locations. Enable restricted access on the WorkSpaces directory.
use AWS Certificate Manager(ACM)

Q439 A company has multiple business units. Each business unit has its own AWS account and runs a single website within that account. The company also has a single logging account Logs from each business unit website are aggregated into a single Amazon 53 bucket in the logging account. The S3 bucket policy provides each business unit with access to write data into the bucket and requires data to be encrypted. The company needs to encrypt togs uploaded into the bucket using a single AWS Key Management Service (AWS KMS) CMK. The CMK that protects the data must be rotated once every 365 days. Which strategy is the MOST operationally efficient for the company to use to meet these requirements?
B. Create a customer managed CMK in the logging account Update the CMK key policy to provide access to the logging account and business unit accounts Enable automatic rotation of the CMK
Update CMK key policy to provide access to logging accounts and business unit accounts. Enable automatic rotation

Q440 The following AWS Identity and Access Management (IAM) customer managed policy has been attached to an IAM user: { "Version": "2012-10-17", "Statement": [{ "Effect": “Allow", "Action": "s3:", "Resource":["arn:aws:s3: : prod-data", 'arn:aws:s3::prod-data/*"] }. { "Effect"."Deny", "NotAction": "s3:*" "NotResource":["arn:aws:s3 :prod-data", "'arn: aws:s3 : prod-data/*”] }] } which statement describes the access that this policy provides to the user?

D. This policy grants access to all Amazon S3 actions in the prod-data S3 bucket, but explicitly denies access to all other AWS services

explicitly denies access to all other AWS services

Q441 A company is using AWS Organizations to manage 15 AWS accounts. A solutions architect wants to run advanced analytics on the company's cloud expenditures. The cost data must be gathered and made available from an analytics account. The analytics application runs in a VPC and must receive the raw cost data each night to run the analytics. The solution architect has decided to use the Cost Explorer API to fetch the raw data and store the data in Amazon S3 in Json format. Access to the raw cost data must be restricted to the analytics application. The solution architect has already created an AWS Lambda function to collect data by using the Cost Explorer API. Which additional actions should the solutions architect take to meet these requirements?

A. Create an IAM role in the Organization's master account with permissions to use the Cost Explorer API, and establish trust between the role and the analytics account. Update the Lambda function role and add sts AssumeRole permissions. Assume the role in the master account from the Lambda function code by using the AWS security Token Service (AWS STS) AssumeRole API call. Create a gateway-endpoint for Amazon S3 in the analytics VPC. Create an S3 bucket policy that allows access only from S3 endpoint.

create a gateway-endpoint, create S3 bucket policy that allows access only from S3 endpoint

Q442 A new application is running on Amazon Elastic Container Service (Amazon ECS) with AWS Fargate. The application uses an Amazon Aurora MySQL database. The application and the database run in the same subnets of a VPC with distinct security groups that are configured. The password for the database is stored in AWS Secrets Manager and is passed to the application through the DB_PASSWORD environment variable. The hostname of the database is passed to the application through the DB_HOST environment variable. The application is failing to access the database. Which combination of actions should a solutions architect take to resolve this error? (Select THREE.)

A. Ensure that the container has the environment variable with name "DB_PASSWORD" specified with a "ValueFrom" and the ARN of the secret.

D. Ensure that the Aurora MySQL database security group allows inbound network traffic from the Fargate service on the MySQL TCP port 3306.

F. Ensure that the container has the environment variable with name "DB_HOST" specified with the hostname of the DB cluster endpoint.

ARN of secret
allow inbound traffic from Fargate
host name of DB cluster endpoint

Q443 A company has deployed its corporate website in a VPC on two Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances are deployed in private subnets. The ALB is in a public subnet. A route to an internet gateway exists in the public subnet route table. The company has deployed an Amazon CloudFront distribution with the ALB as the origin. The company's security team

recently identified that malicious traffic is accessing the ALB directly. The company must deploy security controls to prevent common attack techniques, including cross-site scripting. and to protect against volumetric denials of service. Which strategy should a solutions architect recommend to meet these requirements?
D. Associate an AWS WAF web ACL with the CloudFront distribution. Configure AWS WAF to add a custom header to the requests that are sent to the ALB. Configure advanced routing on the ALB to only forward requests that include the custom header that is set by CloudFront.
configure AWS WAF to add a custom header to request

Q444 A company has a media metadata extraction pipeline running on AWS. Notifications containing a reference to a file Amazon S3 are sent to an Amazon Simple Notification Service (Amazon SNS) topic. The pipeline consists of a number of AWS Lambda functions that are subscribed to the SNS topic. The Lambda functions extract the S3 file and write metadata to an Amazon RDS PostgreSQL DB instance. Users report that updates to the metadata are sometimes slow to appear 01 are lost. During these times, the CPU utilization on the database is high and the number of failed Lambda invocations increases. Which combination of actions should a solutions architect take to help resolve this issue? (Select TWO)
C. Create an RDS proxy for the RDS instance Update the Lambda functions to connect to the RDS instance using the proxy
E. Create an Amazon Simple Queue Service (Amazon SQS) standard queue for each Lambda function and subscribe the queues to the SNS topic Configure the Lambda functions to consume messages from their respective SQS queue
create RDS proxy for RDS instance
Create Amazon SQS standard queue

Q445 A company is planning to host a three tier application in the AWS Cloud. The application layer will use Amazon EC2 in an Auto Scaling group. A custom EC2 role named AppServer will be created and associated with the application instances. The entire application stack will be deployed using AWS Cloud Formation. The company's security team requires encryption of all AMI snapshots and Amazon Plastic Block Store (Amazon TBS) volumes with an AWS Key Management Service (AWS KMS) CMK. Which action will deploy the stack correctly after the AMI snapshot is encrypted with the KMS key?
D. Update the CloudFormation stack role to have the required permissions to access the KMS key
update CloudFormation stack role

Q446 An AWS customer has a web application that runs on premises. The web application (etches data from a third party API that is behind a firewall. The third party accepts only one public CIDR block in each client's allow list. The customer wants to migrate their web application to the AWS Cloud. The application will be hosted on a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in a VPC. The ALB is located in public subnets. The EC2 instances are located on private subnets. NAT gateways provide internet access to the private subnets. How should a solutions architect ensure that the web application can continue to call the third- party API after the migration?
B. Register a block of customer-owned public IP addresses in the AWS account Create Elastic IP addresses from the address block and assign them to the NAT gateways in the VPC
assign IP to NAT gateways in VPC

Q447 A company has a data late in Amazon S3 that needs to be accessed by hundreds of applications across many AWS accounts. The company's information security policy states that the S3 bucket must

not be accessed over the public internet and that each application should have the minimum permissions necessary to function. To meet these requirements, a solution architect plans to use an S3 access point that is restricted to specific VPCs for each application. Which combination of steps should the solutions architect take to implement this solution? (Choose Two)
A. Create an S3 access point for each application in the AWS account that owns the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.
C. Create a gateway endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Specify the route table that is used to access the access point.
create S3 access point in account that own S3 bucket
create gateway endpoint in application VPC

Q448 A company is running an Apache Hadoop cluster on Amazon EC2 instances. The Hadoop cluster stores approximately 100 TB of data for weekly operational reports and allows occasional access for data scientists to retrieve data. The company needs to reduce the cost and operational complexity for strong and serving this data. Which solution meets these requirements in the MOST cost-effective manner?
C. Move the data to Amazon S3 and use Amazon Athena to query the data for reports. Allow the data scientists to access the data directly in Amazon S3.
use Amazon Athena to query data for report

Q449 A government agency is building a forms submission portal using AWS to allow citizens to submit and retrieve sensitive documents. The solution was built using serverless architecture, with the front-end code developed using HTML and JavaScript and the backend architecture using Amazon API Gateway and Amazon S3. The portal must meet the following security requirements:-Requests to the backend infrastructure should be allowed only if they originate from a specific country. -Requests to the backend infrastructure should prevent brute-attacks from individual IP addresses by not allowing more than 3000 requests per minute for 10 requests per seconds for each IP address. -All access attempts to the backend infrastructure must be logged. Which steps should a solution architect take to meet these requirements? (Select Two)
B. Create an AWS WAP web ACL with a custom condition that allows access attempts from the authorized country only, and a rate-based rule with a rate-based rule with rate limit 3000 requests per 5 minutes. Then associate the web ACL with the API Gateway API
E. Configure the AWS WAF web ACL to an Amazon CloudWatch Logs group. Configure API Gateway to log to an Amazon Cloudwatch Logs group
create AWS WAP web ACL
Configure AWS WAF web ACL to CloudWatch Logs

Q450 A company uses multiple AWS accounts in a single AWS Region. A solution architect is designing a solution to consolidate logs generated by Elastic Load Balancers (ELBs) in the AppDev, AppTest and AppProd accounts. The logs should be stored in an existing Amazon S3 bucket named s3- eib-logs in the central AWS accounts. The central account is used for log consolidation only does not have ELBs deployed. ELB logs must be encrypted at rest. Which combination of steps should the solutions architect take to build the solution? (Select Two)

C. Update the S3 bucket policy for the s3-elb-logs bucket to allow the s3:PutObject action for the AppDev.AppTest and AppProd account IDs.
E. Enable Amazon S3 default encryption using server-side encryption with s3 managed encryption keys (SSE-S3) for the s3-elb-logs s3 bucket.
allow s3:PutObject action for AppDev
enable S3 default encryption

Q451 A company is collecting a large amount of data from a fleet of IoT devices. Data is stored as Optimized ROW Columnar (ORC) files in the Hadoop Distributed File System (HDFS) on a persistent Amazon EMR cluster. The company's data analytics team queries the data by using SQL in APache Presto deployed on the same EMR cluster. Queries scan large amounts of data, always run for less than 15 minutes, and run only between 5 PM and 10 PM. The company is concerned about the high cost associated with the current solution. A solution architect must propose the most cost-effective solution that will allow SQL data queries. Which solution will meet these requirements?
B. Store data in Amazon S3. Use the AWS Glue Data Catalog and Amazon Athena to query data.
use AWS Glue Data Catalog and Athena to query data

Q452 A company recently completed a large-scale migration to AWS Development teams that support various business units have their own accounts in AWS Organizations. A central cloud team is responsible for controlling which services and resources can be accessed, and for creating operational strategies for all teams with the company. Some teams are approaching their account service quotas. The cloud team needs to create an automated and operationally efficient solution to proactively monitor service quotas. Monitoring should account every 15 minutes and send alerts when a team exceeds 80% utilization. Which solution will meet these requirements?
B. Create an Amazon EvenBridge (Amazon CloudWatch Events) rule that triggers an AWS Lambda function to refresh the AWS Trusted Advisor service limit checks and retrieve the most current utilization and service limit data. If the current utilization is above 80% publish a message to an Amazon Simple Notification Service (Amazon SNS) topic to alert the cloud team. Create AWS CloudFormation StackSets that deploy the necessary resources to all Organizations accounts.
Create EventBridge rule, publish message to SNS topic

Q453 A company recently deployed a new application that runs on a group of Amazon EC2 Linux instances in a VPC. In a peered VPC, the company launched an EC2 Linux instance that serves as bastion host. The security group of the application instances allows access only on TCP port 22 from the private IP of the bastion host. The security group of the bastion host allows access to TCP port 22 from 0.0.0.0/0 so that system administrators can use SSH to remotely log in to the application instances from several branch offices. While looking through operating system logs on the bastion host, a cloud engineer notices thousands of failed SSH logins to the bastion host from locations around the world. The cloud engineer wants to change how remote access is granted to the application instances and wants to meet the following requirements:-Eliminate brute-force SSH login attempts -Retain a log of commands run during an SSH session -Retain the ability to forward ports Which solution meets these requirements for remote access to the application instances?

A. Configure the application instances to communicate with AWS Systems Manager Grant access to the system administrators to use Session Manager to establish a session with the application instances Run Terminate the bastion host Command.
use Session Manager to establish a session

Q454 A company runs an application in Amazon VPC. The application requires that all traffic to their different third party networks be encrypted. The network traffic between the application and the third party networks is expected to be no more than 500 Mbps for each connection. To facilitate network connectivity, a solutions architect has created a transit gateway and attached the application VPC. Which set of actions should the solutions architect perform to complete the solution while MINIMIZING costs?
A. Use AWS Certificate Manager (ACM) to generate three public/private key pairs. Instal the private keys on a public facing Application Load Balancer (ALB). Have each third party network connect to the ALB using HTTPS/TLS. Update the transit gateway route table to route traffic between the application and the third party networks through the ALB
use AWS Certificate Manager(ACM)

Q455 A company needs to create and manage multiple AWS accounts for a number of departments from a central location. The security team requires read-only access to all accounts from its own AWS account. The company is using AWS Organizations and created an account for the security team. How should a solutions architect meet these requirements?
D. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the member account from the security account. Use the generated temporary credentials to gain access
call AssumeRole API for Organization AccountAccessRole IAM role in member accounts

Q456 A company has grown through numerous mergers and acquisitions. Due to increasing AWS usage costs, management wants each business unit to submit monthly cost reports with costs allocated to specific projects through the AWS Billing and Cost Management console. A resource tagging strategy involving BusinessUnit and Project tags is already defined. Which combination of steps should each business unit take to meet these requirements? (Select Two)
A. Create an AWS Cost and Usage Report rule to group resources by the BusinessUnit and Project tags. Create a budget in AWS Budget and attach
D. Create an AWS Budgets report for each business unit to be sent as an email notification to the finance team monthly. Attach the budget for each of the business unit's projects to the report.
create aws Cost and Usage Report rule
attach budget for each of business unit’s report

Q457 A car rental company has built a serverless REST API to provide data to its mobile app. The app consists of an Amazon API Gateway API with a Regional endpoint, AWS Lambda function and an Amazon Aurora MySQL Serverless DB cluster. The company recently opened the API to mobile apps of partners. A significant increase in the number of requests resulted, causing sporadic database memory errors. Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time. Traffic is concentrated during business hours, with spikes around holidays and other events. The company needs to improve its ability to support the additional usage while minimizing the increase in costs associated with the solution. Which strategy meets these requirements?

A. Convert the API Gateway Regional endpoint to an edge-optimized endpoint Enable caching in the production stage.
convert API Gateway Regional endpoint to edge-optimized endpoint

Q458 A company is developing a web application that runs on Amazon EC2 instances in an Auto Scaling group behind a public facing Application Load Balancer (ALB). Only users from a specific country are allowed to access the application. The company needs the ability to log the access requests that have been blocked. The solution should require the least possible maintenance. Which solution meets these requirements?
B. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from a specified country. Associate the rule with the web ACL. Associate the web ACL with the ALB
configure a rule to block any requests that do not originate from specified country

Q459 A company uses AWS Organizations to manage more than 1,000 AWS accounts. The company has creates a new developer organization. There are 540 developer member in that must be moved to the new developer organization. All accounts are set up with all the required information so that each account can be operated as a standalone account. Which combination of steps should a solutions architect take to move all of the developer accounts to the new developer organization? (Select THREE)
B. From the master account, remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API
E. Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's master account to send invitations to the developer accounts
F. Have each developer sign in to their account and confirm to join the new developer organization.
from master account, remove dev account
call InviteAccountToOrganization operation
have dev sign in

Q460 A development team has created a new flight tracker application that provides near-real-time data to users. The application has a front end that consists of an Application Load Balancer (ALB) in front of two large Amazon EC2 instances in a single Availability Zone. Data is stored in a single Amazon RDS MySQL DB instance. An Amazon Route 53 DNS record points to the ALB. Management wants the development team to improve the solution to achieve maximum reliability with the least amount of operational overhead. Which set of actions should the team take?
D. Replace the DB instance with Amazon Aurora with Aurora Replicas. Deploy the application to multiple smaller EC2 instances across multiple Availability Zones in an Auto Scaling group behind an ALB
replace db instance with Aurora with Aurora replicas

Q461 A company is using AWS Organizations to manage multiple AWS accounts. For security purposes, the company requires the creation of an Amazon Simple Notification Service (Amazon SNS) topic that enables integration with a third-party alerting system in all the Organization's member accounts. A solutions architect used an AWS CloudFormation template to create the SNS topic and stack sets to

automate the deployment of CloudFormation attacks. Trusted access has been enabled in Organizations. What should the solutions architect do to deploy the CloudFormation StackSets in all AWS accounts?
C. Create stacks in the Organizations master account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.
Create stack in master account. Enable CloudFormation automatic deployment

Q462 A company runs an application in the cloud that consists of a database and a website. Users can post data to the website, have the data processed, and have the data sent back to them in an email. Data is stored as a MySQL database running on an Amazon EC2 Instance. The database is running in a VPC with two private subnets. The website is running on Apache Tomcat in a single EC2 instance in a different VPC with one public subnet. There is a single VPC peering connection between the database and website VPC. The website has suffered several outages during the last month due to high traffic. Which actions should a solutions architect take to increase the reliability of the application? (Select THREE)
A. Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer
C. Migrate the MySQL database to Amazon Aurora with one Aurora Replica
F. Create an additional public subnet in a different Availability Zone in the website VPC.
place Tomcat server
Migrate MySQL db to Aurora
Create additional public subnet

Q463 A company wants to provide desktop as a service (Daas) to a number of employees using Amazon WorkSpaces. Workspaces will need to access files and services hosted on premises with authorization based on the company's Active Directory Network connectivity will be provided through an existing AWS Direct Connect connection. The solution has the following requirements:-Credentials from Active Directory should be used to access on- premises files and services -Credentials from Active Directory should not be stored outside the company -End users should haw single sign-on (SSO) to on-premises files and services once connected to Workspaces Which strategy should the solutions architect use for and user authentication?
C. Create a service account in the on premises Active Directory with the required permissions Create an AD Connector in AWS Directory Service within the Workspaces VPC using the service account to communicate with the on-premises Active Directory Use the AD Connector as the directory for WorkSpeces.
Create service account in on-premises AD.VPC using service account

Q464 A company is running an application in a single VPC on an Amazon EC2 instance with Amazon RDS as the datastore. The application does not support encryption in transit Security guidelines do not allow SSH access to any resource within the VPC. The Application has issues throughout the day which causes outages in the production environment. The issues are not present in nonproduction environments Application logs have been given to a vendor to troubleshoot the application. The vendor also requires IP packets for its analysis. Which solution allows for the IP packets to be extracted for troubleshooting?
B. Create a VPC traffic mirror source on the application instance's elastic network interface with a filter that captures all traffic. Launch a new EC2 instance and configure the traffic minor target to use the elastic network interface of the new EC2 instance. Start the traffic mirror session and download the packet capture from the new EC2 instance using AWS Systems Manager Provide the packet capture to the vendor.
use AWS Systems Manager

Q465 A company needs to store and process image data that will be uploaded from mobile devices using a custom mobile app. Usage peaks between 8 AM and 5 PM on weekdays, with thousands of uploads per minute. The app is rarely used at any other time. A user is notified when image processing is complete When a combination of actions should a solutions architect take to ensure image processing can scale to handle the load? (Select THREE)

B. Upload files from the mobile software directly to Amazon S3 Use S3 event notifications to create a message in an Amazon Simple Queue Service (Amazon SQS) standard queue.

C. Invoke an AWS Lambda function to perform image processing when a message is available in the queue

E. Send a push notification to the mobile app by using Amazon Simple Notification Service (Amazon SNS) when processing is complete.

Create message in SQS standard queue.

Invoke Lambda function to perform processing

Using SNS when processing is complete

Q466 A software company hosts an application on AWS with resources in multiple AWS accounts and Regions. The application runs on a group of Amazon EC2 instances an application VPC located in the us-east-1 Region with an IPy4 CIDR block of 10.10.0.0/16. In a different AWS account, a shared services VPC is located in the us-east-2 Region with an IPv4 CIDR block of 10.10.10.0/24. When a cloud engineer uses AWS CloudFormation to attempt to peer the application VPC with the shared services VPC. an error message indicates a peering failure. Which factors could cause this error? (Select TWO)

A. The IPv4 CIDR ranges of the two VPCs overlap

E. The IAM role in the peer accepter account does not have the correct permissions.

IPv4 CIDR range

IAM role does not have correct permissio**n**

Q467 A company needs to implement a patching process for its servers. The on-premises servers and Amazon EC2 instances use a variety of tools to perform patching. Management requires a single report showing the patch status of all the servers and instances. Which set of actions should a solutions architect take to meet these requirements?

A. Use AWS Systems Manager to manage patches on the on-premises servers and EC2 instances. Use Systems Manager to generate patch compliance reports

use AWS Systems Manager to manage patches

Q468 A solutions architect is designing an application to accept timesheet entries from employees on their mobile devices. Timesheets will be submitted weekly, with most of the submissions occurring on Friday. The data must be stored in a format that allows payroll administrators to run monthly reports. The infrastructure must be highly available and scale to match the rate of incoming data and reporting requests. Which combination of steps meets these requirements while minimizing operational overhead? (Select TWO)

B. Deploy the application in a container using Amazon Elastic Container Service (Amazon ECS) with load balancing across multiple Availability Zones. Use scheduled Service Auto Scaling to add capacity before the high volume of submissions on Fridays.

D. Store the timesheet submission data in Amazon Redshift. Use Amazon QuickSight to generate the reports using Amazon Redshift as the data source.
Deploy app in container using ECS
Store data in Redshift

Q469 A company that is developing a mobile game is making game assets available in two AWS Regions. Game assets are served from a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The company requires game assets to be fetched from the closest Region. If game assets become unavailable in the closest Region, they should be fetched from the other Region. What should a solutions architect do to meet these requirements?
D. Create an Amazon Route 53 health check for each ALB Create a Route 53 latency alias record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.
create Route 53 latency alias record

Q470 A company wants to control its cost of Amazon Athena usage. The company has allocated a specific monthly budget for Athena usage. A solutions architect must design a solution that will prevent the company from exceeding the budgeted amount. Which solution will moot these requirements?
D. Use Athena workgroups to set a limit on the amount of data that can be scanned.Set a limit that is appropriate for the monthly budget and the current pricing for Athena.
use Athena workgroups to set a limit

Q471 A company is designing a data processing platform to process a Large number of files in an Amazon S3 bucket and store the results in Amazon DynamoDB. These files will be processed once and must be retained for 1 year. The company wants to ensure that the original files and resulting data are highly available in multiple AWS Regions. Which solution will meet these requirements?
D. Copy the files to an S3 bucket in another Region by using cross-Region replication. Create an S3 CreateObject event notification on the original bucket to execute an AWS Lambda function to process each file and store the results in a DynamoDB global table in multiple Regions. Configure both S3 buckets to use the S3 Standard-infrequent Access (S3 Standard-IA) storage class and an S3 Lifecycle policy to delete the files after 1 year
Copy file to S3. store result in DynamoDB global table

Q472 A solution architect works for a government agency that has strict recovery requirements. All Amazon Elastic Block Store (Amazon EBS) snapshots are required to be saved in at least two additional AWS Regions. The agency also is required to maintain the lowest possible operational overhead. Which solution meets These requirements?
A. Configure a policy in Amazon Data lifecycle Manager (Amazon DLM) to run once dairy to copy the EBS snapshots to the additional Regions
configure a policy in Amazon Data lifecycle Manager(DLM)

Q473 A company is running a web application on Amazon EC2 instances in a production AWS account. The company requires all logs generated from the web application to be copied to a central AWS account for analysis and archiving. The company's AWS accounts are currently managed independently. Logging agents are configured on the EC2 instances to upload the log files to an Amazon S3 bucket in the central AWS account. A solution architect needs to provide access for a solution that will allow the production

account to store log files in the central account. The central account also needs to have read access to the log files. What should the solutions architect do to meet these requirements?
A. Create a cross-account role in the central account. Assume the role from the production account when the logs are being copied.
create a cross-account role in central account

Q474 A solution architect is evaluating the reliability of a recently migrated application running on AWS. The front end is hosted on Amazon S3 and accelerated by Amazon CloudFront. The application layer runs in a stateless Docker container on an Amazon EC2 On-Demand instance with an Elastic IP address. The storage layer is a MongoDB database running on an EC2 Reserved instance in the same Availability Zone as the application layer. Which combination of steps should the solution architect take to eliminate single points of failure with minimal application code changes? (Select Two)
B. Create an Application Load Balancer and migrate the Docker container to AWS Fargate.
D. Migrate the storage layer to Amazon DocumentDB (With MongoDB compatibility)
create ALB and migrate docker container to AWS Fargate
Migrate storage layer to DocumentDB(with MongoDB compatibility)

Q475 A financial company with multiple departments wants to expand its on-premises to the AWS Cloud. The company must retain centralized access control using an existing-premises Active Directory (AD) service. Each department should be allowed to create AWS accounts with preconfigured networking and should have access to only a specific list of approved services. Departments are not permitted to have account administrator permissions. What should a solutions architect do to meet these security requirements?
B. Deploy an AWS Control Tower landing zone. Create an AD Connector linked to the on-premises Active Directory. Change the identity source in AWS Single Sign-On to use Active Directory. Allow department administrators to use Account Factory to create new member accounts and networking. Grant the departments AWS power user permissions on the created accounts
Deploy AWE Control Tower landing zone

Q476 A company runs a software-as-a-service (Saas) application on AWS. The application consists of AWS Lambda functions and an Amazon RDS for MySQL Multi-AZ database. During market events the application has a much higher workload than normal Users notice slow response times during the peak period because of many database connections. The company needs to improve the scalable performance and availability of the database. Which solution meets these requirements?
D. Migrate the database to Amazon Aurora, and add an Aurora Replica Configure Amazon RDS Proxy to manage database connection pools
configure Amazon RDS Proxy to manage database connection pools

Q477 A company stores customer data in an Amazon S3 bucket with S3 Versioning enabled in the us west-2 Region. The S3 bucket is encrypted with an AWS Key Management Service (AWS KMS) customer managed CMK. A compliance policy states that redundant copies of all S3 objects must be stored in the us-east-2 Region. The S3 buckets are allowed to stay in the same AWS account. Which combination of steps will meet these requirements with the LEAST operational effort? (Select THREE)
B. Create a destination S3 bucket in us-east-2 with S3 Versioning enabled
C. Set up S3 Cross-Region Replication between the two S3 buckets.

E. Create and assign to Amazon S3 an IAM role with a policy that allows reading from the source S3 bucket and replication to the destination S3 bucket
Create destination S3 bucket with S3 versioning enabled
Set up S3 Corss-Region replication
Create and assign to S3 an IAM role

Q478 A company that runs applications on AWS recently subscribed to a new software-as-a-service (Saas) data vendor. The vendor provides the data by way of a REST API that the vendor hosts in its AWS environment. The vendor offers multiple options for connectivity to the API and is working with the company to find the best way to connect. The company's AWS account does not allow outbound internet access from its AWS environment. The vendor's services run on AWS in the same AWS Region as my company's applications. A solutions architect must implement connectivity to the vendor's API so that the API is highly available in the company's VPC. Which solution will meet these requirements?
C. Connect to the vendor by way of a VPC endpoint service that uses AWS PrivateLink
connect to vendor by way of a VPC endpoint service that uses AWS PrivateLinke

Q479 A company recently deployed multiple Amazon Elastic File System (Amazon EFS) file systems in an AWS account. The company wants to access the EFS file systems in Amazon Linux EC2 instance in a second AWS account Permissions are already granted from the source account. Which combination of actions should the solutions architect recommend to meet these requirements? (Select TWO.)
D. Call the DescribeMount Targets operation in the source account for the file system to identify the mount target IP address for the Availability Zone that matches the Availability Zone of the EC2 instance
E. Add a line to the /etc/hosts file on the EC2 instance that references the IpAddress of the EFS mount target
Identify mount target IP address
References IP address.

Q480 A solutions architect needs to provide AWS Cost and Usage Report data from a company's AWS Organizations master account. The company already has an Amazon S3 bucket to store the reports. The reports must be automatically ingested into a database that can be visualized with other tools. Which combination of steps should the solutions architect take to meet these requirements? (Select Three)
B. Create an AWS Cost and Usage Report configuration to deliver the data into the S3 bucket
D. Create an AWS Lambda function that a new object creation in the S3 bucket will trigger E. Create an AWS Glue crawler that the AWS Lambda function will trigger to crawl objects in the S3 bucket
create AWS Cost and Usage Report
Create AWS Lambda function
Create AWS Glue crawler that Lambda function will trigger

Q481 A company runs several workloads on a mix of Amazon EC2 instances and Amazon RDS instances. The company is using an organization in AWS Organizations to manage multiple AWS accounts. The company's security standards require evaluation of AWS resources against the CIS Benchmarks and to automatically remediate issues where possible What should a solutions architect recommend to meet these requirements?

D. Enable Amazon Inspector to audit the environment against the CIS controls ingest results from Amazon Inspector into AWS (Amazon CloudWatch Events) to schedule AWS Lambda functions to remediate issues
enable Amazon Inspector

Q482 A company needs to architect a hybrid DNS solution. This solution will use an Amazon Route 53 private hosted zone for the domain cloud.example.com for the resource stored within VPCs. The company has the following DNS resolution requirements:-On-premises systems should be able to resolve and connect to cloud.example.com. -All VPCs should be able to resolve cloud.example.com. There is already an AWS Direct Connect connection between the on-premises corporate network and AWS Transit Gateway. Which architecture should the company use to meet these requirements with the HIGHEST performance?
A. Associate the private hosted zone to all the VPCs. Create a Route 53 inbound resolver in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud example.com that point to the inbound resolver.
Create Route 53 inbound resolver, attach all VPCs to transit gateway

Q483 A company runs a proprietary stateless ETL application on an Amazon EC2 Linux instance. The application is a Linux binary, and the source code cannot be modified. The application is single-threaded, uses 2 GB of RAM. and is highly CPU intensive. The application is scheduled to run every 4 hours and runs for up to 20 minutes. A solutions architect wants to revise the architecture for the solution. Which strategy should the solutions architect use?
C. Use AWS Fargate to run the application. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke the Fargate task every 4 hours.
use AWS Farget

Q484 A multimedia company needs to deliver its video-on-demand (VOD) content to its subscribers in a cost-effective way. The video files range in size from 1-15 GB and are typically viewed frequently for the first 6 months after creation, and then access decreases considerably. The company requires all video files to remain immediately available for subscribers. There are now roughly 30.000 files, and the company anticipates doubling that number over time. What is the MOST cost-effective solution for delivering the company's VOD content?
A. Store the video files in an Amazon S3 bucket using S3 Intelligent-Tiering. Use Amazon CloudFront to deliver the content with the S3 bucket as the origin.
store video files in S3 bucket

Q485 A company has implemented an ordering system using an event-driven architecture. During initial testing, the system stopped processing orders. Further log analysis revealed that one order message in an Amazon Simple Queue Service (Amazon SQS) standard queue was causing an error on the backend and blocking all subsequent order messages. The visibility timeout of the queue is set to 30 seconds, and the backend processing timeout is set to 10 seconds. A solutions architect needs to analyze faulty order messages and ensure that the system continues to process subsequent messages. Which step should the solutions architect take to meet these requirements?
D. Configure a new SQS standard queue as a dead-letter queue to isolate the faulty messages.
configure a new SQS Standard queue

Q486 A company has 50 AWS accounts that are members of an organization in AWS Organizations. Each account contains multiple VPCs. The company wants to use AWS Transit Gateway to establish connectivity between the VPCs in each member account. Each time a new member account is created, the company wants to automate the process of creating a new VPC and a transit gateway attachment. Which combination of steps will meet these requirements? (Select TWO.)
A. From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager.
C. Launch an AWS CloudFormation stack set from the master account that automatically creates a new VPC and a VPC transit gateway attachment in a member account. Associate the attachment with the transit gateway in the master account by using the transit gateway ID.
Share transit gateway by using AWS RAM
Associate attachment with transit gateway

Q487 A finance company hosts a data lake in Amazon S3. The company receives financial data records over SFTP each night from several third parties The company runs its own SFTP server on an Amazon EC2 instance in a public subnet of a VPC. After the files are uploaded, they are moved to the data lake by a cron job that runs on the same instance. The SFTP server is reachable on DNS sftp.example.com through the use of Amazon Route 53. What should a solutions architect do to improve the reliability and scalability of the SFTP solution?
B. Migrate the SFTP server to AWS Transfer for SFTP. Update the DNS record sftp.example.com in Route 53 to point to the server endpoint hostname.
migrate SFTP server to AWS Transfer for SFTP

Q488 A scientific company needs to process text and image data during a live, time-critical phase of a deep space mission. The radar stations upload the data to the source S3 bucket. The data is prefixed by radar station identification number. The company created a destination S3 bucket in a second account. Data must be copied from the source S3 bucket to the destination S3 bucket to meet a compliance objective This replication occurs through the use of an S3 replication rule to cover all objects in the source S3 bucket. One specific radar station is identified as having the most accurate data. Data replication at this radar station must be monitored for completion within 30 minutes after the radar station uploads the objects to the source S3 bucket. What should a solutions architect do to meet these requirements?
D. Create a new S3 replication rule on the source S3 bucket that filters for the keys that use the prefix of the radar station with the most accurate data Enable S3 Replication Time Control (S3 RTC)Monitor the maximum replication time to the destination. Create an Amazon EventBridge (Amazon Cloud Watch Events) rule to trigger an alert when the time exceeds the desired threshold
Create new S3 replication rule

Q489 A software development company has multiple engineers who are working remotely. The company is running Active Directory Domain Services (AD DS) on an Amazon EC2 instance. The company's security policy states that all internal, nonpublic services that are deployed in a VPC must be accessible through a VPN. Multi-factor authentication (MFA) must be used for access to a VPN. What should a solutions architect do to meet these requirements?
B. Create an AWS Client VPN endpoint. Create an AD Connector directory for integration with AD DS. Enable MFA for AD Connector. Use AWS Client VPN to establish a VPN connection.

create AWS Client VPN endpoint

Q490 A large company in Europe plans to migrate its applications to the AWS Cloud. The company uses multiple AWS accounts for various business groups. A data privacy law requires the company to restrict developers' access to AWS European Regions only. What should the solutions architect do to meet this requirement with the LEAST amount of management overhead?
B. Enable AWS Organizations, attach the AWS accounts, and create OUs for European Regions and non-European Regions. Create SCPs to limit access to non-European Regions and attach the policies to the OUs.
create SCPs to limit access to non-European Regions

Q491 A company is planning to host a web application on AWS and wants to loadbalance the traffic across a group of Amazon EC2 instances. One of the security requirements is to enable end-to-end encryption in transit between the client and the web server. Which solution will meet this requirement?
C. Place the EC2 instances behind an Application Load Balancer (ALB). Provision an SSL certificate using AWS Certificate Manager (ACM), and associate the SSL certificate with the ALB. Provision a third-party SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances.
Provision a third-party SSL certificate and install it on each EC2 instance

Q492 A company has two VPCs within the same AWS account that are connected through a transit gateway. A solutions architect adds a new subnet to one of the VPCs. Resources that are hosted in the new subnet are not able to communicate with resources in the other VPC. What should the solutions architect do to allow network traffic communication?
A. Configure the new subnet to propagate to the appropriate transit gateway route table. Associate the new subnet with the appropriate VPC route table. configure new subnet
configure new subnet

Q493 A company is running several workloads in a single AWS account. A new company policy states that engineers can provision only approved resources and that engineers must use AWS CloudFormation to provision these resources. A solutions architect needs to create a solution to enforce the new restriction on the IAM role that the engineers use for access. What should the solutions architect do to create the solution?
C. Update the IAM policy for the engineers' IAM role with permissions to only allow AWS CloudFormation actions. Create a new IAM policy with permission to provision approved resources, and assign the policy to a new IAM service role. Using the IAM service role to AWS CloudFormation during stack creation
create new IAM policy with permission

Q494 A company that develops consumer electronics with offices in Europe and Asia has 60 TB of software images stored on premises in Europe. The company wants to transfer the images to an Amazon S3 bucket in the north-east-1 Region. New software images are created daily and must be encrypted in transit. The company needs a solution that does not require custom development to automatically transfer all existing and new software images to Amazon S3. What is the next step in the transfer process?

