



- Expert Verified, Online, **Free**.

Custom View Settings

Topic 1 - Exam A

Question #1

Topic 1

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 resources 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.
- B. Associate the private hosted zone to all the VPCs. Deploy an Amazon EC2 conditional forwarder 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 conditional forwarder.
- C. Associate the private hosted zone to the shared services VPC. Create a Route 53 outbound 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 outbound resolver.
- D. Associate the private hosted zone to the shared services VPC. Create a Route 53 inbound resolver in the shared services VPC. Attach the shared services VPC to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.

Question #2

Topic 1

A company is providing weather data over a REST-based API to several customers. The API is hosted by Amazon API Gateway and is integrated with different AWS Lambda functions for each API operation. The company uses Amazon Route 53 for DNS and has created a resource record of weather.example.com. The company stores data for the API in Amazon DynamoDB tables. The company needs a solution that will give the API the ability to fail over to a different AWS Region.

Which solution will meet these requirements?

- A. Deploy a new set of Lambda functions in a new Region. Update the API Gateway API to use an edge-optimized API endpoint with Lambda functions from both Regions as targets. Convert the DynamoDB tables to global tables.
- B. Deploy a new API Gateway API and Lambda functions in another Region. Change the Route 53 DNS record to a multivalue answer. Add both API Gateway APIs to the answer. Enable target health monitoring. Convert the DynamoDB tables to global tables.
- C. Deploy a new API Gateway API and Lambda functions in another Region. Change the Route 53 DNS record to a failover record. Enable target health monitoring. Convert the DynamoDB tables to global tables.
- D. Deploy a new API Gateway API in a new Region. Change the Lambda functions to global functions. Change the Route 53 DNS record to a multivalue answer. Add both API Gateway APIs to the answer. Enable target health monitoring. Convert the DynamoDB tables to global tables.

Question #3

Topic 1

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?

- A. Remove the organization's root SCPs that limit access to AWS Config. Create AWS Service Catalog products for the company's standard AWS Config rules and deploy them throughout the organization, including the new account.
- B. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to allow AWS Config actions. Move the new account to the Production OU when adjustments to AWS Config are complete.
- C. Convert the organization's root SCPs from deny list SCPs to allow list SCPs to allow the required services only. Temporarily apply an SCP to the organization's root that allows AWS Config actions for principals only in the new account.
- 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.

Question #4

Topic 1

A company is running a two-tier web-based application in an on-premises data center. The application layer 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?

- A. Enable Aurora Auto Scaling for Aurora Replicas. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.
- B. Enable Aurora Auto Scaling for Aurora writers. Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled.
- C. Enable Aurora Auto Scaling for Aurora Replicas. Use an Application Load Balancer with the round robin routing and sticky sessions enabled.
- D. Enable Aurora Scaling for Aurora writers. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.

Question #5

Topic 1

A company uses a service to collect metadata from applications that the company hosts on premises. Consumer devices such as TVs and internet radios access the applications. Many older devices do not support certain HTTP headers and exhibit errors when these headers are present in responses. The company has configured an on-premises load balancer to remove the unsupported headers from responses sent to older devices, which the company identified by the User-Agent headers.

The company wants to migrate the service to AWS, adopt serverless technologies, and retain the ability to support the older devices. The company has already migrated the applications into a set of AWS Lambda functions.

Which solution will meet these requirements?

- A. Create an Amazon CloudFront distribution for the metadata service. Create an Application Load Balancer (ALB). Configure the CloudFront distribution to forward requests to the ALB. Configure the ALB to invoke the correct Lambda function for each type of request. Create a CloudFront function to remove the problematic headers based on the value of the User-Agent header.
- B. Create an Amazon API Gateway REST API for the metadata service. Configure API Gateway to invoke the correct Lambda function for each type of request. Modify the default gateway responses to remove the problematic headers based on the value of the User-Agent header.
- C. Create an Amazon API Gateway HTTP API for the metadata service. Configure API Gateway to invoke the correct Lambda function for each type of request. Create a response mapping template to remove the problematic headers based on the value of the User-Agent. Associate the response data mapping with the HTTP API.
- D. Create an Amazon CloudFront distribution for the metadata service. Create an Application Load Balancer (ALB). Configure the CloudFront distribution to forward requests to the ALB. Configure the ALB to invoke the correct Lambda function for each type of request. Create a Lambda@Edge function that will remove the problematic headers in response to viewer requests based on the value of the User-Agent header.

Question #6

Topic 1

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.)

A. Turn on the cross-origin resource sharing (CORS) feature for the S3 bucket in Account A.

B. In Account A, set the S3 bucket policy to the following:

```
{  
    "Effect": "Allow",  
    "Action": [  
        "s3:GetObject",  
        "s3>ListBucket"  
    ],  
    "Resource": "arn:aws:s3:::AccountABucketName/*"  
}
```

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/*"  
}
```

E. In Account B, set the permissions of User_DataProcessor to the following:

```
{  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"  
    },  
    "Action": [  
        "s3:GetObject",  
        "s3>ListBucket"  
    ],  
    "Resource": [  
        "arn:aws:s3:::AccountABucketName/*"  
    ]  
}
```

Question #7

Topic 1

A company is running a traditional web application on Amazon EC2 instances. The company needs to refactor the application as microservices that run on containers. Separate versions of the application exist in two distinct environments: production and testing. Load for the application is variable, but the minimum load and the maximum load are known. A solutions architect needs to design the updated application with a serverless architecture that minimizes operational complexity.

Which solution will meet these requirements MOST cost-effectively?

- A. Upload the container images to AWS Lambda as functions. Configure a concurrency limit for the associated Lambda functions to handle the expected peak load. Configure two separate Lambda integrations within Amazon API Gateway: one for production and one for testing.
- B. Upload the container images to Amazon Elastic Container Registry (Amazon ECR). Configure two auto scaled Amazon Elastic Container Service (Amazon ECS) clusters with the Fargate launch type to handle the expected load. Deploy tasks from the ECR images. Configure two separate Application Load Balancers to direct traffic to the ECS clusters.
- C. Upload the container images to Amazon Elastic Container Registry (Amazon ECR). Configure two auto scaled Amazon Elastic Kubernetes Service (Amazon EKS) clusters with the Fargate launch type to handle the expected load. Deploy tasks from the ECR images. Configure two separate Application Load Balancers to direct traffic to the EKS clusters.
- D. Upload the container images to AWS Elastic Beanstalk. In Elastic Beanstalk, create separate environments and deployments for production and testing. Configure two separate Application Load Balancers to direct traffic to the Elastic Beanstalk deployments.

Question #8

Topic 1

A company has a multi-tier web application that runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The ALB and the Auto Scaling group are replicated in a backup AWS Region. The minimum value and the maximum value for the Auto Scaling group are set to zero. An Amazon RDS Multi-AZ DB instance stores the application's data. The DB instance has a read replica in the backup Region. The application presents an endpoint to end users by using an Amazon Route 53 record.

The company needs to reduce its RTO to less than 15 minutes by giving the application the ability to automatically fail over to the backup Region. The company does not have a large enough budget for an active-active strategy.

What should a solutions architect recommend to meet these requirements?

- A. Reconfigure the application's Route 53 record with a latency-based routing policy that load balances traffic between the two ALBs. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Create an Amazon CloudWatch alarm that is based on the HTTPCode_Target_5XX_Count metric for the ALB in the primary Region. Configure the CloudWatch alarm to invoke the Lambda function.
- B. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Configure Route 53 with a health check that monitors the web application and sends an Amazon Simple Notification Service (Amazon SNS) notification to the Lambda function when the health check status is unhealthy. Update the application's Route 53 record with a failover policy that routes traffic to the ALB in the backup Region when a health check failure occurs.
- C. Configure the Auto Scaling group in the backup Region to have the same values as the Auto Scaling group in the primary Region. Reconfigure the application's Route 53 record with a latency-based routing policy that load balances traffic between the two ALBs. Remove the read replica. Replace the read replica with a standalone RDS DB instance. Configure Cross-Region Replication between the RDS DB instances by using snapshots and Amazon S3.
- D. Configure an endpoint in AWS Global Accelerator with the two ALBs as equal weighted targets. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Create an Amazon CloudWatch alarm that is based on the HTTPCode_Target_5XX_Count metric for the ALB in the primary Region. Configure the CloudWatch alarm to invoke the Lambda function.

Question #9

Topic 1

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? (Choose three.)

- A. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances. Ensure that the EC2 instances are part of an Auto Scaling group that has a minimum capacity of two instances.
- B. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances. Ensure that the EC2 instances are configured in unlimited mode.
- 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.
- F. Create a replication group for the ElastiCache for Redis cluster. Enable Multi-AZ on the cluster.

Question #10

Topic 1

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.
- B. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Target.FailedHealthChecks is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a publicly accessible web server.
- C. Modify the existing Amazon Route 53 records by adding health checks. Configure a fallback target if the health check fails. Modify DNS records to point to a publicly accessible webpage.
- D. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Elb.InternalError is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a public accessible web server.
- E. Add a custom error response by configuring a CloudFront custom error page. Modify DNS records to point to a publicly accessible web page.

Question #11

Topic 1

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? (Choose two.)

- A. Create a transit gateway in the infrastructure account.
- B. Enable resource sharing from the AWS Organizations management account.
- C. Create VPCs in each AWS account within the organization in AWS Organizations. Configure the VPCs to share the same CIDR range and subnets as the VPC in the infrastructure account. Peer the VPCs in each individual account with the VPC in the infrastructure 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.
- E. 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 prefix list to associate with the resource share.

Question #12

Topic 1

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.
- B. Create an AWS Site-to-Site VPN connection between the third-party SaaS application and the company VPC. Configure network ACLs to limit access across the VPN tunnels.
- C. Create a VPC peering connection between the third-party SaaS application and the company VPC. Update route tables by adding the needed routes for the peering connection.
- D. Create an AWS PrivateLink endpoint service. Ask the third-party SaaS provider to create an interface VPC endpoint for this endpoint service. Grant permissions for the endpoint service to the specific account of the third-party SaaS provider.

Question #13

Topic 1

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.
- B. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances. Use Amazon QuickSight integration with OpsWorks to generate patch compliance reports.
- C. Use an Amazon EventBridge rule to apply patches by scheduling an AWS Systems Manager patch remediation job. Use Amazon Inspector to generate patch compliance reports.
- D. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances. Use AWS X-Ray to post the patch status to AWS Systems Manager OpsCenter to generate patch compliance reports.

Question #14

Topic 1

A company is running an application on several Amazon EC2 instances in 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?

- A. Create a script to copy log files to Amazon S3, and store the script in a file on the EC2 instance. Create an Auto Scaling lifecycle hook and an Amazon EventBridge rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to send ABANDON to the Auto Scaling group to prevent termination, run the script to copy the log files, and terminate the instance using the AWS SDK.
- 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 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.
- C. Change the log delivery rate to every 5 minutes. Create a script to copy log files to Amazon S3, and add the script to EC2 instance user data. Create an Amazon EventBridge rule to detect EC2 instance termination. Invoke an AWS Lambda function from the EventBridge rule that uses the AWS CLI to run the user-data script to copy the log files and terminate the instance.
- D. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook that publishes a message to an Amazon Simple Notification Service (Amazon SNS) topic. From the SNS notification, call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send ABANDON to the Auto Scaling group to terminate the instance.

Question #15

Topic 1

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.)

- A. Deploy the database on a separate EC2 instance in the new VPC. Create a record set for the instance's private IP in the private hosted zone.
- B. Use SSH to connect to the application tier EC2 instance. Add an RDS endpoint IP address to the /etc/resolv.conf file.
- C. Create an authorization to associate the private hosted zone in Account A with the new VPC in Account B.
- D. Create a private hosted zone for the example com domain in Account B. Configure Route 53 replication between AWS accounts.
- E. Associate a new VPC in Account B with a hosted zone in Account A. Delete the association authorization in Account A.

Question #16

Topic 1

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 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?

- A. Reconfigure Amazon EFS to enable maximum I/O.
- B. Update the blog site to use instance store volumes for storage. Copy the site contents to the volumes at launch and to Amazon S3 at shutdown.
- C. Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.
- D. Set up an Amazon CloudFront distribution for all site contents, and point the distribution at the ALB.

Question #17

Topic 1

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 interface on each connection, and connect both private virtual interfaces to the Direct Connect gateway. Connect the Direct Connect gateway to the single VPC.
- B. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC.
- C. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new public virtual interface on the new connection, and connect the new public virtual interface to the single VPC.
- D. Provision a transit gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gateway. Associate the transit gateway with the single VPC.

Question #18

Topic 1

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?

- A. Use Amazon ECS containers for the web application and Spot instances for the Auto Scaling group that processes the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.
- B. Store the uploaded videos in Amazon EFS and mount the file system to the EC2 instances for the web application. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
- 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.
- D. Use AWS Elastic Beanstalk to launch EC2 instances in an Auto Scaling group for the web application and launch a worker environment to process the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.

Question #19

Topic 1

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 reverts 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?

- A. Create and deploy nested AWS CloudFormation stacks with the parent stack consisting of the AWS CloudFront distribution and API Gateway, and the child stack containing the Lambda function. For changes to Lambda, create an AWS CloudFormation change set and deploy; if errors are triggered, revert the AWS CloudFormation change set to the previous version.
- 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 CloudWatch alarms are triggered.
- C. Refactor the AWS CLI scripts into a single script that deploys the new Lambda version. When deployment is completed, the script tests execute. If errors are detected, revert to the previous Lambda version.
- D. Create and deploy an AWS CloudFormation stack that consists of a new API Gateway endpoint that references the new Lambda version. Change the CloudFront origin to the new API Gateway endpoint, monitor errors and if detected, change the AWS CloudFront origin to the previous API Gateway endpoint.

Question #20

Topic 1

A company is planning to store a large number of archived documents and make the documents available to employees through the corporate intranet. Employees will access the system by connecting through a client VPN service that is attached to a VPC. The data must not be accessible to the public.

The documents that the company is storing are copies of data that is held on physical media elsewhere. The number of requests will be low. Availability and speed of retrieval are not concerns of the company.

Which solution will meet these requirements at the LOWEST cost?

- A. Create an Amazon S3 bucket. Configure the S3 bucket to use the S3 One Zone-Infrequent Access (S3 One Zone-IA) storage class as default. Configure the S3 bucket for website hosting. Create an S3 interface endpoint. Configure the S3 bucket to allow access only through that endpoint.
- B. Launch an Amazon EC2 instance that runs a web server. Attach an Amazon Elastic File System (Amazon EFS) file system to store the archived data in the EFS One Zone-Infrequent Access (EFS One Zone-IA) storage class. Configure the instance security groups to allow access only from private networks.
- C. Launch an Amazon EC2 instance that runs a web server. Attach an Amazon Elastic Block Store (Amazon EBS) volume to store the archived data. Use the Cold HDD (sc1) volume type. Configure the instance security groups to allow access only from private networks.
- D. Create an Amazon S3 bucket. Configure the S3 bucket to use the S3 Glacier Deep Archive storage class as default. Configure the S3 bucket for website hosting. Create an S3 interface endpoint. Configure the S3 bucket to allow access only through that endpoint.

Question #21

Topic 1

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 IAM Identity Center (AWS Single Sign-On) 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).
- B. Configure AWS IAM Identity Center (AWS Single Sign-On) by using IAM Identity Center as an identity source. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol. Grant access to the AWS accounts by using IAM Identity Center permission sets.
- C. In one of the company's AWS accounts, configure AWS Identity and Access Management (IAM) to use a SAML 2.0 identity provider. Provision IAM users that are mapped to the federated users. Grant access that corresponds to appropriate groups in Active Directory. Grant access to the required AWS accounts by using cross-account IAM users.
- D. In one of the company's AWS accounts, configure AWS Identity and Access Management (IAM) to use an OpenID Connect (OIDC) identity provider. Provision IAM roles that grant access to the AWS account for the federated users that correspond to appropriate groups in Active Directory. Grant access to the required AWS accounts by using cross-account IAM roles.

Question #22

Topic 1

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?

- A. Implement retry logic with exponential backoff and irregular variation in the client application. Ensure that the errors are caught and handled with descriptive error messages.
- B. Implement API throttling through a usage plan at the API Gateway level. Ensure that the client application handles code 429 replies without error.
- C. Turn on API caching to enhance responsiveness for the production stage. Run 10-minute load tests. Verify that the cache capacity is appropriate for the workload.
- D. Implement reserved concurrency at the Lambda function level to provide the resources that are needed during sudden increases in traffic.

Question #23

Topic 1

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 compute 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.
- B. Migrate the data from the existing shared file system to a large Amazon Elastic Block Store (Amazon EBS) volume with Multi-Attach enabled. Attach the EBS volume to each of the instances by using a user data script in the Auto Scaling group launch template. Use the EBS volume as the shared storage for the duration of the job. Detach the EBS volume when the job is complete
- C. Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Standard 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 batch 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.
- D. Migrate the data from the existing shared file system to an Amazon S3 bucket. Before the job runs each month, use AWS Storage Gateway to create a file gateway with the data from Amazon S3. Use the file gateway as the shared storage for the job. Delete the file gateway when the job is complete.

Question #24

Topic 1

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?

- A. Create Amazon EC2 instances with an Elastic IP address for each instance. Create a Network Load Balancer (NLB) and expose the static TCP port. Register EC2 instances with the NLB. Create a new name server record set named my.service.com, and assign the Elastic IP addresses of the EC2 instances to the record set. Provide the Elastic IP addresses of the EC2 instances to the other companies to add to their allow lists.
- B. Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP addresses for the ECS cluster. Create a Network Load Balancer (NLB) and expose the TCP port. Create a target group and assign the ECS cluster name to the NLB. Create a new A record set named my.service.com, and assign the public IP addresses of the ECS cluster to the record set. Provide the public IP addresses of the ECS cluster to the other companies to add to their allow lists.
- 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.
- D. Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP address for each host in the cluster. Create an Application Load Balancer (ALB) and expose the static TCP port. Create a target group and assign the ECS service definition name to the ALB. Create a new CNAME record set and associate the public IP addresses to the record set. Provide the Elastic IP addresses of the Amazon EC2 instances to the other companies to add to their allow lists.

Question #25

Topic 1

A company uses an on-premises data analytics platform. The system is highly available in a fully redundant configuration across 12 servers in the company's data center.

The system runs scheduled jobs, both hourly and daily, in addition to one-time requests from users. Scheduled jobs can take between 20 minutes and 2 hours to finish running and have tight SLAs. The scheduled jobs account for 65% of the system usage. User jobs typically finish running in less than 5 minutes and have no SLA. The user jobs account for 35% of system usage. During system failures, scheduled jobs must continue to meet SLAs. However, user jobs can be delayed.

A solutions architect needs to move the system to Amazon EC2 instances and adopt a consumption-based model to reduce costs with no long-term commitments. The solution must maintain high availability and must not affect the SLAs.

Which solution will meet these requirements MOST cost-effectively?

- A. Split the 12 instances across two Availability Zones in the chosen AWS Region. Run two instances in each Availability Zone as On-Demand Instances with Capacity Reservations. Run four instances in each Availability Zone as Spot Instances.
- B. Split the 12 instances across three Availability Zones in the chosen AWS Region. In one of the Availability Zones, run all four instances as On-Demand Instances with Capacity Reservations. Run the remaining instances as Spot Instances.
- C. Split the 12 instances across three Availability Zones in the chosen AWS Region. Run two instances in each Availability Zone as On-Demand Instances with a Savings Plan. Run two instances in each Availability Zone as Spot Instances.
- D. Split the 12 instances across three Availability Zones in the chosen AWS Region. Run three instances in each Availability Zone as On-Demand Instances with Capacity Reservations. Run one instance in each Availability Zone as a Spot Instance.

Question #26

Topic 1

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.
- B. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Create an AWS Lambda function resource to rotate the database password. Specify a Parameter Store RotationSchedule resource to rotate the database password every 90 days.
- C. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Create an Amazon EventBridge scheduled rule resource to trigger the Lambda function password rotation every 90 days.
- D. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Specify an AWS AppSync DataSource resource to automatically rotate the database password every 90 days.

Question #27

Topic 1

A company is storing data in several Amazon DynamoDB tables. A solutions architect must use a serverless architecture to make the data accessible publicly through a simple API over HTTPS. The solution must scale automatically in response to demand. Which solutions meet these requirements? (Choose two.)

- A. Create an Amazon API Gateway REST API. Configure this API with direct integrations to DynamoDB by using API Gateway's AWS integration type.
- B. Create an Amazon API Gateway HTTP API. Configure this API with direct integrations to DynamoDB by using API Gateway's AWS integration type.
- C. Create an Amazon API Gateway HTTP API. Configure this API with integrations to AWS Lambda functions that return data from the DynamoDB tables.
- D. Create an accelerator in AWS Global Accelerator. Configure this accelerator with AWS Lambda@Edge function integrations that return data from the DynamoDB tables.
- E. Create a Network Load Balancer. Configure listener rules to forward requests to the appropriate AWS Lambda functions.

Question #28

Topic 1

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.)

- A. Create a dynamic webpage that runs on an Amazon EC2 instance. Configure the webpage to use the JSON document in combination with the event message to look up and respond with a redirect URL.
- B. Create an Application Load Balancer that includes HTTP and HTTPS listeners.
- 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.
- D. Use an Amazon API Gateway API with a custom domain to publish an AWS Lambda function.
- 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.

Question #29

Topic 1

A company that has multiple AWS accounts is using AWS Organizations. The company's AWS accounts host VPCs, Amazon EC2 instances, and containers.

The company's compliance team has deployed a security tool in each VPC where the company has deployments. The security tools run on EC2 instances and send information to the AWS account that is dedicated for the compliance team. The company has tagged all the compliance-related resources with a key of "costCenter" and a value or "compliance".

The company wants to identify the cost of the security tools that are running on the EC2 instances so that the company can charge the compliance team's AWS account. The cost calculation must be as accurate as possible.

What should a solutions architect do to meet these requirements?

- A. In the management account of the organization, activate the costCenter user-defined tag. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account. Use the tag breakdown in the report to obtain the total cost for the costCenter tagged resources.
- B. In the member accounts of the organization, activate the costCenter user-defined tag. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account. Schedule a monthly AWS Lambda function to retrieve the reports and calculate the total cost for the costCenter tagged resources.
- C. In the member accounts of the organization activate the costCenter user-defined tag. From the management account, schedule a monthly AWS Cost and Usage Report. Use the tag breakdown in the report to calculate the total cost for the costCenter tagged resources.
- D. Create a custom report in the organization view in AWS Trusted Advisor. Configure the report to generate a monthly billing summary for the costCenter tagged resources in the compliance team's AWS account.

Question #30

Topic 1

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? (Choose two.)

- A. From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager.
- B. From the management account, share the transit gateway with member accounts by using an AWS Organizations SCP.
- C. Launch an AWS CloudFormation stack set from the management 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 management account by using the transit gateway ID.
- D. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a peering transit gateway attachment in a member account. Share the attachment with the transit gateway in the management account by using a transit gateway service-linked role.
- E. From the management account, share the transit gateway with member accounts by using AWS Service Catalog.

Question #31

Topic 1

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 organizational 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 and use Private Marketplace in AWS Marketplace to achieve this requirement. The procurement team wants administration of Private Marketplace to be restricted to a role named procurement-manager-role, which could be assumed by procurement managers. Other IAM users, groups, roles, and account administrators in the company should be denied Private Marketplace administrative access.

What is the MOST efficient way to design an architecture to meet these requirements?

- A. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the PowerUserAccess managed policy to the role. Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.
- B. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the AdministratorAccess managed policy to the role. Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.
- C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization. Add the AWSPrivateMarketplaceAdminFullAccess 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.
- D. Create an IAM role named procurement-manager-role in all AWS accounts that will be used by developers. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Apply the SCP to all the shared services accounts in the organization.

Question #32

Topic 1

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:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowEC2",  
            "Effect": "Allow",  
            "Action": "ec2:*",  
            "Resource": "*"  
        },  
        {  
            "Sid": "AllowDynamoDB",  
            "Effect": "Allow",  
            "Action": "dynamodb:*",  
            "Resource": "*"  
        },  
        {  
            "Sid": "AllowS3",  
            "Effect": "Allow",  
            "Action": "s3:*",  
            "Resource": "*"  
        }  
    ]  
}
```

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?

- A. Create an explicit deny statement for each AWS service that should be constrained.
- B. Remove the FullAWSAccess SCP from the developers account's OU.
- C. Modify the FullAWSAccess SCP to explicitly deny all services.
- D. Add an explicit deny statement using a wildcard to the end of the SCP.