A. Deploy an AWS DataSync agent and configure a task to transfer the images to the S3 bucket
deploy AWS DataSync agent

Q495 A company has an organization in AWS Organizations that has a large number of AWS accounts. One of the AWS accounts is designated as a transit account and has a transit gateway that is shared with all of the other AWS accounts AWS Site-to-Site VPN connections are configured between all of the company's global offices and the transit account. The company has AWS Config enacted on all of its accounts. The company's networking team needs to centrally manage a list of internal IP address ranges that belong to the global offices. Developers will reference this list to gain access to their applications Securely. Which solution meets these requirements with the LEAST amount of operational overhead?
C. In the transit account, create a VPC prefix list with all of the internal IP address ranges. Use AWS Resource Access Manage* to share the prefix list with all of the other accounts Use the snored prefix list to configure security group rules in the other accounts.
create VPC prefix list

Q496 A company wants to integrate its data analytıcs environment from on premises to AWS. The environment consists of two simple Node.js applications. One of the applications collects sensor data and loads it into a MySQL database. The other application aggregates the data into reports. When the aggregation jobs run. Some of the load jobs fail to run correctly. The company must resolve the cala loading issue. The company also needs the migration to occur without interruptions or changes for the company's customers. What should a solutions architect do to meet those requirements?
C. Set up an Amazon Aurora MySQL database. Use AWS Database Mig-alion Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Create an Aurora Replica for One Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions beninc an Application Load Balancer (ALB).And use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, point to local DNS record to One ALB. Disable the AWS DMS sync task alter the culovef from on premises to AWS
Use DMS to perform data replication. createAurora Replica

Q497 A financial services company has an on-premises environment that ingests market data feeds from stock exchanges, transforms the data, and sends the data to an internal Apache Kafka cluster. Management wants to leverage AWS services to build a scalable and near-real-time solution with consistent network performance to provide stock market data to a web application. Which steps should a solutions architect take to build the solution? (Select THREE.)
A. Establish an AWS Direct Connect connection from the on-premises data center to AWS.
C. Create an Amazon EC2 Auto Scaling group to pull the messages from the on-premises Kafka cluster and use the Amazon Kinesis Producer Library to put the data into a Kinesis data stream.
D. Create a WebSocket API in Amazon API Gateway, create an AWS Lambda function to process an Amazon Kinesis data stream, and use the @connections command to send callback messages to connected clients.
Establish Direct Connect connection
Use Kinesis Producer Library to put data
Create WebSocket API

Q498 A software company has deployed a web application on AWS in a VPC. The application uses an Application Load Balancer and Amazon EC2 instances in an Auto Scaling group for the application tier. The EC2 instances access an IBM Db2 database that is hosted on separate EC2 instances Db2 credentials are stored in the configuration file on the application tier and are deployed with AWS AppConfig. The company has a new requirement to prove that the learn in charge or the operations of the platform cannot access the cleartext data that is stored in Db2. A solutions architect must implement a solution to meet this requirement with the least possible redevelopment needed. Which combination of steps should the solutions architect take?

D. Use AWS Secrets Manager to ensure that a password is not stored in the application configuration.

use AWS Secrets Manager

Q499 A company is building a hybrid solution between its existing on-premises systems and a new backend in AWS. The company has a management application to monitor the state of its current IT infrastructure and automate responses to issues. The company wants to incorporate the status of its consumed AWS services into the application. The application uses an HTTPS endpoint to receive updates. Which approach meets these requirements with the LEAST amount of operational overhead?

D. Configure Amazon EventBndge (Amazon CloudWatch Events) to detect and react to changes for AWS Health events from the AWS Service Health Dashboard. Configure the EventBridge (CloudWatch Events) event to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic and subscribe the topic to an HTTPS endpoint for the management application with a topic filter corresponding to the services being used.

AWS Service Health Dashboard

Q500 A company hosts a web application that runs on a group of Amazon EC2 instances that are behind an Application Load Balancer (ALB) in a VPC. The company wants to analyze the network payloads to reverse- engineer a sophisticated attack of the application. Which approach should the company take to achieve this goal?

B. Enable Traffic Mirroring on the network interface of the EC2 instances Send the mirrored traffic to a target for storage and analysis

enable Traffic Mirroring

Q501 A company is deploying a distributed in-memory database on a fleet of Amazon EC2 instances. The fleet consists of a primary node and eight worker nodes. The primary node is responsible for monitoring cluster health, accepting user requests, distributing user requests to worker nodes, and sending an aggregate response back to a client Worker nodes communicate with each other to replicate data partitions. The company requires the lowest possible networking latency to achieve maximum performance. Which solution will meet these requirements?

C. Launch memory optimized EC2 instances in a cluster placement group

launch memory optimized EC2 in a cluster placement group

Q502 A company is running an application in the AWS Cloud. The application uses AWS Lambda functions and Amazon Elastic Container Service(Amazon ECS)containers that run with AWS Fargate technology compute. The load on the application is irregular. The application experiences long periods of

no usage, followed by sudden and significant increases and decreases in traffic. The application is write-heavy and shows that. in an Amazon Aurora MySQL database. The database runs on an Amazon RDS memory optimized DB instance that is not able to handle the load. What is the MOST cost-effective way for the company to handle the sudden and significant changes in traffic?
D. Migrate the database to Aurora Serverless v1.Purchase Compute Savings Plans.
migrate db to Aurora serverless V1. Purchase compute saving plans

Q503 A solutions architect is planning the migration of a complete on-premises data center to the AWS Cloud. The solutions architect must map all the dependencies between the on-premises servers and must propose a migration order and timeline. The solutions architect will determine dependencies by using a combination of data that is taken from the on-premises VMs. This data will include network traffic and processes that are running. The on- premises servers are in a VMware environment. What should the solutions architect do to collect dependency information from the on-premises servers to guide the order of migration?
B. Deploy the AWS Application Discovery Agent to all servers in the VMware environment
deploy AWS Application DIscovery Agent to all servers

Q504 A company is running a serverless application that consists of several AWS Lambda functions and Amazon DynamoDB tables. The company has created new functionality that requires the Lambda functions to access an Amazon Neptune DB cluster. The Neptune DB cluster is located in three subnets in a VPC. Which of the possible solutions will allow the Lambda functions to access the Neptune DB cluster and DynamoDB tables? (Select TWO.)
B. Create three private subnets in the Neptune VPC, and route internet traffic through a NAT gateway. Host the Lambda functions in the three new private subnets.
D. Host the Lambda functions outside the VPC. Create a VPC endpoint for the Neptune database, and have the Lambda functions access Neptune over the VPC endpoint.
Route internet traffic through NAT gateway
Create VPC endpoint for Neptune db

Q505 A company that designs multiplayer online games wants to expand its user base outside of Europe. The company transfers a significant amount of UDP traffic to keep all the live and interactive sessions of the games. The company has plans for rapid expansion and wants to build its architecture to provide an optimized online experience to its users. Which architecture will meet these requirements with the LOWEST latency for users?
B. Set up environments in multiple AWS Regions. Create an accelerator in AWS Global Accelerator, and add endpoints from different Regions to it.
Create an accelerator in AWS Global Accelerator

Q506 A company is running multiple workloads in the AWS Cloud. The company has separate units for software development. The company uses AWS Organizations and federation with SAML to give permissions to developers to manage resources on their AWS accounts. The development units each deploy their production workloads into a common production account. Recently, an incident occurred in the production account in which members of a development unit terminated an EC2 instance that belonged to a different development unit. A solutions architect must create a solution that prevents a

similar incident from happening in the future. The solution also must allow developers the possibility to manage the instances used for their workloads. Which strategy will meet these requirements?
B. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Update the AM policy for the developers assume IAM role with a deny action and a StringNotEquals condition for the DevelopmentUnit resource lag and aws:PrincipalTag/'DevelopmentUnit.
update IAM policy for developers's assume IAM role with a deny action

Q507 A marketing company is m-grating an application that stores data on premises in a PostgreSQL database. The company wants to migrate the database to Amazon Aurora PostgreSQL. The database size grows at an average rate of 5 GB daily and is currently 50 TB. The data center has an internet connection with 50 Mbps of available bandwidth. The migration to AWS must be completed as soon as possible within the next 45 days. Which data transfer strategy meets those requirements with the LEAST amount of application downtime?
D. Take the application offline. Back up the database to a shared local file system. Instal an AWS DataSync agent on a VM in the data center. Configure the file system as the source location, and configure an Amazon S3 bucket as the destination. Use native database tools to restore the backup onto the new database. Modify the database connection string, and bring the application online.
install DataSync agent

Q508 A company with global offices has a single 1 Gbps AWS Direct Connect connection to a single AWS Region.The company's on-premises network uses the connection to communicate with the company's resources in the AWS Cloud. The connection has a single private virtual interface that connects to a single VPC.A solutions architect must implement a solution that adds a redundant Direct Connect connection in the same Region. The solution also must provide connectivity to other Regions through the same pair of Direct Connect connections as the company expands into other Regions. Which solution meets these requirements?
A. Provision a Direct Connect gateway.Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interlace on each connection, and connect both private virtual interfaces to the Direct Connect gateway.Connect the Direct Connect gateway to the single VPC.
Provision a Direct Connect gateway

Q509 A company runs an application on AWS.An AWS Lambda function uses credentials to authenticate to an Amazon RDS for MySQL DB instance.A security risk assessment identified that these credentials are not frequently rotated.Also, encryption at rest is not enabled for the DB instance. The security team requires that both of these issues be resolved. Which strategy should a solutions architect recommend to remediate these security risks?
A. Configure the Lambda function to store and retrieve the database credentials in AWS Secrets Manager and enable rotation of the credentials. Take a snapshot ol the DB instance and encrypt a copy of that snapshot. Replace the DB instance with a new DB instance that is based on the encrypted snapshot.
enable rotation of credentials

Q510 A medical company is running a REST API on a set of Amazon EC2 instances. The EC2 instances turn into an Auto Scaling group behind an Application Load Balancer (ALB). The ALB runs in three public subnets, and the EC2 instances run in three private subnets. The company has deployed an Amazon CloudFront distribution that has the AL8 as the only origin. Which solution should a solutions architect recommend to enhance the origin security?
A. Store a random string in AWS Secrets Manager. Create an AWS Lambda function for automatic secret rotation.Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Create an AWS WAF web ACL rule with a string match rule for the custom header.Associate the web ACL with the AL8.
store a random string in AWS Secrets Manager

Q511 A financial company is building a system to generate monthly, immutable bank account statements (or its users. Statements are stored in Amazon S3. Users should have immediate access to their monthly statements for up to 2 years. Some users access their statements frequently, whereas others rarely access their statements. The company's security and compliance policy requires that the statements be retained for at least 7 years. What is the MOST cost-effective solution to meet the company's needs?
C. Create an S3 bucket with Object Lock enabled. Store statements in S3 Intelligent-Tiering.Enable compliance mode with a default retention period of 2 years.Define an S3 Lifecycle policy to move the data to S3 Glacier after 2 years. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old.
enable compliance mode with a default retention period of 2 years

Q512 A company is running an application distributed over several Amazon EC2 instances in an Auto Seating group behind an Application Load Balancer. The security team requires that all application access attempts be made available for analysis information about the client IP address, connection type, and user agent must be included. Which solution will meet these requirements?
C. Enable access logs for the Application Load Balancer, and publish the logs to an Amazon S3 bucket. Have the security team use Amazon Athena to query and analyze the logs
enable access logs for ALB

Q513 A company uses AWS Transit Gateway for a hub-and-spoke model to manage network traffic between many VPCs. The company is developing a new service that must be able to send data at 100 Gbps. The company needs a faster connection to other VPCs in the same AWS Region. Which solution will meet these requirements?
D. Create an additional attachment from the necessary VPCs to the existing transit gateway.
create additional attachment from VPC to existing transit gateway

Q514 A company has a policy that all Amazon EC2 instances that are running a database must exist within the same subnets in a sharedVPC.Administrators must follow security compliance requirements and are not allowed to directly log in to the shared account.All company accounts are members of the same organization in AWS Organizations. The number of accounts will rapidly increase as the company grows.A solutions architect uses AWS Resource Access Manager to create a resource share in the shared account. What is the MOST operationally efficient configuration to meet these requirements?
C. Add all subnets within the VPC to the resource share.Add the organization as a principal.
add all subnets within VPC to resource share. Add organization as a principal

Q515 A solutions architect is building a web application that uses an Amazon RDS for PostgreSQL DB instance The DB instance is expected to receive many more reads than writes. The solutions architect needs to ensure that the large amount of read traffic can be accommodated and that the DB instance is highly available. Which steps should the solutions architect take to meet these requirements? (Select THREE)

B. Create multiple read replicas in different Availability Zones.

C. Create an Amazon Route 53 hosted zone and a record set for each read replica with a TTL and a weighted routing policy.

F. Configure an Amazon Route 53 health check for each read replica using its endpoint

create multiple read replicas in different availability zones

create Amazon Route 53 hosted zone

configure Amazon Route S3 health check

Q516 A company wants to deploy an AWS WAF solution to manage AWS WAF rules across multiple AWS accounts. The accounts are managed under different OUs in AWS Organizations.Administrators must be able to add or remove accounts or OUs from managed AWS WAF rule sets as needed. Administrators also must have the ability to automatically update and remediate noncompliant AWS WAF rules in all accounts. Which solution meets these requirements with the LEAST amount of operational overhead?

B. Deploy an organization-wide AWS Config rule that requires all resources in the selected OUs to associate the AWS WAF rules.Deploy automated remediation actions by using AWS Lambda to fix noncompliant resources.Deploy AWS WAF rules by using an AWS CloudFormation stack set to target the same OUs where the AWS Config rule is applied.

deploy an organization-wide AWS config rule

Q517 A company runs an application that gives users the ability to search for videos and related information by using keywords that are curated from content providers. The application data is stored in an on-premises Oracle database that is 800 GB in size. The company wants to migrate the data to an Amazon Aurora MySQL DB instance. A solutions architect plans to use the AWS Schema Conversion Tool and AWS Database Migration Service (AWS DMS) for the migration. During the migration, the existing database must serve ongoing requests. The migration must be completed with minimum downtime. Which solution will meet these requirements?

B. Use AWS DMS to run the conversion report for Oracle to Aurora MySQL. Remediate any issues Then use AWS DMS to migrate the data

use AWS DMS to run conversion report

Q518 A solution architect needs to deploy an application on a fleet of Amazon EC2 instances. The EC2 instances run in private subnets in An Auto Scaling group. The application is expected to generate logs at a rate of 100 MB each second on each of the EC2 instances. The logs must be stored in an Amazon S3 bucket so that an Amazon EMR cluster can consume them for further processing. The logs must be quickly accessible for the first 90 days and should be retrievable within 48 hours thereafter. What is the MOST cost-effective solution that meets these requirements?

B. Set up an S3 sync job to copy logs from each EC2 instance to the S3. bucket with S3 Standard storage.Use a gateway VPC endpoint for Amazon S3 to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier Deep Archive
use a gateway VPC endpoint for S3. Create S3 lifecycle policies to move logs that are older than 90 days to S3 Glacier Deep Archive.

Q519 A company warns to migrate a 30 TB Oracle data warehouse from on premises to Amazon Redshift. The company used the AWS Schema Conversion Tool (AWS SCT) to convert the schema of the existing data warehouse to an Amazon Redshift schema. The company also used a migration assessment report to identify manual tasks to complete. The company needs to migrate the data to the new Amazon Redshift cluster during an upcoming data freeze period of 2 weeks. The only network connection between the on-premises data warehouse and AWS is a 50 Mops internet connection. Which migration strategy meets these requirements?
D. Create a job in AWS Snowball Edge to import data into Amazon S3 Install AWS SCT extraction agents on the on-premises servers.Define the local and AWS Database Migration Service (AWS DMS) tasks to send the data to the Snowball Edge device. When the Snowball Edge device is returned to AWS and the data is available in Amazon S3, run the AWS DMS subtask to copy the data to Amazon Redshift.
Create a job in AWS Snowball Edge to import data into S3

Q520 A media company uses Amazon DynamoDB to store metadata for its catalog of movies that are available to stream. Each media item Contains user- facing content that concludes a description of the media, a list of search tags, and similar data. In addition, media items include a list of Amazon S3 key names that relate to movie files. The company stores these movie files in a single S3 bucket that has versioning enabled. The company uses Amazon CloudFront to serve these movie files. The company has 100.000 media items, and each media item can have many different S3 objects that represent different encodings of the same media S3 objects that belong to the same media item are grouped together under the same key prefix, which is a random unique ID Because of an expiring contract with a media provider, the company must remove 2.000 media Items. The company must completely delete all DynamoDB keys and movie files on Amazon S3 that are related to these media items within 36 hours The company must ensure that the content cannot be recovered. Which combination of actions will meet these requirements? (Select TWO.)
C. Write a script to perform a conditional delete on all the affected DynamoDB records
D. Temporarily suspend versioning on the S3 bucket. Create and invoke an AWS Lambda function that deletes affected objects Reactivate versioning when the operation is complete
Write script to perform conditional delete
Temporarily suspend versioning on S3 bucket

Q521 A solution architect is designing an AWS account structure for a company that consists of multiple terms.Al the team will work in the same AWS Region. The company needs a VPC that is connected to the on-premises network. The company expects less than 50 Mbps of total to and from the on- premises network. Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO)
B. Create an AWS CloudFormation template that provisions a VPC and the required subnets.Deploy the template to a shared services account. Share the subnets by using AWS Resource Access Manager
D. Use AWS Site-to-Site VPN for connectivity to the on-premises network
deploy template to a shared service account

use AWS site-to-site VPN for connectivity

Q522 A company is migrating applications from on premises to the AWS Cloud. These applications power the company's internal web forms. These web forms collect data for specific events several times each quarter. The web forms use simple SQL statements to save the data to a local relational database. Data collection occurs for each event, and the on-premises servers are idle most of the time. The company needs to minimize the amount of idle infrastructure that supports the web forms. Which solution will meet these requirements?

D. Provision an Amazon Aurora Serverless cluster.Build multiple schemas for each web form's data storage.Use Amazon API Gateway and an AWS Lambda function to recreate the data input forms .Use Amazon Route 53 to point the DNS names of the web forms to their corresponding API Gateway endpoint.

provision an Aurora Serverless cluster

Q523 A company is running its AWS infrastructure across two AWS Regions. The company has four VPCs in the eu-west-1 Region and has two VPCs in the us-east-1 Region. The company also has an on-premises data center in Europe that has two AWS Direct Connect connections in eu-west-1. The company needs a solution in which Amazon EC2 instances in each VPC can connect to each other by using private IP addresses. Servers in the on- premises data center also must be able to connect to those VPCs by using private IP addresses. What is the MOST cost-effective solution that meets these requirements?

B. Create VPC peering between each VPC in the same Region. Create cross-Region peering between each VPC in different Regions. Create two private VIFs, and attach them to a single Direct Connect gateway.Associate each VPC with the Direct Connect gateway.

create VPC peering between each VPC. Create two private VIFs

Q524 A company is using multiple AWS accounts. The company has a shared service account and several other accounts for different projects.A team has a VPC in a project account. The team wants to connect this VPC to a corporate network through an AWS Direct Connect gateway that exists in the shared services account. The team wants to automatically perform a virtual private gateway association with the Direct Connect gateway by using an already- tested AWS Lambda function while deploying its VPC networking stack. The Lambda function code can assume a role by using AWS Security Token Service (AWS STS).The team is using AWS CloudFormation to deploy its infrastructure. Which combination of steps will meet these requirements? (Choose three.)

A. Deploy the Lambda function to the project account. Update the Lambda function's IAM role with the directconnect:* permission

C. Add a custom resource to the CloudFormation networking stack that references the Lambda function in the project account.

E. Create a cross-account IAM role in the shared services account that grants the sts:AssumeRole permission to the Lambda function with the directconnect:* permission acting as a resource.Add the sts:AssumeRole permission with this cross-account IAM role as a resource to the IAM role that belongs to the Lambda function in the project account.

deploy Lambda function to project account
reference Lambda function in project account
belongs to Lambda function in project account

Q525 A company is migrating a legacy application from an on-premises data center to AWS. The application consists of a single application server and a Microsoft SQL Server database server.Each server is deployed on a VMware VM that consumes 500 TB of data across multiple attached volumes. The company has established a 10 Gbps AWS Direct Connect connection from the closest AWS Region to its on-premises data center.The Direct Connect connection is not currently in use by other services. Which combination of steps should a solutions architect take to migrate the application with the LEAST amount of downtime? (Choose two.)

D. Use an AWS Server Migration Service (AWS SMS) replication job to migrate the application server VM to AWS.

E. Use an AWS Database Migration Service (AWS DMS) replication instance to migrate the database to an Amazon RDS DB instance.

use AWS (SMS) replication job to migrate application server VM to AWS

use AWS (DMS) replication to migrate db to Amazon RDS DB

Q526 A company has a new application that needs to run on five Amazon EC2 instances in a single AWS Region. The application requires high-throughput, low-latency network connections between all of the EC2 instances where the application will run. There is no requirement for the application to be fault tolerant. Which solution will meet these requirements?

A. Launch five new EC2 instances into a cluster placement group.Ensure that the EC2 instance type supports enhanced networking.

launch 5 new EC2 into a cluster placement group

Q527 A company is deploying a new cluster for big data analytics on AWS. The cluster will run across many Linux Amazon EC2 instances that are spread across multiple Availability Zones. All of the nodes in the cluster must have read and write access to common underlying file storage. The file storage must be highly available, must be resilient, must be compatible with the Portable Operating System Interface (POSIX), and must accommodate high levels of throughput. Which storage solution will meet these requirements?

D. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses Max I/O performance mode.Mount the EFS file system on each EC2 instance in the cluster.

use Max I/O performance mode

Q528 A company needs to design and implement a solution in which users can receive electronic copies of their receipts after making a purchase. The users should have up to 1 week to download the receipt, and the company wants receipts to be stored for 1 year. The receipt images will be provided in jpg format, along with the user's email address. The solution should handle the storage and delivery of the receipts to the users while minimizing the cost and changes to the existing infrastructure. Which strategy should a solutions architect use?

B. Store the receipt image in Amazon S3. Configure an AWS Lambda function to execute in response to an S3 event notification to send an email with a presigned URL link of the receipt through Amazon Simple Email Service (Amazon SES). Create an S3 Lifecycle rule to delete receipts older than 1 year

store receipt image in S3. Configure AWS Lambda function

Q529 A company has developed a single-page web application in JavaScript. The source code is stored in a single Amazon S3 bucket in the us-east-1 Region. The company serves the web application to a global user base through Amazon CloudFront. The company wants to experiment with two versions of the website without informing application users.Each version of the website will reside in its own S3 bucket. The company wants to determine which version is most successful in marketing a new product. The solution must send application users that are based in Europe to the new website design. The solution must send application users that are based in the United States to the current website design. However, some exceptions exist. The company needs to be able to redirect specific users to the new website design, regardless of the users' location. Which solution meets these requirements?
D. Configure a single CloudFront distribution with Lambda@Edge. Use Lambda@Edge to send user requests to different origins based on request attributes
Use Lambda@Edge to send user request

Q530 A company is running a data-intensive application on AWS.The application runs on a cluster of hundreds of Amazon EC2 instances.A shared file system also runs on several EC2 instances that store 200 TB of data. The application reads and modifies the data on the shared file system and generates a report. The job runs once monthly, reads a subset of the files from the shared file system, and takes about 72 hours to complete. The computer instances scale in an Auto Scaling group, but the instances that host the shared file system run continuously. The compute and storage instances are all in the same AWS Region.A solutions architect needs to reduce costs by replacing the shared file system instances. The file system must provide high performance access to the needed data for the duration of the 72-hour run. Which solution will provide the LARGEST overall cost reduction while meeting these requirements?
A. Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Intelligent-Tiering storage class.Before the job runs each month, use Amazon FSx for Lustre to create a new file system with the data from Amazon S3 by using lazy loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete.
use S3 Intelligent-Tiering storage class

Q531 A company runs a popular web application in an on-premises data center. The application receives four million views weekly. The company expects traffic to increase by 200% because of an advertisement that will be published soon. The company needs to decrease the load on the origin before the increase of traffic occurs. The company does not have enough time to move the entire application to the AWS Cloud. Which solution will meet these requirements?
A. Create an Amazon CloudFront content delivery network (CDN).Enable query forwarding to the origin. Create a managed cache policy that includes query strings. Use an on-premises load balancer as the origin.Offload the DNS querying to AWS to handle CloudFront CDN traffic.
create a managed cache policy

Q532 A an Auto Scaling group behind an Application Load Balancer. The load on the application varies throughout the day, and EC2 instances are scaled in and out on a regular basis.Log files from the EC2 instances are copied to a central Amazon S3 bucket every 15 minutes. The security team discovers that log files are missing from some of the terminated EC2 instances. Which set of actions will ensure that log files are copied to the central S3 bucket from the terminated EC2 instances?

B. Create an AWS Systems Manager document with a script to copy log files to Amazon S3.Create an Auto Scaling lifecycle hook and an Amazon EventBridge (Amazon Cloud Watch Events) rule to detect lifecycle events from the Auto Scaling group.Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send CONTINUE to the Auto Scaling group to terminate the instance.
send CONTINUE to Auto Scaling group to terminate instance

Q533 A company has developed a web application. The company is hosting the application on a group of Amazon EC2 instances behind an Application Load Balancer. The company wants to improve the security posture of the application and plans to use AWS WAF web ACLs. The solution must not adversely affect legitimate traffic to the application. How should a solutions architect configure the web ACLs to meet these requirements?
A. Set the action of the web ACL rules to Count.Enable AWS WAF logging Analyze the requests for false positives.Modify the rules to avoid any false positive.Over time change the action of the web ACL rules from Count to Block.
Set action of web ACL rules, Enable AWS WAF logging

Q534 A company manages an on-premises JavaScript front-end web application. The application is hosted on two servers secured with a corporate Active Directory. The application calls a set of Java-based microservices on an application server and stores data in a clustered MySQL database. The application is heavily used during the day on weekdays.It is lightly used during the evenings and weekends.Daytime traffic to the application has increased rapidly. and reliability has diminished as a result. The company wants to migrate the application to AWS with a solution that eliminates the need for server maintenance, with an API to securely connect to the microservices. Which combination of actions will meet these requirements? (Select THREE.)
A. Host the web application on Amazon S3.Use Amazon Cognito identity pools (federated identities) with SAML for authentication and authorization
C. Create an API layer with Amazon API Gateway.Rehost the microservices on AWS Fargate containers.
F. Replatform the database to Amazon Aurora MySQL Serverless.
host web app on S3
rehost micro services on AWS Fargate containers
replatform db to Aurora MySQL serverless

Q535 A company wants to host a new global website that consists of static content.A solutions architect is working on a solution that uses Amazon CloudFront with an origin access identity (OAI) to access website content that is stored in a private Amazon S3 bucket. During testing, the solutions architect receives 404 errors from the S3 bucket.Error messages appear only for attempts to access paths that end with a forward slash. such as example.com/ path/.These requests should return the existing S3 object path/index.html.Any potential solution must not prevent CloudFront from caching the content. What should the solutions architect do to resolve this problem?
C. Change the CloudFront configuration to use an AWS Lambda@Edge function that is invoked by a viewer request event to rewrite the S3 request URL.
AWS Lambda@Edge function that is invoked by a viewer request event

Q536 A company has developed an application that is running Windows Server on VMware vSphere VMs that the company hosts or premises. The application data is stored in a proprietary format that must be read through the application. The company manually provisioned the servers and the application.As pan of us disaster recovery plan, the company warns the ability to host its application on AWS temporarily me company's on-premises environment becomes unavailable The company wants the application to return to on-premises hosting after a disaster recovery event is complete the RPO in 5 minutes. Which solution meets these requirements with the LEAST amount of operational overhead?

B. Configure CloudEndure Disaster Recovery.Replicate the data to replication Amazon EC2 instances that are attached to Amazon Elastic Block Store (Amazon EBS) volumes. When the on-premises environment is unavailable, use CloudEndure to launch EC2 instances that use the replicated volumes

Configure CloudEndure DR

Q537 A company plans to refactor a monolithic application into a modern application designed deployed or AWS. The CLCD pipeline needs to be upgraded to support the modem design for the application with the following requirements ?It should allow changes to be released several times every hour.* It should be able to roll back the changes as quickly as possible. Which design will meet these requirements?

B. Specify AWS Elastic Beanstalk to sage in a secondary environment as the deployment target for the CI/CD pipeline of the application. To deploy swap the staging and production environment URLs

specify AWS Elastic Beanstalk to sage

Q538 A data analytics company has an Amazon Redshift cluster that consists of several reserved nodes. The duster is experiencing unexpected bursts of usage because a team of employees is compiling a deep audit analysis report. The queries to generate the report are complex read queries and are CPU intensive.Business requirements dictate that the cluster must be able to service read and write queries at times.A solutions architect must devise a solution that accommodates the bursts of usage. Which solution meets these requirements MOST cost-effectively?

D. Turn on the Concurrency Scaling feature for the Amazon Redshift duster

turn on Concurrency Scaling feature for Redshift duster

Q539 A company is creating a sequel for a popular online game. A large number of users from all over the world will play the game within the first week after launch.Currently, the game consists of the following components deployed in a single AWS Region:- Amazon S3 bucket that stores game assets. Amazon DynamoDB table that stores player scores. A solutions architect needs to design a multi-Region solution that will reduce latency, improve reliability, and require the least effort to implement. What should the solutions architect do to meet these requirements?

C. Create another S3 bucket in a new Region and configure S3 Cross-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Region.Configure DynamoDB global tables by enabling Amazon DynamoDB Streams, and add a replica table in a new Region

Create another S3 bucket in a new Region

Q540 A company's solution architect is designing a disaster recovery (DR) solution for an application that runs on AWS.The application uses PostgreSQL 11.7 as its database. The company has a PRO of 30 seconds. The solutions architect must design a DR solution with the primary database in the us-east-1 Region and the database in the us-west-2 Region. What should the solution architect do to meet these requirements with minimum application change?

C. Migrate the database to an Amazon Aurora PostgreSQL global database with the primary Region as us-east-1 and the secondary Region as us- west-2.Set the managed PRO for the Aurora database to 30 seconds.

migrate db to Aurora PostgreSQL global database

Q541 A company is planning to migrate an application from on premises to the AWS Cloud. The company will begin the migration by moving the application's underlying data storage to AWS. The application data is stored on a shared file system on premises, and the application servers connect to the shared We system through SMB.A solutions architect must implement a solution that uses an Amazon S3 bucket tor shared storage.Until the application Is fully migrated and code is rewritten to use native Amazon S3 APIs, the application must continue to have access to the data through SMB. The solutions architect must migrate the application data to AWS to its new location while still allowing the on-premises application to access the data. Which solution will meet these requirements?

D. Create an S3 bucket for the application.Deploy a new AWS Storage Gateway file gateway on an on-premises VM.Create a new file share that stores data in the S3 bucket and is associated with the file gateway.Copy the data from the on-premises storage to the new file gateway endpoint.

deploy a new AWS Storage Gateway file gateway on an on-premises VM

Q542 An organization is creating a VPC for their application hosting. The organization has created two private subnets in the same AZ and created one subnet in a separate zone. The organization wants to make a HA system with the internal ELB. Which of these statements is true with respect to an internal ELB in this scenario?

A. ELB can support only one subnet in each availability zone.

ELB can support only one subnet

Q543 A company is migrating its data center from on premises to the AWS Cloud. The migration will take several months to complete. The company will use Amazon Route 53for private DNS zones During the migration, the company must keep its AWS services pointed at the VPC's Route 53 Resolver for DNS. The company also must maintain the ability to resolve addresses from its on-premises DNS server. A solutions architect must set up DNS so that Amazon EC2 instances can use native Route 53 endpoints to resolve on-premises DNS queries. Which configuration will meet these requirements?

C. Create a new outbound endpoint in Route 53 and attach the endpoint to the VPC.Ensure that the security groups that are attached to the endpoint can access the on-premises DNS server IP address on port 53.Create a new Route 53 Resolver rule that routes on-premises designated traffic to the on-premises DNS server.

create a new outbound endpoint in Route 53

Q544 A company is migrating its infrastructure to the AWS Cloud. The company must comply with a variety of regulatory standards for different projects. The company needs a multi-account environment.A

solutions architect needs to prepare the baseline infrastructure The solution must provide a consistent baseline of management and security but it must allow flexibility for different compliance requirements within various AWS accounts. The solution also needs to integrate with the existing on-premises Active Directory Federation Services (AD FS) server. Which solution meets these requirements with the LEAST amount of operational overhead?

A. Create an organization In AWS Organizations. Create a single SCP for least privilege access across all accounts.Create a single OU for all accounts.Configure an IAM identity provider tor federation with the on-premises AD FS server.Configure a central togging account with a defined process for log generating services to send log events to the central account.Enable AWS Config in the central account with conformance packs for all accounts.

create a single SCP for least privilege access across all accounts

Q545 A company runs applications on Amazon EC2 instances. The company plans to begin using an Auto Scaling group for the instances.As part of this transition, a solutions architect must ensure that Amazon CloudWatch Logs automatically collects logs from all new instances. The new Auto Scaling group will use a launch template that includes the Amazon Linux 2 AMI and no key pair. Which solution meets these requirements?

B. Create an Amazon CloudWatch agent configuration for the workload In AWS Systems Manager Parameter Store Create a Systems Manager document that Installs and configures the CloudWatch agent by using the configuration Create an Amazon EventBridge (Amazon CloudWatch Events) rule on the default event bus with a Systems Manager Run Command target that runs the document whenever an instance enters the running state

create Amazon EventBridge(CloudWatch Events) rule on default event bus

Q546 A company has used infrastructure as code (IaC) to provision a set of two Amazon EC2 instances. The instances have remained the same for several years. The company's business has grown rapidly in the past few months. In response, the company's operations team has implemented an Auto Scaling group to manage the sudden increases in traffic Company policy requires a monthly installation of security updates on all operating systems that are running. The most recent security update required a reboot.As a result the Auto Scaling group terminated the instances and replaced them with new, unpatched instances. Which combination of steps should a sol-tons architect recommend to avoid a recurrence of this issue? (Select TWO)

A. Modify the Auto Scaling group by setting the Update policy to target the oldest launch configuration for replacement.

D. Create automation scripts to patch an AMI. Update the launch configuration, and invoke an Auto Scaling instance refresh.

modify Auto Scaling group by setting Update policy

Create automation scripts to patch an AMI

Q547 A solutions architect uses AWS Organizations to manage several AWS accounts for a company. The full Organizations feature set is activated for the organization.All production AWS accounts exist under an OU that is named 'production' Systems operators have full administrative privileges within these accounts by using IAM roles. The company wants to ensure that security groups in all production accounts do not allow inbound traffic for TCP port 22.All noncompliant security groups must be remediated immediately, and no new rules that allow port 22 can be created. Which solution will meet these requirements?

D. Create an AWS CloudFormation template to turn on AWS Config Activate the INCOMING_SSH_DISABLED AWS Config managed rule Deploy an AWS Lambda function that will run based on AWS Config findings and will remediate noncompliant resources Deploy the CloudFormation template by using a StackSet that is assigned to the "production" OU.Apply an SCP to the OU to deny modification of the resources that the CloudFormation template provisions.
create AWS CloudFormation template to turn on AWS config Activate

Q548 A company has a web application that runs on a single on-premises Apache server. The Apache server maintains browsing sessions for users. The web application is used only at the start of the workday and after lunchtime. The company is migrating the web application to the AWS Cloud and can implement changes to the application code. The company wants to minimize maintenance efforts and maximize resiliency. What should a solutions architect recommend to meet these requirements?
A. Create an AWS Elastic Beanstalk application. Migrate the on-premises web application to the Elastic Beanstalk application Adapt the web application to store user session data in Amazon DynamoDB
create AWS Elastic Beanstalk application

Q549 A solutions architect needs to provide AWS Cost and Usage Report data from a company's AWS Organizations management account. The company already has an Amazon S3 bucket to store the reports. The reports must be automatically ingested into a database that can be visualized with other toots. Which combination of steps should the solutions architect take to meet these requirements? (Select THREE)
A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that a new object creation in the S3 bucket will trigger
B. Create an AWS Cost and Usage Report configuration to deliver the data into the S3 bucket
F. Create an AWS Glue crawler that the Amazon EventBridge (Amazon CloudWatCh Events) rule will trigger to crawl objects m the S3 bucket
Create EventBridge rule
Create Cost and Usage Report
Create Glue crawler that EventBridge rule will trigger

Q550 A company used Amazon EC2 instances to deploy a web fleet to host a blog site. The EC2 instances are behind an Application Load Balancer (ALB) and are configured in an Auto Scaling group. The web application stores all blog content on an Amazon EFS volume. The company recently added a feature 'or Moggers to add video to their posts, attracting 10 times the previous user traffic. At peak times of day, users report buffering and timeout issues while attempting to reach the site or watch videos. Which is the MOST cost-efficient and scalable deployment that will resolve the issues for users?
C. Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.
configure CloudFront distribution

Q551 A company has created an OU in AWS Organizations for each of its engineering teams. Each OU owns multiple AWS accounts. The organization has hundreds of AWS accounts. A solutions architect must design a solution so that each OU can view a breakdown of usage costs across its AWS accounts. Which solution meets these requirements?

B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard
create AWS Cost and Usage Report(CUR) from Organizations management account

Q552 A company is planning to migrate an application from on premises to AWS. The application currently uses an Oracle database and the company can tolerate a brief downtime of 1 hour when performing the switch to the new infrastructure As part of the migration. the database engine will be changed to MySQL. A solutions architect needs to determine which AWS services can be used to perform the migration while minimizing the amount of work and time required. Which of the following will meet the requirements?
B. Use AWS SCT to generate the schema scripts and apply them on the target prior to migration. Use AWS DMS to begin moving data from the on- premises database to AWS. After the initial copy continues to use AWS DMS to keep the databases in sync until cutting over to the new database. Use AWS SCT to identify what embedded SOL code in the application can be converted and what has to be done manually. During tests, the solutions architect was able to successfully get existing test objects in the S3 bucket. However, attempts to upload a new object resulted in an error message. The error message stated that the action was forbidden. Which action must the solutions architect add to the IAM policy to meet all the requirements? A. kms: GenerateDatakey
use AWS SCT to generate schema scripts. Use AWS DMS to begin moving data from on-premises db to AWS

Q553 A solutions architect needs to implement a client-side encryption mechanism for objects that will be stored in a new Amazon S3 bucket. The solutions architect created a CMK that is stored in AWS Key Management Service (AWS KMS) for this purpose. The solutions architect created the following IAM policy and attached it to an IAM role:

```
{
   “version": "2012-10-17",
   "statement": [
        {
          "sid": "DownloadUpload",
          "Action": [
                  "s3: Getobject"
                  "s3: GetobjectVersion",
                  "s3: Putobject",
                  "s3: PutobjectAc1"
            ],
           "Effect": "Allow",
           “Resource”: “arn: aws: : s3: :: BucketName/*”
       },
       {
          "sid": "KMSAccess",
          "Action": :[
                "kms: Decrypt”,
                "kms : Encrypt"
          ],
          "Effect": "Allow",
          "Resource!: "arn: aws: kms : Region: Account: key/Key ID"
```

```
    }
  }
}
```

During tests, the solutions architect was able to successfully get existing test objects in the S3 bucket. However, attempts to upload a new object resulted in an error message. The error message stated that the action was forbidden. Which action must the solutions architect add to the IAM policy to meet all the requirements?
A. kms: GenerateDatakey
A. kms: GenerateDatakey

Q554 A company is building an application on AWS. The application sends logs to an Amazon Elasticsearch Service (Amazon ES) cluster for analysis. All data must be stored within a VPC. Some of the company's developers work from home. Other developers work from three different company office locations. The developers need to access Amazon ES to analyze and visualize logs directly from their local development machines. Which solution will meet these requirements?
A. Configure and set up an AWS Client VPN endpoint. Associate the Client VPN endpoint with a subnet in the VPC. Configure a Client VPN self- service portal. Instruct the developers to connect by using the client for Client VPN
configure and set up AWS Client VPN endpoint

Q555 A media company is hosting a high-traffic news website on AWS. The website's front end is based solely on HTML and JavaScript. The company loads all dynamic content by using dynamic asynchronous JavaScript requests to a dedicated backend infrastructure. The front end runs on four Amazon EC2 instances as web servers. The dynamic backend runs in containers on an Amazon Elastic Container Service (Amazon ECS) cluster that uses an Auto Scaling group of EC2 instances. The ECS tasks are behind an Application Load Balancer (ALB). Which solutions should a solutions architect recommend to optimize costs? (Choose two.)
A. Migrate the front end of the website to an Amazon S3 bucket Deploy an Amazon CloudFront distribution. Set the $3 bucket as the distribution's
B. Deploy an Amazon CloudFront distribution. Configure the distribution to use the ALB endpoint as the origin.
migrate front end of website to S3 bucket
deploy amazon CloudFront distribution

Q556 A software development company has multiple engineers who are working remotely. The company is running Active Directory Domain Services (AD DS) on an Amazon EC2 instance. The company's security policy states that all internal, nonpublic services that are deployed in a VPC must be accessible through a VPN Multi-factor authentication (MFA) and must be used for access to a VPN. What should a solution architect do to meet these requirements?
B. Create an AWS Client VPN endpoint Create an AD Connector directory for integration with AD DS. Enable MFA for AD Connector Use AWS Client VPN to establish a VPN connection.
create AWS Client VPN endpoint

Q557 A solutions architect has implemented a SAML 2.0 federated identity solution with their company's on-premises identity provider (IdP) to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal access to the AWS environment is granted. However, when test users attempt to authenticate through the federated identity web portal, they are not able to access the AWS environment. Which items should the solutions architect check to ensure identity federation is property configured? (Select THREE)

B. The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principle.

D. The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider the ARN of the IAM role, and the SAML assertion from Idp

F. The company's IdP defines SAML assertions that property map users or groups m the company to IAM roles with appropriate permissions

IAM roles created for federated user's

web portal calls AWS STS

company's idP defines SAML assertions

Q558 An AWS partner company is building a service in AWS Organizations using Its organization named org. This service requires the partner company to have access to AWS resources in a customer account, which is in a separate organization named org2. The company must establish least privilege security access using an API or command line tool to the customer account. What is the MOST secure way to allow org1 to access resources in org2?

D. The customer should create an IAM rote and assign the required permissions to the IAM rote. The partner company should then use the IAM rote's Amazon Resource Name (ARN). Including the external ID in the IAM role's trust pokey, when requesting access to perform the required tasks

including external ID in the IAM role's trust key

Q559 What should the solutions architect do to meet this requirement?

B. Use Amazon CloudWatch to monitor service quotas that are published under the AWS-'Usage metric namespace Set an alarm for when the math expression metricSERVICE QUOTA(metric)"100 is greater than 80 Notify the development team by using Amazon Simple Notification Service (Amazon SNS).

use CloudWatch to monitor service quotas

Q560 A finance company is storing financial records in an Amazon S3 bucket. The company persists a record for every financial transaction. According to regulatory requirements, the records cannot be modified for at least 1 year after they are written. The records are read on a regular basis and must be immediately accessible. Which solution will meet these requirements?

A. Create a new S3 bucket. Turn on S3 Object Lock, set a default retention period of 1 year, and set the retention mode to compliance mode. Store all records in the new S3 bucket.

set retention mode to compliance mode

Q561 A digital marketing company has multiple AWS accounts that belong to various teams. The creative team uses an Amazon S3 bucket in its AWS account to securely store images and media files that are used as content for the company's marketing campaigns. The creative team wants to share the S3 bucket with the strategy team so that the strategy team can view the objects. A solutions architect has created an

IAM role that is named strategy_reviewer in the Strategy account. The solutions architect also has set up a custom AWS Key Management Service (AWS KMS) key in the Creative account and has associated the key with the S3 bucket. However, when users from the Strategy account assume the IAM role and try to access objects in the S3 bucket, they receive an Account. The solutions architect must ensure that users in the Strategy account can access the S3 bucket. The solution must provide these users with only the minimum permissions that they need. Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)

A. Create a bucket policy that includes read permissions for the S3 bucket. Set the principal of the bucket policy to the account ID of the Strategy account

C. Update the custom KMS key policy in the Creative account to grant decrypt permissions to the strategy_reviewer IAM role.

F. Update the strategy_reviewer IAM role to grant read permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key

set principles of bucket policy to account ID of strategy account
grant decrypt permissions to strategy_reviewer IAM role
grant read permissions for S3

Q562 A company wants to deploy an API to AWS. The company plans to run the API on AWS Fargate behind a load balancer. The API requires the use of header-based routing and must be accessible from on-premises networks through an AWS Direct Connect connection and a private VIF. The company needs to add the client IP addresses that connect to the API to an allow list in AWS. The company also needs to add the IP addresses of the API to the allow list. The company's security team will allow /27 CIDR ranges to be added to the allow list. The solution must minimize complexity and operational overhead. Which solution will meet these requirements?

C. Create two new '27 subnets. Create a new Network Load Balancer (NLB) that extends across the new subnets. Create a new Application Load Balancer (ALB) within the new subnets. Create a security group that includes only the client IP addresses that need access to the API. Attach the security group to the ALB. Add the ALB's IP addresses as targets behind the NLB. Provide the security team with the NLB's IP addresses for the allow list

Create two new 27 subnet. Create new NLB

Q563 A company is running an application in the AWS Cloud. The application runs on containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The ECS tasks use the Fargate launch type. The application's data is relational and is stored in Amazon Aurora MySQL. To meet regulatory requirements, the application must be able to recover to a separate AWS Region in the event of an application failure. In case of a failure, no data can be lost. Which solution will meet these requirements with the LEAST amount of operational overhead?

A. Provision an Aurora Replica in a different Region.

provision Aurora Replica in a different Region

Q564 A software company has deployed an application that consumes a REST API by using Amazon API Gateway. AWS Lambda functions, and an Amazon DynamoDB table. The application is showing an increase in the number of errors during PUT requests. Most of the PUT calls come from a small number of clients that are authenticated with specific API keys. A solutions architect has identified that a large number of the PUT requests originate from one client. The API is noncritical, and clients can tolerate

retries of unsuccessful calls. However, the errors are displayed to customers and are causing damage to the API's reputation. What should the solutions architect recommend to improve the customer experience?
B. Implement API throttling through a usage plan at the API Gateway level. Ensure that the client application handles code 429 replies without error.
implement API throttling

Q565 A company is planning to migrate its on-premises data analysis application to AWS. The application is hosted across a fleet of servers and requires consistent system time. The company has established an AWS Direct Connect connection from its on-premises data center to AWS. The company has a high-precision stratum-0 atomic dock network appliance that acts as an NTP source for all on-premises servers. After the migration to AWS is complete, the clock on all Amazon EC2 instances that host the application must be synchronized with the on-premises atomic clock network appliance. Which solution will meet these requirements with the LEAST administrative overhead?
A. Configure a DHCP options set with the on-premises NTP server address. Assign the options set to the VPC. Ensure that NTP traffic is allowed between AWS and the on-premises networks
Configure a DHCP options set

Q566 A company is processing videos in the AWS Cloud by using Amazon EC2 instances in an Auto Scaling group. It takes 30 minutes to process a video. Several EC2 instances scale in and out depending on the number of videos in an Amazon Simple Queue Service (Amazon SQS) queue. The company has configured the SQS queue with a redrive policy that specifies a target dead-letter queue and a maxReceiveCount of 1. The company has set the visibility timeout for the SQS queue to 1 hour. The company has set up an Amazon CloudWatch alarm to notify the development team when there are messages in the dead-letter queue. Several times during the day, the development team receives notification that messages are in the dead-letter queue and that videos have not been processed properly. An investigation finds no errors in the application logs. How can the company solve this problem?
C. Configure scale-in protection for the instances during processing
configure scale-in protection

Q567 An ecommerce company runs its infrastructure on AWS. The company exposes its APIs to its web and mobile clients through an Application Load Balancer (ALB) in front of an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster runs thousands of pods that provide the APIs. After extending delivery to a new continent, the company adds an Amazon CloudFront distribution and sets the ALB as the origin. The company also adds AWS WAF to its architecture. After implementation of the new architecture, API calls are significantly. However, there is a sudden increase in HTTP status code 504 (Gateway Timeout) errors and HTTP status code 502 (Bad Gateway) errors. This increase in errors seems to be for a specific domain. Which factors could be a cause of these errors? (Select TWO.)
A. AWS WAF is blocking suspicious requests.
E. Some pods are taking more than 30 seconds to answer API calls.
AWS WAF is blocking suspicious request
Some pods are taking more than 30 sec to answer API calls

Q568 A gaming company created a game leaderboard by using a Multi-AZ deployment of an Amazon RDS database. The number of users is growing. and the queries to get individual player rankings are

getting slower over time. The company expects a surge in users for an upcoming version and wants to optimize the design for scalability and performance. Which solution will meet these requirements?
B. Keep the leaderboard data in the RDS DB instance. Provision a Multi-AZ deployment of an Amazon ElastiCache for Redis cluster.
keep leaderboard data in RDS DB instance

Q569 A company has a serverless multi-tenant content management system on AWS. The architecture contains a web-based front end that interacts with an Amazon API Gateway API that uses a custom AWS Lambda authorizer. The authorizer authenticates a user to its tenant ID and encodes the information in a JSON Web Token (JWT) token. After authentication, each API call through API Gateway targets a Lambda function that interacts with a single Amazon DynamoDB table to fulfill requests. To comply with security standards, the company needs a stronger isolation between tenants. The company will have hundreds of customers within the first year. Which solution will meet these requirements with the LEAST operational overhead?
B. Add tenant ID information to the partition key of the DynamoDB table. Create a service that uses the JWT token to retrieve the appropriate Lambda execution role that is tenant-specific. Attach IAM policies to the execution role to allow access to items in the table only when the key matches the tenant ID
add tenant ID information to partition key of DynamoDB table

Q570 A company manages multiple AWS accounts by using AWS Organizations. Under the root OU. The company has two OUs:Research and DataOps Because of regulatory requirements, all resources that the company deploys in the organization must reside in the ap-northeast-1 Region. Additionally, EC2 instances that the company deploys in the DataOps OU must use a predefined list of instance types. A solutions architect must implement a solution that applies these restrictions. The solution must maximize operational efficiency and must minimize ongoing maintenance. Which combination of steps will meet these requirements? (Select TWO)
C. Create an SCP Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU.
E. Create an SCP Use the ec2:InstanceType condition key to restrict access to specific instance types. Apply the SCP to the DataOps OU.
created SCP use aws:requestedRegion condition key
Create SCP use ec2:InstanceType condition key

Q571 A solutions architect is designing a solution to connect a company's on-premises network with all the company's current and future VPCs on AWS. The company is running VPCs in five different AWS Regions and has at least 15 VPCs in each Region. The company's AWS usage is constantly increasing and will continue to grow. Additionally, all the VPCs throughout all five Regions must be able to communicate with each other. The solution must maximize scalability and ease of management. Which solution meets these requirements?
A. Set up a transit gateway in each Region Establish a redundant AWS Site-to-Site VPN connection between the on-premises firewalls and the transit gateway in the Region that is closest to the on-premises network Peer all the transit gateways with each other Connect all the VPCs to the transit gateway in their Region
transit gateway in the region that is closest to on-premises network

Q572 A company has implemented a global multiplayer gaming platform. The platform requires gaming clients to have reliable, low-latency access to the server infrastructure that is hosted on a fleet of Amazon EC2 instances in a single AWS Region The gaming clients use a custom TCP protocol to connect to the server infrastructure. The application architecture requires client IP addresses to be available to the server software. Which solution meets these requirements?

A. Create a Network Load Balancer (NLB), and add the EC2 instances to a target group Create an Amazon CloudFront Real Time Messaging Protocol (RTMP) distribution and configure the origin to point to the DNS endpoint of the NLB Use proxy protocol version 2 headers to preserve client IP addresses

Create NLB

Q573 A solutions architect is importing a VM from an on-premises environment by using the Amazon EC2 VM Import feature of AWS Import/Export. The solutions architect has created an AMI and has provisioned an Amazon EC2 instance that is based on that AMI. The EC2 instance runs inside a public subnet in a VPC and has a public IP address assigned. The EC2 instance does not appear as a managed instance in the AWS Systems Manager console. Which combination of steps should the solutions architect take to troubleshoot this issue? (Select TWO)

A. Verify that Systems Manager Agent is installed on the instance and is running

B. Verify that the instance is assigned an appropriate IAM role for Systems Manager

verify Systems Manager Agent is installed

verify that instance is assigned an IAM role for Systems Manager

Q574 A retail company has a small ecommerce web application that uses an Amazon RDS for PostgreSQL DB instance. The DB instance is deployed with the Multi-AZ option turned on. Application usage recently increased exponentially and users experienced frequent HTTP 503 errors. Users reported the errors, and the company's reputation suffered. The company could not identify a definitive root cause. The company wants to improve its operational readiness and receive alerts before users notice an incident. The company also wants to collect enough information to determine the root cause of any future incident. Which solution will meet these requirements with the LEAST operational overhead?

D. Turn on Performance Insights for the DB instance Modify the corresponding parameter group to turn on query logging for all the slow queries Create Amazon CloudWatch alarms Set the alarms to appropriate thresholds that are based on performance metrics in CloudWatch

turn on performance insights

Q575 A company is running a legacy application on Amazon EC2 instances in multiple Availability Zones behind a software load balancer that runs on an active/standby set of EC2 instances. For disaster recovery, the company has created a warm standby version of the application environment that is deployed in another AWS Region. The domain for the application uses a hosted zone from Amazon Route 53. The company needs the application to use static IP addresses, even in the case of a failover event to the secondary Region. The company also requires the client's source IP address to be available for auditing purposes. Which solution meets these requirements with the LEAST amount of operational overhead?

A. Replace the software load balancer with an AWS Application Load Balancer. Create an AWS Global Accelerator accelerator. Add an endpoint group for each Region. Configure Route 53 health checks. Add an alias record that points to the accelerator.
add an alias record that points to accelerator

Q576 A medical company is running an application in the AWS Cloud. The application simulates the effect of medical drugs in development. The application consists of two parts:configuration and simulation. The configuration part runs in AWS Fargate containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The simulation part runs on large, compute optimized Amazon EC2 instances. Simulations can restart if they are interrupted. The configuration part runs 24 hours a day with a steady load. The simulation part runs only for a few hours each night with a variable load. The company stores simulation results in Amazon S3, and researchers use the results for 30 days. The company must store simulations for 10 years and must be able to retrieve the simulations within 5 hours. Which solution meets these requirements MOST cost-effectively?
C. Purchase Compute Savings Plans to cover the usage for the configuration part. Run the simulation part by using EC2 Spot Instances. Create an S3 Lifecycle policy to transition objects that are older than 30 days to S3 Glacier.
purchase Compute Saving Plans to cover usage for configuration part. Run simulation part by using EC2 Spot instance

Q577 A company is hosting an image-processing service on AWS in a VPC. The VPC extends across two Availability Zones. Each Availability Zone contains one public subnet and one private subnet. The service runs on Amazon EC2 instances in the private subnets. An Application Load Balancer in the public subnets is in front of the service. The service needs to communicate with the internet and does so through two NAT gateways. The service uses Amazon S3 for image storage. The EC2 instances retrieve approximately 1 TB of data from an S3 bucket each day. The company has promoted the service as highly secure. A solutions architect must reduce cloud expenditures as much as possible without compromising the service's security posture or increasing the time spent on ongoing operations. Which solution will meet these requirements?
C. Set up an S3 gateway VPC endpoint in the VPC. Attach an endpoint policy to the endpoint to allow the required actions on the S3 bucket.
set up S3 gateway VPC endpoint in VPC

Q578 A company is running a large containerized workload in the AWS Cloud. The workload consists of approximately 100 different services. The company uses Amazon Elastic Container Service (Amazon ECS) to orchestrate the workload. Recently, the company's development team started using AWS Fargate instead of Amazon EC2 instances in the ECS cluster. In the past, the workload has come close to running the maximum number of EC2 instances that are available in the account. The company is worried that the workload could reach the maximum number of ECS tasks that are allowed. A solutions architect must implement a solution that will notify the development team when Fargate reaches 80% of the maximum number of tasks. What should the solutions architect do to meet this requirement?
B. Use Amazon CloudWatch to monitor service quotas that are published under the AWS/Usage metric namespace. Set an alarm for when the math expression metric/SERVICE_QUOTA(metric)*100 is greater than 80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS)
Use CloudWatch to monitor service quotas

Q579 A company has a large number of AWS accounts in an organization in AWS Organizations. A different business group owns each account. All the AWS accounts are bound by legal compliance requirements that restrict all operations outside the eu-west-2 Region. The company's security team has mandated the use of AWS Systems Manager Session Manager across all AWS accounts. Which solution should a solutions architect recommend to meet these requirements?
C. Create an SCP that denies access to all requests that do not target eu-west-2. Use the NotAction element to exempt global services from the restriction. In AWS Organizations, apply the SCP to the root of the organization. In each AWS account, create an IAM permissions boundary that allows access to the IAM role that is associated with the Session Manager instance profile
create IAM permissions boundary

Q580 A company uses AWS Organizations. The company has an organization that has a central management account. The company plans to provision multiple AWS accounts for different departments. All department accounts must be a member of the company's organization. Compliance requirements state that each account must have only one VPC. Additionally, each VPC must have an identical network security configuration that includes fully configured subnets, gateways, network ACLs, and security groups. The company wants this security setup to be automatically applied when a new department account is created. The company wants to use the central management account for all security operations, but the central management account should not have the security setup. Which approach meets these requirements with the LEAST amount of setup?
A. Create an OU within the company's organization. Add department accounts to the OU. From the central management account, create an AWS CloudFormation template that includes the VPC and the network security configurations. Create a CloudFormation stack set by using this template file with automated deployment enabled. Apply the CloudFormation stack set to the OU.
Create an OU within the company’s organization

Q581 A company owns a chain of travel agencies and is running an application in the AWS Cloud. Company employees use the application to search for information about travel destinations. Destination content is updated four times each year. Two fixed Amazon EC2 instances serve the application. The company uses an Amazon Route 53 public hosted zone with a multivalue record of travel.example.com that returns the Elastic IP addresses for the EC2 instances. The application uses Amazon DynamoDB as its primary data store. The company uses a self-hosted Redis instance as a caching solution. During content updates, the load on the EC2 instances and the caching solution increases drastically. This increased load has led to downtime on several occasions. A solutions architect must update the application so that the application is highly available and can handle the load that is generated by the content updates. Which solution will meet these requirements?
A. Set up DynamoDB Accelerator (DAX) as in-memory cache. Update the application to use DAX. Create an Auto Scaling group for the EC2 instances. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias. Configure scheduled scaling for the EC2 instances before the content updates.
set up DynamoDB Accelerator(DAX) as in-memory cache. Create an ALB

Q582 A medical company is building a data lake on Amazon S3. The data must be encrypted in transit and at rest. The data must remain protected even if S3 bucket is inadvertently made public. Which combination of steps will meet these requirements? (Choose three.)
A. Ensure that each S3 bucket has a bucket policy that includes a Deny statement if the aws: SecureTransport condition is not present.
B. Create a CMK in AWS Key Management Service (AWS KMS). Turn on server-side encryption (SSE) on the S3 buckets, select SSE-KMS for the encryption type, and use the CMK as the key.
C. Ensure that each S3 bucket has a bucket policy that includes a Deny statement for PutObject actions if the request does not include an "s3:x-amz-server-side-encryption".aws:kms" condition.
aws:SecureTransport condition is not present
Create CMK
Aws:kms condition

Q583 A company is building an electronic document management system in which users upload their documents. The application stack is entirely serverless and runs on AWS in the eu-central-1 Region. The system includes a web application that uses an Amazon CloudFront distribution for delivery with Amazon S3 as the origin. The web application communicates with Amazon API Gateway Regional endpoints. The API Gateway APIs call AWS Lambda functions that store metadata in an Amazon Aurora Serverless database and put the documents into an S3 bucket. The company is growing steadily and has completed a proof of concept with its largest customer. The company must improve latency outside of Europe. Which combination of actions will meet these requirements? (Choose two.)
A. Enable S3 Transfer Acceleration on the S3 bucket. Ensure that the web application uses the Transfer Acceleration signed URLs.
C. Change the API Gateway Regional endpoints to edge-optimized endpoints.
enable S3 Transfer Acceleration on S3
change API Gateway Regional endpoints

Q584 A large mobile gaming company has successfully migrated all of its on-premises infrastructure to the AWS Cloud. A solutions architect is reviewing the environment to ensure that it was built according to the design and that it is running in alignment with the Well-Architected Framework While reviewing previous monthly costs in Cost Explorer, the solutions architect notices that the creation and subsequent termination of several large instance types account for a high proportion of the costs. The solutions architect finds out that the company's developers are launching new Amazon EC2 instances as part of their testing and that the developers are not using the appropriate instance types. The solutions architect must implement a control mechanism to limit the instance types that only the developers can launch. Which solution will meet these requirements?
C. Create a new IAM policy. Specify the instance types that are allowed. Attach the policy to an IAM group that contains the IAM accounts for the developers
Create a new IAM policy

Q585 A company plans to deploy a new private intranet service on Amazon EC2 instances inside a VPC. An AWS Site-to-Site VPN connects the VPC to the company's on-premises network. The new service must communicate with existing on-premises services. The on-premises services are accessible through the use of hostnames that reside in the company.example DNS zone. This DNS zone is wholly hosted on premises and is available only on the company's private network. A solutions architect must ensure that

the new service can resolve hostnames on the company example domain to integrate with existing services. Which solution meets these requirements?
B. Turn on DNS hostnames for the VPC. Configure a new outbound endpoint with Amazon Route 53 Resolver. Create a Resolver rule to forward requests for company.example to the on-premises name servers.
configure a new outbound endpoint

Q586 A solutions architect must implement a multi-Region architecture for an Amazon RDS for PostgreSQL database that supports a web application. The database launches from an AWS CloudFormation template that includes AWS services and features that are present in both the primary and secondary Regions. The database is configured for automated backups, and it has an RTO of 15 minutes and an RPO of 2 hours. The web application is configured to use an Amazon Route 53 record to route traffic to the database. Which combination of steps will result in a highly available architecture that meets all the requirements? (Choose two.)
A. Create a cross-Region read replica of the database in the secondary Region. Configure an AWS Lambda function in the secondary Region to promote the read replica during failover events.
D. Create a failover routing policy in Route 53 for the database DNS record. Set the primary and secondary endpoints to the endpoints in each Region
create a cross-region read replica of db in secondary region
create a failover routing policy in Route 53

Q587 A financial services company in North America plans to release a new online web application to its customers on AWS. The company will launch the application in the us-east-1 Region on Amazon EC2 instances. The application must be highly available and must dynamically scale to meet user traffic. The company also wants to implement a disaster recovery environment for the application in the us-west-1 Region by using active-passive failover. Which solution will meet these requirements?
C. Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC. Place the Auto Scaling group behind the ALB. Set up the same configuration in the us-west-1 VPC. Create an Amazon Route 53 hosted zone. Create separate records for each ALB. Enable health checks and configure a failover routing policy for each record.
enable health checks and configure a failover routing policy for each record

Q588 A company's solutions architect is analyzing costs of a multi-application environment. The environment is deployed across multiple Availability Zones in a single AWS Region. After a recent acquisition, the company manages two organizations in AWS Organizations. The company has created multiple service provider applications as AWS PrivateLink-powered VPC endpoint services in one organization. The company has created multiple service consumer applications in the other organization. Data transfer charges are much higher than the company expected, and the solutions architect needs to reduce the costs. The solutions architect must recommend guidelines for developers to follow when they deploy services. These guidelines must minimize data transfer charges for the whole environment. Which guidelines meet these requirements? (Choose two.)
C. Turn off cross-zone load balancing for the Network Load Balancer in all service provider application deployments.