Question #33

Topic 1

A company is hosting a monolithic REST-based API for a mobile app on five Amazon EC2 instances in public subnets of a VPC. Mobile clients connect to the API by using a domain name that is hosted on Amazon Route 53. The company has created a Route 53 multivalue answer routing policy with the IP addresses of all the EC2 instances. Recently, the app has been overwhelmed by large and sudden increases to traffic. The app has not been able to keep up with the traffic.

A solutions architect needs to implement a solution so that the app can handle the new and varying load.

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

- A. Separate the API into individual AWS Lambda functions. Configure an Amazon API Gateway REST API with Lambda integration for the backend. Update the Route 53 record to point to the API Gateway API.
- B. Containerize the API logic. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Run the containers in the cluster by using Amazon EC2. Create a Kubernetes ingress. Update the Route 53 record to point to the Kubernetes ingress.
- C. Create an Auto Scaling group. Place all the EC2 instances in the Auto Scaling group. Configure the Auto Scaling group to perform scaling actions that are based on CPU utilization. Create an AWS Lambda function that reacts to Auto Scaling group changes and updates the Route 53 record.
- D. Create an Application Load Balancer (ALB) in front of the API. Move the EC2 instances to private subnets in the VPC. Add the EC2 instances as targets for the ALB. Update the Route 53 record to point to the ALB.

Question #34

Topic 1

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?

- A. Create an AWS Cost and Usage Report (CUR) for each OU by using AWS Resource Access Manager. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- 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.
- C. Create an AWS Cost and Usage Report (CUR) in each AWS Organizations member account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- D. Create an AWS Cost and Usage Report (CUR) by using AWS Systems Manager. Allow each team to visualize the CUR through Systems Manager OpsCenter dashboards.

Question #35

Topic 1

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?

- A. Use the file gateway option in AWS Storage Gateway to replace the existing Windows file server, and point the existing file share to the new file gateway.
- B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.
- C. Use AWS Data Pipeline to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).
- D. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).

Question #36

Topic 1

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?

- A. Configure the application to write each object to both S3 buckets. Set up an Amazon Route 53 public hosted zone with a record set by using a weighted routing policy for each S3 bucket. Configure the application to reference the objects by using the Route 53 DNS name.
- B. Create an AWS Lambda function to copy objects from the S3 bucket in us-east-1 to the S3 bucket in the second Region. Invoke the Lambda function each time an object is written to the S3 bucket in us-east-1. Set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins.
- C. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region. Set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins.
- 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.

Question #37

Topic 1

A company is hosting a three-tier web application in an on-premises environment. Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in .NET and has a dependency on a MySQL database. A solutions architect must design a scalable and highly available solution to meet the demand of 200,000 daily users.

Which steps should the solutions architect take to design an appropriate solution?

- A. Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance. The environment should launch a Network Load Balancer (NLB) in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones. Use an Amazon Route 53 alias record to route traffic from the company's domain to the NLB.
- 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.
- C. Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer (ALB) in each Region. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica. Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions.
- D. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon ECS cluster of Spot instances spanning three Availability Zones. The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

Question #38

Topic 1

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 Organizations member accounts.

A solutions architect used an AWS CloudFormation template to create the SNS topic and stack sets to automate the deployment of CloudFormation stacks. Trusted access has been enabled in Organizations.

What should the solutions architect do to deploy the CloudFormation StackSets in all AWS accounts?

- A. Create a stack set in the Organizations member accounts. Use service-managed permissions. Set deployment options to deploy to an organization. Use CloudFormation StackSets drift detection.
- B. Create stacks in the Organizations member accounts. Use self-service permissions. Set deployment options to deploy to an organization. Enable the CloudFormation StackSets automatic deployment.
- C. Create a stack set in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.
- D. Create stacks in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection.

Question #39

Topic 1

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 processes, and network connections of its on-premises workloads. 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? (Choose three.)

- A. Assess the existing applications by installing AWS Application Discovery Agent on the physical machines and VMs.
- B. Assess the existing applications by installing AWS Systems Manager Agent on the physical machines and VMs.
- C. Group servers into applications for migration by using AWS Systems Manager Application Manager.
- D. Group servers into applications for migration by using AWS Migration Hub.
- E. Generate recommended instance types and associated costs by using AWS Migration Hub.
- F. Import data about server sizes into AWS Trusted Advisor. Follow the recommendations for cost optimization.

Question #40

Topic 1

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?

- A. Replace the NAT gateways with NAT instances. In the VPC route table, create a route from the private subnets to the NAT instances.
- B. Move the EC2 instances to the public subnets. Remove the NAT gateways.
- C. Set up an S3 gateway VPC endpoint in the VPAttach an endpoint policy to the endpoint to allow the required actions on the S3 bucket.
- D. Attach an Amazon Elastic File System (Amazon EFS) volume to the EC2 instances. Host the images on the EFS volume.

Question #41

Topic 1

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 for 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?

- A. Use AWS Application Auto Scaling to increase capacity during the peak period. Purchase reserved RCUs and WCUs to match the average load.
- B. Configure on-demand capacity mode for the table.
- C. Configure DynamoDB Accelerator (DAX) in front of the table. Reduce the provisioned read capacity to match the new peak load on the table.
- D. Configure DynamoDB Accelerator (DAX) in front of the table. Configure on-demand capacity mode for the table.

Question #42

Topic 1

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?

- A. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in an Amazon S3 bucket.
- B. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the files. Store the processed files in Amazon EFS. Shut down the EC2 instance after the task is complete.
- C. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in Amazon EFS.
- 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 Scaling 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.

Question #43

Topic 1

A company is using Amazon OpenSearch Service to analyze data. The company loads data into an OpenSearch Service cluster with 10 data nodes from an Amazon S3 bucket that uses S3 Standard storage. The data resides in the cluster for 1 month for read-only analysis. After 1 month, the company deletes the index that contains the data from the cluster. For compliance purposes, the company must retain a copy of all input data.

The company is concerned about ongoing costs and asks a solutions architect to recommend a new solution.

Which solution will meet these requirements MOST cost-effectively?

- A. Replace all the data nodes with UltraWarm nodes to handle the expected capacity. Transition the input data from S3 Standard to S3 Glacier Deep Archive when the company loads the data into the cluster.
- B. Reduce the number of data nodes in the cluster to 2 Add UltraWarm nodes to handle the expected capacity. Configure the indexes to transition to UltraWarm when OpenSearch Service ingests the data. Transition the input data to S3 Glacier Deep Archive after 1 month by using an S3 Lifecycle policy.
- C. Reduce the number of data nodes in the cluster to 2. Add UltraWarm nodes to handle the expected capacity. Configure the indexes to transition to UltraWarm when OpenSearch Service ingests the data. Add cold storage nodes to the cluster Transition the indexes from UltraWarm to cold storage. Delete the input data from the S3 bucket after 1 month by using an S3 Lifecycle policy.
- D. Reduce the number of data nodes in the cluster to 2. Add instance-backed data nodes to handle the expected capacity. Transition the input data from S3 Standard to S3 Glacier Deep Archive when the company loads the data into the cluster.

Question #44

Topic 1

A company has 10 accounts that are part of an organization in AWS Organizations. AWS Config is configured in each account. All accounts belong to either the Prod OU or the NonProd OU.

The company has set up an Amazon EventBridge rule in each AWS account to notify an Amazon Simple Notification Service (Amazon SNS) topic when an Amazon EC2 security group inbound rule is created with 0.0.0.0/0 as the source. The company's security team is subscribed to the SNS topic.

For all accounts in the NonProd OU, the security team needs to remove the ability to create a security group inbound rule that includes 0.0.0.0/0 as the source.

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

- A. Modify the EventBridge rule to invoke an AWS Lambda function to remove the security group inbound rule and to publish to the SNS topic. Deploy the updated rule to the NonProd OU.
- B. Add the vpc-sg-open-only-to-authorized-ports AWS Config managed rule to the NonProd OU.
- C. Configure an SCP to allow the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:Sourcelp condition key is not 0.0.0.0/0. Apply the SCP to the NonProd OU.
- D. Configure an SCP to deny the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:Sourcelp condition key is 0.0.0.0/0. Apply the SCP to the NonProd OU.

Question #45

Topic 1

A company hosts a Git repository in an on-premises data center. The company uses webhooks to invoke functionality that runs in the AWS Cloud. The company hosts the webhook logic on a set of Amazon EC2 instances in an Auto Scaling group that the company set as a target for an Application Load Balancer (ALB). The Git server calls the ALB for the configured webhooks. The company wants to move the solution to a serverless architecture.

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

- A. For each webhook, create and configure an AWS Lambda function URL. Update the Git servers to call the individual Lambda function URLs.
- B. Create an Amazon API Gateway HTTP API. Implement each webhook logic in a separate AWS Lambda function. Update the Git servers to call the API Gateway endpoint.
- C. Deploy the webhook logic to AWS App Runner. Create an ALB, and set App Runner as the target. Update the Git servers to call the ALB endpoint.
- D. Containerize the webhook logic. Create an Amazon Elastic Container Service (Amazon ECS) cluster, and run the webhook logic in AWS Fargate. Create an Amazon API Gateway REST API, and set Fargate as the target. Update the Git servers to call the API Gateway endpoint.

Question #46

Topic 1

A company is planning to migrate 1,000 on-premises servers to AWS. The servers run on several VMware clusters in the company's data center. As part of the migration plan, the company wants to gather server metrics such as CPU details, RAM usage, operating system information, and running processes. The company then wants to query and analyze the data.

Which solution will meet these requirements?

- A. Deploy and configure the AWS Agentless Discovery Connector virtual appliance on the on-premises hosts. Configure Data Exploration in AWS Migration Hub. Use AWS Glue to perform an ETL job against the data. Query the data by using Amazon S3 Select.
- B. Export only the VM performance information from the on-premises hosts. Directly import the required data into AWS Migration Hub. Update any missing information in Migration Hub. Query the data by using Amazon QuickSight.
- C. Create a script to automatically gather the server information from the on-premises hosts. Use the AWS CLI to run the put-resource-attributes command to store the detailed server data in AWS Migration Hub. Query the data directly in the Migration Hub console.
- D. Deploy the AWS Application Discovery Agent to each on-premises server. Configure Data Exploration in AWS Migration Hub. Use Amazon Athena to run predefined queries against the data in Amazon S3.

Question #47

Topic 1

A company is building a serverless application that runs on an AWS Lambda function that is attached to a VPC. The company needs to integrate the application with a new service from an external provider. The external provider supports only requests that come from public IPv4 addresses that are in an allow list.

The company must provide a single public IP address to the external provider before the application can start using the new service.

Which solution will give the application the ability to access the new service?

- A. Deploy a NAT gateway. Associate an Elastic IP address with the NAT gateway. Configure the VPC to use the NAT gateway.
- B. Deploy an egress-only internet gateway. Associate an Elastic IP address with the egress-only internet gateway. Configure the elastic network interface on the Lambda function to use the egress-only internet gateway.
- C. Deploy an internet gateway. Associate an Elastic IP address with the internet gateway. Configure the Lambda function to use the internet gateway.
- D. Deploy an internet gateway. Associate an Elastic IP address with the internet gateway. Configure the default route in the public VPC route table to use the internet gateway.

Question #48

Topic 1

A solutions architect has developed a web application that uses an Amazon API Gateway Regional endpoint and an AWS Lambda function. The consumers of the web application are all close to the AWS Region where the application will be deployed. The Lambda function only queries an Amazon Aurora MySQL database. The solutions architect has configured the database to have three read replicas.

During testing, the application does not meet performance requirements. Under high load, the application opens a large number of database connections. The solutions architect must improve the application's performance.

Which actions should the solutions architect take to meet these requirements? (Choose two.)

- A. Use the cluster endpoint of the Aurora database.
- B. Use RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database.
- C. Use the Lambda Provisioned Concurrency feature.
- D. Move the code for opening the database connection in the Lambda function outside of the event handler.
- E. Change the API Gateway endpoint to an edge-optimized endpoint.

Question #49

Topic 1

A company is planning to host a web application on AWS and wants to load balance 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?

- A. 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. Export the 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.
- B. Associate the EC2 instances with a target group. Provision an SSL certificate using AWS Certificate Manager (ACM). Create an Amazon CloudFront distribution and configure it to use the SSL certificate. Set CloudFront to use the target group as the origin server.
- 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.
- D. Place the EC2 instances behind a Network Load Balancer (NLB). Provision a third-party SSL certificate and install it on the NLB and on each EC2 instance. Configure the NLB to listen on port 443 and to forward traffic to port 443 on the instances.

Question #50

Topic 1

A company wants to migrate its data analytics 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 data 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 these requirements?

- A. Set up an Amazon Aurora MySQL database as a replication target for the on-premises database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind a Network Load Balancer (NLB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the NLB.
- B. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Move the aggregation jobs to run against the Aurora MySQL database. Set up collection endpoints behind an Application Load Balancer (ALB) as Amazon EC2 instances in an Auto Scaling group. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.
- C. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind an Application Load Balancer (ALB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.
- D. Set up an Amazon Aurora MySQL database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as an Amazon Kinesis data stream. Use Amazon Kinesis Data Firehose to replicate the data to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the Kinesis data stream.

Question #51

Topic 1

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.
- B. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to deny unencrypted PutObject requests. Use the AWS CLI to re-upload all objects in the S3 bucket.
- C. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to automatically encrypt objects on GetObject and PutObject requests.
- D. In the S3 bucket properties, change the default encryption to AES-256 with a customer managed key. Attach a policy to deny unencrypted PutObject requests to any entities that access the S3 bucket. Use the AWS CLI to re-upload all objects in the S3 bucket.

Question #52

Topic 1

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?

- A. Provision a full, secondary application deployment in a different AWS Region. Update the Route 53 A record to be a failover record. Add both of the CloudFront distributions as values. Create Route 53 health checks.
- 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.
- C. Provision an Auto Scaling group and EC2 instances in a different AWS Region. Create a second target for the new Auto Scaling group in the ALB. Set up the failover routing algorithm on the ALB.
- D. Provision a full, secondary application deployment in a different AWS Region. Create a second CloudFront distribution, and add the new application setup as an origin. Create an AWS Global Accelerator accelerator. Add both of the CloudFront distributions as endpoints.

Question #53

Topic 1

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 enabled 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?

- A. Create a JSON file that is hosted in Amazon S3 and that lists all of the internal IP address ranges. Configure an Amazon Simple Notification Service (Amazon SNS) topic in each of the accounts that can be invoked when the JSON file is updated. Subscribe an AWS Lambda function to the SNS topic to update all relevant security group rules with the updated IP address ranges.
- B. Create a new AWS Config managed rule that contains all of the internal IP address ranges. Use the rule to check the security groups in each of the accounts to ensure compliance with the list of IP address ranges. Configure the rule to automatically remediate any noncompliant security group that is detected.
- C. In the transit account, create a VPC prefix list with all of the internal IP address ranges. Use AWS Resource Access Manager to share the prefix list with all of the other accounts. Use the shared prefix list to configure security group rules in the other accounts.
- D. In the transit account, create a security group with all of the internal IP address ranges. Configure the security groups in the other accounts to reference the transit account's security group by using a nested security group reference of "/sg-1a2b3c4d".

Question #54

Topic 1

A company runs a new application as a static website in Amazon S3. The company has deployed the application to a production AWS account and uses Amazon CloudFront to deliver the website. The website calls an Amazon API Gateway REST API. An AWS Lambda function backs each API method.

The company wants to create a CSV report every 2 weeks to show each API Lambda function's recommended configured memory, recommended cost, and the price difference between current configurations and the recommendations. The company will store the reports in an S3 bucket.

Which solution will meet these requirements with the LEAST development time?

- A. Create a Lambda function that extracts metrics data for each API Lambda function from Amazon CloudWatch Logs for the 2-week period. Collate the data into tabular format. Store the data as a .csv file in an S3 bucket. Create an Amazon EventBridge rule to schedule the Lambda function to run every 2 weeks.
- B. Opt in to AWS Compute Optimizer. Create a Lambda function that calls the ExportLambdaFunctionRecommendations operation. Export the .csv file to an S3 bucket. Create an Amazon EventBridge rule to schedule the Lambda function to run every 2 weeks.
- C. Opt in to AWS Compute Optimizer. Set up enhanced infrastructure metrics. Within the Compute Optimizer console, schedule a job to export the Lambda recommendations to a .csv file. Store the file in an S3 bucket every 2 weeks.
- D. Purchase the AWS Business Support plan for the production account. Opt in to AWS Compute Optimizer for AWS Trusted Advisor checks. In the Trusted Advisor console, schedule a job to export the cost optimization checks to a .csv file. Store the file in an S3 bucket every 2 weeks.

Question #55**Topic 1**

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 has software engineers spread across three teams. One of the three teams owns each application, and each team is responsible for the cost and performance of all of its applications. Team resources have tags that represent their application and team. The teams use IAM access for daily activities.

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? (Choose three.)

- A. Activate the user-defined cost allocation tags that represent the application and the team.
- B. Activate the AWS generated cost allocation tags that represent the application and the team.
- C. Create a cost category for each application in Billing and Cost Management.
- D. Activate IAM access to Billing and Cost Management.
- E. Create a cost budget.
- F. Enable Cost Explorer.

Question #56**Topic 1**

An AWS customer has a web application that runs on premises. The web application fetches 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 in 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?

- A. Associate a block of customer-owned public IP addresses to the VPC. Enable public IP addressing for public subnets in the VPC.
- 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.
- C. Create Elastic IP addresses from the block of customer-owned IP addresses. Assign the static Elastic IP addresses to the ALB.
- D. Register a block of customer-owned public IP addresses in the AWS account. Set up AWS Global Accelerator to use Elastic IP addresses from the address block. Set the ALB as the accelerator endpoint.