D. Ensure that service consumers compute resources using the Availability Zone-specific endpoint service by using the endpoint's local DNS name.
turn off cross-zone load balancing
ensure service consumer compute resource

Q589 A company has an environment that has a single AWS account. A solutions architect is reviewing the environment to recommend what the company could improve specifically in terms of access to the AWS Management Console. The company's IT support workers currently access the console for administrative tasks, authenticating with named IAM users that have been mapped to their job role. The IT support workers no longer want to maintain both their Active Directory and IAM user accounts. They want to be able to access the console by using their existing Active Directory credentials. The solutions architect is using AWS Single Sign-On (AWS SSO) to implement this functionality. Which solution will meet these requirements MOST cost-effectively?
D. Create an organization in AWS Organizations. Turn on all features for the organization. Create and configure an AD Connector to connect to the company's on-premises Active Directory. Configure AWS SSO and select the AD Connector as the identity source. Create permission sets and map them to the existing groups within the company's Active Directory.
Turn on all features.create and configure AD Connector.

Q590 A company has multiple AWS accounts. The company recently had a security audit that revealed many unencrypted Amazon Elastic Block Store (Amazon EBS) volumes attached to Amazon EC2 instances. A solutions architect must encrypt the unencrypted volumes and ensure that unencrypted volumes will be detected automatically in the future. Additionally, the company wants a solution that can centrally manage multiple AWS accounts with a focus on compliance and security. Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)
A. Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the strongly recommended guardrails. Join all accounts to the organization. Categorize the AWS accounts into OUs.
C. Create a snapshot of each unencrypted volume. Create a new encrypted volume from the unencrypted snapshot. Detach the existing volume, and replace it with the encrypted volume.
turn on strongly recommended guardrails
create a snapshot of each unencrypted volume

Q591 A company in the United States (US) has acquired a company in Europe. Both companies use the AWS Cloud. The US company has built a new application with a microservices architecture. The US company is hosting the application across five VPCs in the us-east-2 Region. The application must be able to access resources in one VPC in the eu-west-1 Region. However, the application must not be able to access any other VPCs. The VPCs in both Regions have no overlapping CIDR ranges. All Accounts are already consolidated in one organization in AWS Organizations. Which solution will meet these requirements MOST cost-effectively?
D. Create one VPC peering connection for each VPC in us-east-2 to the VPC in eu-west-1. Create the necessary route entries in each VPC so that the traffic is routed through the VPC peering connection.
create one VPC peering connection

Q592 A United Kingdom (UK) company recently completed a successful proof of concept in Amazon WorkSpaces. The company also has a large office in the United States (US). Staff members from each office regularly travel between the two locations and need access to a corporate WorkSpace without any reconfiguration of their WorkSpaces client. The company has purchased a domain by using Amazon Route 53 for the connection alias. The company will use a Windows profile and document management solution. A solutions architect needs to design the full solution. The solution must use a configuration of WorkSpaces in two AWS Regions and must provide Regional resiliency. Which solution will meet these requirements?

C. Create a connection alias in a UK Region and a US Region. Associate the connection aliases with a directory in each Region. Configure the DNS service for the domain in the connection alias. Configure a geolocation routing policy. Distribute the connection string to the WorkSpaces users.

Associated connection alias with a directory in each region

Q593 A company is running a custom database in the AWS Cloud. The database uses Amazon EC2 for compute and uses Amazon Elastic Block Store (Amazon EBS) for storage. The database runs on the latest generation of EC2 instances and uses a General Purpose SSD (gp2) EBS volume for data. The current data volume has the following characteristics:The volume is 512 GB in size. The volume never goes above 256 GB utilization. The volume consistently uses around 1,500 IOPS. A solutions architect needs to conduct an analysis of the current database storage layer and make a recommendation about ways to reduce cost. Which solution will provide the MOST cost savings without impacting the performance of the database?

D. Convert the data volume to the General Purpose SSD (gp3) type. Resize the volume to 256 GB. Set the volume IOPS to 1,500.

Convert to General Purpose SSD(gp3)

Q594 A retail company is hosting an ecommerce website on AWS across multiple AWS Regions. The company wants the website to be operational at all times for online purchases. The website stores data in an Amazon RDS for MySQL DB instance. Which solution will provide the HIGHEST availability for the database?

D. Configure read replicas on Amazon RDS. In the case of disruption, promote a cross-Region and read replica to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source.

configure read replicas on RDS

Q595 A company wants to use Amazon S3 to back up its on-premises file storage solution. The company's on-premises file storage solution supports NFS, and the company wants its new solution to support NFS. The company wants to archive the backup files after 5 days. If the company needs archived files for disaster recovery, the company is willing to wait a few days for the retrieval of those files. Which solution meets these requirements MOST cost-effectively?

E. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.

Deploy AWS Storage Gateway file gateway. Create S3 Lifecycle rule to move files t S3 Glacier Deep Archive after 5 days

Q596 A video processing company wants to build a machine learning (ML) model by using 600 TB of compressed data that is stored as thousands of files in the company's on-premises network attached storage system. The company does not have the necessary compute resources on premises for ML experiments and wants to use AWS. The company needs to complete the data transfer to AWS within 3 weeks. The data transfer will be a one-time transfer. The data must be encrypted in transit. The measured upload speed of the company's internet connection is 100 Mbps, and multiple departments share the connection. Which solution will meet these requirements MOST cost-effectively?

A. Order several AWS Snowball Edge Storage Optimized devices by using the AWS Management Console. Configure the devices with a destination S3 bucket. Copy the data to the devices. Ship the devices back to AWS. LAS

order several AWS Snowball Edge Storage Optimized devices

Q597 A company has several AWS accounts. A development team is building an automation framework for cloud governance and remediation processes. The automation framework uses AWS Lambda functions in a centralized account. A solutions architect must implement a least privilege permissions policy that allows the Lambda functions to run in each of the company's AWS accounts. Which combination of steps will meet these requirements? (Choose two.)

A. In the centralized account, create an IAM role that has the Lambda service as a trusted entity. Add an inline policy to assume the roles of the other AWS accounts.

B. In the other AWS accounts, create an IAM role that has minimal permissions. Add the centralized account's Lambda IAM role as a trusted entity.

In centralized account, create an IAM role that has Lambda service as a trusted entity

add centralized account’s Lambda IAM role as a trusted entity

Q598 A hedge fund company is developing a new web application to handle trades. Traders around the world will use the application. The application will handle hundreds of thousands of transactions, especially during overlapping work hours between Europe and the United States. According to the company's disaster recovery plan, the data that is generated must be replicated to a second AWS Region. Each transaction item will be less than 100 KB in size. The company wants to simplify the CICD pipeline as much as possible. Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

A. Deploy the application in multiple Regions. Use Amazon Route 53 latency-based routing to route users to the nearest deployment.

D. Provision an Amazon DynamoDB global table. Use DynamoDB Accelerator (DAX) to improve response time.

Deploy app in multiple regions

Provision DynamoDB global table

Q599 A company is migrating some of its applications to AWS. The company wants to migrate and modernize the applications quickly after it finalizes networking and security strategies. The company has set up an AWS Direct Connection connection in a central network account. The company expects to have hundreds of AWS accounts and VPCs in the near future. The corporate network must be able to access the resources on AWS seamlessly and also must be able to communicate with all the VPCs. The company also wants to route its cloud resources to the internet through its on-premises data center. Which combination of steps will meet these requirements? (Choose three.)

B. Create a Direct Connect gateway and a transit gateway in the central network account. Attach the transit gateway to the Direct Connect gateway by using a transit VIF.
D. Share the transit gateway with other accounts. Attach VPCs to the transit gateway.
F. Provision only private subnets. Open the necessary route on the transit gateway and customer gateway to allow outbound internet traffic from AWS to flow through NAT services that run in the data center.
Create Direct Connect gateway and transit gateway
Share transit gateway
Provision only private subnet**s**

Q600 A company is building a software-as-a-service (Saas) solution on AWS. The company has deployed an Amazon API Gateway REST API with AWS Lambda integration in multiple AWS Regions and in the same production account. The company offers tiered pricing that gives customers the ability to pay for the capacity to make a certain number of API calls per second. The premium tier offers up to 3,000 calls per second, and customers are identified by a unique API key. Several premium tier customers in various Regions report that they receive error responses of 429 Too Many Requests from multiple API methods during peak usage hours. Logs indicate that the Lambda function is never invoked. What could be the cause of the error messages for these customers?
C. The company reached its API Gateway account limit for calls per second.
company reached its API Gateway account limit for call per second

Q601 A company has registered 10 new domain names. The company uses the domains for online marketing. The company needs a solution that will redirect online visitors to a specific URL for each domain. all domains and target URLS are defined in a JSON document. All DNS records are managed by Amazon Route 53. A solutions architect must implement a redirect service that accepts HTTP and HTTPS requests. Which combination of steps should the solutions architect take to meet these requirements with the LEAST amount of operational effort? (Choose three.)
C. Create an AWS Lambda function that uses the JSON document in combination with the event message to look up and respond with a redirect URL.
E. Create an Amazon CloudFront distribution. Deploy a Lambda@Edge function.
F. Create an SSL certificate by using AWS Certificate Manager (ACM). Include the domains as Subject Alternative Names.
Create Lambda function
Create CLoudFront
Create SSL

Q602 A company asks a solution architect to optimize the cost of a solution. The solution handles requests from multiple customers. The solution includes a multi-tier architecture that uses Amazon API Gateway, AWS Lambda, AWS Fargate, Amazon Simple Queue Service (Amazon SQS), and Amazon EC2. In the current setup, requests go through API Gateway to Lambda and either start a container in Fargate or push a message to an SQS queue. An EC2 Fleet provides EC2 instances that serve as workers for the SQS queue. The EC2 Fleet scales based on the number of items in the SQS queue. Which combination of steps should the solutions architect recommend to reduce cost the MOST? (Choose three.)

B. Examine the last 6 months of compute utilization across the services. Use this information to determine the needed compute for the solution. Commit to a Savings Plan for this amount.
D. Remove the SQS queue from the solution and from the solution infrastructure.
E. Change the solution so that it runs as a container instead of on EC2 instances. Configure Lambda to start up the solution in Fargate by using environment variables to give the solution the message.
Examine last 6 months
Remove SQS
Change solution

Q603 A company is developing a messaging application that is based on a microservices architecture. A separate team develops each microservice by using Amazon Elastic Container Service (Amazon ECS). The teams deploy the microservices multiple times daily by using AWS CloudFormation and AWS CodePipeline. The application recently grew in size and complexity. Each service operates correctly on its own during development, but each service produces error messages when it has to interact with other services in production. A solutions architect must improve the application's availability. Which solution will meet these requirements with the LEAST amount of operational overhead?
B. Add an AWS:CodeDeployBlueGreen Transform section and Hook section to the template to enable blue/green deployments by using AWS CodeDeploy in CloudFormation. Configure the template to perform ECS blue/green deployments in production
Add AWS:CodeDeployBlueGreen

Q604 A company is migrating mobile banking applications to run on Amazon EC2 instances in a VPC. Backend service applications run in an on- premises data center. The data center has an AWS Direct Connect connection into AWS. The applications that run in the VPC need to resolve DNS requests to an on-premises Active Directory domain that runs in the data center. Which solution will meet these requirements with the LEAST administrative overhead?
C. Create DNS endpoints by using Amazon Route 53 Resolver Add conditional forwarding rules to resolve DNS namespaces between the on- premises data center and the VPC
Crate DNS endpoint

Q605 A company has a new security policy. The policy requires the company to log any event that retrieves data from Amazon S3 buckets. The company must save these audit logs in a dedicated S3 bucket. The company created the audit logs S3 bucket in an AWS account that is designated for centralized logging. The S3 bucket has a bucket policy that allows write-only cross-account access. A solutions architect must ensure that all S3 object-level access is being logged for current S3 buckets and future S3 buckets. Which solution will meet these requirements?
D. Enable AWS CloudTrail, and use the audit logs S3 bucket to store logs. Enable data event logging for S3 event sources, current S3 buckets, and future S3 buckets.
enable AWS CloudTrail

Q606 A retail company is operating its ecommerce application on AWS. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The company uses an Amazon RDS DB

instance as the database backend. Amazon CloudFront is configured with one origin that points to the ALB. Static content is cached. Amazon Route 53 is used to host all public zones. After an update of the application, the ALB occasionally returns a 502 status code (Bad Gateway) error. The root cause is malformed HTTP headers that are returned to the ALB. The webpage returns successfully when a solutions architect reloads the webpage immediately after the error occurs. While the company is working on the problem, the solutions architect needs to provide a custom error page instead of the standard ALB error page to visitors. Which combination of steps will meet this requirement with the LEAST amount of operational overhead? (Choose two.)

A. Create an Amazon S3 bucket. Configure the S3 bucket to host a static webpage. Upload the custom error pages to Amazon S3.

E. Add a custom error response by configuring a CloudFront custom error page. Modify DNS records to point to a publicly accessible web page

Create S3 bucket

Add custom error response

Q607 A financial services company sells its software-as-a-service (Saas) platform for application compliance to large global banks. The Saas platform runs on AWS and uses multiple AWS accounts that are managed in an organization in AWS Organizations. The SaaS platform uses many AWS resources globally. For regulatory compliance, all API calls to AWS resources must be audited, tracked for changes, and stored in a durable and secure data store. Which solution will meet these requirements with the LEAST operational overhead?

C. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket with versioning turned on to store the logs. Deploy the trail for all accounts in the organization. Enable MFA delete and encryption on the S3 bucket.

Create S3 bucket with versioning

Q608 A retail company runs a business-critical web service on an Amazon Elastic Container Service (Amazon ECS) cluster that runs on Amazon EC2 instances. The web service receives POST requests from end users and writes data to a MySQL database that runs on a separate EC2 instance. The company needs to ensure that data loss does not occur. The current code deployment process includes manual updates of the ECS service. During a recent deployment, end users encountered intermittent 502 Bad Gateway errors in response to valid web requests. The company wants to implement a reliable solution to prevent this issue from recurring. The company also wants to automate code deployments. The solution must be highly available and must optimize cost-effectiveness. Which combination of steps will meet these requirements? (Choose three.)

A. Run the web service on an ECS cluster that has a Fargate launch type. Use AWS CodePipeline and AWS CodeDeploy to perform a blue/green deployment with validation testing to update the ECS service.

C. Configure an Amazon Simple Queue Service (Amazon SQS) queue as an event source to receive the POST requests from the web service. Configure an AWS Lambda function to poll the queue. Write the data to the database.

F. Migrate the MySQL database to run on an Amazon RDS for MySQL Multi-AZ DB instance that uses General Purpose SSD (gp3) storage

Use CodePipeline and CodeDeploy to perform blue/green deployment

configure AWS Lambda function to poll the queue

use General Purpose SSD(gp3) storage

Q609 A company is using an Amazon EMR cluster to run its big data jobs. The cluster's jobs are invoked by AWS Step Functions Express Workflows that consume various Amazon Simple Queue Service (Amazon SQS) queues. The workload of this solution is variable and unpredictable. Amazon CloudWatch metrics show that the cluster's peak utilization is only 25% at times and that the cluster sits idle the rest of the time. A solutions architect must optimize the costs of the cluster without negatively impacting the time it takes to run the various jobs. What is the MOST cost-effective solution that meets these requirements?
D. Modify the EMR. cluster to use capacity-optimized Spot Instances and a diversified task fleet. Define target capacity for each node type with a mix of On-Demand Instances and Spot Instances.
modify EMR cluster to use capacity-optimized Spot instance

Q610 A company needs to establish a connection from its on-premises data center to AWS. The company needs to connect all of its VPCs that are located in different AWS Regions with transitive routing capabilities between VPC networks. The company also must reduce network outbound traffic costs. increase bandwidth throughput, and provide a consistent network experience for end users. Which solution will meet these requirements?
B. Create an AWS Direct Connect connection between the on-premises data center and AWS. Provision a transit VIF, and connect it to a Direct Connect gateway. Connect the Direct Connect gateway to all the other VPCs by using a transit gateway in each Region.
Provision a transit VIF

Q611 A company is running an application in the AWS Cloud. The application consists of microservices that run on a fleet of Amazon EC2 instances in multiple Availability Zones behind an Application Load Balancer. The company recently added a new REST API that was implemented in Amazon API Gateway. Some of the older microservices that run on EC2 instances need to call this new API. The company does not want the API to be accessible from the public internet and does not want proprietary data to traverse the public internet. What should a solutions architect do to meet these requirements?
B. Create an interface VPC endpoint for API Gateway, and set an endpoint policy to only allow access to the specific API. Add a resource policy to API Gateway to only allow access from the VPC endpoint. Change the API Gateway endpoint type to private.
create an interface VPC endpoint for API Gateway

Q612 A mobile gaming company is expanding into the global market. The company's game servers run in the us-east-1 Region. The game's client application uses UDP to communicate with the game servers and needs to be able to connect to a set of static IP addresses. The company wants its game to be accessible on multiple continents. The company also wants the game to maintain its network performance and global availability. Which solution meets these requirements?
C. Provision game servers in each AWS Region. Provision a Network Load Balancer (NLB) in front of the game servers. Create an accelerator in AWS Global Accelerator, and configure endpoint groups in each Region. Associate the NLBs with the corresponding Regional endpoint groups. Point the game client's application to the Global Accelerator endpoints.
Create accelerator in AWS Global Accelerator

Q613 A company is using an on-premises Active Directory service for user authentication. The company wants to use the same authentication service to sign in to the company's AWS accounts, which are using AWS Organizations. AWS Site-to-Site VPN connectivity already exists between the on- premises environment and all the company's AWS accounts. The company's security policy requires conditional access to the accounts based on user groups and roles. User identities must be managed in a single location. Which solution will meet these requirements?

A. Configure AWS Single Sign-On (AWS SSO) to connect to Active Directory by using SAML 2.0. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol. Grant access to the AWS accounts by using attribute-based access controls (ABACs).

Configure AWS SSo to connect to AD

Q614 A company is deploying a third-party firewall appliance solution from AWS Marketplace to monitor and protect traffic that leaves the company's AWS environments. The company wants to deploy this appliance into a shared services VPC and route all outbound internet-bound traffic through the appliances. A solutions architect needs to recommend a deployment method that prioritizes reliability and minimizes failover time between firewall appliances within a single AWS Region. The company has set up routing from the shared services VPC to other VPCs. Which steps should the solutions architect recommend to meet these requirements? (Choose three.)

A. Deploy two firewall appliances into the shared services VPC, each in a separate Availability Zone.

C. Create a new Gateway Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Gateway Load Balancer. Add each of the firewall appliance instances to the target group.

F. Create a VPC Gateway Load Balancer endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs

Each in separate AZ
Create new Gateway LB
Create VPC Gateway LB endpoint

Q615 A company has a legacy monolithic application that is critical to the company's business. The company hosts the application on an Amazon EC2 instance that runs Amazon Linux 2. The company's application team receives a directive from the legal department to back up the data from the instance's encrypted Amazon Elastic Block Store (Amazon EBS) volume to an Amazon S3 bucket. The application team does not have the administrative SSH key pair for the instance. The application must continue to serve the users. Which solution will meet these requirements?

A. Attach a role to the instance with permission to write to Amazon S3. Use the AWS Systems Manager Session Manager option to gain access to the instance and run commands to copy data into Amazon S3

Systems Manager Session Manager

Q616 A greeting card company recently advertised that customers could send cards to their favorite celebrities through the company's platform. Since the advertisement was published, the platform has

received constant traffic from 10,000 unique users each second. The platform runs on m5.xlarge Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Auto Scaling group and use a custom AMI that is based on Amazon
Linux. The platform uses a highly available Amazon Aurora MySQL DB cluster that uses primary and reader endpoints. The platform also uses an Amazon ElastiCache for Redis cluster that uses its cluster endpoint. The platform generates a new process for each customer and holds open database connections to MySQL for the duration of each customer's session. However, resource usage for the platform is low. Many customers are reporting errors when they connect to the platform. Logs show that connections to the Aurora database are failing. Amazon CloudWatch metrics show that the CPU load is low across the platform and that connections to the platform are successful through the ALB. Which solution will remediate the errors MOST cost- effectively ?
B. Use Amazon RDS Proxy. Reconfigure the database connections to use the proxy.
Use RDS proxy

Q617 A company has an application that runs on Amazon EC2 instances in an Amazon EC2 Auto Scaling group. The company uses AWS CodePipeline to deploy the application. The instances that run in the Auto Scaling group are constantly changing because of scaling events. When the company deploys new application code versions, the company installs the AWS CodeDeploy agent on any new target EC2 instances and associates the instances with the CodeDeploy deployment group. The application is set to go live within the next 24 hours. What should a solutions architect recommend to automate the application deployment process with the LEAST amount of operational overhead?
D. Create a new AMI that has the CodeDeploy agent installed. Configure the Auto Scaling group's launch template to use the new AMI. Associate the CodeDeploy deployment group with the Auto Scaling group instead of the EC2 instances.
Create AMI that has CodeDeploy agent install.

Q618 A video streaming company recently launched a mobile app for video sharing. The app uploads various files to an Amazon S3 bucket in the us- east-1 Region. The files range in size from 1 GB to 10 GB. Users who access the app from Australia have experienced uploads that take long periods of time. Sometimes the files fail to completely upload for these users. A solutions architect must improve the app's performance for these uploads. Which solutions will meet these requirements? (Choose two.)
A. Enable S3 Transfer Acceleration on the S3 bucket. Configure the app to use the Transfer Acceleration endpoint for uploads.
D. Configure the app to break the video files into chunks. Use a multipart upload to transfer files to Amazon S3.
enable S3 transfer Acceleration on S3 bucket
configure app to break video files into chunks

Q619 A company is migratıng an application to the AWS Cloud. The applıcation runs in an on-premises data center and writes thousands of images into a mounted NFS file system each night. After the company migrates the application, the company will host the application on an Amazon EC2 instance with a mounted Amazon Elastic File System (Amazon EFS) file system. The company has established an AWS Direct Connect connection to AWS. Before the migration cutover, a solutions architect must build a

process that will replicate the newly created on-premises images to the EFS file system. What is the MOST operationally efficient way to replicate the images?
D. Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system. Send data over the Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Configure a DataSync scheduled task to send the images to the EFS file system every 24 hours.
Send data over Direct Connect connection to PrivateLink

Q620 A company has more than 10,000 sensors that send data to an on-premises Apache Kafka server by using the Message Queuing Telemetry Transport (MQTT) protocol. The on-premises Kafka server transforms the data and then stores the results as objects in an Amazon S3 bucket. Recently. the Kafka server crashed. The company lost sensor data while the server was being restored. A solutions architect must create a new design on AWS that is highly available and scalable to prevent a similar occurrence. Which solution will meet these requirements?
B. Migrate the on-premises Kafka server to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Create a Network Load Balancer (NLB) that points to the Amazon MSK broker. Enable NLB health checks. Route the sensors to send the data to the NLB. D. In Account B, set the permissions of User_DataProcessor to the following? { “Effect": "Allow", "Action": ["s3: Getobject", "s3:ListBucket"], "Resource": "arn: aws : s3: : :AccountABucketName/*" }
migrate on-premises Kafka server to Amazon Managed Streaming

Q621 A retail company needs to provide a series of data files to another company, which is its business partner. These files are saved in an Amazon S3 bucket under Account A, which belongs to the retail company. The business partner company wants one of its IAM users, User_DataProcessor, to access the files from its own AWS account (Account B). Which combination of steps must the companies take so that User_DataProcessor can access the S3 bucket successfully? (Choose two.)
C. In Account A, set the S3 bucket policy to the following:

```
{
    "Effect": "Allow",
    "Principal": (
        "AWS": "arn: aws:iam: :AccountB:user/User DataProcessor"
    },
    "Action": [
        "s3: Getobject",
        "s3:ListBucket"
    ],
    "Resource": [
        arn: aws : s3: : :AccountABucketName/*"
    ]
}
```

D. In Account B, set the permissions of User_DataProcessor to the following

```
{
    “Effect": "Allow",
    "Action": [
        "s3: Getobject",
        "s3:ListBucket"
```

```
        ],
        "Resource": "arn: aws : s3: : :AccountABucketName/*"
}
```

Q622 A company has an organization that has many AWS accounts in AWS Organizations. A solutions architect must improve how the company manages common security group rules for the AWS accounts in the organization. The company has a common set of IP CIDR ranges in an allow list in each AWS account to allow access to and from the company's on-premises network. Developers within each account are responsible for adding new IP CIDR ranges to their security groups. The security team has its own AWS account. Currently, the security team notifies the owners of the other AWS accounts when changes are made to the allow list. The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts. Which solution meets these requirements with the LEAST amount of operational overhead?

C. Create a new customer-managed prefix list in the security team's AWS account. Populate the customer-managed prefix list with all internal CIDR ranges. Share the customer-managed prefix list with the organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups.

create new customer-managed prefix list in security team's AWS account

Q623 A company has an application. Once a month, the application creates a compressed file that contains every object within an Amazon S3 bucket. The total size of the objects before compression is 1 TB. The application runs by using a scheduled cron job on an Amazon EC2 instance that has a 5 TB Amazon Elastic Block Store (Amazon EBS) volume attached. The application downloads all the files from the source S3 bucket to the EBS volume, compresses the file, and uploads the file to a target S3 bucket. Every invocation of the application takes 2 hours from start to finish. Which combination of actions should a solutions architect take to OPTIMIZE costs for this application? (Choose two.)

B. Configure the application to download the source files by using streams. Direct the streams into a compression library. Direct the output of the compression library into a target object in Amazon S3

D. Configure the application to run as a container in AWS Fargate. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the task to run once each month.

Download source files by using streams

Run as container in Fargate

Q624 A company is running several large workloads on Amazon EC2 instances. Each EC2 instance has multiple Amazon Elastic Block Store (Amazon EBS) volumes attached to it. Once each day, an AWS Lambda function invokes the creation of EBS volume snapshots. These snapshots accumulate until an administrator manually purges them. The company must maintain backups for a minimum of 30 days. A solutions architect needs to reduce the costs of this process. Which solution meets these requirements MOST cost-effectively?

D. Migrate the backup functionality to Amazon Data Lifecycle Manager (Amazon DLM). Create a lifecycle policy for the daily backup of the EBS volumes. Set the retention period for the EBS snapshots to 30 days.

migrate backup functionality to Amazon Data Lifecycle Manager(DLM)

Q625 A company runs a serverless application in a single AWS Region. The application accesses external URLs and extracts metadata from those sites. The company uses an Amazon Simple Notification Service (Amazon SNS) topic to publish URLs to an Amazon Simple Queue Service (Amazon SQS) queue. An AWS Lambda function uses the queue as an event source and processes the URLs from the queue. Results are saved to an Amazon S3 bucket. The company wants to process each URL in other Regions to compare possible differences in site localization. URLs must be published from the existing Region. Results must be written to the existing S3 bucket in the current Region. Which combination of changes will produce multi-Region deployment that meets these requirements? (Choose two.)
A. Deploy the SOS queue with the Lambda function to other Regions
C. Subscribe the SQS queue in each Region to the SNS topic.
deploy SQS queue with Lambda function to other regions
subscribe SQS queue in each region to SNS topic

Q626 A company is deploying a distributed in-memory database on a fleet of Amazon EC2 instances. The fleet consists of a primary node and eight worker nodes. The primary node is responsible for monitoring cluster health, accepting user requests, distributing user requests to worker nodes, and sending an aggregate response back to a client Worker nodes communicate with each other to replicate data partitions. The company requires the lowest possible networking latency to achieve maximum performance. Which solution will meet these requirements?
C. Launch memory optimized EC2 instances in a cluster placement group
Launch memory optimized EC2 instances in a cluster placement group

Q627 A company has a multi-tier web application deployed on AWS The web tier consists of an Auto Scaling group of Amazon EC2 Spot Instances and On-Demand Instances behind an Application Load Balancer. The application tier connects to an Amazon Aurora MySQL DB cluster. During times of peak order volume, users report slow application performance. In addition, Amazon RDS Performance Insights indicates that database wait metrics are high. The company has limited operational resources and asks a solutions architect to resolve the current scalability issues while ensuring the least possible ongoing operational maintenance. Which actions should the solutions architect recommend to meet these requirements? (Select TWO)
A. Deploy an Amazon ElastiCache for Redis cluster alongside the database, and modify the application to use the Redis cluster.
C. Enable Aurora Auto Scaling, and modify the application to segregate database read traffic to the Aurora reader endpoint.
deploy Amazon ElastiCache for Redis cluster alongside the db
Enable Aurora Auto Scaling

Q628 A company recently started hosting new application workloads in the AWS Cloud. The company is using Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) file systems, and Amazon RDS DB instances. To meet regulatory and business requirements, the company must make the following changes for data backups:-Backups must be retained based on custom daily, weekly, and monthly requirements. -Backups must be replicated to at least one other AWS Region immediately after capture. -The backup solution must provide a single source of backup status across the AWS environment. -The backup solution must send immediate notifications upon failure of any resource backup. Which

combination of steps will meet these requirements with the LEAST amount of operational overhead? (Select THREE)
A. Create an AWS Backup plan with a backup rule for each of the retention requirements. B. Configure an AWS Backup plan to copy backups to another Region.
D. Add an Amazon Simple Notification Service (Amazon SNS) topic to the backup plan to send a notification for finished jobs that have any status except BACKUP_JOB COMPLETED
Create AWS Backup plan
Configure AWS Backup plan
Add Amazon SNS

Q629 A company uses AWS Organizations to manage its AWS accounts. A solutions architect must design a solution in which only administrator roles are allowed to use IAM actions. However, the solutions architect does not have access to all the AWS accounts throughout the company. Which solution meets these requirements with the LEAST operational overhead?
C. Create an SCP that applies to all the AWS accounts to deny IAM actions for all users except for those with administrator roles. Apply the SCP to the root OU.
create SCP that applies to all AWS accounts to deny IAM action

Q630 A company uses AWS Organizations. The company creates a central VPC in an AWS account that is designated for networking in a single AWS Region. The central VPC has an AWS Site-to-Site VPN connection to the company's on-premises network A solutions architect must create another AWS account that uses the same networking resources that the central VPC uses. Which solution meets these requirements MOST cost-effectively?
D. Use AWS Resource Access Manager to share the subnets in the central VPC with the new AWS account.
use AWS Resource Access Manager to share subnets in central VPC

Q631 A solutions architect is designing a data processing system that will use Amazon EC2 instances. Data that needs to be processed will wait in an Amazon Simple Queue Service (Amazon SQS) queue. At least two data processing instances must run at all times. Which combination of actions will meet these requirements MOST cost-effectively? (Select TWO.)
B. Purchase two Reserved Instances for the target platform and instance type in the target Aws Region.
D. Create an Auto Scaling group that uses Spot Instance requests. Configure the scaling policy to scale with the size of the SQS queue. Set the minimum value to 2.
purchase two reserved instances
create an Auto Scaling group

Q632 A company migrated its stateless, compute-intensive web application to AWS. The application was deployed on a single compute-optimized Amazon EC2 instance. Detailed monitoring in Amazon CloudWatch shows an average of 70% CPU utilization during business hours Unfortunately, random large increases in user traffic quickly drive the CPU to a sustained level of 100% utilization. and the application becomes unresponsive. Which combination of actions is the MOST cost-effective solution to improve application availability and performance? (Select THREE.)

C. Create and configure an Application Load Balancer with an Auto Scaling group use Auto Scaling .
D. Reserve extra Spot Instances of the matching type.
F. Launch instances that have the unlimited burst CPU feature turned on.
Create and configure an ALB
Reserve extra Spot instances
Launch instances that have unlimited burst CPU

Q633 A company wants to use a hybrid cloud architecture between an on-premises data center and AWS. The company already has deployed a multi- account structure in AWS Organizations while following the AWS Well-Architected Framework.Due to strict security requirements, connectivity between the data center and AWS must be encrypted in transit. Only a single entry point into AWS is permitted from the data center. The data center must be able to access all the AWS accounts. Which solution meets these requirements?
A. Connect the AWS accounts with AWS Transit Gateway. Establish an AWS Site-to-Site VPN connection with the data center and attach the connection to the transit gateway. Route traffic from the data center to all AS accounts.
Establish AWS Site-to-SIte VPN connection with data center and attach connection to transit gateway

Q634 A company is offering one of its applications as a multi-tenant software-as-a-service (Saas) solution. The application has a REST API that runs on a set of Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Auto Scaling group Last week, one of the tenants ran a campaign that significantly increased traffic to the REST API. The resource constraints affected the performance of other tenants that were running on the same set ofEC2 instances. The company wants the ability to throttle API calls for each tenant. Which combination of steps should a solutions architect take to meet these requirements? (Select THREE)
A. Create an AWS WAF web ACL. Add a rate-based rule statement to the web ACL Set the action to block
C. Create an Amazon API Gateway API. Assign the AWS WAF web ACL to the API Gateway API.
F. Modify the application's API requests to target the newly created endpoint.
Create WAF web ACL
Assign WAF web ACL to API Gateway API
Modify app API request

Q635 A flood monitoring agency has deployed more than 10,000 water-level monitoring sensors. Sensors send continuous data updates, and each update is less than 1MB in size. The agency has a fleet of on-premises application servers. These servers receive updates from the sensors, convert the raw data into a human readable format, and write the results to an on-premises relational database server. Data analysts then use simple SQL queries to monitor the data. The agency wants to increase overall application availability and reduce the effort that is required to perform maintenance tasks. These maintenance tasks, which include updates and patches to the application servers, cause downtime. While an application server is down. data is lost from sensors because the remains in a server cannot handle the entire workload. The agency wants a solution that optimizes operational overhead and costs. A solutions architect recommends the use of AWS IoT Core to collect the sensor data. What else should the solutions architect recommend to meet these requirements?

B. Send the sensor data to Amazon Kinesis Data Firehose. Use an AWS Lambda function to read the Kinesis Data Firehose data, convert it to Apache Parquet format, and save it to an Amazon S3 bucket Instruct the data analysts to query the data by using Amazon Athena.
Send sensor data to Kinesis Data Firehose. Query data by using Athena

Q636 A company collects user clickstream data from a website. The company plans to use the clickstream data to provide product recommendations in near-real time. The product recommendations require aggregation of item view data and purchase data. A user's clickstream data must be sent from the browser to a single endpoint. Which solution meets these requirements?
A. Use Amazon Kinesis Data Streams to ingest the user clickstream data. Use Amazon Kinesis Data Analytics to query the Kinesis data stream and to invoke AWS Lambda functions to generate real-time recommendations
use Amazon Kinesis Data Streams to ingest user clickstream data

Q637 A company writes application log files to AmazonS3 The log files are encrypted with server-side encryption with AWS KMS managed keys (SSE - KMS). The company uses an S3 bucket policy to control access to the logs. The company's support team requires access to the logs and uses dedicated IAM roles for each team member. The KMS key policy and the s3 bucket policy allow each team member's role to access the logs. Members of the support team change frequently. The company wants to minimize the administrative overhead whenever someone joins the team or leaves the team As a first step the company will update the KMS key policy and the S3 Bucket policy, and remove the existing list of support team member IAM roles. What else must the company do to ensure that the support team members have access to the logs?
B. In the KMS key policy and the S3 bucket policy add Allow statements with a condition that looks at the aws:PrincipaliTag condition key for Key-Team and Value-Support. Create an IAM group for the support team with a tag of Key=Team and Value-Support Add each support team member IAM role to the IAM group
aws:PrincipaliTag condition. Create IAM group for support team

Q638 A solutions architect needs to design a VPC to host critical infrastructure No subnets within the VPC can be connected to the public internet Resources within the VPC must be able to access Amazon S3 buckets within the same AWS Region. The solution also must include an encrypted connection between the VPC and an on-premises network for management of AmazonEC2instances. Which solution meets these requirements?
B. Deploy a MPC that has only private subnets. Provision a gateway VPC endpoint for Amazon S3 Connect the VPC to the on-premises network by using an AWS Site-to-site VPN connection
deploy MPC that has only private subnets.

Q639 A retail company has an on-premises data center in Europe The company also has a multi-Region AWS presence that includes the eu-west-1 and us-east-1 Regions. The company wants to be able to route network traffic from its on-premises infrastructure into VPCs in either of those Regions. The company also needs to support traffic that is routed directly between VPCs in those Regions.No single points of failure can exist on the network. The company already has created two 1 Gbps AWS Direct connect connections from its on-premises data center. Each connection goes into a separate Direct Connect location in Europe for high availability. These two locations are named DX-A and DX-B,

respectively Each Region has a single AWS Transit Gateway that is configured to route all inter-VPC traffic within that Region. Which solution will meet these requirements?
D. Create a transit VIF from the DX-A connection into a Direct Connect gateway Create a transit VIF from the DX-Bconnection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway. Peer the transit gateways with each other to support cross-Region routing.
Create transit VIF. Peer transit gatewa**y**

Q640 A company is using Amazon CloudFront to implement a data distribution solution. The company uses a multi-account AWS environment. The company has a single services account and multiple project accounts. The company uses AWS CloudFormation to deploy the solution infrastructure in one of the project accounts. The company's data must remain private Content access must be authorized, and deployment must be fully automated. Content caching in CloudFront must be part of the solution. Which solutions meet these requirements? (Select TWO).
B. Use a LambdaEdge function that is invoked by a viewer request event to authorize access to content.
E. Use a CloudFormation custom resource to import a CloudFront key pair. Perform URL or cookie signing to authorize content access.
use a Lambda@Edge function that is invoked by a viewer request event
use CLoudFormation custom resource to import a CLoudFront key pair

Q641 A software-as-a-service (Saas) provider exposes APIs through an Application Load Balancer (ALB). The ALB connects to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that is deployed in the us-east-1Region. The exposed APIs contain usage of a few non-standard REST methods: LINK, UNLINK, LOCK and UNLOCK.Users outside the United States are reporting long and inconsistent response times for these APIs. A solutions architect needs to resolve this problem with a solution that minimizes operational overhead. Which solution meets these requirements?
B. Add an Amazon API Gateway edge-optimized API endpoint to expose the APIs Configure the ALB as the target.
Add Amazon API Gateway edge-optimized AIP endpoint

Q642 A company hosts a software-as-a-service (Saas) solution on AWS. The solution consists of an Amazon API Gateway API that serves an HTTPS endpoint and that uses AWS Lambda functions for compute. The Lambda functions store data in an Amazon Aurora Serverless version 1 (v1) database The company used the AWS Serverless Application Model (AWS SAM) to deploy the solution. The solution is constructed for high availability and extends across multiple Availability Zones. The solution has no disaster recovery (DR) plan. The company wants to implement a DR strategy that can recover the solution in another AWS Region. The company has identified an RTO of 5 minutes and an RPO of 1 minute. What should a solutions architect do to meet these requirements?
B. Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Create a runbook for deploying the solution to the new Region by using AWS SAM.
change Aurora Serverless V1 db to standard Aurora MySQL global db. create a run book for deploying

Q643 A company's solutions architect has inherited a microservices application that uses many Amazon DynamoDB tables for its storage.Developers continually add new microservices with new tables. The tables are created dynamically by the framework that the microservices use. A security review shows that all tables are encrypted at rest and are using the default key for encryption. The company now requires the use of AWS Key Management Service (AWS KMS) CMKs on all data. AWS CMKs are already in use for other services. The solutions architect must design a solution to meet the encryption requirements for all existing and future DynamoDB tables. Which solution will meet these requirements with the LEAST amount of ongoing operational overhead?

B. Setup the dynamodb-table-encrypted-kms AwS Config managed rule to detect all tables that are encrypted with the default key. Set the rule to automatically remediate by using an AWS Systems Manager Automation runbook

setup dynamodb-table-encrypted -kms AWS config managed rule

Q644 A finance company wants to store a backup of sensitive documents on Amazon S3. All the documents must be encrypted at rest If the encryption key is compromised, the company must prevent the documents from being decrypted any longer. Which solution will meet these requirements in the LEAST amount of time?

D. Use an AWS Key Management Service (AWS KMS) AWS managed CMK. Rotate the CMK immediately if a compromise event occurs .

Rotate CMK immediately if a compromise event occurs

Q645 A company is concerned about an increase in usage of AWS Key Management Service (AWS KMS).The company wants to optimize the usage and cost of AWS KMS. A solutions architect discovers that the majority of the company's KMS usage is associated with access to a large number of KMS encrypted objects in Amazon S3 buckets. The company has a policy that requires all data to be encrypted at rest with an AWS managed CMK. What should the solutions architect do to minimize cost while ensuring compliance with the company policy?

B. Create a new key pair by using the OpenSSL keygen command. Use elient- side encryption to encrypt and decrypt objects in the S3 buckets.

create a new key pair by using OpenSSL keygen command

Q646 An application uses an event processing service that runs on an Amazon EC2 instance. The service reads events from an Amazon Simple Queue Service (Amazon SQS) queue and then processes data in response. To ensure data integrity, only one instance of the event service can run at any time. The developers who manage the service are concerned that this requirement creates a single point of failure in their application. They want the application to recover automatically if the service crashes or if the instance becomes unresponsive. Which solution will meet these requirements?

A. Create an Auto Scaling group that has a warm pool. Configure a minimum capacity, maximum capacity, and desired capacity of 1, Configure a health check for the service on the Auto Scaling group.

create Auto Scaling group that has a warm pool

Q647 A software company is using three AWS accounts for each of its 10 development teams. The company has developed an AWS CloudFormation standard VPC template that includes three NAT gateways. The template is added to each account for each team. The company is concerned that network

costs will increase each time a new development team is added. A solutions architect must maintain the reliability of the company's solutions and minimize operational complexity. What should the solutions architect do to reduce the network costs while meeting these requirements?
A. Create a single VPC with three NAT gateways in a shared services account. Configure each account VPC with a default route through a transit gateway to the NAT gateway in the shared services account VPC. Remove all NAT gateways from the standard VPC template.
Create vpc with 3 NAT gateways.configure each through transit gateway

Q648 A research center is migrating to the AWS Cloud and has moved its on-premises 1 PB object storage to an Amazon S3 bucket. One hundred scientists are using this object storage to store their work-related documents. Each scientist has a personal folder on the object store. All the scientists are members of a single IAM user group. The research center's compliance officer is worried that scientists will be able to access each other's work. The research center has a strict obligation to report on which scientist accesses which documents. The team that is responsible for these reports has little AWS experience and wants a ready-to-use solution that minimizes operational overhead. Which combination of actions should a solutions architect take to meet these requirements?(choose two)
A. Create an identity policy that grants the user read and write access. Add a condition that specifies that the S3 paths must be prefixed with S(aws:username). Apply the policy on the scientists' IAM user group
C. Enable S3 server access logging. Configure another S3 bucket as the target for log delivery. Use Amazon Athena to query the logs and generate reports.
Create identity policy
Enable s3 server access logging

Q649 A pharmaceutical company is migrating an existing web application from on-premises servers to AWS The application involves personally identifiable information. The company plans to host the application on Amazon EC2 instances behind an Application Load Balancer (ALB). Only internal users access the application. The company has provisioned an AWS Site-to-Site VPN connection from the on-premises environment to AWS. The application requires the traffic to be encrypted at all times while in transit and at rest. Which combination of steps will meet these requirements with the LEAST amount of implementation overhead? (Select TWO)
B. Procure the certificate by using AWS Certificate Manager (ACM) Use the certificate on the ALB to encrypt traffic between the ALB and the on- premises environment.
C. Enable Amazon Elastic Block Store (Amazon EBS) volume encryption.
procure the certificate are by using (ACM)
Enable (EBS) volume encryption

Q650 A company has developed a hybrid solution between its data center and AWS. The company uses Amazon VPC and Amazon EC2 instances that send application logs to Amazon CloudWatch. The EC2 instances read data from multiple relational databases that are hosted on premises. The company wants to monitor which EC2 instances are connected to the databases in near-real time. The company already has a monitoring solution that uses Splunk on premises. A solutions architect needs to determine how to send networking traffic to Splunk. How should the solutions architect meet these requirements?

B. Create an Amazon Kinesis Data Firehose delivery stream with Splunk as the destination. Configure a pre-processing AWS Lambda function with a Kinesis Data Firehose stream processor that extracts individual log events from records sent by CloudWatch Logs subscription filters. Enable VPC flow logs, and send them to CloudWatch. Create aCloudWatch Logs subscription that sends log events to the Kinesis Data Firehose delivery stream
create Kinesis Data Firehose delivery stream with splunk

Q651 A health insurance company stores personally identifiable information (PII) in an Amazon S3 bucket. The company uses server-side encryption with S3 managed encryption keys (SSE-S3) to encrypt the objects.According to a new requirement, all current and future objects in the S3 bucket must be encrypted by keys that the company's security team manages. The S3 bucket does not have versioning enabled. Which solution will meet these requirements?
A. In the S3 Bucket properties, change the default encryption to SSE-S3 with a customer managed key.Use the AWS CLI to re-upload all objects in the S3 bucket. Set an S3 bucket policy to deny unencrypted PutObject requests
change default encryption to SSE-S3

Q652 A company has set up its entire infrastructure on AWS. The company uses AmazonEC2instances to host its ecommerce website and uses Amazon S3 to store static data. Three engineers at the company handle the cloud administration and development through one AWS account. Occasionally an engineer alters an EC2 security group configuration of another engineer and causes noncompliance issues in the environment.A solutions architect must set up a system that tracks changes that the engineers make. The system must send alerts when the engineers make noncompliant changes to the security settings for the EC2 instances. What is the FASTEST way for the solutions architect to meet these requirements?
D. Enable AWS Config on the EC2 security groups to track any noncompliant changes Send the changes as alerts through an Amazon Simple Notification Service (Amazon SNS) topic
enable AWS Config on EC2 security group

Q653 A company is running an application in the AWS Cloud. The application uses AWS Lambda functions and Amazon Elastic Container Service(Amazon ECS)containers that run with AWS Fargate technology compute. The load on the application is irregular. The application experiences long periods of no usage, followed by sudden and significant increases and decreases in traffic. The application is write-heavy and shows that. in an Amazon Aurora MySQL database. The database runs on an Amazon RDS memory optimized DB instance that is not able to handle the load. What is the MOST cost-effective way for the company to handle the sudden and significant changes in traffic?
D. Migrate the database to Aurora Serverless v1.Purchase Compute Savings Plans.
migrate db to Aurora Serverless V1. Purchase Compute Savings plans

Q654 A company has a three-tier image-sharing application it uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application. Which solution meets these requirements'?
D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers.Move the database to an Amazon RDS instance with a Multi-AZ deployment Use Amazon S3 to store and serve users' images.
Use Elastic beanstalk for frontend and backend.use S3 store and serve images

Q655 A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on a separate EC2 instance. The backend application then stores the data in Amazon RDS What should a solutions architect do to decouple the architecture and make it scalable"
D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon
use S3 to serve static front-end application

Q656 A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access. Which of the following would be the LEAST complicated implementation?
C. Use an Amazon CloudFront distribution with an OAIConfigure the distribution with an Amazon S3 origin to provide access to the file through signed URLs Design the application to sot an expiration of 14 days for the URL
design application to set an expiration of 14 days for URL

Q657 A solutions architect is moving the static content from a public website hosted on Amazon EC2 instances to an Amazon S3 bucket. An Amazon CloudFront distribution will be used to deliver the static assets. The security group used by the EC2 instances restricts access to a limited set of IP ranges. Access to the static content should be similarly restricted. Which combination of steps will meet these requirements? (Select TWO.)
A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.
B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution
create an origin access identity(OAI)
create AWS WAF web ACL

Q658 During a review of business applications, a Solutions Architect identifies a critical application with a relational database that was built by a business user and is running on the user's desktop. To reduce the risk of a business interruption, the Solutions Architect wants to migrate the application to a highly available, multi-tiered solution in AWS.What should the Solutions Architect do to accomplish this with the LEAST amount of disruption to the business?
D. Use AWS DMS to migrate the backend database to an Amazon RDS Multi-AZ DB instance. Migrate the application code to AWS Elastic Beanstalk
use AWS DMS to migrate backend db

Q659 A solution architect is performing a security review of a recently migrated workload. The workload is a web application that consists of amazon EC2 instances in an Auto Scaling group behind an Application Load balancer. The solution architect must improve the security posture and minimize the impact of a DDoS attack on resources. Which solution is MOST effective?

A. Configure an AWS WAF ACL with rate-based rules Create an Amazon CloudFront distribution that points to the Application Load Balancer. Enable the EAF ACL on the CloudFront distribution
Configure AWS WAF ACL with rate-based rules.

Q660 A company is designing a web application using AWS that processes insurance quotes Users will request quotes from the application. Quotes must be separated by quote type, must be responded to within 24 hours, and must not be lost. The solution should be simple to set up and maintain. Which solution meets these requirements?
C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic.Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type.Configure each backend application server to work its own SQS queue.
subscribe Amazon SQS queues to SNS topic.

Q661 A company has migrated an on-premises Oracle database to an Amazon RDS (or Oracle Multi-AZ DB instance In the us-east-I Region.A solutions architect is designing a disaster recovery strategy to have the database provisioned In the us-west-2 Region In case the database becomes unavailable in the us-east-1 Region. The design must ensure the database is provisioned in the us-west-2 Region in a maximum of 2 hours, with a data loss window of no more than 3 hours.How can these requirements be met?
A. Edit the DB instance and create a read replica in us-west-2.Promote the read replica to master In us-west-2 in case the disaster recovery environment needs to be activated.
Edit db instance and create a read replica

Q662 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.
deploy a NAT gateway inside public subnet

Q663 A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts. The company has created a central AWS account for streamlining management and audit reviews. An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users. The solution must be secure and optimized. How should a solutions architect meet these requirements?
C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
Configure CloudTrail , Create an IAM role in central account

Q664 A company is building a media-sharing application and decides to use Amazon S3 for storage. When a media file is uploaded the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation. The amount of traffic is variable The solution must be able to scale to handle spikes in load without unnecessary expenses. What should a solutions architect recommend to support this workload?
B. Trigger AWS Step Functions when an object is stored in the S3 bucket.Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table
Trigger AWS Step Functions

Q665 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?
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.
use AWS (KMS) with (CMKs)

Q666 A company is designing a message-driven order processing application on AWS. The application consists of many services and needs to communicate the results of its processing to multiple consuming services. Each of the consuming services may take up to 5 days to receive the messages. Which process will meet these requirements?
D. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic.An Amazon Simple Queue Service (Amazon SQS) queue is created for each service and each queue is configured to be a subscriber of the SNS topic.
application sends results of processing to Amazon SNS topic. Amazon SQS queue is created.

Q667 A company stores call recordings on a monthly basis Statistically, the recorded data may be referenced randomly within a year but accessed rarely after 1 year. Files that are newer than 1 year old must be queried and retrieved as quickly as possible. A delay in retrieving older files is acceptable. A solutions architect needs to store the recorded data at a minimal cost. Which solution is MOST cost-effective?
B. Store individual files in Amazon S3 Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files from Amazon S3 or S3 Glacier.
query and retrieve the files from Amazon S3 or S3 Glacier

Q668 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?

C. 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 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
add and remove nodes based on number of items in SQS queue

Q669 A company is building a media sharing application and decides to use Amazon S3 for storage. When a media file is uploaded, the company starts a multi-step to create thumbnails, identify objects in the image, transcode videos into standard formats and resolutions, and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation. The amount of traffic is variable. The solution must be able to handle spikes in load without unnecessary expenses. What should a solution architect recommend to support this workload?
B. Trigger an AWS Lambda function when an object is stored in the $3 bucket. Have the step functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.
have step functions perform the steps needed to process object

Q670 A recently created startup built a three-tier web application. The front end has static content. The application layer is based on microservices. User data is stored as JSON documents that need to be accessed with low latency. The company expects regular traffic to be low during the first year, with peaks in traffic when it publicizes new features every month. The startup team needs to minimize operational overhead costs. What should a solutions architect recommend to accomplish this?
C. Use Amazon S3 static website hosting to store and serve the front end.Use Amazon API Gateway and Lambda functions for application layer.Use Amazon DynamoDB to store user data.
use Amazon API Gateway and Lambda functions for the application layer. use DynamoDB to store data

Q671 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 issue so they can scale out resource Company management wants a solution that automatically responds to such events. Which solution meets these requirements?
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.
set up AWS Auto Scaling to scale out ECS service when service’s CPU utilization is too high

Q672 A company receives inconsistent service from its data center provider because the company is headquartered in an area affected by natural disasters. The company is not ready to fully migrate to the AWS Cloud, but it wants a failure environment on AWS in case the on-premises data center fails. The company runs web servers that connect to external vendors. The data available on AWS and on premises must be uniform. Which solution should a solutions architect recommend that has the LEAST amount of downtime?

A. Configure an Amazon Route 53 failover record. Run application servers on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group.Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3
run application server on EC2

Q673 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?
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.
Store credentials in Secrets Manager.setup credential rotation schedule

Q674 A web application must persist order data to Amazon S3 to support near-real-time processing. A solutions architect needs to create an architecture that is both scalable and fault tolerant. Which solutions meet these requirements? (Select TWO.)
A. Write the order event to an Amazon DynamoDB table. Use DynamoDB Streams to trigger an AWS Lambda function that parses the payload and writes the data to Amazon B. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue.Use the queue to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3
write order event to Amazon DynamoDB table
write order event to SQS queue. use queue to trigger an AWS Lambda function

Q675 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?
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.
subscribe to RDS event notification and send Amazon SNS topic fanned out to SQS

Q676 A media company has an application that tracks user clicks on its websites and performs analytics to provide near-real time recommendations. The application has a fleet of Amazon EC2 instances that receive data from the websites and send the data to an Amazon RDS DB instance. Another fleet of EC2 instances hosts the portion of the application that is continuously checking changes in the database and executing SQL queries to provide recommendations. Management has requested a redesign to decouple the infrastructure. The solution must ensure that data analysts are writing SQL to analyze the data only. No data can be lost during the deployment. What should a solutions architect recommend?
B. Use Amazon Kinesis Data Streams to capture the data from the websites, Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3. Amazon Kinesis Data Streams
Kinesis Data Analytics to query data

Q677 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?
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.
stream transactions data into Amazon Kinesis Data Streams

Q678 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
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.
use one ALB with two target groups

Q679 A company wants to improve the availability and performance of its stateless UDP based workload. The workload is deployed on Amazon EC2 instances in multiple AWS Regions. What should a solutions architect recommend to accomplish this?
A. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the NLBs as endpoints for the accelerator.
place EC2 behind NLB in each region. Create an accelerator

Q680 One of the criteria for a new deployment is that the customer wants to use AWS Storage Gateway. However you are not sure whether you should use gateway-cached volumes or gateway-stored volumes or even what the differences are. Which statement below best describes those differences?
A. Gateway-cached lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally.Gateway-stored enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point- in-time snapshots of this data to Amazon S3.
Gateway-cached lets you store data in S3

Q681 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.
configure an accelerator in AWS Global Accelerator

Q682 A solutions architect is creating a new VPC design. There are two public subnet for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web server use only HTTPS. The solutions architect has already created a security group for the load Balancer allowing port 443 from 0.0 0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks. Which additional configuration strategy should the solution architect use to meet these requirements?
C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group tor the MySQL servers and allow port 3306 from the web sewers security group .
allow port 443 from load balancer. create a security group for MySQL servers

Q683 A company Is designing an internet-facing web application. The application runs on Amazon EC2 for Linux-based instances that store sensitive user data in Amazon RDS MySQL Multi-AZ DB instances. The EC2 instances are in public subnets, and the RDS DB instances are in private subnets. The security team has mandated that the DB instances be secured against web-based attacks. What should a solutions architect recommend?
C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Create a security group for the web application servers and a security group for the DB instances.Configure the RDS security group to only allow port 3306 inbound from the web application server security group.
create a security group for web application servers

Q684 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?
C. Use the AWS Schema Conversion Tool with AWS DataBase Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
using a memory optimized replication instance

Q685 A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in another AWS Region with minimal downtime. What should a solutions architect do to meet these requirements with the LEAST amount of downtime?
A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global tablc. Configure DNS failover to point to the now disaster recovery Region's load balancer.
create an Auto Scaling group and a load balancer in DR region. Configure DNS failover

Q686 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?
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.
Add an Auto Scaling group for consumer

Q687 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?
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
configure a stored volume gateway

Q688 A company hosts historical weather records in Amazon S3. The records are downloaded from the company's website by way of a URL that resolves to a domain name. Users all over the world access this content through subscriptions. A third-party provider hosts the company's root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers. Which solution meets these requirements?
B. Create a web distribution on Amazon CloudFront to serve the $3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name. Amazon CloudFront
Create an ALIAS record in Route 53

Q689 A company provides a three-tier web application to its customers. Each customer has an AWS account in which the application is deployed, and these accounts are members of the company's organization in AWS Organizations. To protect its customers' AWS accounts and applications the company wants to monitor them for unusual and unexpected behavior. The company needs to analyze and monitor customer VPC Flow Logs. AWS CloudTrail logs, and DNS logs. What should a solutions architect do to meet these requirements?
B. Designate an account in the organization as the Amazon GuardDuty master account Enable GuardDuty in every account and invite the accounts to join the GuardDuty master account Analyze GuardDuty finding in the GuardDuty master account.
designate account as Amazon GuardDuty master account

Q690 A company is building a web application that servers a content management system. The content management system runs on Amazon EC2 instances behind an application Load Balancer (ALB). The EC2 instances run in an Auto Scaling group across Availability Zones. Users are constantly adding and updating files, blogs, and other website assets in the content management system. Which solution meets these requirements?

B. Copy the website assets to an Amazon Elastic File System (Amazon EFS) Me system.Configure each EC2 instance to mount the EFS m system locally. Configure the website hosting application to reference the website assets that are stored in the EFS file system.
copy website assets to an Amazon Elastic File System (EFS)

Q691 A company sells datasets to customers who do research in artificial intelligence and machine learning (AIMU.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 mutated 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?
B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin Direct customer requests to the CloudFront URLSwitch to CloudFront signed URLs for access control
deploy an CLoudFront distribution with existing S3 bucket

Q692 A company has an application mat 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 tiles that contain personally identifiable information (PII) mat 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 LEAS F development effort?
B. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Macie to scan the objects in the bucketIf objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
use Amazon Macie to scan objects in bucket

Q693 A company is automating an order management application. The company's development team has decided to use SFTP to transfer and store the business-critical information files. The files must be encrypted and must be highly available. The files also must be automatically deleted a month after they are created. Which solution meets these requirements with the LEAST operational overhead?
D. Configure an Amazon S3 bucket with encryption enabled Use AWS Transfer for SFTP to securely transfer the files to the S3 bucket. Apply S3 Lifecycle rules to automatically delete the files after a month.
Apply S3 Lifecycle rules to automatically delete files after a month

Q694 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.

create a backup vault in AWS Backup to retain RDS backups

Q695 A company has an application that calls AWS Lambda functions. A code review shows that database credentials are stored in a Lambda function's source code, which violates the company's security policy. The credentials must be securely stored and must be automatically rotated on an ongoing basis to meet security policy requirements. What should a solutions architect recommend to meet these requirements in the MOST secure manner?
B. Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can use the secret ID to retrieve the password from Secrets Manager. Use Secrets Manager to automatically rotate the password.
store password in AWS Secrets Manager

Q696 A company is running a global application. The application's users submit multiple videos that are then merged into a single video file. The application uses a single Amazon S3 bucket in the us-east-1 Region to receive uploads from users. The same S3 bucket provides the download location of the single video file that is produced. The final video file output has an average size of 250 GB. The company needs to develop a solution that delivers faster uploads and downloads of the video files that are stored in Amazon S3. The company will offer the solution as a subscription to users who want to pay for the increased speed. What should a solutions architect do to meet these requirements?
D. Enable S3 Transfer Acceleration for the S3 bucket in us-east-1. Configure the application to use the bucket's S3-accelerate endpoint domain name for the upload and download links for users who have a subscription.
enable S3 Transfer Acceleration for S3 bucket

Q697 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?
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.
create a db user to use with IAM authentication

Q698 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 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 the security group of the web servers.
allow inbound traffic on port 443 from 0.0.0.0/0, allow inbound traffic on port 3306 from. security group of web servers

Q699 A company is using Amazon Redshift for analytics and to generate customer reports. The company recently acquired 50 TB of additional customer demographic data. The data is stored in csv files in Amazon S3. The company needs a solution that joins the data and visualizes the results with the least possible cost and effort. What should a solutions architect recommend to meet these requirements?
B. Use Amazon Athena to query the data in Amazon S3. Use Amazon QuickSightto join the data from Athena with the existing data in Amazon Redshift and to build the visualizations
use Athena to query data in S3

Q700 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?
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
move database to Aurora with a read replica in another availability zone

Q701 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
create a new AWS KMS encryption key

Q702 A company is building its web application by using containers on AWS. The company requires three instances of the web application run at all times. The application must be highly available and must be able to scale to meet increases in demand. Which solution meets these requirements?
C. Use the AWS Fargate launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has three container instances in three different Availability Zones. Create a task definition for the web application. Create an ECS service that has a desired count of three tasks
cluster that has 3 container instances in 3 different availability zones

Q703 A company has designed an application where users provide small sets of textual data by calling a public API The application runs on AWS and includes a public Amazon API Gateway API that forwards requests to an AWS Lambda function for processing. The Lambda function then writes the data to an Amazon Aurora Serverless database for consumption. The company is concerned that it could lose some user data if a Lambda function fails to process the request property or reaches a concurrency limit. What should a solutions architect recommend to resolve this concern?
A. Split the existing Lambda function into two Lambda functions. Configure one function to receive API Gateway requests and put relevant items into Amazon Simple Queue Service (Amazon SQS). Configure the other function to read items from Amazon SQS and save the data into Aurora

put relevant items into Amazon SQS

Q704 A company's web application consists of multiple Amazon EC2 instances that run behind an Application Load Balancer in a VPC An Amazon RDS for MySQL DB instance contains the data. The company needs the ability to automatically detect and respond to suspicious or unexpected behavior in its AWS environment. The company already has added AS WAF to its architecture. What should a solutions architect do next to protect against threats?

A. Use Amazon GuardDuty to perform threat detection. Configure Amazon EventBridge (Amazon Cloud Watch Events) to filter for GuardDuty findings and to invoke an AWS Lambda function to adjust the AWS WAF rules

use Amazon GuardDuty to perform threat detection

Q705 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?