Question #57

Topic 1

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

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowsAllActions",  
            "Effect": "Allow",  
            "Action": "*",  
            "Resource": "*"  
        },  
        {  
            "Sid": "DenyCloudTrail",  
            "Effect": "Deny",  
            "Action": "cloudtrail:*",  
            "Resource": "*"  
        }  
    ]  
}
```

Developers working in account 1111-1111-1111 complain that they cannot create Amazon S3 buckets. How should the administrator address this problem?

- A. Add s3:CreateBucket with "Allow" effect to the SCP.
- B. Remove the account from the OU, and attach the SCP directly to account 1111-1111-1111.
- C. Instruct the developers to add Amazon S3 permissions to their IAM entities.
- D. Remove the SCP from account 1111-1111-1111.

Question #58

Topic 1

A company has a 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.
- B. Create an image of the instance with the reboot option turned on. Launch a new EC2 instance from the image. Attach a role to the new instance with permission to write to Amazon S3. Run a command to copy data into Amazon S3.
- C. Take a snapshot of the EBS volume by using Amazon Data Lifecycle Manager (Amazon DLM). Copy the data to Amazon S3.
- D. Create an image of the instance. Launch a new EC2 instance from the image. Attach a role to the new instance with permission to write to Amazon S3. Run a command to copy data into Amazon S3.

Question #59

Topic 1

A solutions architect needs to copy data from an Amazon S3 bucket in an AWS account to a new S3 bucket in a new AWS account. The solutions architect must implement a solution that uses the AWS CLI.

Which combination of steps will successfully copy the data? (Choose three.)

- A. Create a bucket policy to allow the source bucket to list its contents and to put objects and set object ACLs in the destination bucket. Attach the bucket policy to the destination bucket.
- B. Create a bucket policy to allow a user in the destination account to list the source bucket's contents and read the source bucket's objects. Attach the bucket policy to the source bucket.
- C. Create an IAM policy in the source account. Configure the policy to allow a user in the source account to list contents and get objects in the source bucket, and to list contents, put objects, and set object ACLs in the destination bucket. Attach the policy to the user.
- D. Create an IAM policy in the destination account. Configure the policy to allow a user in the destination account to list contents and get objects in the source bucket, and to list contents, put objects, and set objectACLs in the destination bucket. Attach the policy to the user.
- E. Run the aws s3 sync command as a user in the source account. Specify the source and destination buckets to copy the data.
- F. Run the aws s3 sync command as a user in the destination account. Specify the source and destination buckets to copy the data.

Question #60

Topic 1

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.
- B. Deploy the application into a new CloudFormation stack. Use an Amazon Route 53 weighted routing policy to distribute the load.
- C. Create a version for every new deployed Lambda function. Use the AWS CLI update-function-configuration command with the routing-config parameter to distribute the load.
- D. Configure AWS CodeDeploy and use CodeDeployDefault.OneAtATime in the Deployment configuration to distribute the load.

Question #61

Topic 1

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?

- A. Move the EC2 instance into an Auto Scaling group. Place the EC2 instance behind an Application Load Balancer (ALB). Update the DNS record sftp.example.com in Route 53 to point to the ALB.
- 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.
- C. Migrate the SFTP server to a file gateway in AWS Storage Gateway. Update the DNS record sftp.example.com in Route 53 to point to the file gateway endpoint.
- D. Place the EC2 instance behind a Network Load Balancer (NLB). Update the DNS record sftp.example.com in Route 53 to point to the NLB.

Question #62

Topic 1

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?

- A. Configure the AWS DataSync agent to start replicating the data store to Amazon FSx for Windows File Server. Use the SMB share to host the VMware data store. Use VM Import/Export to move the VMs to Amazon EC2.
- B. Use the VMware vSphere client to export the application as an image in Open Virtualization 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.
- C. Configure AWS Storage Gateway for files service to export a Common Internet File System (CIFS) share. Create a backup copy to the shared folder. Sign in to the AWS Management Console and create an AMI from the backup copy. Launch an EC2 instance that is based on the AMI.
- D. Create a managed-instance activation for a hybrid environment in AWS Systems Manager. Download and install Systems Manager Agent on the on-premises VM. Register the VM with Systems Manager to be a managed instance. Use AWS Backup to create a snapshot of the VM and create an AMI. Launch an EC2 instance that is based on the AMI.

Question #63

Topic 1

A video processing company has an application that downloads images from an Amazon S3 bucket, processes the images, stores a transformed image in a second S3 bucket, and updates metadata about the image in an Amazon DynamoDB table. The application is written in Node.js and runs by using an AWS Lambda function. The Lambda function is invoked when a new image is uploaded to Amazon S3.

The application ran without incident for a while. However, the size of the images has grown significantly. The Lambda function is now failing frequently with timeout errors. The function timeout is set to its maximum value. A solutions architect needs to refactor the application's architecture to prevent invocation failures. The company does not want to manage the underlying infrastructure.

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

- A. Modify the application deployment by building a Docker image that contains the application code. Publish the image to Amazon Elastic Container Registry (Amazon ECR).
- B. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of AWS Fargate. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
- C. Create an AWS Step Functions state machine with a Parallel state to invoke the Lambda function. Increase the provisioned concurrency of the Lambda function.
- D. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of Amazon EC2. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
- E. Modify the application to store images on Amazon Elastic File System (Amazon EFS) and to store metadata on an Amazon RDS DB instance. Adjust the Lambda function to mount the EFS file share.

Question #64

Topic 1

A company has an organization in AWS Organizations. The company is using AWS Control Tower to deploy a landing zone for the organization. The company wants to implement governance and policy enforcement. The company must implement a policy that will detect Amazon RDS DB instances that are not encrypted at rest in the company's production OU.

Which solution will meet this requirement?

- A. Turn on mandatory guardrails in AWS Control Tower. Apply the mandatory guardrails to the production OU.
- B. Enable the appropriate guardrail from the list of strongly recommended guardrails in AWS Control Tower. Apply the guardrail to the production OU.
- C. Use AWS Config to create a new mandatory guardrail. Apply the rule to all accounts in the production OU.
- D. Create a custom SCP in AWS Control Tower. Apply the SCP to the production OU.

Question #65

Topic 1

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 run by the engineers.

Which strategy should a solutions architect use?

- A. Install and configure EC2 Instance Connect on the fleet of EC2 instances. Remove all security group rules attached to EC2 instances that allow inbound TCP on port 22. Advise the engineers to remotely access the instances by using the EC2 Instance Connect CLI.
- B. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices. Install the Amazon CloudWatch agent on all EC2 instances and send operating system audit logs to CloudWatch Logs.
- C. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices. Enable AWS Config for EC2 security group resource changes. Enable AWS Firewall Manager and apply a security group policy that automatically remediates changes to rules.
- D. Create an IAM role with the AmazonSSMManagedInstanceCore managed policy attached. Attach the IAM role to all the EC2 instances. Remove all security group rules attached to the EC2 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.

Question #66

Topic 1

A company that uses AWS Organizations allows developers to experiment on AWS. As part of the landing zone that the company has deployed, developers use their company email address to request an account. The company wants to ensure that developers are not launching costly services or running services unnecessarily. The company must give developers a fixed monthly budget to limit their AWS costs.

Which combination of steps will meet these requirements? (Choose three.)

- A. Create an SCP to set a fixed monthly account usage limit. Apply the SCP to the developer accounts.
- B. Use AWS Budgets to create a fixed monthly budget for each developer's account as part of the account creation process.
- C. Create an SCP to deny access to costly services and components. Apply the SCP to the developer accounts.
- D. Create an IAM policy to deny access to costly services and components. Apply the IAM policy to the developer accounts.
- E. Create an AWS Budgets alert action to terminate services when the budgeted amount is reached. Configure the action to terminate all services.
- F. Create an AWS Budgets alert action to send an Amazon Simple Notification Service (Amazon SNS) notification when the budgeted amount is reached. Invoke an AWS Lambda function to terminate all services.

Question #67

Topic 1

A company has applications in an AWS account that is named Source. The account is in an organization in AWS Organizations. One of the applications uses AWS Lambda functions and stores inventory data in an Amazon Aurora database. The application deploys the Lambda functions by using a deployment package. The company has configured automated backups for Aurora.

The company wants to migrate the Lambda functions and the Aurora database to a new AWS account that is named Target. The application processes critical data, so the company must minimize downtime.

Which solution will meet these requirements?

- A. Download the Lambda function deployment package from the Source account. Use the deployment package and create new Lambda functions in the Target account. Share the automated Aurora DB cluster snapshot with the Target account.
- B. Download the Lambda function deployment package from the Source account. Use the deployment package and create new Lambda functions in the Target account. Share the Aurora DB cluster with the Target account by using AWS Resource Access Manager (AWS RAM). Grant the Target account permission to clone the Aurora DB cluster.
- C. Use AWS Resource Access Manager (AWS RAM) to share the Lambda functions and the Aurora DB cluster with the Target account. Grant the Target account permission to clone the Aurora DB cluster.
- D. Use AWS Resource Access Manager (AWS RAM) to share the Lambda functions with the Target account. Share the automated Aurora DB cluster snapshot with the Target account.

Question #68

Topic 1

A company runs a Python script on an Amazon EC2 instance to process data. The script runs every 10 minutes. The script ingests files from an Amazon S3 bucket and processes the files. On average, the script takes approximately 5 minutes to process each file. The script will not reprocess a file that the script has already processed.

The company reviewed Amazon CloudWatch metrics and noticed that the EC2 instance is idle for approximately 40% of the time because of the file processing speed. The company wants to make the workload highly available and scalable. The company also wants to reduce long-term management overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the data processing script to an AWS Lambda function. Use an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure Amazon S3 to send event notifications to the SQS queue. Create an EC2 Auto Scaling group with a minimum size of one instance. Update the data processing script to poll the SQS queue. Process the S3 objects that the SQS message identifies.
- C. Migrate the data processing script to a container image. Run the data processing container on an EC2 instance. Configure the container to poll the S3 bucket for new objects and to process the resulting objects.
- D. Migrate the data processing script to a container image that runs on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. Create an AWS Lambda function that calls the Fargate RunTaskAPI operation when the container processes the file. Use an S3 event notification to invoke the Lambda function.

Question #69

Topic 1

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?

- A. Create a VPC in us-east-1 and a VPC in us-west-1. Configure VPC peering. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs. Place the Auto Scaling group behind the ALB.
- B. 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 to ensure high availability between Regions.
- 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.
- D. Create a VPC in us-east-1 and a VPC in us-west-1. Configure VPC peering. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs. Place the Auto Scaling group behind the ALB. Create an Amazon Route 53 hosted zone. Create a record for the ALB.

Question #70

Topic 1

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 IAM Identity Center (AWS Single Sign-On) to implement this functionality.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an organization in AWS Organizations. Turn on the IAM Identity Center feature in Organizations. Create and configure a directory in AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) with a two-way trust to the company's on-premises Active Directory. Configure IAM Identity Center and set the AWS Managed Microsoft AD directory as the identity source. Create permission sets and map them to the existing groups within the AWS Managed Microsoft AD directory.
- B. Create an organization in AWS Organizations. Turn on the IAM Identity Center feature in Organizations. Create and configure an AD Connector to connect to the company's on-premises Active Directory. Configure IAM Identity Center 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.
- C. Create an organization in AWS Organizations. Turn on all features for the organization. Create and configure a directory in AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) with a two-way trust to the company's on-premises Active Directory. Configure IAM Identity Center and select the AWS Managed Microsoft AD directory as the identity source. Create permission sets and map them to the existing groups within the AWS Managed Microsoft AD directory.
- 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 IAM Identity Center and set the AD Connector as the identity source. Create permission sets and map them to the existing groups within the company's Active Directory.

Question #71

Topic 1

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.
- B. Configure an S3 bucket in each Region to receive the uploads. Use S3 Cross-Region Replication to copy the files to the distribution S3 bucket.
- C. Set up Amazon Route 53 with latency-based routing to route the uploads to the nearest S3 bucket Region.
- D. Configure the app to break the video files into chunks. Use a multipart upload to transfer files to Amazon S3.
- E. Modify the app to add random prefixes to the files before uploading.

Question #72

Topic 1

An application is using an Amazon RDS for MySQL Multi-AZ DB instance in the us-east-1 Region. After a failover test, the application lost the connections to the database and could not re-establish the connections. After a restart of the application, the application re-established the connections.

A solutions architect must implement a solution so that the application can re-establish connections to the database without requiring a restart.

Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL Serverless v1 DB instance. Migrate the RDS DB instance to the Aurora Serverless v1 DB instance. Update the connection settings in the application to point to the Aurora reader endpoint.
- B. Create an RDS proxy. Configure the existing RDS endpoint as a target. Update the connection settings in the application to point to the RDS proxy endpoint.
- C. Create a two-node Amazon Aurora MySQL DB cluster. Migrate the RDS DB instance to the Aurora DB cluster. Create an RDS proxy. Configure the existing RDS endpoint as a target. Update the connection settings in the application to point to the RDS proxy endpoint.
- D. Create an Amazon S3 bucket. Export the database to Amazon S3 by using AWS Database Migration Service (AWS DMS). Configure Amazon Athena to use the S3 bucket as a data store. Install the latest Open Database Connectivity (ODBC) driver for the application. Update the connection settings in the application to point to the Athena endpoint

Question #73

Topic 1

A company is building a solution in the AWS Cloud. Thousands of devices will connect to the solution and send data. Each device needs to be able to send and receive data in real time over the MQTT protocol. Each device must authenticate by using a unique X.509 certificate.

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

- A. Set up AWS IoT Core. For each device, create a corresponding Amazon MQ queue and provision a certificate. Connect each device to Amazon MQ.
- B. Create a Network Load Balancer (NLB) and configure it with an AWS Lambda authorizer. Run an MQTT broker on Amazon EC2 instances in an Auto Scaling group. Set the Auto Scaling group as the target for the NLConnect each device to the NLB.
- C. Set up AWS IoT Core. For each device, create a corresponding AWS IoT thing and provision a certificate. Connect each device to AWS IoT Core.
- D. Set up an Amazon API Gateway HTTP API and a Network Load Balancer (NLB). Create integration between API Gateway and the NLB. Configure a mutual TLS certificate authorizer on the HTTP API. Run an MQTT broker on an Amazon EC2 instance that the NLB targets. Connect each device to the NLB.

Question #74

Topic 1

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?

- A. Upload AWS CloudFormation templates that contain approved resources to an Amazon S3 bucket. Update the IAM policy for the engineers' IAM role to only allow access to Amazon S3 and AWS CloudFormation. Use AWS CloudFormation templates to provision resources.
- B. Update the IAM policy for the engineers' IAM role with permissions to only allow provisioning of approved resources and AWS CloudFormation. Use AWS CloudFormation templates to create stacks with approved resources.
- 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. Assign the IAM service role to AWS CloudFormation during stack creation.
- D. Provision resources in AWS CloudFormation stacks. Update the IAM policy for the engineers' IAM role to only allow access to their own AWS CloudFormation stack.

Question #75

Topic 1

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 solutions 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 and meets the design requirements?

- A. Design the application to store each incoming record as a single .csv file in an Amazon S3 bucket to allow for indexed retrieval. Configure a lifecycle policy to delete data older than 120 days.
- B. Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale. Configure the DynamoDB Time to Live (TTL) feature to delete records older than 120 days.
- C. Design the application to store each incoming record in a single table in an Amazon RDS MySQL database. Run a nightly cron job that runs a query to delete any records older than 120 days.
- D. Design the application to batch incoming records before writing them to an Amazon S3 bucket. Update the metadata for the object to contain the list of records in the batch and use the Amazon S3 metadata search feature to retrieve the data. Configure a lifecycle policy to delete the data after 120 days.

Question #76

Topic 1

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?

- A. Configure automated backups on Amazon RDS. In the case of disruption, promote an automated backup 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.
- B. Configure global tables and read replicas on Amazon RDS. Activate the cross-Region scope. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region.
- C. Configure global tables and automated backups on Amazon RDS. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region.
- 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.

Question #77

Topic 1

Example Corp. has an on-premises data center and a VPC named VPC A in the Example Corp. AWS account. The on-premises network connects to VPC A through an AWS Site-To-Site VPN. The on-premises servers can properly access VPC A. Example Corp. just acquired AnyCompany, which has a VPC named VPC B. There is no IP address overlap among these networks. Example Corp. has peered VPC A and VPC B.

Example Corp. wants to connect from its on-premise servers to VPC B. Example Corp. has properly set up the network ACL and security groups.

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

- A. Create a transit gateway. Attach the Site-to-Site VPN, VPC A, and VPC B to the transit gateway. Update the transit gateway route tables for all networks to add IP range routes for all other networks.
- B. Create a transit gateway. Create a Site-to-Site VPN connection between the on-premises network and VPC B, and connect the VPN connection to the transit gateway. Add a route to direct traffic to the peered VPCs, and add an authorization rule to give clients access to the VPCs A and B.
- C. Update the route tables for the Site-to-Site VPN and both VPCs for all three networks. Configure BGP propagation for all three networks. Wait for up to 5 minutes for BGP propagation to finish.
- D. Modify the Site-to-Site VPN's virtual private gateway definition to include VPC A and VPC B. Split the two routers of the virtual private gateway between the two VPCs.

Question #78

Topic 1

A company recently completed the migration from an on-premises data center to the AWS Cloud by using a replatforming strategy. One of the migrated servers is running a legacy Simple Mail Transfer Protocol (SMTP) service that a critical application relies upon. The application sends outbound email messages to the company's customers. The legacy SMTP server does not support TLS encryption and uses TCP port 25. The application can use SMTP only.

The company decides to use Amazon Simple Email Service (Amazon SES) and to decommission the legacy SMTP server. The company has created and validated the SES domain. The company has lifted the SES limits.

What should the company do to modify the application to send email messages from Amazon SES?

- A. Configure the application to connect to Amazon SES by using TLS Wrapper. Create an IAM role that has ses:SendEmail and ses:SendRawEmail permissions. Attach the IAM role to an Amazon EC2 instance.
- B. Configure the application to connect to Amazon SES by using STARTTLS. Obtain Amazon SES SMTP credentials. Use the credentials to authenticate with Amazon SES.
- C. Configure the application to use the SES API to send email messages. Create an IAM role that has ses:SendEmail and ses:SendRawEmail permissions. Use the IAM role as a service role for Amazon SES.
- D. Configure the application to use AWS SDKs to send email messages. Create an IAM user for Amazon SES. Generate API access keys. Use the access keys to authenticate with Amazon SES.

Question #79

Topic 1

A company recently acquired several other companies. Each company has a separate AWS account with a different billing and reporting method. The acquiring company has consolidated all the accounts into one organization in AWS Organizations. However, the acquiring company has found it difficult to generate a cost report that contains meaningful groups for all the teams.

The acquiring company's finance team needs a solution to report on costs for all the companies through a self-managed application.

Which solution will meet these requirements?

- A. Create an AWS Cost and Usage Report for the organization. Define tags and cost categories in the report. Create a table in Amazon Athena. Create an Amazon QuickSight dataset based on the Athena table. Share the dataset with the finance team.
- B. Create an AWS Cost and Usage Report for the organization. Define tags and cost categories in the report. Create a specialized template in AWS Cost Explorer that the finance department will use to build reports.
- C. Create an Amazon QuickSight dataset that receives spending information from the AWS Price List Query API. Share the dataset with the finance team.
- D. Use the AWS Price List Query API to collect account spending information. Create a specialized template in AWS Cost Explorer that the finance department will use to build reports.

Question #80

Topic 1

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.)

- A. Resize the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS.
- B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas.
- C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data.
- D. Use AWS X-Ray to analyze and debug application issues and add more API servers to match the load.
- E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance.

Question #81

Topic 1

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.
- B. Create an accelerator in AWS Global Accelerator. Attach the accelerator to the CloudFront distribution.
- C. Change the API Gateway Regional endpoints to edge-optimized endpoints.
- D. Provision the entire stack in two other locations that are spread across the world. Use global databases on the Aurora Serverless cluster.
- E. Add an Amazon RDS proxy between the Lambda functions and the Aurora Serverless database.

Question #82

Topic 1

An adventure company has launched a new feature on its mobile app. Users can use the feature to upload their hiking and rafting photos and videos anytime. The photos and videos are stored in Amazon S3 Standard storage in an S3 bucket and are served through Amazon CloudFront.

The company needs to optimize the cost of the storage. A solutions architect discovers that most of the uploaded photos and videos are accessed infrequently after 30 days. However, some of the uploaded photos and videos are accessed frequently after 30 days. The solutions architect needs to implement a solution that maintains millisecond retrieval availability of the photos and videos at the lowest possible cost.

Which solution will meet these requirements?

- A. Configure S3 Intelligent-Tiering on the S3 bucket.
- B. Configure an S3 Lifecycle policy to transition image objects and video objects from S3 Standard to S3 Glacier Deep Archive after 30 days.
- C. Replace Amazon S3 with an Amazon Elastic File System (Amazon EFS) file system that is mounted on Amazon EC2 instances.
- D. Add a Cache-Control: max-age header to the S3 image objects and S3 video objects. Set the header to 30 days.

Question #83

Topic 1

A company uses Amazon S3 to store files and images in a variety of storage classes. The company's S3 costs have increased substantially during the past year.

A solutions architect needs to review data trends for the past 12 months and identify the appropriate storage class for the objects.

Which solution will meet these requirements?

- A. Download AWS Cost and Usage Reports for the last 12 months of S3 usage. Review AWS Trusted Advisor recommendations for cost savings.
- B. Use S3 storage class analysis. Import data trends into an Amazon QuickSight dashboard to analyze storage trends.
- C. Use Amazon S3 Storage Lens. Upgrade the default dashboard to include advanced metrics for storage trends.
- D. Use Access Analyzer for S3. Download the Access Analyzer for S3 report for the last 12 months. Import the .csv file to an Amazon QuickSight dashboard.

Question #84**Topic 1**

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?

- A. Use AWS CloudFormation templates. Add IAM policies to control the various accounts, Deploy the templates across the multiple Regions.
- B. Use AWS Organizations. Deploy AWS CloudFormation templates from the management account Use AWS Control Tower to manage deployments across accounts.
- C. Use AWS Organizations and AWS CloudFormation StackSets. Deploy a Cloud Formation template from an account that has the necessary IAM permissions.
- D. Use nested stacks with AWS CloudFormation templates. Change the Region by using nested stacks.

Question #85**Topic 1**

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?

- A. Use AWS CloudFormation templates. Add IAM policies to control the various accounts, Deploy the templates across the multiple Regions.
- B. Use AWS Organizations. Deploy AWS CloudFormation templates from the management account Use AWS Control Tower to manage deployments across accounts.
- C. Use AWS Organizations and AWS CloudFormation StackSets. Deploy a Cloud Formation template from an account that has the necessary IAM permissions.
- D. Use nested stacks with AWS CloudFormation templates. Change the Region by using nested stacks.

Question #86**Topic 1**

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 roll back the changes as quickly as possible.

Which design will meet these requirements?

- A. Deploy a CI/CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances.
- B. Specify AWS Elastic Beanstalk to stage 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.
- C. Use AWS Systems Manager to re-provision the infrastructure for each deployment. Update the Amazon EC2 user data to pull the latest code artifact from Amazon S3 and use Amazon Route 53 weighted routing to point to the new environment.
- D. Roll out the application updates as part of an Auto Scaling event using prebuilt AMIs. Use new versions of the AMIs to add instances. and phase out all instances that use the previous AMI version with the configured termination policy during a deployment event.

Question #87

Topic 1

A company has an application that runs on Amazon EC2 instances. A solutions architect is designing VPC infrastructure in an AWS Region where the application needs to access an Amazon Aurora DB Cluster. The EC2 instances are all associated with the same security group. The DB cluster is associated with its own security group.

The solutions architect needs to add rules to the security groups to provide the application with least privilege access to the DB Cluster.

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

- A. Add an inbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the source over the default Aurora port.
- B. Add an outbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the destination over the default Aurora port.
- C. Add an inbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the source over the default Aurora port.
- D. Add an outbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the destination over the default Aurora port.
- E. Add an outbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the destination over the ephemeral ports.

Question #88

Topic 1

A company wants to change its internal cloud billing strategy for each of its business units. Currently, the cloud governance team shares reports for overall 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?

- A. Configure AWS Budgets in each 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 each account to create monthly reports for each business unit.
- B. Configure AWS Budgets in the organization's management 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 management account to create monthly reports for each business unit.
- C. Configure AWS Budgets in each 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 the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit.
- D. Enable AWS Cost and Usage Reports in the organization's management account and configure reports grouped by application, environment, and owner. Create an AWS Lambda function that processes AWS Cost and Usage Reports, sends budget alerts, and sends monthly reports to each business unit's email list.

Question #89

Topic 1

A company is using AWS CloudFormation to deploy its infrastructure. The company is concerned that, if a production CloudFormation 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.
- B. Configure a stack policy that disallows the deletion of RDS and EBS resources.
- C. Modify IAM policies to deny deleting RDS and EBS resources that are tagged with an "aws:cloudformation:stack-name" tag.
- D. Use AWS Config rules to prevent deleting RDS and EBS resources.

Question #90

Topic 1

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 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.
- 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.
- C. Open the AWS CloudTrail 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 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
- D. 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 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.

Question #91

Topic 1

A company consists of two separate business units. Each business unit has its own AWS account within a single organization in AWS Organizations. The business units regularly share sensitive documents with each other. To facilitate sharing, the company created an Amazon S3 bucket in each account and configured low-way replication between the S3 buckets. The S3 buckets have millions of objects.

Recently, a security audit identified that neither S3 bucket has encryption at rest enabled. Company policy requires that all documents must be stored with encryption at rest. The company wants to implement server-side encryption with Amazon S3 managed encryption keys (SSE-S3).

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

- A. Turn on SSE-S3 on both S3 buckets. Use S3 Batch Operations to copy and encrypt the objects in the same location.
- B. Create an AWS Key Management Service (AWS KMS) key in each account. Turn on server-side encryption with AWS KMS keys (SSE-KMS) on each S3 bucket by using the corresponding KMS key in that AWS account. Encrypt the existing objects by using an S3 copy command in the AWS CLI.
- C. Turn on SSE-S3 on both S3 buckets. Encrypt the existing objects by using an S3 copy command in the AWS CLI.
- D. Create an AWS Key Management Service (AWS KMS) key in each account. Turn on server-side encryption with AWS KMS keys (SSE-KMS) on each S3 bucket by using the corresponding KMS key in that AWS account. Use S3 Batch Operations to copy the objects into the same location.

Question #92

Topic 1

A company is running an application in the AWS Cloud. The application collects and stores a large amount of unstructured data in an Amazon S3 bucket. The S3 bucket contains several terabytes of data and uses the S3 Standard storage class. The data increases in size by several gigabytes every day.

The company needs to query and analyze the data. The company does not access data that is more than 1 year old. However, the company must retain all the data indefinitely for compliance reasons.

Which solution will meet these requirements MOST cost-effectively?

- A. Use S3 Select to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- B. Use Amazon Redshift Spectrum to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- C. Use an AWS Glue Data Catalog and Amazon Athena to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- D. Use Amazon Redshift Spectrum to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Intelligent-Tiering.

Question #93

Topic 1

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.
- B. Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.
- C. Create a VPN connection between the on-premises network attached storage and the nearest AWS Region. Transfer the data over the VPN connection.
- D. Deploy an AWS Storage Gateway file gateway on premises. Configure the file gateway with a destination S3 bucket. Copy the data to the file gateway.

Question #94

Topic 1

A company has migrated its forms-processing application to AWS. When users interact with the application, they upload scanned forms as files through a web application. A database stores user metadata and references to files that are stored in Amazon S3. The web application runs on Amazon EC2 instances and an Amazon RDS for PostgreSQL database.

When forms are uploaded, the application sends notifications to a team through Amazon Simple Notification Service (Amazon SNS). A team member then logs in and processes each form. The team member performs data validation on the form and extracts relevant data before entering the information into another system that uses an API.

A solutions architect needs to automate the manual processing of the forms. The solution must provide accurate form extraction, minimize time to market, and minimize long-term operational overhead.

Which solution will meet these requirements?

- A. Develop custom libraries to perform optical character recognition (OCR) on the forms. Deploy the libraries to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster as an application tier. Use this tier to process the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data into an Amazon DynamoDB table. Submit the data to the target system's API. Host the new application tier on EC2 instances.
- B. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use artificial intelligence and machine learning (AI/ML) models that are trained and hosted on an EC2 instance to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.
- C. Host a new application tier on EC2 instances. Use this tier to call endpoints that host artificial intelligence and machine learning (AI/ML) models that are trained and hosted in Amazon SageMaker to perform optical character recognition (OCR) on the forms. Store the output in Amazon ElastiCache. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.