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.

configure a public ALB with multiple EC2 in private subnets. Configure CloudFront to deliver HTTPS content using public ALB as the origin

Q706 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

Configure Kinesis Data Firehose Stream to deliver alerts to S3 bucket

Q707 A company has an application that processes customer orders. The company hosts the application on an Amazon Ec2 instance that saves the orders to an Amazon Aurora database Occasionally when traffic is high, the workload does not process orders fast enough. What should a solutions architect do to write the orders reliably to the database as quickly as possible?

B. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database

write orders to Amazon SQS queue. use EC2 in Auto Scaling group behind an ALB to read from SQS queue and process

Q708 A company is designing an application to run in a VPC on AWS. The application consists of Amazon EC2 instances that run in private subnets as part of an Auto Scaling group The application also

includes a Network Load Balancer that extends across public subnets. The application stores data in an Amazon RDS DB instance. The company has attached a security group that is named"web-servers" to the EC2 instances. The company has attached a security group that is named"database" to the DB instance. How should a solutions architect configure the communication between the EC2 instances and the DB instance?
B. Configure the "web-servers" security group to allow access to the "database" security group. Configure the "database" security group to allow access from the "web-servers security group.
"Web-servers" allow access to "database". "database" allow access from "web-servers"

Q709 A company is deploying a new application to Amazon Elastic Kubernetes Service (Amazon EKS) with an AWS Fargate cluster. The application needs a storage solution for data persistence. The solution must be highly available and fault tolerant The solution also must be shared between multiple application containers. Which solution will meet these requirements with the LEAST operational overhead?
B. Create an Amazon Elastic File System (Amazon EFS) file system. Register the file system in a StorageClass object on an EKS cluster Use the same file system for all containers
use the same file system for all containers

Q710 A solutions architect needs to design a solution that retrieves data every 2 minutes from a third-party web service that is accessible through the internet. A Python script runs the data retrieval in less than 100 milliseconds for each retrieval. The response is a JSON object that contains sensor data that is less than 1 KB in size. The solutions architect needs to store the JSON object along with the timestamp. Which solution meets these requirements MOST cost-effectively?
C. Deploy an AWS Lambda function to extend the script to store the JSON object along with the timestamp in an Amazon DynamoDB table that uses the timestamp as the primary key. Use an Amazon EventBridge (Amazon Cloud Watch Events) scheduled event that is initiated every 2 minutes to invoke the Lambda function
deploy Lambda function to extend script to store JSON object along with timestamp

Q711 A company has deployed a business-critical application in the AWS Cloud. The application uses Amazon EC2 instances that run in the us-east-1 Region. The application uses Amazon S3 for storage of all critical data. To meet compliance requirements, the company must create a disaster recovery (DR) plan that provides the capability of a full failover to another AWS Region. What should a solutions architect recommend for this DR plan?
D. Use S3 Cross-Region Replication for the data that is stored in Amazon S3. Create an AWS CloudFormation template for the application with an S3 bucket parameter. In the event of a disaster, deploy the template to the destination Region and specify the local S3 bucket as the parameter .
use S3 cross-region replication for data

Q712 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?

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
provision an AWS Storage Gateway Volume Gateway stored volume

Q713 You have deployed a web application, targeting a global audience across multiple AWS Regions under the domain name example.com. You decide to use Route53 Latency-Based Routing to serve web requests to users from the region closest to the user. To provide business continuity in the event of server downtime you configure weighted record sets associated with two web servers in separate Availability Zones per region. During a DR test you notice that when you disable all web servers in one of the regions Route53 does not automatically direct all users to the other region. What could be happening? Choose 2 answers
A. You did not set "Evaluate Target Health" to 'Yes" on the latency alias resource record set associated with example.com in the region where you disabled the servers E. You did not setup an HTTP health check for one or more of the weighted resource record sets associated with the disabled web servers
you didn't set "Evaluate Target Health" to "YES". you didn't setup an HTTP health check

Q714 An international company has deployed a multi-tier web application that relies on DynamoDB in a single region.For regulatory reasons they need disaster recovery capability in a separate region with a Recovery Time Objective of 2 hours and a Recovery Point Objective of 24 hours. They should synchronize their data on a regular basis and be able to provision the web application rapidly using CloudFormation. The objective is to minimize changes to the existing web application, control the throughput of DynamoDB used for the synchronization of data, and synchronize only the modified elements. Which design would you choose to meet these requirements?
A. Use AWS Data Pipeline to schedule a DynamoDB cross region copy once a day, create a "LastUpdated" attribute in your DynamoDB table that would represent the timestamp of the last update and use it as a filter
use AWS Data Pipeline to schedule a DynamoDB

Q715 Your startup wants to implement an order fulfillment process for selling a personalized gadget that needs an average of 3-4 days to produce with some orders taking up to 6 months. You expect 10 orders per day on your first day, 1000 orders per day after 6 months and 10,000 orders after 12 months.Orders coming in are checked for consistency, then dispatched to your manufacturing plant for production, quality control, packaging, shipment and payment processing.If the product does not meet the quality standards at any stage of the process, employees may force the process to repeat a step. Customers are notified via email about order status and any critical issues with their orders such as payment failure. Your base architecture includes AWS Elastic Beanstalk for your website with an RDS MySQL instance for customer data and orders.How can you implement the order fulfillment process while making sure that the emails are delivered reliably?
B. Use SWF with an Auto Scaling group of activity workers and a decider instance in another Auto Scaling group with min/max=1.Use SES to send emails to customers.
Use SWF , Use SES to send emails to customers

Q716 Your company runs a customer facing event registration site. This site is built with a 3-tier architecture with web and application tier servers and a MySQL database. The application requires 6 web tier servers and 6 application tier servers for normal operation, but can run on a minimum of 65% server capacity and a single MySQL database. When deploying this application in a region with three availability zones (AZs), which architecture provides high availability?
B. A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 3 AZs with 2 EC2 instances In each AZ inside an Auto Scaling Group behind an ELB. and a Multi-AZ RDS (Relational Database Service) deployment.
A web tier deployed across 3 AZs with 2 EC2, an Auto scaling group o behind ELB and Multi-AZ RDS deployment

Q717 Your application is using an ELB in front of an Auto Scaling group of web/application servers deployed across two AZs and a Multi-AZ RDS Instance for data persistence. The database CPU is often above 80% usage and 90% of I/O operations on the database are read. To improve performance you recently added a single-node Memcached ElastiCache Cluster to cache frequent DB query results.In the next weeks the overall workload is expected to grow by 30%.Do you need to change anything in the architecture to maintain the high availability of the application with the anticipated additional load? Why?
A. Yes, you should deploy two Memcached ElastiCache Clusters in different AZs because RDS instance will not be able to handle the load if the cache node fails.
Yes. deploy two Memcached ElastiCache

Q718 Your system recently experienced down time. During the troubleshooting process you found that a new administrator mistakenly terminated several production EC2 instances. Which of the following strategies will help prevent a similar situation in the future? The administrator still must be able to:- launch, start, stop, and terminate development resources,-launch and start production instances.
B. Leverage resource based tagging, along with an IAM user which can prevent specific users from terminating production EC2 resources.
leverage resource based tagging

Q719 Your customer wishes to deploy an enterprise application to AWS, which will consist of several web servers, several application servers, and a smal (50GB) Oracle database. Information is stored both in the database and the filesystems of the various servers. The backup system must support database recovery, whole server and whole disk restores, and individual file restores with a recovery time of no more than two hours. They have chosen to use RDS Oracle as the database. Which backup architecture will meet these requirements?
A. Backup RDS using automated daily DB backups.Backup the EC2 Instances using AMIs, and supplement with file-level backup to S3 using traditional enterprise backup software to provide file level restore.
backup RDS using automated daily DB backups, backup EC2 using AMIs

Q720 You have launched an EC2 instance with four (4) 500 GB EBS Provisioned IOPS volumes attached.The EC2 instance is EBS-Optimized and supports 500 Mbps throughput between EC2 and EBS.The four EBS volumes are configured as a single RAID 0 device, and each Provisioned IOPS volume is provisioned with 4,000 IOPS (4,000 16KB reads or writes), for a total of 16,000 random IOPS on the instance. The EC2 instance initially delivers the expected 16,000 IOPS random read and write performance. Sometime later, in order to increase the total random I/O performance of the instance, you add an additional two 500 GB EBS Provisioned IOPS volumes to the RAID.Each volume is provisioned to 4,000 IOPs like the original four, for a total of 24,000 IOPS on the EC2 instance.Monitoring shows that the EC2 instance CPU utilization increased from 50% to 70%, but the total random IOPS measured at the instance level does not increase at all. What is the problem and a valid solution?
A. The EBS-Optimized throughput limits the total IOPS that can be utilized; use an EBS-Optimized instance that provides larger throughput.
EBS-Optimized throughput limits total IOPS that can be utilized

Q721 Your company plans to host a large donation website on Amazon Web Services (AWS). You anticipate a large and undetermined amount of traffic that will create many database writes. To be certain that you do not drop any writes to a database hosted on AWS, which service should you use?
A. Amazon Simple Queue Service (SQS) for capturing the writes and draining the queue to write to the database.
Amazon SQS for capturing writes

Q722 You have been asked to design the storage layer for an application. The application requires disk performance of at least 100,000 IOPS.In addition, the storage layer must be able to survive the loss of an individual disk, EC2 instance, or Availability Zone without any data loss. The volume you provide must have a capacity of at least 3 TB. Which of the following designs will meet these objectives?
D. Instantiate an 12 xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance. Configure synchronous, block-level replication to an identically configured instance in us-east-1b.
configure synchronous, block-level replication to an identically configured instance

Q723 A Company B is launching a new game app for mobile devices. Users will log into the game using their existing social media account. To streamline data capture, Company B would like to directly save player data and scoring information from the mobile app to a DynamoDB table named ScoreData. When a user saves their game, the progress data will be stored to the GameState S3 bucket. What is the best approach for storing data to DynamoDB and S3?
B. Use temporary security credentials that assume a role providing access to the ScoreData DynamoDB table and the GameState S3 bucket using web identity federation
use temporary security credentials

Q724 You have recently joined a startup company building sensors to measure street noise and air quality in urban areas. The company has been running a pilot deployment of around 100 sensors for 3 months.Each sensor uploads 1KB of sensor data every minute to a backend hosted on AWS.During the pilot, you measured a peak of 10 IOPS on the database, and you stored an average of 3GB of sensor data per month in the database. The current deployment consists of a load-balanced, auto scaled Ingestion layer using EC2 instances, and a PostgreSQL RDS database with 500GB standard storage The

pilot is considered a success and your CEO has managed to get the attention of some potential Investors. The business plan requires a deployment of at least 100k sensors which needs to be supported by the backend. You also need to store sensor data for at least two years to be able to compare year over year improvements. To secure funding, you have to make sure that the platform meets these requirements and leaves room for further scaling. Which setup will meet the requirements?
C. Ingest data into a DynamoDB table and move old data to a Redshift cluster
ingest data into a DynamoDB table

Q725 A web design company currently runs several FTP servers that their 250 customers use to upload and download large graphic files. They wish to move this system to AWS to make it more scalable, but they wish to maintain customer privacy and keep costs to a minimum. What AWS architecture would you recommend?
A. Ask their customers to use an S3 client instead of an FTP client. Create a single S3 bucket.Create an IAM User for each customer.Put the IAM Users in a Group that has an IAM policy that permits access to sub-directories within the bucket via use of the 'username' Policy Variable.
ask customers to use S3 client instead of an FTP client

Q726 You need a persistent and durable storage to trace call activity of an IVR (Interactive Voice Response) system. Call duration is mostly in the 2-3 minutes time frame. Each traced call can be either active or terminated.An external application needs to know each minute the list of currently active calls. Usually there are a few calls/second, but once per month there is a periodic peak up to 1000 calls/second for a few hours. The system is open 24/7 and any downtime should be avoided. Historical data is periodically archived to files.Cost saving is a priority for this project. What database implementation would better fit this scenario, keeping costs as low as possible?
D. Use DynamoDB with a "Calls" table and a Global Secondary Index on a "IsActive" attribute that is present for active calls only.In this way the Global Secondary Index is sparse and more effective.
use DynamoDB with a “calls” table and a Global Secondary index on “IsActive” attribute

Q727 A 3-Ber e-commerce web application is currently deployed on-premises, and will be migrated to AWS for greater scalability and elasticity. The web tier currently shares read-only data using a network distributed file system. The app server tier uses a clustering mechanism for discovery and shared session state that depends on IP multicast. The database tier uses shared-storage clustering to provide database failover capability, and uses several read slaves for scaling.Data on all servers and the distributed file system directory is backed up weekly to off-site tapes. Which AWS storage and database architecture meets the requirements of the application?
C. Web servers:store read-only data in S3, and copy from S3 to root volume at boot time.App servers: share state using a combination of DynamoDB and IP unicast. Database:use RDS with multi-AZ deployment and one or more Read Replicas.Backup:web and app servers backed up weekly via AMIs, database backed up via DB snapshots
Store read-only data in S3. More Read Replicas,db backed up via DB snapshots

Q728 You are the new IT architect in a company that operates a mobile sleep tracking application. When activated at night, the mobile app is sending collected data points of 1 kilobyte every 5 minutes to your backend. The backend takes care of authenticating the user and writing the data points into an Amazon DynamoDB table.Every morning, you scan the table to extract and aggregate last night's data on a per

user basis, and store the results in Amazon S3.Users are notified via Amazon SNS mobile push notifications that new data is available, which is parsed and visualized by the mobile app. Currently you have around 100k users who are mostly based out of North America. You have been tasked to optimize the architecture of the backend system to lower cost. What would you recommend? Choose 2 answers
C. Introduce an Amazon SQS queue to buffer writes to the Amazon DynamoDB table and reduce provisioned write throughput.
E. Create a new Amazon DynamoDB table each day and drop the one for the previous day after its data is on Amazon S3.
introduce SQS queue to buffer writes
Create a new DynamoDB table each day

Q729 Your department creates regular analytics reports from your company's log files.All log data is collected in Amazon S3 and processed by daily Amazon Elastic MapReduce (EMR) jobs that generate daily PDF reports and aggregated tables in .csv format for an Amazon Redshift data warehouse. Your CFO requests that you optimize the cost structure for this system. Which of the following alternatives will lower costs without compromising average performance of the system or data integrity for the raw data?
A. Use reduced redundancy storage (RRS) for all data In S3.Use a combination of Spot Instances and Reserved Instances for Amazon EMR jobs. Use Reserved Instances for Amazon Redshift
use reduced redundancy storage(RRS) for all data in S3. use combination of Spot instances and Reserved instance for EMR jobs

Q730 You deployed your company website using Elastic Beanstalk and you enabled log file rotation to S3.An Elastic MapReduce Job is periodically analyzing the logs on S3 to build a usage dashboard that you share with your CIO. You recently improved the overall performance of the website using CloudFront for dynamic content delivery and your website as the origin.After this architectural change, the usage dashboard shows that the traffic on your website dropped by an order of magnitude.How do you fix your usage dashboard?
C. Enable CloudFront to deliver access logs to S3 and use them as input of the Elastic MapReduce job.
enable CloudFront to deliver access logs to S3

Q731 A web company is looking to implement an intrusion detection and prevention system into their deployed VPC. This platform should have the ability to scale to thousands of instances running inside of the VPC.How should they architect their solution to achieve these goals?
A. Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.
Configure each host with an agent that collects all network traffic

Q732 Your firm has uploaded a large amount of aerial image data to S3.In the past, in your on-premises environment, you used a dedicated group of servers to batch process this data and used RabbitMQ, an open source messaging system, to get job information to the servers.Once processed the data would go to tape and be shipped offsite. Your manager told you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost. Which is correct?
D. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS.Once data is processed, change the storage class of the S3 objects to Glacier.

setup Auto-scaled workers triggered by queue depth. change storage class of S3 objects to Glacier

Q733 You're running an application on-premises due to its dependency on non-x86 hardware and want to use AWS for data backup. Your backup application is only able to write to POSIX-compatible, block-based storage. You have 140TB of data and would like to mount it as a single folder on your file server.Users must be able to access portions of this data while the backups are taking place. What backup solution would be most appropriate for this use case?
B. Use Storage Gateway and configure it to use Gateway Stored volumes doudpasson
use Storage Gateway and configure it to use Gateway Stored volumes

Q734 A corporate web application is deployed within an Amazon Virtual Private Cloud (VPC), and is connected to the corporate data center via an IPsec VPN. The application must authenticate against the on-premises LDAP server.After authentication, each logged-in user can only access an Amazon Simple Storage Space (S3) keyspace specific to that user. Which two approaches can satisfy these objectives? Choose 2 answers
B. Develop an identity broker that authenticates against LDAP, and then calls IAM Security Token Service to get IAM federated user credentials. The application calls the Identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.
C. The application authenticates against LDAP, and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service to assume that IAM role. The application can use the temporary credentials to access the appropriate S3 bucket.
develop an identity broker that authenticates against LDAP
the app authenticates against LDAP and retrieves name of an IAM role associated with user

Q735 You are designing a multi-platform web application for AWS. The application will run on EC2 instances and will be accessed from PCs, tablets and smartphones, supported accessing platforms are Windows, MacOS, IOS and Android. Separate sticky session and SSL certificate setups are required for different platform types. Which of the following describes the most cost effective and performance efficient architecture setup?
C. Assign multiple ELBs to an EC2 Instance or group of EC2 instances running the common components of the web application.One ELB for each platform type.Session stickiness and SSL termination are done at the ELBs
assign multiple ELB to an EC2

Q736 You are designing an intrusion detection prevention (IDS/IPS) solution for a customer web application in a single VPC. You are considering the options for Implementing IDS/IPS protection for traffic coming from the Internet. Which of the following options would you consider? Choose 2 answers
A. Implement IDS/IPS agents on each instance running in VPC.
C. Implement a reverse proxy layer in front of web servers, and configure IDS/IPS agents on each reverse proxy server.
implement IDS/IPS agents on each instance
implement a reverse proxy layer

Q737 An enterprise wants to use a third-party Saas application. The Saas application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege, and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions?
A. Create an IAM role for cross-account access, allow the Saas provider's account to assume the role, and assign it a policy that allows only the actions required by the SaaS application.
create an IAM role for cross-account access

Q738 You are designing a photo-sharing mobile app. The application will store all pictures in a single Amazon S3 bucket. Users will upload pictures from their mobile device directly to Amazon S3 and will be able to view and download their own pictures directly from Amazon S3. You want to configure security to handle potentially millions of users in the most secure manner possible. What should your server-side application do when a new user registers on the photo-sharing mobile application?
D. Record the user's information in Amazon RDS and create a role in IAM with appropriate permissions. When the user uses their mobile app, create temporary credentials using the AWS Security Token Service "AssumeRole" function.Store these credentials in the mobile app's memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.
record user's information in RDS

Q739 You are designing a social media site and are considering how to mitigate distributed denial-of-service (DDoS) attacks. Which of the below are viable mitigation techniques? Choose 3 answers
B. Add alerts to Amazon CloudWatch to look for high Network In and CPU utilization.
D. Use an Elastic Load Balancer with auto scaling groups at the web, app, and Amazon Relational Database Service (RDS) tiers.
E. Use an Amazon CloudFront distribution for both static and dynamic content.
add alerts to CloudWatch
use an Elastic Load Balancer(ELB) with auto scaling groups
use CloudFront distribution for content

Q740 You currently operate a web application in the AWS US-East region. The application runs on an auto-scaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your EC2, IAM, and RDS resources. The solution must ensure the integrity and confidentiality of your log data. Which of these solutions would you recommend?
C. Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles, S3 bucket policies, and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs
use IAM roles, S3 bucket policy and Multi Factor Authentication(MFA) Delete on S3 bucket that stored your log

Q741 You have an application running on an EC2 instance which will allow users to download files from a private S3 bucket using a pre-signed URL. Before generating the URL, the application should verify the

existence of the file in S3.How should the application use AWS credentials to access the S3 bucket securely?
B. Create an IAM role for EC2 that allows list access to objects In the S3 bucket; launch the Instance with the role, and retrieve the role's credentials from the EC2 instance metadata
Create an IAM role for EC2 that allows list access to objects in S3

Q742 A benefits enrollment company is hosting a 3-tier web application running in a VPC on AWS which includes a NAT (Network Address Translation) instance in the public Web tier. There is enough provisioned capacity for the expected workload for the new fiscal year benefit enrollment period plus some extra overhead.Enrollment proceeds nicely for a few days and then the web tier becomes unresponsive. Upon investigation using CloudWatch and other monitoring tools it is discovered that there is an extremely large and unanticipated amount of inbound traffic coming from a set of 15 specific IP addresses over port 80 from a country where the benefits company has no customers. The web tier instances are so overloaded that benefit enrollment administrators cannot even SSH into them. Which activity would be useful in defending against this attack?
D. Create an inbound NACL (Network Access Control List) associated with the Web tier subnet with deny rules to block the attacking IP addresses
create an inbound (NACL) associated with Web tier subnet

Q743 You are designing an SSL/TLS solution that requires HTTPS clients to be authenticated by the Web server using client certificate authentication. The solution must be resilient. Which of the following options would you consider for configuring the Web server infrastructure? Choose 2 answers
B. Configure ELB with TCP listeners on TCP/443, and place the Web servers behind it.
C. Configure your Web servers with EIPs. Place the Web servers in a Route53 Record Set, and configure health checks against all Web servers.
Configure ELB with TCP listeners on TCP/443
Configure web servers with EIPs

Q744 You've been hired to enhance the overall security posture for a very large e-commerce site. They have a well architected, multi-tier application running in a VPC that uses ELBs in front of both the web and the app tier with static assets served directly from S3.They are using a combination of RDS and DynamoDB for their dynamic data and then archiving nightly into S3 for further processing with EMR. They are concerned because they found questionable log entries and suspect someone is attempting to gain unauthorized access. Which approach provides a cost effective, scalable mitigation to this kind of attack?
C. Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB.The WAF tier would then pass the traffic to the current web tier. The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group.
add a WAF tier by creating a new ELB

Q745 Your company has recently extended its datacenter into a VPC on AWS to add burst computing capacity as needed.Members of your Network Operations Center need to be able to go to the AWS Management Console and administer Amazon EC2 instances as necessary. You don't want to create new

IAM users for each NOC member and make those users sign in again to the AWS Management Console. Which option below will meet the needs for your NOC members?
A. Use your on-premises SAML 2.0-compliant identity provider (IdP) to grant the NOC members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint.
grant NOC members federated access to AWS Management Console via AWS SSO endpoint

Q746 An administrator is using Amazon CloudFormation to deploy a three tier web application that consists of a web tier and application tier that will utilize Amazon DynamoDB for storage. When creating the CloudFormation template which of the following would allow the application Instance access to the DynamoDB tables without exposing API credentials?
B. Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and reference the Role in the instance profile property of the application instance.
reference role in the instance profile property

Q747 An AWS customer is deploying an application that is composed of an AutoScaling group of EC2 instances. The customers security policy requires that every outbound connection from these instances to any other service within the customers Virtual Private Cloud must be authenticated using a unique X.509 certificate that contains the specific Instance-id. In addition, all X.509 certificates must be signed by the customer's key management service in order to be trusted for authentication. Which of the following configurations will support these requirements?
B. Configure the Auto Scaling group to send an SNS notification of the launch of a new instance to the trusted key management service.Have the key management service generate a signed certificate and send it directly to the newly launched instance
Configure auto scaling group to send SNS

Q748 You are looking to migrate your Development (Dev) and Test environments to AWS. You have decided to use separate AWS accounts to host each environment. You plan to link each account's bill to a Master AWS account using Consolidated Billing. To make sure you keep within budget you would like to implement a way for administrators in the Master account to have access to stop, delete and/or terminate resources in both the Dev and Test accounts. Identify which option will allow you to achieve this goal.
D. Create IAM users in the Master account. Create cross-account roles in the Dev and Test accounts that have full Admin permissions and grant the Master account access.
create IAM users in Master account. Create cross-account roles in DEV and Test account that have full admin permission

Q749 You are migrating a legacy client-server application to AWS. The application responds to a specific DNS domain (e.g.www.example.com) and has a 2-tier architecture, with multiple application servers and a database server.Remote clients use TCP to connect to the application servers. The application servers need to know the IP address of the clients in order to function properly and are currently taking that information from the TCP socket.A Multi-AZ RDS MySQL instance will be used for the database.During the migration you can change the application code, but you have to file a change request.How would you implement the architecture on AWS in order to maximize scalability and high availability?
D. File a change request to implement Proxy Protocol support in the application. Use an ELB with a TCP Listener and Proxy Protocol enabled to distribute load on two application servers in different AZs.

file a change request to implement Proxy Protocol support

Q750 Your company produces customer commissioned one-of-a-kind skiing helmets, combining high fashion with custom technical enhancements. Customers can show off their individuality on the ski slopes and have access to head-up-displays, GPS, rear-view cams and any other technical Innovation they wish to embed in the helmet. The current manufacturing process is data rich and complex, including assessments to ensure that the custom electronics and materials used to assemble the helmets are to the highest standards. Assessments are a mixture of human and automated assessments. You need to add a new set of assessments to model the failure modes of the custom electronics using GPUs with CUDA, across a cluster of servers with low latency networking. What architecture would allow you to automate the existing process using a hybrid approach, and ensure that the architecture can support the evolution of processes over time.
A. Use Amazon Simple Workflow (SWF) to manage assessments, movement of data & meta-data. Use an auto-scaling group of G2 instances in a placement group.
use (SWF) to manage assessments. use auto-scaling group of G2 instances

Q751 A newspaper organization has a on-premises application which allows the public to search Its back catalog and retrieve individual newspaper pages via a website written in Java. They have scanned the old newspapers into JPEGs (approx.17TB) and used Optical Character Recognition (OCR) to populate a commercial search product. The hosting platform and software are now end of life and the organization wants to migrate its archive to AWS and produce a cost efficient architecture and still be designed for availability and durability. Which is the most appropriate?
D. Use S3 with standard redundancy to store and serve the scanned files, use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones
use CloudSearch for query processing

Q752 You have deployed a three-tier web application in a VPC with a CIDR block of 10.0.0.0/28. You initially deploy two web servers, two application servers, two database servers and one NAT instance for a total of seven EC2 instances. The web, application and database servers are deployed across two availability zones (AZs). You also deploy an ELB in front of the two web servers, and use Route53 for DNS. Web traffic gradually increases in the first few days following the deployment, so you attempt to double the number of instances in each tier of the application to handle the new load. Unfortunately some of these new Instances fail to launch. Which of the following could be the root cause? Choose 2 answers
C. The ELB has scaled-up, adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches
E. AWS reserves the first four and the last IP address in each subnet's CIDR block so you do not have enough addresses left to launch all of the new EC2 instances
ELB has scaled-up, adding more instances to handle traffic spike
AWS reserved first four and last IP address

Q753 Your company previously configured a heavily used, dynamically routed VPN connection between your on-premises data center and AWS. You recently provisioned a DirectConnect connection and would like to start using this new connection.After configuring DirectConnect settings in the AWS Console, which of the following options will provide the most seamless transition for your users?

C. Update your VPC route tables to point to the DirectConnect connection, configure your DirectConnect router with the appropriate settings, verify network traffic is leveraging DirectConnect, and then delete the VPN connection.
configure DirectConnect router with settings, verify network traffic is leveraging DirectConnect, and then delete VPN connection

Q754 Your customer is willing to consolidate their log streams (access logs, application logs, security logs, etc.) in one single system. Once consolidated, the customer wants to analyze these logs in real time based on heuristics. From time to time, the customer needs to validate heuristics, which requires going back to data samples extracted from the last 12 hours. What is the best approach to meet your customer's requirements?
D. Send all the log events to Amazon Kinesis, develop a client process to apply heuristics on the logs
send all log events to Kinesis

Q755 Your team has a tomcat-based java application you need to deploy into development, test and production environments.After some research, you opt to use Elastic Beanstalk due to its tight integration with your developer tools and RDS due to its ease of management. Your QA team lead points out that you need to roll a sanitized set of production data into your environment on a nightly basis. Similarly, other software teams in your org want access to that same restored data via their EC2 instances in your VPC. The optimal setup for persistence and security that meets the above requirements would be the following:
D. Create your RDS instance separately and pass its DNS name to your app's DB connection string as an environment variable. Create a security group for client machines and add it as a valid source for DB traffic to the security group of the RDS instance itself.
create a security group for client machines

Q756 Your company has an on-premises, multi-tier PHP web application, which recently experienced downtime due to a large burst in web traffic due to a company announcement.Over the coming days, you're expecting similar announcements to drive similar unpredictable bursts, and are looking to find ways to quickly improve your infrastructures ability to handle unexpected increases in traffic. The application currently consists of 2 tiers:A web tier, which consists of a load balancer and several Linux Apache web servers, as well as a database tier, which hosts a Linux server hosting a MySQL database. Which scenario below will provide full site functionality, while helping to improve the availability of your application in the short timeframe required?
C. Offload traffic from on-premises environment:Setup a CloudFront distribution, and configure CloudFront to cache objects from a custom origin. Choose to customize your object cache behavior, and select a TTL that objects should exist in cache.
offload traffic from on-premises environment

Q757 A read only news reporting site with a combined web and application tier and a database tier that receives large and unpredictable traffic demands must be able to respond to these traffic fluctuations automatically. What AWS services should be used to meet these requirements?
A. Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaling group monitored with CloudWatch, and RDS with read replicas
Stateless instances for web. RDS with read replicas

Q758 A large real-estate brokerage is exploring the option of adding a cost-effective location based alert to their existing mobile application. The application backend infrastructure currently runs on AWS.Users who opt in to this service will receive alerts on their mobile device regarding real-estate offers in proximity to their location. For the alerts to be relevant delivery time needs to be in the low minute count. The existing mobile app has 5 million users across the US. Which one of the following architectural suggestions would you make to the customer?
A. The mobile application will send device location using SQS, EC2 instances will retrieve the relevant offers from DynamoDB.AWS Mobile Push will be used to send offers to the mobile application.
mobile app will send device location using SQS

Q759 You have a periodic image analysis application that gets some files in input, analyzes them and for each file writes some data in output to a text file. The number of files in input per day is high and concentrated in a few hours of the day.Currently you have a server on EC2 with a large EBS volume that hosts the input data and the results.It takes almost 20 hours per day to complete the process. What services could be used to reduce the elaboration time and improve the availability of the solution?
A. S3 to store I/O files, SQS to distribute elaboration commands to a group of hosts working in parallel, Auto Scaling to dynamically size the group of hosts depending on the length of the SQS queue.
S3 to store I/O files, SQS to distribute elaboration commands

Q760 You are implementing a URL whitelisting system for a company that wants to restrict outbound HTTP/S connections to specific domains from their EC2-hosted applications. You deploy a single EC2 instance running proxy software and configure it to accept traffic from all subnets and EC2 instances in the VPC. You configure the proxy to only pass through traffic to domains that you define in its whitelist configuration. You have a nightly maintenance window of 10 minutes where all instances fetch new software updates.Each update is about 200MB in size and there are 500 instances in the VPC that routinely fetch updates. After a few days you notice that some machines are falling to successfully download some, but not all, of their updates within the maintenance window. The download URLs used for these updates are correctly listed in the proxy's whitelist configuration and you are able to access them manually using a web browser on the instances. What might be happening? Choose 2 answers
A. You are running the proxy on an undersized EC2 instance type so network throughput is not suficient for all instances to download their updates in time
B. You are running the proxy on a sufficiently-sized EC2 instance in a private subnet and its network throughput is being throttled by a NAT running on an undersized EC2 instance
running proxy on an undersized EC2
running proxy on a sufficiently-size EC2

Q761 A company is running a batch analysis every hour on their main transactional DB.running on an RDS MySQL instance to populate their central Data Warehouse running on Redshift During the execution of the batch their transactional applications are very slow. When the batch completes they need to update the top management dashboard with the new data The dashboard is produced by another system running on-premises that is currently started when a manually-sent email notifies that an update is required The

on-premises system cannot be modified because is managed by another team. How would you optimize this scenario to solve performance issues and automate the process as much as possible?
C. Create an RDS Read Replica for the batch analysis and SNS to notify me on-premises system to update the dashboard
create RDS Read Replica for batch analysis and SNS to notify me

Q762 You are developing a new mobile application and are considering storing user preferences in AWS. This would provide a more uniform cross- device experience to users using multiple mobile devices to access the application. The preference data for each user is estimated to be 50KB in size. Additionally, 5 million customers are expected to use the application on a regular basis. The solution needs to be cost-effective, highly-available, scalable and secure.How would you design a solution to meet the above requirements?
D. Setup a DynamoDB table with an item for each user having the necessary attributes to hold the user preferences. The mobile application will query the user preferences directly from the DynamoDB table.Utilize STS, Web Identity Federation, and DynamoDB Fine Grained Access Control to authenticate and authorize access.
mobile app will query user preferences directly from DynamoDB table

Q763 You are designing a data leak prevention solution for your VPC environment. You want your VPC instances to be able to access software depots and distributions on the Internet for product updates. The depots and distributions are accessible via third party CDNs by their URLs. You want to explicitly deny any other outbound connections from your VPC instances to hosts on the Internet. Which of the following options would you consider?
B. Configure a web proxy server in your VPC and enforce URL-based rules for outbound access.Remove default routes.
configure a web proxy server in VPC

Q764 You want to use AWS CodeDeploy to deploy an application to Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC). What criterion must be met for this to be possible?
C. The AWS CodeDeploy agent installed on the Amazon EC2 instances must be able to access the public AWS CodeDeploy and Amazon S3 service endpoints.
AWS CodeDeploy agent must be able to access public AWS CodeDeploy and S3 service endpoint

Q765 An organization is planning to host a Wordpress blog as well a joomla CMS on a single instance launched with VPC. The organization wants to have separate domains for each application and assign them using Route 53.The organization may have about ten instances each with two applications as mentioned above. While launching the instance, the organization configured two separate network interfaces (primary + ENI) and wanted to have two elastic IPs for that instance.It was suggested to use a public IP from AWS instead of an elastic IP as the number of elastic IPs is restricted. What action will you recommend to the organization?
B. I do not agree as it is required to have only an elastic IP since an instance has more than one ENI and AWS does not assign a public IP to an instance with multiple ENIs
I don’t agree as it is required to have only an elastic IP

Q766 A customer has a website which shows all the deals available across the market. The site experiences a load of 5 large EC2 instances generally.However, a week before Thanksgiving vacation they encounter a load of almost 20 large instances. The load during that period varies over the day based on the office timings. Which of the below mentioned solutions is cost effective as well as help the website achieve better performance?
A. Setup to run 10 instances during the pre-vacation period and only scale up during the office time by launching 10 more instances using the AutoScaling schedule.
setup to run 10 instances during pre-vacation period

Q767 An organization has 4 people in the IT operations team who are responsible for managing the AWS infrastructure. The organization wants to set up that each user will have access to launch and manage an instance in a zone which the other user cannot modify. Which of the below mentioned options is the best solution to set this up?
D. Create a VPC with four subnets and allow access to each subnet for the individual IAM user.
create a VPC with 4 subnets

Q768 MapMySite is setting up a web application in the AWS VPC. The organization has decided to use an AWS RDS instead of using its own DB instance for HA and DR requirements. The organization also wants to secure RDS access.How should the web application be setup with RDS?
B. Setup a public and two private subnets in different AZs within a VPC and create a subnet group. Launch RDS with that subnet group.
setup a public and two private subnets in different AZs

Q769 An organization is having an application which can start and stop an EC2 instance as per schedule. The organization needs the MAC address of the instance to be registered with its software. The instance is launched in EC2-CLASSIC.How can the organization update the MAC registration every time an instance is booted?
A. The organization should write a bootstrapping script which will get the MAC address from the instance metadata and use that script to register with the application
organization should write a bootstrapping script

Q770 An organization is setting up a backup and restore system in AWS of their in premise system. The organization needs High Availability(HA) and Disaster Recovery(DR) but is okay to have a longer recovery time to save costs. Which of the below mentioned setup options helps achieve the objective of cost saving as well as DR in the most effective way?
B. Setup the backup data on S3 and transfer data to S3 regularly using the storage gateway.
setup backup data on S3

Q771 A solutions architect needs to define a reference architecture for a solution for three-tier applications with web, application, and NoSQL data layers. The reference architecture must meet the following requirements:-High availability within an AWS Region-Able to fail over in 1 minute to another AWS Region for disaster recovery-Provide the most efficient solution while minimizing the impact on the user experience. Which combination of steps will meet these requirements? (Choose three.)

B. Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region.Set Time to Live (TTL) to 30 seconds
C. Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.
E. Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources
Use Route 53 failover routing policy
Use a global table within DynamoDB
Implement hot standby model

Q772 A company has several Amazon EC2 instances to both public and private subnets within a VPC that is not connected to the corporate network.A security group associated with the EC2 instances allows the company to use the Windows remote desktop protocol (RDP) over the internet to access the instances. The security team has noticed connection attempts from unknown sources. The company wants to implement a more secure solution to access the EC2 instances. Which strategy should a solutions architect implement?
B. Deploy AWS Systems Manager Agent on the EC2 instances. Access the EC2 instances using Session Manager restricting access to users with permission.
Deploy Systems Manager Agent on EC2

Q773 A sys admin is maintaining an application on AWS. The application is installed on EC2 and user has configured ELB and Auto Scaling.Considering future load increase, the user is planning to launch new servers proactively so that they get registered with ELB.How can the user add these instances with Auto Scaling?
D. Increase the desired capacity of the Auto Scaling group
increase desired capacity of Auto Scaling group

Q774 After moving an E-Commerce website for a client from a dedicated server to AWS you have also set up auto scaling to perform health checks on the instances in your group and replace instances that fail these checks. Your client has come to you with his own health check system that he wants you to use as it has proved to be very useful prior to his site running on AWS. What do you think would be an appropriate response to this given all that you know about auto scaling and CloudWatch?
D. It is possible to implement your own health check system and then send the instance's health information directly from your system to CloudWatch.
it’s possible to implement your own health check system and send from your system to CLoudWatch

Q775 An organization hosts an app on EC2 instances which multiple developers need access to in order to perform updates. The organization plans to implement some security best practices related to instance access. Which one of the following recommendations will not help improve its security in this way?
B. Create an IAM policy allowing only IAM users to connect to the EC2 instances with their own SSH key.
Create an IAM policy

Q776 A user has created a VPC with public and private subnets.The VPC has CIDR 20.0.0.0/16.The private subnet uses CIDR 20.0.1.0/24 and the public subnet uses CIDR 20.0.0.0/24.The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group of the NAT instance. Which of the below mentioned entries is not required in NAT's security group for the database servers to connect to the Internet for software updates ?
C. For Inbound allow Source:20.0.0.0/24 on port 80
for inbound allow Source: 20.0.0.0/24 on port 80

Q777 Someone is creating a VPC for their application hosting. He has created two private subnets in the same availability zone and created one subnet in a separate availability zone.He wants to make a High Availability system with an internal Elastic Load Balancer. Which choice is true regarding internal ELBs in this scenario? (Choose 2 answers)
A. Internal ELBs should only be launched within private subnets.
C. Internal ELBs can support only one subnet in each availability zone.
Internal ELBs should only be launched with private subnets
internal ELBs can support only one subnet

Q778 You have custom Network File System (NFS) client settings for your Amazon Elastic File System (EFS).It takes up to three seconds for an Amazon Elastic Compute Cloud (EC2) instance to see a write operation performed on a file system from another Amazon EC2 instance. Which of the following actions should you take to solve the custom NFS settings from causing delays in the write operation?
A. Unmount and remount the file system with the noac option to disable attribute caching.
unmount and remount file system

Q779 You have set up a huge amount of network infrastructure in AWS and you now need to think about monitoring all of this. You decide CloudWatch will best fit your needs but you are unsure of the pricing structure and the limitations of CloudWatch. Which of the following statements is TRUE in relation to the limitations of Cloud Watch?
A. You get 10 CloudWatch metrics, 10 alarms, 1,000,000 API requests, and 1,000 Amazon SNS email notifications per customer per month for free.
you get 10 CloudWatch metrics, 10 alarms, 1 millions API request

Q780 An AWS account owner has setup multiple IAM users.One of these IAM users, named John, has CloudWatch access, but no access to EC2 services.John has setup an alarm action which stops EC2 instances when their CPU utilization is below the threshold limit. When an EC2 instance's CPU Utilization rate drops below the threshold John has set, what will happen and why?
C. Nothing will happen.John can setup the action, but it will not be executed because he does not have EC2 access through IAM policies.
john can setup action, but it will not be executed because he doesn’t have EC2 access

Q781 A company is planning to migrate an Amazon RDS for Oracle database to an RDS for PostgreSQL DB instance in another AWS account.A solutions architect needs to design a migration strategy that will

require no downtime and that will minimize the amount of time necessary to complete the migration. The migration strategy must replicate all existing data and any new data that is created during the migration. The target database must be identical to the source database at completion of the migration process.All applications currently use an Amazon Route 53 CNAME record as their endpoint for communication with the RDS for Oracle DB instance. The RDS for Oracle DB instance is in a private subnet. Which combination of steps should the solutions architect take to meet these requirements? (Select THREE)
B. Use the AWS Schema Conversion Tool (AWS SCT) to create a new RDS for PostgreSQL DB instance in the target account with the schema and initial data from the source database
C. Configure VPC peering between the VPCs in the two AWS accounts to provide connectivity to both DB instances from the target account. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account
E. Use AWS Database Migration Service (AWS DMS) in the target account to perform a full load plus change data capture (CDC) migration from the source database to the target database. When the migration is complete, change the CNAME record to point to the target DB instance endpoint
Use (SCT) to create a new RDS
Configure VPC peering between VPCs
Use (DMS) to perform a full load

Q782 A company has introduced a new policy that allows employees to work remotely from their homes if they connect by using a VPN. The company is hosting Internal applications with VPCs in multiple AWS accounts Currently the applications are accessible from the company's on-premises office network through an AWS Site-to-Site VPN connection. The VPC in the company's main AWS account has peering connections established with VPCs in other AWS accounts.A solutions architect must design a scalable AWS Client VPN solution for employees to use while they work from home. What is the MOST cost-effective solution that meets these requirements?
B. Create a Client VPN endpoint in the main AWS account. Configure required routing that allows access to internal applications
Create a Client VPN endpoint in the main AWS account. Configure required routing that allows access to internal applications

Q783 A solutions architect has deployed a web application that serves users across two AWS Regions under a custom domain. The application uses Amazon Route 53 latency-based routing. The solutions architect has associated weighted record sets with a pair of web servers in separate Availability Zones for each Region. The solutions architect runs a disaster recovery scenario. When all the web servers in one Region are stopped Route 53 does not automatically redirect users to the other Region. Which of the following are possible root causes of this issue? (Select TWO.)
A. The weight for the Region where the web servers were stopped is higher than the weight for the other Region
E. An HTTP health check has not been set up for one or more of the weighted resource record sets associated with the stopped web servers
weight for region where web server were stopped is high
An HTTP health check has not been set up

Q784 A company is refactoring its on-premises order-processing platform in the AWS Cloud. The platform includes a web front end that is hosted on a fleet of VMs RabbitMQ to connect the front end to the

backend, and a Kubernetes cluster to run a containerized backend system to process the orders. The company does not want to make any major changes to the application. Which solution will meet these requirements with the LEAST operational overhead?
A. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer.Set up Amazon MQ to replace the on-premises messaging queue.Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order- processing backend
create AMI of web server VM.set up Amazon MQ to replace on-premises messaging queue. Configure Amazon EKS

Q785 A company wants to send data from its on-premises systems to Amazon S3 buckets. The company created the S3 buckets in three different accounts. The company must send the data privately without the data traveling across the internet. The company has no existing dedicated connectivity to AWS. Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)
A. Establish a networking account in the AWS Cloud.Create a private VPC in the networking account. Set up an AWS Direct Connect connection with a private VIF between the on-premises environment and the private VPC
C. Create an Amazon S3 interface endpoint in the networking account.Establish a networking account in the AWS Cloud.
Set up Direct Connect connection with private VIF
Create S3 interface endpoint

Q786 An organization is planning to setup a management network on the AWS VPC. The organization is trying to secure the webserver on a single VPC instance such that it allows the internet traffic as well as the back-end management traffic. The organization wants to make so that the back end management network interface can receive the SSH traffic only from a selected IP range, while the internet facing webserver will have an IP address which can receive traffic from all the internet IPs. How can the organization achieve this by running web server on a single instance?
C. The organization should create two network interfaces with separate subnets so one instance can have two subnets and the respective security groups for controlled access.
organization should create two network interfaces with separate subnets

Q787 ExamKiller has three separate departments and each department has their own AWS accounts. The HR department has created a file sharing site where all the on roll employees' data is uploaded. The Admin department uploads data about the employee presence in the office to their DB hosted in the VPC. The Finance department needs to access data from the HR department to know the on roll employees to calculate the salary based on the number of days that an employee is present in the office. How can ExamKiller setup this scenario?
C. Setup VPC peering for the VPCs of Finance and HR as well as between the VPCs of Finance and Admin.
setup VPC peering for VPC of Finance and HR

Q788 An organization is undergoing a security audit. The auditor wants to view the AWS VPC configurations as the organization has hosted all the applications in the AWS VPC. The auditor is from a

remote place and wants to have access to AWS to view all the VPC records.How can the organization meet the expectations of the auditor without compromising on the security of their AWS infrastructure?
C. Create an IAM user who will have read-only access to the AWS VPC and share those credentials with the auditor.
create IAM user who will have read only access to AWS VPC

Q789 An organization is planning to create a secure scalable application with AWS VPC and ELB. The organization has two instances already running and each instance has an ENI attached to it in addition to a primary network interface. The primary network interface and additional ENI both have an elastic IP attached to it.If those instances are registered with ELB and the organization wants ELB to send data to a particular EIP of the instance, how can they achieve this?
A. The organization should ensure that the IP which is required to receive the ELB traffic is attached to a primary network interface.
IP which is required to receive ELB traffic is attached to a primary network interface

Q790 A company plans to migrate to AWS.A solutions architect uses AWS Application Discovery Service over the fleet and discovers that there is an Oracle data warehouse and several PostgreSQL databases. Which combination of migration patterns will reduce licensing costs and operational overhead? (Choose two.)
B. Migrate the Oracle data warehouse to Amazon Redshift using AWS SCT and AWS DMS D. Migrate the PostgreSQL databases to Amazon RDS for PostgreSQL using AWS DMS.
Migrate oracle to Redshift
Migrate PostgreSQL to RDS for PostgreSQL

Q791 An organization has hosted an application on the EC2 instances. There will be multiple users connecting to the instance for setup and configuration of the application. The organization is planning to implement certain security best practices. Which of the below mentioned pointers will not help the organization achieve better security arrangement?
A. Allow only IAM users to connect with the EC2 instances with their own secret access key.
allow only IAM users to connect with EC2

Q792 A company deploys a new web application As part of the setup, the company configures AWS WAF to log to Amazon S3 through Amazon Kinesis Data Firehose. The company develops an Amazon Athena query that runs once daily to return AWS WAF log data from the previous 24 hours. The volume of daily logs is constant. However over time, the same query is taking more time to run.A solutions architect needs to design a solution to prevent the query time from continuing to increase. The solution must minimize operational overhead. Which solution will meet these requirements?
D. Modify the Kinesis Data Firehose configuration and Athena table definition to partition the data by date and time. Change the Athena query to view the relevant partitions
modify Kinesis Data Firehose configuration and Athena table definition

Q793 A company has a platform that contains an Amazon S3 bucket for user content. The S3 bucket has thousands of terabytes of objects, all in the S3 Standard storage class. The company has an RTO of 6

hours. The company must replicate the data from its primary AWS Region to a replication S3 bucket in another Region. The user content S3 bucket contains user-uploaded files such as videos and photos. The user content S3 bucket has an unpredictable access pattern. The number of users is increasing quickly, and the company wants to create an S3 Lifecycle policy to reduce storage costs. Which combination of steps will meet these requirements MOST cost-effectively'? (Select TWO)

A. Move the objects in the user content S3 bucket to S3 Intelligent-Tiering immediately

D. Move the objects in the replication S3 bucket to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and to S3 Glacier Deep Archive after 90 days

Move objects in user content S3 bucket to S3 intelligent-Tiering immediately

Move objects in replication S3 bucket to S3 One Zone-infrequent Access

Q794 A company is migrating a legacy application from an on-premises data center to AWS. The application uses MangeDB as a key-value database.According to the company's technical guidelines, all Amazon EC2 instances must be hosted in a private subnet without an internet connection. In addition, all connectivity between applications and databases must be encrypted. The database must be able to scale based on demand. Which solution will meet these requirements?

D. Create new Amazon DocumentDB (with MangeDB compatibility) tables for the application with Provisioned IOPS volumes.Use the cluster endpoint to connect to Amazon DocumentDB

Use cluster endpoint to connect to DocumentDB

Q795 A large education company recently introduced Amazon Workspaces to provide access to internal applications across multiple universities. The company is storing user proxies on an Amazon FSx for Windows File Server tile system. The Me system is configured with a DNS alias and is connected to a self-managed Active Directory.As more users begin to use the Workspaces login time increases to unacceptable levels.An investigation reveals a degradation in performance of the file system. The company created the file system on HDD storage with a throughput of 16 MBps.A solutions architect must improve the performance of the file system during a defined maintenance window. What should the solutions architect do to meet these requirements with the LEAST administrative effort?

D. Enable shadow copies on the existing file system by using a Windows PowerShell command. Schedule the shadow copy job to create a point-in- time backup of the file system. Choose to restore previous versions. Create a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput. When the copy job is completed, adjust the DNS alias.Delete the original file system

enable shadow copies on existing file system

Q796 A company has loT sensors that monitor traffic patterns throughout a large city. The company wants to read and collect data from the sensors and perform aggregations on the data.A solutions architect designs a solution in which the loT devices are streaming to Amazon Kinesis Data Streams. Several applications are reading from the stream.However, several consumers are experiencing throttling and are periodically encountering a ReadProvisionedThroughputExceeded error. Which actions should the solutions architect take to resolve this issue? (Select THREE.)

A. Reshard the stream to increase the number of shards in the stream

C. Use consumers with the enhanced fan-out feature.

D. Reshard the stream to reduce the number of shards in the stream.

Increase number of shards

Use consumers

Use error retry

Q797 A company is using multiple AWS accounts. The company has a shared services account and several other accounts (or different projects.A team has a VPC in a project account. The team wants to connect this VPC to a corporate network through an AWS Direct Connect gateway that exists in the shared services account. The team wants to automatically perform a virtual private gateway association with the Direct Connect gateway by using an already-tested AWS Lambda function while deploying its VPC networking stack. The Lambda function code can assume a role by using AWS Security Token Service (AWS STS). The team is using AWS Cloud Formation to deploy its infrastructure. Which combination of steps will meet these requirements? (Select THREE.)

A. Deploy the Lambda function to the project account. Update the Lambda function's IAM role with the directconnect:* permission

C. Add a custom resource to the Cloud Formation networking stack that references the Lambda function in the project account.

E. Create a cross-account IAM role in the shared services account that grants the sts:Assume Role permission to the Lambda function with the directconnect:" permission acting as a resource.Add the sts AssumeRole permission with this cross-account IAM role as a resource to the IAM role that belongs to the Lambda function in the project account.

Deploy Lambda function to project account

Reference Lambda function in project account

IAM role that Belongs to Lambda function in project account

Q798 A company is using a single AWS Region (or its ecommerce website. The website includes a web application that runs on several Amazon EC2 instances behind an Application Load Balancer (ALB). The website also includes an Amazon DynamoDB table.A custom domain name in Amazon Route 53 is linked to the ALB. The company created an SSL/TLS certificate in AWS Certificate Manager (ACM) and attached the certificate to the ALB. The company is not using a content delivery network as part of its design. The company wants to replicate its entire application stack in a second Region to provide disaster recovery, plan for future growth, and provide improved access time to users.A solutions architect needs to implement a solution that achieves these goals and minimizes administrative overhead. Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)

A. Create an AWS Cloud Formation template for the current infrastructure design. Use parameters for important system values, including Region. Use the CloudFormation template to create the new infrastructure in the second Region

D. Update the Route 53 hosted zone record for the application to use latency-based routing. Send traffic to the ALB in each Region.

F. Create a new DynamoDB table.Enable DynamoDB Streams for the new table. Add the second Region to create a global table.Copy the data from the existing DynamoDB table to the new table as a one-time operation.

create AWS CLoud Formation template for current infrastructure design

update Route 53 to use latency-based routing

create a new DynamoDB

Q799 A company's solutions architect is reviewing a web application that runs on AWS. The application references static assets in an Amazon S3 bucket in the us-east-1 Region.The company needs resiliency

across multiple AWS Regions. The company already has created an S3 bucket in a second Region. Which solution will meet these requirements with the LEAST operational overhead?
D. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region.If failover is required, update the application code to load S3 objects from the S3 bucket in the second Region.
if failover is required, update app code

Q800 With Amazon Elastic MapReduce (Amazon EMR) you can analyze and process vast amounts of data. The cluster is managed using an open-source framework called Hadoop. You have set up an application to run Hadoop jobs. The application reads data from DynamoDB and generates a temporary file of 100 TBs.The whole process runs for 30 minutes and the output of the job is stored to S3.Which of the below mentioned options is the most cost effective solution in this case?
B. Use Spot Instances to run Hadoop jobs and configure them with ephermal storage for output file storage.
use Spot instances to run Hadoop jobs and configure them with ephermal storage for output file storage

Q801 An organization is setting up a highly scalable application using Elastic Beanstalk. They are using Elastic Load Balancing (ELB) as well as a Virtual Private Cloud (VPC) with public and private subnets. They have the following requirements:-All the EC2 instances should have a private IP-All the EC2 instances should receive data via the ELB's. Which of these will not be needed in this setup?
A. Launch the EC2 instances with only the public subnet.
Launch EC2 instances with only public subnet

Q802 An EC2 instance that performs source/destination checks by default is launched in a private VPC subnet.All security, NACL, and routing definitions are configured as expected.A custom NAT instance is launched. Which of the following must be done for the custom NAT instance to work?
A. The source/destination checks should be disabled on the NAT instance
the source/destination checks should be disabled on NAT instance

Q803 An organization has created multiple components of a single application for compartmentalization.Currently all the components are hosted on a single EC2 instance.Due to security reasons the organization wants to implement two separate SSLs for the separate modules although it is already using VPC.How can the organization achieve this with a single instance?
B. Create a VPC instance which will have multiple network interfaces with multiple elastic IP addresses.
create a VPC instance which will have multiple network interfaces

Q804 An organization making software for the CIA in USA.CIA agreed to host the application on AWS but in a secure environment. The organization is thinking of hosting the application on the AWS GovCloud region. Which of the below mentioned differences is not correct when the organization is hosting on the AWS GovCloud in comparison with the AWS standard region?
A. The billing for the AWS GovCLoud will be in a different account than the Standard AWS account.
the billing for AWS GovCloud will be in a different account

Q805 A company is running its solution on AWS in a manually created VPC. The company is using AWS Cloud Formation to provision other parts of the infrastructure.According to a new requirement, the company must manage all infrastructure in an automatic way. What should the company do to meet this new requirement with the LEAST effort?
D. Create a new CloudFormation template that creates the VPC.Use the AWS Serverless Application Model (AWS SAM) CLI to import the VPC.
use AWS (SAM) CLI to import VPC

Q806 A company is running a three-tier web application in an on-premises data center. The frontend is served by an Apache web server, the middle tier is a monolithic Java application, and the storage tier is a PostgreSOL database.During a recent marketing promotion, customers could not place orders through the application because the application crashed An analysis showed that all three tiers were overloaded. The application became unresponsive, and the database reached its capacity limit because of read operations. The company already has several similar promotions scheduled in the near future.A solutions architect must develop a plan for migration to AWS to resolve these issues. The solution must maximize scalability and must minimize operational effort. Which combination of steps will meet these requirements? (Select THREE.)
B. Rehost the Apache web server of the frontend on Amazon EC2 instances that are in an Auto Scaling group.Use a load balancer in front of the Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) to host the static assets that the Apache web server needs.
C. Rehost the Java application in an AWS Elastic Beanstalk environment that includes auto scaling.
F. Rehost the PostgreSOL database on an Amazon EC2 instance that has twice as much memory as the on-premises server.
rehost Apache web server of front end on EC2
rehost java app in AWS Elastic Beanstalk
rehost PostgreSQL db on EC2

Q807 AWS Direct Connect itself has NO specific resources for you to control access to. Therefore, there are no AWS Direct Connect Amazon Resource Names (ARNs) for you to use in an Identity and Access Management (IAM) policy. With that in mind, how is it possible to write a policy to control access to AWS Direct Connect actions?
C. You can use an asterisk (*) as the resource.
use an asterisk (*) as resource

Q808 An organization has developed an application which provides a smarter shopping experience. They need to show a demonstration to various stakeholders who may not be able to access the in premise application so they decide to host a demo version of the application on AWS.Consequently they will need a fixed elastic IP attached automatically to the instance when it is launched.In this scenario which of the below mentioned options will not help assign the elastic IP automatically?
A. Write a script which will fetch the instance metadata on system boot and assign the public IP using that metadata.
write a script which will fetch instance metadata

Q809 An organization is having a VPC for the HR department, and another VPC for the Admin department. The HR department requires access to all the instances running in the Admin VPC while the Admin department requires access to all the resources in the HR department.How can the organization setup this scenario?

A. Setup VPC peering between the VPCs of Admin and HR

setup VPC peering between VPCs of Admin and HR

Q810 ExamKiller has created a multi-tenant Learning Management System (LMS). The application is hosted for five different tenants (clients) in the VPCs of the respective AWS accounts of the tenant.ExamKiller wants to setup a centralized server which can connect with the LMS of each tenant upgrade if required.ExamKiller also wants to ensure that one tenant VPC should not be able to connect to the other tenant VPC for security reasons. How can ExamKiller setup this scenario?

A. ExamKiller has to setup one centralized VPC which will peer into all the other VPCs of the tenants.

ExamKiller has to setup one centralized VPC

Q811 AWS has launched T2 instances which come with CPU usage credit.An organization has a requirement which keeps an instance running for 24 hours.However, the organization has high usage only during 11 AM to 12 PM.The organization is planning to use a T2 small instance for this purpose.If the organization already has multiple instances running since Jan 2012, which of the below mentioned options should the organization implement while launching a T2 instance?

C. Create a VPC and launch a T2 instance as part of one of the subnets of that VPC.

create a VPC and a T2 instance

Q812 A company hosts its primary API on AWS by using an Amazon API Gateway API and AWS Lambda functions that contain the logic for the API methods. The company's internal applications use the API for core functionality and business logic. The company's customers use the API to access data from their accounts Several customers also have access to a legacy API that is running on a single standalone Amazon EC2 instance. The company wants to increase the security for these APIs to better prevent denial of service (DoS) attacks, check for vulnerabilities, and guard against common exploits. What should a solutions architect do to meet these requirements?

C. Use AWS WAF to protect the API Gateway API.Configure Amazon inspector to analyze the legacy API.Configure Amazon GuardDuty to monitor for malicious attempts to access the APIs.

use AWS WAF to protect API Gateway API. Configure Amazon inspector to analyze legacy API

Q813 A company has its cloud infrastructure on AWS.A solutions architect needs to define the infrastructure as code. The infrastructure is currently deployed in one AWS Region. The company's business expansion plan includes deployments in multiple Regions across multiple AWS accounts. What should the solutions architect do to meet these requirements?

C. Use AWS Organizations and AWS CloudFormation StackSets.Deploy a CloudFormation template from an account that has the necessary IAM permissions

Use Organizations and CloudFormation StackSets

Q814 A solutions architect needs to review the design of an Amazon EMR cluster that is using the EMR File System (EMRFS).The cluster performs tasks that are critical to business needs. The cluster is running Amazon EC2 On-Demand Instances at all times for all task, master, and core nodes. The EMR tasks run each morning, starting at 1:00 AM, and take 6 hours to finish running. The amount of time to complete the processing is not a priority because the data is not referenced until late in the day. The solutions architect must review the architecture and suggest a solution to minimize the compute costs. Which solution should the solutions architect recommend to meet these requirements?
B. Launch the master and core nodes on On-Demand Instances.Launch the task nodes on Spot Instances In an instance fleet. Terminate the cluster, including all instances, when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.
launch master and core nodes on on-demand instances. terminate cluster, including all instances when process is completed.

Q815 A company is hosting a critical application on a single Amazon EC2 instance. The application uses an Amazon ElastiCache for Redis single-node cluster for an in-memory data store. The application uses an Amazon RDS for MariaDB DB instance for a relational database.For the application to function, each piece of the infrastructure must be healthy and must be in an active state.A solutions architect needs to improve the application's architecture so that the infrastructure can automatically recover from failure with the least possible downtime. Which combination of steps will meet these requirements? (Select THREE.)
C. Modify the DB instance to create a read replica in the same Availability Zone. Promote the read replica to be the primary DB instance in failure scenarios.
D. Modify the DB instance to create a Multi-AZ deployment that extends across two Availability Zones.
E. Create a replication group for the ElastiCache for Redis cluster.Configure the cluster to use an Auto Scaling group that has a minimum capacity of two instances.
modify DB instance to create a read replica
modify db instance to create a multi-AZ deployment
Configure the cluster to use an Auto Scaling group

Q816 A company has automated the nightly retraining ot its machine learning models by using AWS Step Functions. The workflow consists of multiple steps that use AWS LambdA.Each step can fail for various reasons, and any failure causes a failure of the overall workflow.A review reveals that the retraining has failed multiple nights in a row without the company noticing the failure. A solutions architect needs to improve the workflow so that notifications are sent for all types of failures in the retraining process. Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)
A. Create an Amazon Simple Notification Service (Amazon SNS) topic with a subscription of type "Email" that targets the team's mailing list.
B. Create a task named "Email" that forwards the input arguments to the SNS topic
C. Add a Catch field to all Task. Map.and Parallel states that have a statement of "ErrorEquals":["states.all"] and "Next": "Email".
Create SNS topic
Forward input arguments to SNS topic
ErrorEquals: state.all

Q817 A company wants to migrate its workloads from on premises to AWS. The workloads run on Linux and Windows. The company has a large on- premises infrastructure that consists of physical machines and VMs that host numerous applications. The company must capture details about the system configuration. system performance.running procedure and network coi. net lions of its on-premises ,on boards. The company also must divide the on- premises applications into groups for AWS migrations. The company needs recommendations for Amazon EC2 instance types so that the company can run its workloads on AWS in the most cost-effective manner. Which combination of steps should a solutions architect take to meet these requirements? (Select THREE.)

B. Assess the existing applications by installing AWS Systems Manager.Agent on the physical machines and VMs

D. Group servers into applications for migration by using AWS Migration Hub.

F. Import data about server sizes into AWS Trusted Advisor. Follow the recommendations for cost optimization.

assess existing app by installing AWS Systems Manager

group servers into app for migration by using AWS Migration Hub

import data about server sizes into AWS Trusted Advisor

Q818 A government client needs you to set up secure cryptographic key storage for some of their extremely confidential data. You decide that the AWS CloudHSM is the best service for this. However, there seem to be a few pre-requisites before this can happen, one of those being a security group that has certain ports open. Which of the following is correct in regards to those security groups?

D. A security group that has port 22 (for SSH) or port 3389 (for RDP) open to your network.

a security group that has port 22(for SSH) or port 3389(for RDP) open to network

Q819 An organization is setting up a web application with the JEE stack. The application uses the JBoss app server and MySQL DB. The application has a logging module which logs all the activities whenever a business function of the JEE application is called. The logging activity takes some time due to the large size of the log file. If the application wants to setup a scalable infrastructure, which of the below mentioned options will help achieve this setup?

D. Create a separate module for logging and using SQS compartmentalize the module such that all calls to logging are asynchronous. ###

create a separate module for logging

Q820 A company is migrating an on-premises application and a MySQL database to AWS. The application processes highly sensitive data, and new data is constantly updated in the database. The data must not be transferred over the internet. The company also must encrypt the data in transit and at rest. The database is 5 TB in size. The company already has created the database schema in an Amazon RDS for MySQL DB instance. The company has set up a 1
Gbps AWS Direct Connect connection to AWS.The company also has set up a public VIF and a private VIF.A solutions architect needs to design a solution that will migrate the data to AWS with the least possible downtime. Which solution will meet these requirements?

D. Use Amazon S3 File Gateway.Set up a private connection to Amazon S3 by using AWS PrivateLink. Perform a database backup.Copy the backup files to Amazon S3.Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest.Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.

use S3 File Gateway

Q821 A company is running an application in the AWS Cloud. The company has several third-party services that integrate with the application through a RESTful API.The API is a serverless implementation with an Amazon API Gateway regional API endpoint that integrates with several different AWS Lambda functions. The application's data is nonrelational and is stored in an Amazon DynamoDB table. The application and the API are running in the eu- west-1 Region. The company needs the API to also be available in the us-east-1 Region. All data must be available in both Regions.A solutions architect already has deployed all the Lambda functions in us-east-1. Which additional steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Deploy a second API Gateway regional API endpoint in us-east-1.Create Lambda integration with the functions in us-east-1.

C. Modify the DynamoDB table to be a global table in eu-west-1 and in us-east-1.

deploy a second API Gateway regional API endpoint

modify DynamoDB table to be a global table

Q822 A company uses AWS Cloud Formation to deploy applications within multiple VPCs that are all attached to a transit gateway.Each VPC that sends traffic to the public internet must send the traffic through a shared services VPC.Each subnet within a VPC uses the default VPC route table, and the traffic is routed to the transit gateway. The transit gateway uses its default route table for any VPC attachment.A security audit reveals that an Amazon EC2 instance that is deployed within a VPC can communicate with an EC2 instance that is deployed in any of the company's other VPCs.A solutions architect needs to limit the traffic between the VPCs.Each VPC must be able to communicate only with a predefined, limited set of authorized VPCs. What should the solutions architect do to meet these requirements?

C. Create a dedicated transit gateway route table for each VPC attachment. Route traffic only to the authorized VPCs.

Create dedicated transit gateway route table

Q823 A company recently deployed an application on AWS. The application uses Amazon DynamoDB. The company measured the application load and configured the RCUs and WCUs on the DynamoDB table to match the expected peak load. The peak load occurs once a week for a 4-hour period and is double the average load. The application load is close to the average load tor the rest of the week. The access pattern includes many more writes to the table than reads of the table.A solutions architect needs to implement a solution to minimize the cost of the table. Which solution will meet these requirements?

D. Configure DynamoDB Accelerator (DAX) in front of the table.Configure on-demand capacity mode for the table.

configure DynamoDB Accelerator (DAX) in front of table. Configure on-demand capacity mode for the table

Q824 A company that uses AWS Organizations is creating several new AWS accounts. The company is setting up controls to properly allocate AWS costs to business units. The company must Implement a solution to ensure that all resources include a tag that has a key of costcenter and a value from a predefined list of business units. The solution must send a notification each time a resource tag does not

meet these criteria. The solution must not prevent the creation of resources. Which solution will meet these requirements with the LEAST operational overhead?
B. Create an IAM policy for all actions that create AWS resources.Add a condition to the policy that awsResourceTag/costcenter must exist and must contain a valid business unit value. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that monitors IAM service events and Amazon EC2 service events for noncompliant tag policies. Configure the rule to send notifications through Amazon Simple Notification Service (Amazon SNS).
Create IAM policy

Q825 Mike is appointed as Cloud Consultant in ExamKiller.com.ExamKiller has the following VPCs set-up in the US East Region:A VPC with CIDR block 10.10.0.0/16, a subnet in that VPC with CIDR block 10.10.1.0/24 A VPC with CIDR block 10.40.0.0/16, a subnet in that VPC with CIDR block 10.40.1.0/24 ExamKiller.com is trying to establish network connection between two subnets, a subnet with CIDR block 10.10.1.0/24 and another subnet with CIDR block 10.40.1.0/24. Which one of the following solutions should Mike recommend to ExamKiller.com?
C. Create a VPC Peering connection between both VPCs.
create a VPC Peering connection between both VPCs

Q826 An organization is setting up their website on AWS. The organization is working on various security measures to be performed on the AWS EC2 instances. Which of the below mentioned security mechanisms will not help the organization to avoid future data leaks and identify security weaknesses?
C. Perform a Code Check for any memory leaks
perform a Code Check for any memory leaks

Q827 A company runs many workloads on AWS and uses AWS Organizations to manage its accounts. The workloads are hosted on Amazon EC2, AWS Fargate, and AWS LambdA. Some of the workloads have unpredictable demand. Accounts record high usage in some months and low usage in other months. The company wants to optimize its compute costs over the next 3 years.A solutions architect obtains a 6-month average for each of the accounts across the organization to calculate usage. Which solution will provide the MOST cost savings for all the organization's compute usage?
B. Purchase a Compute Savings Plan for the organization from the management account by using the recommendation at the management account level.
Purchase compute Savings Plan

Q828 A company is running an application in the AWS Cloud. The company's security team must approve the creation of all new IAM users. When a new IAM user is created, all access for the user must be removed automatically. The security team must then receive a notification to approve the user. The company has a multi-Region AWS CloudTrail trail In the AWS account. Which combination of steps will meet these requirements? (Select THREE.)
A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule.Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.
D. Invoke an AWS Step Functions state machine to remove access.
E. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.

create Amazon EventBridge rule.
invoke AWS Step Function state machine to remove access
use (Amazon SNS) to notify security team.

Q829 A company implements a containerized application by using Amazon Elastic Container Service (Amazon ECS) and Amazon API Gateway. The application data is stored in Amazon Aurora databases and Amazon DynamoDB databases. The company automated infrastructure provisioning by using AWS CloudFormation. The company automates application deployment by using AWS CodePipeline. A solutions architect needs to implement a disaster recovery (DR) strategy that meets an RPO of 2 hours and an RTO of 4 hours. Which solution will meet these requirements MOST cost-effectively?
C. Use AWS Backup to create backups of the Aurora databases and the DynamoDB databases in a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region ###
use AWS Backup to create backups of Aurora db

Q830 A company is using a lift-and-shift strategy to migrate applications from several on-premises Windows servers to AWS. The Windows servers will be hosted on Amazon EC2 instances in the us-east-1 Region. The company's security policy allows the installation of migration tools on servers. The migration data must be encrypted in transit and encrypted at rest. The applications are business critical. The company needs to minimize the cutover window and minimize the downtime that results from the migration. The company wants to use Amazon CloudWatch and AWS CloudTrail for monitoring. Which solution will meet these requirements?
A. Use AWS Application Migration Service (CloudEnsure Migration) to migrate the Windows servers to AWS. Create a Replication Settings template. Install the AWS Replication Agent on the source servers
use AWS Application Migration Service to migrate Windows server to AWS

Q831 Your company is storing millions of sensitive transactions across thousands of 100-GB files that must be encrypted in transit and at rest. Analysts concurrently depend on subsets of files, which can consume up to 5 TB of space, to generate simulations that can be used to steer business decisions. You are required to design an AWS solution that can cost effectively accommodate the long-term storage and in-flight subsets of data.
D. Use HDFS on Amazon Elastic MapReduce (EMR), and run simulations on subsets in-memory on Amazon Elastic Compute Cloud (EC2)
use HDFS on Amazon Elastic MapReduce(EMR), and run simulations on subsets in-memory on EC2

Q832 A company processes environmental data. The company has set up sensors to provide a continuous stream of data from different areas in a city. The data is available in JSON format. The company wants to use an AWS solution to send the data to a database that does not require fixed schemas for storage. The data must be sent in real time. Which solution will meet these requirements?
B. Use Amazon Kinesis Data Streams to send the data to Amazon DynamoDB
use Amazon Kinesis Data Streams to send data to DynamoDB

Q833 A company runs an information portal on Amazon Elastic Container Service (Amazon ECS). The portal uses Amazon Cognito with a post Authentication trigger that calls an AWS Lambda function. The Lambda calls an external API to validate specific parameters that determine the permissions that a user receives. Users report that system login is taking a long time. A solutions architect needs to set up an Amazon CloudWalch dashboard to monitor the amount of time it takes for users to log in to the system. Which solution will meet these requirements?

C. Use CloudWatch to track the Amazon ECS application login metric. Add the ECS metric data to the CloudWatch dashboard.

Use CloudWatch to track Amazon ECS application login metric

Q834 A news company wants to implement an AWS Lambda function that calls an external API to receive new press releases every 10 minutes. The API provider is planning to use an IP address allow list to protect the API.so the news company needs to provide any public IP addresses that access the API. The company's current architecture includes a VPC with an interment gateway and a NAT gateway.A solutions architect must impalement.s static IP address for the Lambda function. Which combination of steps should the solutions architect take to meet these requirements?(Select TWO.)

A. Use the Elastic IP address that is associated with the NAT gateway for the IP address allow list.

C. Configure the Lambda function to launch in the private subnet of the VPC.

use Elastic IP address

configure Lambda function to launch in private subnet of VPC

Q835 A large company is migrating its on-premises applications to the AWS Cloud. All the company's AWS accounts belong to an organization in AWS Organizations.Each application is deployed into its own VPC in separate AWS accounts. The company decides to start the migration process by migrating the front-end web services while keeping the databases on premises. The databases are configured with local domain names that are specific to the on- premises environment. The local domain names must be resolvable from the migrated web services. Which solution will meet these requirements with the LEAST operational overhead?

A. Create a shared services VPC in a new AWS account. Deploy Amazon Route 53 outbound resolvers. For relevant on-premises domains, use the outbound resolver settings to create forwarding rules that point to the on-premises DNS servers. Share these rules with the other AWS accounts by using AWS Resource Access Manager.

Deploy Route 53 outbound resolvers

Q836 A company has an organization in AWS Organizations. The organization consists of a large number of AWS accounts that belong to separate business units. The company requires all Amazon EC2 instances to be provisioned with custom, hardened AMIs. The company wants a solution that provides each AWS account access to the AMIs. Which solution will meet these requirements with the MOST operational efficiency?

D. Create the AMIs with EC2 Image Builder. Create an AWS Lambda function to share the AMIs across all AWS accounts.

create Lambda function to share AMIs across all AWS account

Q837 A company has two VPCs: VPC A and VPC B. The company uses a solution in VPC A in the ca-central-1 Region to expose services that are deployed on Amazon EC2 instances. The services read

objects that are stored in an Amazon S3 bucket in ca-central-1. The S3 bucket must not be publicly accessible, and the EC2 instances must use a gateway VPC endpoint. A rule in the S3 bucket policy allows only traffic that comes from the VPC A endpoint. The company recently created another application. The application is hosted on EC2 instances that are deployed in VPC B in the us-east-1Region in the same AWS account. The application needs to access objects that are stored in the S3 bucket in ca-central-1. Which solution will meet these requirements?
A. Create a cross-Region VPC peering connection between the two VPCs. Add a route in the route table of VPC B to use the peering connection to access the S3 gateway VPC endpoint.
create a cross-region VPC peering connection between two VPCs

Q838 A large industrial company has two AWS accounts. One account is for production, and one account is for development. The company manages the production account under its corporate organization in AWS Organizations. The development account is an isolated environment that developers use for testing. The company stores all the application configuration information in an Amazon S3 bucket in the production account. All developers in the development account are members of a single IAM group. A solutions architect must ensure that the developers can update the application configuration information in real time. What is the MOST operationally efficient solution that meets these requirements?
C. Create an IAM role in the production account. Establish a trust relationship between the production account and the development account. Specify a permissions policy in the role to allow trusted users to put objects in the S3 bucket. Grant sts:AssumeRole permissions to the developers' IAM group for the role.
create IAM role in production account

Q839 A media company has a video-streaming application that runs on smart TVs. The application is written in HTML and JavaScript. A configuration exists for each smart TV type to control application behavior, such as whether the application should offer high-definition content. The configuration typically changes each quarter. The company serves the application from a fleet of Amazon EC2 instances that handle the requests from the smart TVs. On each request, an application template and smart TV configuration are retrieved from Amazon S3 and are merged to produce the customized application. The company's current solution produces high response times during peak load. The company wants to use Amazon CloudFront to deliver and cache the application. Which combination of steps should a solutions architect take to meet these requirements? (Choose three.)
A. Create a CloudFront distribution with the EC2 instances as an origin.
B. Create a Lambda@Edge function to be invoked by an origin request event. Determine the smart TV type by inspecting the user agent in the event. Modify the request URI to point to the application file from the S3 bucket.
D. Enable S3 Versioning on the S3 bucket that hosts the object. Modify the application build process to create a single application file for each configuration. Push the file to the S3 bucket by using the same name to create a new version. Set a Maximum TTL on the object.
create CloudFront distribution with EC2 instances as an origin
Create Lambda@Edge function to be invoked by origin request event.
Enable S3 versioning on S3 buckets

Q840 A company wants to use a third-party software-as-a-service (Saas) application. The third-party Saas application is consumed through several API calls. The third- party SaaS application also runs on AWS inside a VPC. The company will consume the third-party SaaS application from inside a VPC. The

company has internal security policies that mandate the use of private connectivity that does not traverse the internet. No resources that run in the company VPC are allowed to be accessed from outside the company's VPC. All permissions must conform to the principles of least privilege. Which solution meets these requirements?

A. Create an AWS PrivateLink interface VPC endpoint. Connect this endpoint to the endpoint service that the third-party SaaS application provides. Create a security group to limit the access to the endpoint. Associate the security group with the endpoint.

create AWS PrivateLink interface VPC endpoint

Q841 A company's compliance audit reveals that some Amazon Elastic Block Store (Amazon EBS) volumes that were created in an AWS account were not encrypted.A solutions architect must implement a solution to encrypt all new EBS volumes at rest. Which solution will meet this requirement with the LEAST effort?

D. Turn on EBS encryption by default in all AWS Regions.

Turn on EBS encryption by default in all regions

Q842 A company runs a web application that provides an HTTP API. The API uses a MySQL-compatible SQL database for session persistence. The existing workload runs in an on-premises environment on a Kubernetes cluster. The company has significant operational overhead associated with managing servers on premises and is considering a migration to AWS.The company wants to remove the need to manage servers or instances by using as many managed AWS offerings as possible. The company does not want to introduce significant changes to the web application or the HTTP API. A solutions architect must recommend different architecture solutions that the company can use to achieve these goals. Which solutions will meet these requirements? (Choose three.)

A. Create a Kubernetes cluster on AWS. Deploy an Amazon Aurora Serverless cluster. Run the web application on Kubernetes by using a managed node group. Use a containerized application that runs on Kubernetes to deploy an Application Load Balancer that exposes the web application.

D. Create a Kubernetes cluster on AWS. Deploy an Amazon Aurora Serverless cluster. Run the web application by using AWS Fargate and Amazon Elastic Kubernetes Service (Amazon EKS). Use containerized application that runs on Kubernetes to deploy an Application Load Balancer that exposes the web application.

F. Create an Amazon Lightsail containers deployment for the web application. Create a highly available Lightsail database in MySQL mode. Specify a public endpoint for the container deployment. Add a custom domain for the public endpoint.

run web app on Kubernetes by using a managed node group
run web app by using AWS Fargate and Elastic Kubernetes Service(EKS)
Create Amazon Lightsail containers deployment for web app

Q843 A company is using Amazon WorkSpaces to provide access to its corporate applications across multiple global locations. User profile data is stored on an Amazon FSx for Windows File Server file system that is configured with a DNS alias. The file system is linked to an existing Active Directory service. Recently, the company added a new application that unexpectedly caused user profiles to grow significantly. The company increased the FSx for Windows File Server file system size from 3 TiB to 6 TiB to prevent any issues. A few days later, the company made changes to the application's configuration. The user profile storage usage decreased significantly, leaving a large amount of free space on the file

system. A solutions architect needs to reduce the size of the file system to avoid unnecessary costs. What should the solutions architect do to achieve this goal?
A. During an agreed upon maintenance window, use AWS Backup to create a point-in-time backup of the file system. Restore the backup to a new, smaller FSx for Windows File Server file system. Adjust the DNS alias after the restore is completed. Delete the original file system.
use AWS Backup to create a point-in-time backup of file system

Q844 A company has an online shop that uses an Amazon API Gateway API, AWS Lambda functions, and an Amazon DynamoDB table provisioned with 900 RCUs. The API Gateway API receives requests from customers, and the Lambda functions handle the requests. Some of the Lambda functions read data from the DynamoDB table. During peak hours, customers are reporting timeout errors and slow performance. An investigation reveals that the Lambda functions that read the DynamoDB table occasionally time out. Amazon CloudWatch metrics show that the peak usage of the DynamoDB table is just below 900 RCUs. Which solution will resolve this issue MOST cost-effectively?
B. Increase the timeout of all the Lambda functions that read from the DynamoDB table.
increase timeout of all Lambda functions that read from DynamoDB table

Q845 A company has implemented a new security requirement. According to the new requirement, the company must scan all traffic from corporate AWS instances in the company's VPC for violations of the company's security policies. As a result of these scans, the company can block access to and from specific IP addresses. To meet the new requirement, the company deploys a set of Amazon EC2 instances in private subnets to serve as transparent proxies. The company installs approved proxy server software on these EC2 instances. The company modifies the route tables on all subnets to use the corresponding EC2 instances with proxy software as the default route. The company also creates security groups that are compliant with the security policies and assigns these security groups to the EC2 instances.Despite these configurations, the traffic of the EC2 instances in their private subnets is not being properly forwarded to the internet. What should a solutions architect do to resolve this issue?
A. Disable source/destination checks on the EC2 instances that run the proxy software.
disable source/destination checks on EC2

Q846 A company is running a web application in the AWS Cloud. The application consists of dynamic content that is created on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group that is configured as a target group for an Application Load Balancer (ALB). The company is using an Amazon CloudFront distribution to distribute the application globally. The CloudFront distribution uses the ALB as an origin. The company uses Amazon Route 53 for DNS and has created an A record of www.example.com for the CloudFront distribution.A solutions architect must configure the application so that it is highly available and fault tolerant. Which solution meets these requirements?
B. Provision an ALB, an Auto Scaling group, and EC2 instances in a different AWS Region. Update the CloudFront distribution, and create a second origin for the new ALB. Create an origin group for the two origins. Configure one origin as primary and one origin as secondary.
provision ALB, Auto Scaling group, EC2

Q847 A company is using AWS Single Sign-On (AWS SSO) to centrally manage permissions and access to multiple AWS accounts in AWS Organizations. A solutions architect needs to provide users with

granular access to AWS accounts based on different job functions. What should the solutions architect do to meet these requirements?
B. Create a group in AWS SSO for each job function. In AWS SSO for the management account, create a permission set for each job function. Add users to the appropriate groups. Assign groups to AWS accounts with corresponding permission sets.
create a group in AWS SSO for each job function

Q848 A company is migrating its applications to the AWS Cloud. Each application will reside in its own AWS account after the migration. The applications will be hosted on Amazon EC2 Linux instances that need to be accessed through the shell for administration. The company's administrators want to use the AWS CLI from their laptops to interact with AWS and the EC2 instances. The company is concerned that SSH access keys might be lost or become public. The company wants to avoid using long-term keys. Which combination of steps should a solutions architect recommend to meet these requirements? (Choose three.)
A. Create subaccounts and cross-account roles for each of the applications. Create users. Assign cross-account roles to the users. Provide users with their initial credentials. B Configure AWS Single Sign-On. Create users. Assign the users the permission sets for the application accounts that they need to access. Provide users with their initial credentials.
B. Use AWS Systems Manager Session Manager to obtain shell access to the EC2 instances.
C. Create an organization in AWS Organizations with all features enabled to manage the accounts. Create subaccounts to host each of the applications.
create sub accounts and cross-account roles
use AWS Systems Manager Session Manager to obtain shell access
Create an organization

Q849 A solutions architect has created a single VPC on AWS. The VPC has one internet gateway and one NAT gateway. The VPC extends across three Availability Zones. Each Availability Zone includes one public subnet and one private subnet. The three private subnets contain Amazon EC2 instances that must be able to connect to the internet. Which solution will increase the network resiliency of this architecture?
A. Add two NAT gateways so that each Availability Zone has a NAT gateway. Configure a route table for each private subnet to send traffic to the NAT gateway in the subnet's Availability Zone.
add two NAT gateways so that each AZ has a NAT gateway.Configure a route table for each private subnet

Q850 A company is building dozens of new workloads by using a variety of AWS services. Each workload will belong to a separate business unit. The company needs to minimize costs as each business unit experiments with ways to innovate. The company also needs to maximize scalability for its security team so that the security team can identify and respond to threats as quickly as possible for all the workloads. Which combination of actions should a solutions architect take to meet these requirements? (Choose three.)
A. Set up a multi-account environment by using AWS Organizations. Organize accounts into the following OUs: Security, Infrastructure, Workloads, and Exception.
D. Use AWS Budgets alerts to invoke an AWS Lambda function to move an AWS account that reaches a predefined budget threshold into the Exception OU. Apply an SCP to the Exception OU to limit usage to core services, including Amazon EC2, Amazon S3, and Amazon RDS.

F. Create a delegated administrator account for Amazon GuardDuty in the organization in AWS Organizations. Create an Amazon Simple Notification Service (Amazon SNS) topic in this account. Subscribe the security team to the topic so that the security team can receive alerts.
organize accounts into following OUs
use AWS Budgets alerts to invoke Lambda function
create a delegated administrator account for GuardDuty

Q851 A company is migrating its development and production workloads to a new organization in AWS Organizations. The company has created a separate member account for development and a separate member account for production. Consolidated billing is linked to the management account. In the management account, a solutions architect needs to create an IAM user that can stop or terminate resources in both member accounts. Which solution will meet this requirement?
A. Create an IAM user and a cross-account role in the management account. Configure the cross-account role with least privilege access to the member accounts.
create IAM user and cross-account role in management account

Q852 A company has introduced a new policy that allows employees to work remotely from their homes if they connect by using a VPN. The company is hosting internal applications with VPCs in multiple AWS accounts. Currently, the applications are accessible from the company's on-premises office network through an AWS Site- to-Site VPN connection. The VPC in the company's main AWS account has peering connections established with VPCs in other AWS accounts. A solutions architect must design a scalable AWS Client VPN solution for employees to use while they work from home. What is the MOST cost-effective solution that meets these requirements?
B. Create a Client VPN endpoint in the main AWS account. Configure required routing that allows access to internal applications.
create a Client VPN endpoint in main AWS account. Configure required routing

Q853 A company has set up a multi-account AWS environment by using AWS Control Tower. Each AWS account that AWS Control Tower creates has its own VPC.The company is developing an application that will integrate with many microservices. The company has designated a specific account to host the application. The company will deploy the microservices on Amazon EC2 instances and will implement the microservices across multiple AWS accounts. The microservices require a high degree of interconnectivity. The company needs a solution that will give the application the ability to communicate privately with the microservices. The solution also must minimize cost and operational overhead. Which solution will meet these requirements?
D. Share the application VPC with the other AWS accounts by using AWS Resource Access Manager (AWS RAM). Deploy the microservices in the shared VPC
share app VPC with other AWS accounts by using (RAM)

Q854 A company is running an image-processing service in the AWS Cloud. Users upload images to an Amazon S3 bucket for processing. When an image is uploaded to the S3 bucket, several microservices that are based on AWS Lambda functions need to perform different processing tasks on the image. Each task's processing must start immediately after an image is uploaded. Which solution will meet these requirements?

D. Create an S3 event notification with an Amazon Simple Notification Service (Amazon SNS) topic as the destination. Create an SNS subscription for each microservice's Lambda function.
create S3 event notification with SNS topic

Q855 A company has deployed its database on an Amazon RDS for MySQL DB instance in the us-east-1 Region. The company needs to make its data available to customers in Europe. The customers in Europe must have access to the same data as customers in the United States (US) and will not tolerate high application latency or stale data. The customers in Europe and the customers in the US need to write to the database. Both groups of customers need to see updates from the other group in real time. Which solution will meet these requirements?
A. Create an Amazon Aurora MySQL replica of the RDS for MySQL DB instance. Pause application writes to the RDS DB instance. Promote the Aurora Replica to a standalone DB cluster. Reconfigure the application to use the Aurora database and resume writes. Add eu-west-1 as a secondary Region to the 06 cluster. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1.
create Amazon Aurora MySQL replica of RDS for MySQL DB instance

Q856 A company wants to move an application from on premises to the AWS Cloud. The application uses MySQL servers to store backend data. However, the application does not scale properly. The databases have become unresponsive as the user base has increased. The company needs a solution to make the application highly available with low latency across multiple AWS Regions. The solution must require the least possible operational overhead and development effort. Which solution will meet these requirements?
C. Create an Amazon Aurora global database. Use native MySQL tools to migrate existing databases.
use native MySQL tools to migrate existing db

Q857 A company provides specialized analytics services to customers. The analytics run on Amazon EC2 instances that need to be launched and terminated in response to requests from customers. A solutions architect is creating automation to manage the EC2 instances that handle customer requests. However, when the automation scripts attempt to launch many EC2 instances at the same time, a RequestLimitExceeded error frequently occurs. What should the solutions architect do to handle this error?
A. Implement an exponential backoff strategy so that the API token bucket can refill
implement an exponential backoff strategy

Q858 A company has VPC flow logs enabled for its NAT gateway. The company is seeing Action =ACCEPT for inbound traffic that comes from public IP address 198.51.100.2 destined for a private Amazon EC2 instance.A solutions architect must determine whether the traffic represents unsolicited inbound connections from the internet. The first two octets of the VPC CIDR block are 203.0.Which set of steps should the solutions architect take to meet these requirements?
A. Open the AWS CloudTrail console. Select the log group that contains the NAT B. Open the Amazon CloudWatch console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the

destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address
open CloudWatch console. run a query to filter with destination “like 203.0” and source like “198.51.100.2”

Q859 A company is planning a migration from an on-premises data center to the AWS Cloud. The company plans to use multiple AWS accounts that are managed in an organization in AWS Organizations. The company will create a small number of accounts initially and will add accounts as needed. A solutions architect must design a solution that turns on AWS CloudTrail in all AWS accounts. What is the MOST operationally efficient solution that meets these requirements?
B. Create a new CloudTrail trail in the organization's management account. Configure the trail to log all events for all AWS accounts in the organization.
configure trail to log all events for all AWS accounts

Q860 A company has an organization in AWS Organizations. The company has enabled trusted access between Organizations and AWS Resource Access Manager (AWS RAM). The organization includes three AWS accounts, one each for shared services, development, and production. The shared services account has a VPC. A solutions architect needs to meet the following requirements: Configure access between the shared services VPC and the development and production accounts. * Ensure that workloads in each account are deployed to at least three Availability Zones. * Ensure that there is no direct communication between the development and production workloads. Which combination of steps will meet these requirements? (Choose three.)
B. In the shared services VPC, create six subnets for three Availability Zones. Create two subnets in each Availability Zone.
C. Configure network ACLs to prevent connectivity between the subnets in the development account and the production account.
F. Use AWS RAM to share three subnets in different Availability Zones with the development account. Additionally, use AWS RAM to share three
other subnets in different Availability Zones with the production account
create six subnets for 3 Availability zones
Configure network ACLs to prevent connectivity between subnet in dev account and prod account
use AWS RAM to share 3 other subnets in different AZ

Q861 An organization is planning to host a Wordpress blog as well as joomla CMS on a single instance launched with VPC. The organization wants to create separate domains for each application using Route 53. The organization may have about ten instances each with these two applications. While launching each instance, the organization configured two separate network interfaces (primary + secondary ENI) with their own Elastic IPs to the instance. The suggestion was to use a public IP from AWS instead of an Elastic IP as the number of elastic IPs allocation per region is restricted in the account. What action will you recommend to the organization?
A. Only Elastic IP can be used by requesting limit increase, since AWS does not assign a public IP to an instance with multiple ENIs. C. Set up the public website on a public subnet and set up the database in a private subnet which connects to the Internet via a NAT instance.
only Elastic IP can be used by requesting limit increase

Q862 You have been asked to set up a public website on AWS with the following criteria: You want the database and the application server running on an Amazon VPC. You want the database to be able to connect to the Internet so that it can be automatically updated to the correct patch level. You do not want to receive any incoming traffic from the Internet to the database. Which solutions would be the best to satisfy all the above requirements for your planned public website on AWS?
C. Set up the public website on a public subnet and set up the database in a private subnet which connects to the Internet via a NAT instance.
Public website on public subnet, db on private subnet

Q863 You need to develop and run some new applications on AWS and you know that Elastic Beanstalk and CloudFormation can both help as a deployment mechanism for a broad range of AWS resources. Which of the following is TRUE statements when describing the differences between Elastic Beanstalk and CloudFormation?
D. You can design and script custom resources in CloudFormation
you can design and script custom resources in CloudFormation

Q864 A user is using CloudFormation to launch an EC2 instance and then configure an application after the instance is launched. The user wants the stack creation of ELB and AutoScaling to wait until the EC2 instance is launched and configured properly. How can the user configure this?
D. The user can use the WaitCondition resource to hold the creation of the other dependent resources.
the user can use WaitCondition resource

Q865 You have a website which requires international presence and consequently you have set it up as follows. It is hosted on 30 EC2 instances. It is in 15 regions around the globe. Each region has 2 instances. all the instances are a public hosted zone. Which of the following is the best way to configure your site to maintain availability with minimum downtime if one of the 15 regions was to lose network connectivity for an extended period? (Choose two.)
A. Create a Route 53 Latency Based Routing Record set that resolves to an Elastic Load Balancer in each region and has the Evaluate Target Health
B. Create a Route 53 failover routing policy and configure an active-passive failover.
Create Route 53 Latency-based routing
Create Route 53 failover routing and configure active-passive failover.

Q866 ABC has created a multi-tenant Learning Management System (LMS). The application is hosted for five different tenants (clients) in the VPCs of the respective AWS accounts of the tenant. ABC wants to setup a centralized server which can connect with the LMS of each tenant upgrade if required. ABC also wants to ensure that one tenant VPC should not be able to connect to the other tenant VPC for security reasons. How can ABC setup this scenario?
A. ABC has to setup one centralized VPC which will peer in to all the other VPCs of the tenants.
ABC has to setup one centralized VPC which peer in to all other VPCs of tenants

Q867 A customer is deploying an SSL enabled web application to AWS and would like to implement a separation of roles between the EC2 service administrators that are entitled to login to instances as well as making API calls and the security officers who will maintain and have exclusive access to the application's X.509 certificate that contains the private key.
D. Configure IAM policies authorizing access to the certificate store only to the security officers and terminate SSL on an ELB
configure IAM policies authorizing access to certificate store only

Q868 You have recently joined a startup company building sensors to measure street noise and air quality in urban areas. The company has been running a pilot deployment of around 100 sensors for 3 months. Each sensor uploads 1KB of sensor data every minute to a backend hosted on AWS. During the pilot, you measured a peak or 10 IOPS on the database, and you stored an average of 3GB of sensor data per month in the database. The current deployment consists of a load-balanced auto scaled Ingestion layer using EC2 instances and a PostgreSQL RDS database with 500GB standard storage. The pilot is considered a success and your CEO has managed to get the attention or some potential investors. The business plan requires a deployment of at least 100K sensors which needs to be supported by the backend. You also need to store sensor data for at least two years to be able to compare year over year Improvements. To secure funding, you have to make sure that the platform meets these requirements and leaves room for further scaling. Which setup will meet the requirements?
B. Ingest data into a DynamoDB table and move old data to a Redshift cluster
ingest data into a DynamoDB table

Q869 Your firm has uploaded a large amount of aerial image data to S3. In the past, in your on-premises environment, you used a dedicated group of servers to oaten process this data and used Rabbit MQ -An open source messaging system to get job information to the servers. Once processed the data would go to tape and be shipped offsite. Your manager told you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost. Which is correct?
C. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS Once data is processed, change the storage class of the S3 objects to Glacier
setup Auto-Scaled workers. change storage class of S3 objects to Glacier

Q870 Your company is in the process of developing a next generation pet collar that collects biometric information to assist families with promoting healthy lifestyles for their pets. Each collar will push 30kb of biometric data in JSON format every 2 seconds to a collection platform that will process and analyze the data providing health trending information back to the pet owners and veterinarians via a web portal. Management has tasked you to architect the collection platform ensuring the following requirements are met. * Provide the ability for real-time analytics of the inbound biometric data; * Ensure processing of the biometric data is highly durable. Elastic and parallel;* The results of the analytic processing should be persisted for data mining ;. Which architecture outlined below win meet the initial requirements for the collection platform?
B. Utilize Amazon Kinesis to collect the inbound sensor data, analyze the data with Kinesis clients and save the results to a Redshift cluster using EMR
Utilize Amazon Kinesis to collect inbound sensor data

Q871 You are implementing AWS Direct Connect. You intend to use AWS public service endpoints such as Amazon S3, across the AWS Direct Connect link. You want other Internet traffic to use your existing link to an Internet Service Provider. What is the correct way to configure AWS Direct connect for access to services such as Amazon S3?

C. Create a public interface on your AWS Direct Connect link. Redistribute BGP routes into your existing routing infrastructure; advertise specific routes for your network to AWS.

advertise specific routes to AWS