- D. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use Amazon Textract and Amazon Comprehend to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.

Question #95

Topic 1

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.
- B. Create a custom AWS Lambda runtime to mimic the web server environment. Create an Amazon API Gateway API to replace the front-end web servers. Set up Amazon MQ to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.
- C. 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. Install Kubernetes on a fleet of different EC2 instances to host the order-processing backend.
- D. 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 an Amazon Simple Queue Service (Amazon SQS) queue to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.

Question #96

Topic 1

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:PutObjectAcl"  
            ],  
            "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
- B. kms:GetKeyPolicy
- C. kms:GetPublicKey
- D. kms:Sign

Question #97

Topic 1

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.
- B. Use only rate-based rules in the web ACLs, and set the throttle limit as high as possible. Temporarily block all requests that exceed the limit. Define nested rules to narrow the scope of the rate tracking.
- C. Set the action of the web ACL rules to Block. Use only AWS managed rule groups in the web ACLs. Evaluate the rule groups by using Amazon CloudWatch metrics with AWS WAF sampled requests or AWS WAF logs.
- D. Use only custom rule groups in the web ACLs, and set the action to Allow. 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 Allow to Block.

Question #98

Topic 1

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?

- A. Set up an Amazon Simple Notification Service (Amazon SNS) topic in the security team's AWS account. Deploy an AWS Lambda function in each AWS account. Configure the Lambda function to run every time an SNS topic receives a message. Configure the Lambda function to take an IP address as input and add it to a list of security groups in the account. Instruct the security team to distribute changes by publishing messages to its SNS topic.
- B. Create new customer-managed prefix lists in each AWS account within the organization. Populate the prefix lists in each account with all internal CIDR ranges. Notify the owner of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security groups. Instruct the security team to share updates with each AWS account owner.
- 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.
- D. Create an IAM role in each account in the organization. Grant permissions to update security groups. Deploy an AWS Lambda function in the security team's AWS account. Configure the Lambda function to take a list of internal IP addresses as input, assume a role in each organization account, and add the list of IP addresses to the security groups in each account.

Question #99

Topic 1

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?

- A. Create a Client VPN endpoint in each AWS account. Configure required routing that allows access to internal applications.
- B. Create a Client VPN endpoint in the main AWS account. Configure required routing that allows access to internal applications.
- C. Create a Client VPN endpoint in the main AWS account. Provision a transit gateway that is connected to each AWS account. Configure required routing that allows access to internal applications.
- D. Create a Client VPN endpoint in the main AWS account. Establish connectivity between the Client VPN endpoint and the AWS Site-to-Site VPN.

Question #100

Topic 1

A company is running an application in the AWS Cloud. Recent application metrics show inconsistent response times and a significant increase in error rates. Calls to third-party services are causing the delays. Currently, the application calls third-party services synchronously by directly invoking an AWS Lambda function.

A solutions architect needs to decouple the third-party service calls and ensure that all the calls are eventually completed.

Which solution will meet these requirements?

- A. Use an Amazon Simple Queue Service (Amazon SQS) queue to store events and invoke the Lambda function.
- B. Use an AWS Step Functions state machine to pass events to the Lambda function.
- C. Use an Amazon EventBridge rule to pass events to the Lambda function.
- D. Use an Amazon Simple Notification Service (Amazon SNS) topic to store events and invoke the Lambda function.

Question #101

Topic 1

A company is running applications on AWS in a multi-account environment. The company's sales team and marketing team use separate AWS accounts in AWS Organizations.

The sales team stores petabytes of data in an Amazon S3 bucket. The marketing team uses Amazon QuickSight for data visualizations. The marketing team needs access to data that the sales team stores in the S3 bucket. The company has encrypted the S3 bucket with an AWS Key Management Service (AWS KMS) key. The marketing team has already created the IAM service role for QuickSight to provide QuickSight access in the marketing AWS account. The company needs a solution that will provide secure access to the data in the S3 bucket across AWS accounts.

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

- A. Create a new S3 bucket in the marketing account. Create an S3 replication rule in the sales account to copy the objects to the new S3 bucket in the marketing account. Update the QuickSight permissions in the marketing account to grant access to the new S3 bucket.
- B. Create an SCP to grant access to the S3 bucket to the marketing account. Use AWS Resource Access Manager (AWS RAM) to share the KMS key from the sales account with the marketing account. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- C. Update the S3 bucket policy in the marketing account to grant access to the QuickSight role. Create a KMS grant for the encryption key that is used in the S3 bucket. Grant decrypt access to the QuickSight role. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- D. Create an IAM role in the sales account and grant access to the S3 bucket. From the marketing account, assume the IAM role in the sales account to access the S3 bucket. Update the QuickSight role, to create a trust relationship with the new IAM role in the sales account.

Question #102

Topic 1

A company is planning to migrate its business-critical applications from an on-premises data center to AWS. The company has an on-premises installation of a Microsoft SQL Server Always On cluster. The company wants to migrate to an AWS managed database service. A solutions architect must design a heterogeneous database migration on AWS.

Which solution will meet these requirements?

- A. Migrate the SQL Server databases to Amazon RDS for MySQL by using backup and restore utilities.
- B. Use an AWS Snowball Edge Storage Optimized device to transfer data to Amazon S3. Set up Amazon RDS for MySQL. Use S3 integration with SQL Server features, such as BULK INSERT.
- C. Use the AWS Schema Conversion Tool to translate the database schema to Amazon RDS for MySQL. Then use AWS Database Migration Service (AWS DMS) to migrate the data from on-premises databases to Amazon RDS.
- D. Use AWS DataSync to migrate data over the network between on-premises storage and Amazon S3. Set up Amazon RDS for MySQL. Use S3 integration with SQL Server features, such as BULK INSERT.

Question #103

Topic 1

A publishing company's design team updates the icons and other static assets that an ecommerce web application uses. The company serves the icons and assets from an Amazon S3 bucket that is hosted in the company's production account. The company also uses a development account that members of the design team can access.

After the design team tests the static assets in the development account, the design team needs to load the assets into the S3 bucket in the production account. A solutions architect must provide the design team with access to the production account without exposing other parts of the web application to the risk of unwanted changes.

Which combination of steps will meet these requirements? (Choose three.)

- A. In the production account, create a new IAM policy that allows read and write access to the S3 bucket.
- B. In the development account, create a new IAM policy that allows read and write access to the S3 bucket.
- C. In the production account, create a role. Attach the new policy to the role. Define the development account as a trusted entity.
- D. In the development account, create a role. Attach the new policy to the role. Define the production account as a trusted entity.
- E. In the development account, create a group that contains all the IAM users of the design team. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the production account.
- F. In the development account, create a group that contains all the IAM users of the design team. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the development account.

Question #104

Topic 1

A company developed a pilot application by using AWS Elastic Beanstalk and Java. To save costs during development, the company's development team deployed the application into a single-instance environment. Recent tests indicate that the application consumes more CPU than expected. CPU utilization is regularly greater than 85%, which causes some performance bottlenecks.

A solutions architect must mitigate the performance issues before the company launches the application to production.

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

- A. Create a new Elastic Beanstalk application. Select a load-balanced environment type. Select all Availability Zones. Add a scale-out rule that will run if the maximum CPU utilization is over 85% for 5 minutes.
- B. Create a second Elastic Beanstalk environment. Apply the traffic-splitting deployment policy. Specify a percentage of incoming traffic to direct to the new environment if the average CPU utilization is over 85% for 5 minutes.
- C. Modify the existing environment's capacity configuration to use a load-balanced environment type. Select all Availability Zones. Add a scale-out rule that will run if the average CPU utilization is over 85% for 5 minutes.
- D. Select the Rebuild environment action with the load balancing option. Select an Availability Zones. Add a scale-out rule that will run if the sum CPU utilization is over 85% for 5 minutes.

Question #105

Topic 1

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 I/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?

- A. Pre-warming Elastic Load Balancers, using a bigger instance type, changing all Amazon EBS volumes to GP2 volumes.
- B. Performing a one-time migration of the database cluster to Amazon RDS, and creating several additional read replicas to handle the load during end of month.
- C. Using Amazon CloudWatch with AWS Lambda to change the type, size, or IOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric.
- D. Replacing all existing Amazon EBS volumes with new PIOPS volumes that have the maximum available storage size and I/O per second by taking snapshots before the end of the month and reverting back afterwards.

Question #106

Topic 1

A company runs a Java application that has complex dependencies on VMs that are in the company's data center. The application is stable, but the company wants to modernize the technology stack. The company wants to migrate the application to AWS and minimize the administrative overhead to maintain the servers.

Which solution will meet these requirements with the LEAST code changes?

- A. Migrate the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate by using AWS App2Container. Store container images in Amazon Elastic Container Registry (Amazon ECR). Grant the ECS task execution role permission to access the ECR image repository. Configure Amazon ECS to use an Application Load Balancer (ALB). Use the ALB to interact with the application.
- B. Migrate the application code to a container that runs in AWS Lambda. Build an Amazon API Gateway REST API with Lambda integration. Use API Gateway to interact with the application.
- C. Migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) on EKS managed node groups by using AWS App2Container. Store container images in Amazon Elastic Container Registry (Amazon ECR). Give the EKS nodes permission to access the ECR image repository. Use Amazon API Gateway to interact with the application.
- D. Migrate the application code to a container that runs in AWS Lambda. Configure Lambda to use an Application Load Balancer (ALB). Use the ALB to interact with the application.

Question #107

Topic 1

A company has an asynchronous HTTP application that is hosted as an AWS Lambda function. A public Amazon API Gateway endpoint invokes the Lambda function. The Lambda function and the API Gateway endpoint reside in the us-east-1 Region. A solutions architect needs to redesign the application to support failover to another AWS Region.

Which solution will meet these requirements?

- A. Create an API Gateway endpoint in the us-west-2 Region to direct traffic to the Lambda function in us-east-1. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure API Gateway to direct traffic to the SQS queue instead of to the Lambda function. Configure the Lambda function to pull messages from the queue for processing.
- C. Deploy the Lambda function to the us-west-2 Region. Create an API Gateway endpoint in us-west-2 to direct traffic to the Lambda function in us-west-2. Configure AWS Global Accelerator and an Application Load Balancer to manage traffic across the two API Gateway endpoints.
- D. Deploy the Lambda function and an API Gateway endpoint to the us-west-2 Region. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints.

Question #108

Topic 1

A retail company has structured its AWS accounts to be part of an organization in AWS Organizations. The company has set up consolidated billing and has mapped its departments to the following OUs: Finance, Sales, Human Resources (HR), Marketing, and Operations. Each OU has multiple AWS accounts, one for each environment within a department. These environments are development, test, pre-production, and production.

The HR department is releasing a new system that will launch in 3 months. In preparation, the HR department has purchased several Reserved Instances (RIs) in its production AWS account. The HR department will install the new application on this account. The HR department wants to make sure that other departments cannot share the RI discounts.

Which solution will meet these requirements?

- A. In the AWS Billing and Cost Management console for the HR department's production account turn off RI sharing.
- B. Remove the HR department's production AWS account from the organization. Add the account to the consolidating billing configuration only.
- C. In the AWS Billing and Cost Management console, use the organization's management account to turn off RI Sharing for the HR department's production AWS account.
- D. Create an SCP in the organization to restrict access to the RIs. Apply the SCP to the OUs of the other departments.

Question #109

Topic 1

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?

- A. Suspend the Auto Scaling group's HealthCheck scaling process. Use Session Manager to log in to an instance that is marked as unhealthy.
- B. Enable EC2 instance termination protection. Use Session Manager to log in to an instance that is marked as unhealthy.
- C. Set the termination policy to OldestInstance on the Auto Scaling group. Use Session Manager to log in to an instance that is marked as unhealthy.
- D. Suspend the Auto Scaling group's Terminate process. Use Session Manager to log in to an instance that is marked as unhealthy.

Question #110

Topic 1

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?

- A. Use AWS Firewall Manager to manage AWS WAF rules across accounts in the organization. Use an AWS Systems Manager Parameter Store parameter to store account numbers and OUs to manage. Update the parameter as needed to add or remove accounts or OUs. Use an Amazon EventBridge rule to identify any changes to the parameter and to invoke an AWS Lambda function to update the security policy in the Firewall Manager administrative account.
- 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.
- C. Create AWS WAF rules in the management account of the organization. Use AWS Lambda environment variables to store account numbers and OUs to manage. Update environment variables as needed to add or remove accounts or OUs. Create cross-account IAM roles in member accounts. Assume the roles by using AWS Security Token Service (AWS STS) in the Lambda function to create and update AWS WAF rules in the member accounts.
- D. Use AWS Control Tower to manage AWS WAF rules across accounts in the organization. Use AWS Key Management Service (AWS KMS) to store account numbers and OUs to manage. Update AWS KMS as needed to add or remove accounts or OUs. Create IAM users in member accounts. Allow AWS Control Tower in the management account to use the access key and secret access key to create and update AWS WAF rules in the member accounts.

Question #111

Topic 1

A solutions architect is auditing the security setup of an AWS Lambda function for a company. The Lambda function retrieves the latest changes from an Amazon Aurora database. The Lambda function and the database run in the same VPC. Lambda environment variables are providing the database credentials to the Lambda function.

The Lambda function aggregates data and makes the data available in an Amazon S3 bucket that is configured for server-side encryption with AWS KMS managed encryption keys (SSE-KMS). The data must not travel across the Internet. If any database credentials become compromised, the company needs a solution that minimizes the impact of the compromise.

What should the solutions architect recommend to meet these requirements?

- A. Enable IAM database authentication on the Aurora DB cluster. Change the IAM role for the Lambda function to allow the function to access the database by using IAM database authentication. Deploy a gateway VPC endpoint for Amazon S3 in the VPC.
- B. Enable IAM database authentication on the Aurora DB cluster. Change the IAM role for the Lambda function to allow the function to access the database by using IAM database authentication. Enforce HTTPS on the connection to Amazon S3 during data transfers.
- C. Save the database credentials in AWS Systems Manager Parameter Store. Set up password rotation on the credentials in Parameter Store. Change the IAM role for the Lambda function to allow the function to access Parameter Store. Modify the Lambda function to retrieve the credentials from Parameter Store. Deploy a gateway VPC endpoint for Amazon S3 in the VPC.
- D. Save the database credentials in AWS Secrets Manager. Set up password rotation on the credentials in Secrets Manager. Change the IAM role for the Lambda function to allow the function to access Secrets Manager. Modify the Lambda function to retrieve the credentials from Secrets Manager. Enforce HTTPS on the connection to Amazon S3 during data transfers.

Question #112

Topic 1

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?

- A. Create a desired-instance-type managed rule in AWS Config. Configure the rule with the instance types that are allowed. Attach the rule to an event to run each time a new EC2 instance is launched.
- B. In the EC2 console, create a launch template that specifies the instance types that are allowed. Assign the launch template to the developers' IAM accounts.
- 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.
- D. Use EC2 Image Builder to create an image pipeline for the developers and assist them in the creation of a golden image.

Question #113

Topic 1

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? (Choose 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.
- C. Use Amazon Inspector in the organization to find resources with missing tags.
- D. Create an IAM policy in each account 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.
- F. Use AWS Security Hub to aggregate a list of EC2 instances with the missing Project tag.

Question #114

Topic 1

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.
- B. Create an Amazon Kinesis data stream to buffer events. Create an AWS Lambda function to process and transform events.
- C. Configure an Amazon Aurora PostgreSQL DB cluster to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.
- 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.
- E. Configure an Amazon Neptune DB instance to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.

Question #115

Topic 1

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 solution 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?

- A. Enable VPC Flow Logs. Use Amazon Athena to analyze the logs for traffic that can be removed. Ensure that security groups are blocking traffic that is responsible for high costs.
- B. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that applications have the correct IAM permissions to use the interface VPC endpoint.
- C. Enable VPC Flow Logs and Amazon Detective. Review Detective findings for traffic that is not related to Kinesis Data Streams. Configure security groups to block that traffic.
- D. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that the VPC endpoint policy allows traffic from the applications.

Question #116

Topic 1

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?

- A. Create a private VIF from the DX-A connection into a Direct Connect gateway. Create a private VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with the Direct Connect gateway. Peer the transit gateways with each other to support cross-Region routing.
- B. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Associate the eu-west-1 transit gateway with this Direct Connect gateway. Create a transit VIF from the DX-B connection into a separate Direct Connect gateway. Associate the us-east-1 transit gateway with this separate Direct Connect gateway. Peer the Direct Connect gateways with each other to support high availability and cross-Region routing.
- C. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Create a transit VIF from the DX-B connection 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. Configure the Direct Connect gateway to route traffic between the transit gateways.
- D. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Create a transit VIF from the DX-B connection 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.

Question #117

Topic 1

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? (Choose 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.
- B. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.
- C. Invoke a container that runs in Amazon Elastic Container Service (Amazon ECS) with AWS Fargate technology to remove access.
- D. Invoke an AWS Step Functions state machine to remove access.
- E. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.
- F. Use Amazon Pinpoint to notify the security team.

Question #118

Topic 1

A company wants to migrate to AWS. The company wants to use a multi-account structure with centrally managed access to all accounts and applications. The company also wants to keep the traffic on a private network. Multi-factor authentication (MFA) is required at login, and specific roles are assigned to user groups.

The company must create separate accounts for development, staging, production, and shared network. The production account and the shared network account must have connectivity to all accounts. The development account and the staging account must have access only to each other.

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

- A. Deploy a landing zone environment by using AWS Control Tower. Enroll accounts and invite existing accounts into the resulting organization in AWS Organizations.
- B. Enable AWS Security Hub in all accounts to manage cross-account access. Collect findings through AWS CloudTrail to force MFA login.
- C. Create transit gateways and transit gateway VPC attachments in each account. Configure appropriate route tables.
- D. Set up and enable AWS IAM Identity Center (AWS Single Sign-On). Create appropriate permission sets with required MFA for existing accounts.
- E. Enable AWS Control Tower in all accounts to manage routing between accounts. Collect findings through AWS CloudTrail to force MFA login.
- F. Create IAM users and groups. Configure MFA for all users. Set up Amazon Cognito user pools and Identity pools to manage access to accounts and between accounts.

Question #119

Topic 1

A company runs its application in the eu-west-1 Region and has one account for each of its environments: development, testing, and production. All the environments are running 24 hours a day, 7 days a week by using stateful Amazon EC2 instances and Amazon RDS for MySQL databases. The databases are between 500 GB and 800 GB in size.

The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day, 7 days a week. The company wants to reduce costs. All resources are tagged with an environment tag with either development, testing, or production as the key.

What should a solutions architect do to reduce costs with the LEAST operational effort?

- A. Create an Amazon EventBridge rule that runs once every day. Configure the rule to invoke one AWS Lambda function that starts or stops instances based on me tag, day, and time.
- B. Create an Amazon EventBridge rule that runs every business day in the evening. Configure the rule to invoke an AWS Lambda function that stops instances based on the tag. Create a second EventBridge rule that runs every business day in the morning. Configure the second rule to invoke another Lambda function that starts instances based on the tag.
- C. Create an Amazon EventBridge rule that runs every business day in the evening. Configure the rule to invoke an AWS Lambda function that terminates instances based on the tag. Create a second EventBridge rule that runs every business day in the morning. Configure the second rule to invoke another Lambda function that restores the instances from their last backup based on the tag.
- D. Create an Amazon EventBridge rule that runs every hour. Configure the rule to invoke one AWS Lambda function that terminates or restores instances from their last backup based on the tag, day, and time.

Question #120

Topic 1

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?

- A. The Lambda function reached its concurrency limit.
- B. The Lambda function its Region limit for concurrency.
- C. The company reached its API Gateway account limit for calls per second.
- D. The company reached its API Gateway default per-method limit for calls per second.

Question #121

Topic 1

A financial company is planning to migrate its web application from on premises to AWS. The company uses a third-party security tool to monitor the inbound traffic to the application. The company has used the security tool for the last 15 years, and the tool has no cloud solutions available from its vendor. The company's security team is concerned about how to integrate the security tool with AWS technology.

The company plans to deploy the application migration to AWS on Amazon EC2 instances. The EC2 instances will run in an Auto Scaling group in a dedicated VPC. The company needs to use the security tool to inspect all packets that come in and out of the VPC. This inspection must occur in real time and must not affect the application's performance. A solutions architect must design a target architecture on AWS that is highly available within an AWS Region.

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

- A. Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC
- B. Deploy the web application behind a Network Load Balancer
- C. Deploy an Application Load Balancer in front of the security tool instances
- D. Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool
- E. Provision a transit gateway to facilitate communication between VPCs.

Question #122

Topic 1

A company has purchased appliances from different vendors. The appliances all have IoT sensors. The sensors send status information in the vendors' proprietary formats to a legacy application that parses the information into JSON. The parsing is simple, but each vendor has a unique format. Once daily, the application parses all the JSON records and stores the records in a relational database for analysis.

The company needs to design a new data analysis solution that can deliver faster and optimize costs.

Which solution will meet these requirements?

- A. Connect the IoT sensors to AWS IoT Core. Set a rule to invoke an AWS Lambda function to parse the information and save a .csv file to Amazon S3. Use AWS Glue to catalog the files. Use Amazon Athena and Amazon QuickSight for analysis.
- B. Migrate the application server to AWS Fargate, which will receive the information from IoT sensors and parse the information into a relational format. Save the parsed information to Amazon Redshift for analysis.
- C. Create an AWS Transfer for SFTP server. Update the IoT sensor code to send the information as a .csv file through SFTP to the server. Use AWS Glue to catalog the files. Use Amazon Athena for analysis.
- D. Use AWS Snowball Edge to collect data from the IoT sensors directly to perform local analysis. Periodically collect the data into Amazon Redshift to perform global analysis.

Question #123

Topic 1

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 Connect 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.)

- A. Create a Direct Connect gateway in the central account. In each of the accounts, create an association proposal by using the Direct Connect gateway and the account ID for every virtual private gateway.
- 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.
- C. Provision an internet gateway. Attach the internet gateway to subnets. Allow internet traffic through the gateway.
- D. Share the transit gateway with other accounts. Attach VPCs to the transit gateway.
- E. Provision VPC peering as necessary.
- 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.

Question #124

Topic 1

A company has hundreds of AWS accounts. The company recently implemented a centralized internal process for purchasing new Reserved Instances and modifying 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. Previously, business units directly purchased or modified Reserved Instances in their own respective AWS accounts autonomously.

A solutions architect needs to enforce the new process in the most secure way possible.

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

- A. Ensure that all AWS accounts are part of an organization in AWS Organizations with all features enabled.
- B. Use AWS Config to report on the attachment of an IAM policy that denies access to the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action.
- C. In each AWS account, create an IAM policy that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action.
- D. Create an SCP that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action. Attach the SCP to each OU of the organization.
- E. Ensure that all AWS accounts are part of an organization in AWS Organizations that uses the consolidated billing feature.

Question #125

Topic 1

A company is running a critical application that uses an Amazon RDS for MySQL database to store data. The RDS DB instance is deployed in Multi-AZ mode.

A recent RDS database failover test caused a 40-second outage to the application. A solutions architect needs to design a solution to reduce the outage time to less than 20 seconds.

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

- A. Use Amazon ElastiCache for Memcached in front of the database
- B. Use Amazon ElastiCache for Redis in front of the database
- C. Use RDS Proxy in front of the database.
- D. Migrate the database to Amazon Aurora MySQL.
- E. Create an Amazon Aurora Replica.
- F. Create an RDS for MySQL read replica

Question #126

Topic 1

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?

- A. The customer should provide the partner company with their AWS account access keys to log in and perform the required tasks.
- B. The customer should create an IAM user and assign the required permissions to the IAM user. The customer should then provide the credentials to the partner company to log in and perform the required tasks.
- C. 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) when requesting access to perform the required tasks.
- 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.

Question #127

Topic 1

A delivery company needs to migrate its third-party route planning application to AWS. The third party supplies a supported Docker image from a public registry. The image can run in as many containers as required to generate the route map.

The company has divided the delivery area into sections with supply hubs so that delivery drivers travel the shortest distance possible from the hubs to the customers. To reduce the time necessary to generate route maps, each section uses its own set of Docker containers with a custom configuration that processes orders only in the section's area.

The company needs the ability to allocate resources cost-effectively based on the number of running containers.

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

- A. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on Amazon EC2. Use the Amazon EKS CLI to launch the planning application in pods by using the --tags option to assign a custom tag to the pod.
- B. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on AWS Fargate. Use the Amazon EKS CLI to launch the planning application. Use the AWS CLI tag-resource API call to assign a custom tag to the pod.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster on Amazon EC2. Use the AWS CLI with run-tasks set to true to launch the planning application by using the --tags option to assign a custom tag to the task.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster on AWS Fargate. Use the AWS CLI run-task command and set enableECSManagedTags to true to launch the planning application. Use the --tags option to assign a custom tag to the task.

Question #128

Topic 1

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 in an application VPC located in the us-east-1 Region with an IPv4 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? (Choose two.)

- A. The IPv4 CIDR ranges of the two VPCs overlap
- B. The VPCs are not in the same Region
- C. One or both accounts do not have access to an Internet gateway
- D. One of the VPCs was not shared through AWS Resource Access Manager
- E. The IAM role in the peer accepter account does not have the correct permissions

Question #129

Topic 1

An external audit of a company's serverless application reveals IAM policies that grant too many permissions. These policies are attached to the company's AWS Lambda execution roles. Hundreds of the company's Lambda functions have broad access permissions such as full access to Amazon S3 buckets and Amazon DynamoDB tables. The company wants each function to have only the minimum permissions that the function needs to complete its task.

A solutions architect must determine which permissions each Lambda function needs.

What should the solutions architect do to meet this requirement with the LEAST amount of effort?

- A. Set up Amazon CodeGuru to profile the Lambda functions and search for AWS API calls. Create an inventory of the required API calls and resources for each Lambda function. Create new IAM access policies for each Lambda function. Review the new policies to ensure that they meet the company's business requirements.
- B. Turn on AWS CloudTrail logging for the AWS account. Use AWS Identity and Access Management Access Analyzer to generate IAM access policies based on the activity recorded in the CloudTrail log. Review the generated policies to ensure that they meet the company's business requirements.
- C. Turn on AWS CloudTrail logging for the AWS account. Create a script to parse the CloudTrail log, search for AWS API calls by Lambda execution role, and create a summary report. Review the report. Create IAM access policies that provide more restrictive permissions for each Lambda function.
- D. Turn on AWS CloudTrail logging for the AWS account. Export the CloudTrail logs to Amazon S3. Use Amazon EMR to process the CloudTrail logs in Amazon S3 and produce a report of API calls and resources used by each execution role. Create a new IAM access policy for each role. Export the generated roles to an S3 bucket. Review the generated policies to ensure that they meet the company's business requirements.

Question #130

Topic 1

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 clusters 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?

- A. Create a dashboard by using AWS Systems Manager OpsCenter. Configure visualizations for Amazon CloudWatch metrics that are associated with the EC2 instances and their EBS volumes. Review the dashboard periodically, and identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.
- B. Turn on Amazon CloudWatch detailed monitoring for the EC2 instances and their EBS volumes. Create and review a dashboard that is based on the metrics. Identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.
- C. Install the Amazon CloudWatch agent on each of the EC2 instances. Turn on AWS Compute Optimizer, and let it run for at least 12 hours. Review the recommendations from Compute Optimizer, and rightsize the EC2 instances as directed.
- D. Sign up for the AWS Enterprise Support plan. Turn on AWS Trusted Advisor. Wait 12 hours. Review the recommendations from Trusted Advisor, and rightsize the EC2 instances as directed.

Question #131

Topic 1

A company uses AWS Organizations for a multi-account setup in the AWS Cloud. The company uses AWS Control Tower for governance and uses AWS Transit Gateway for VPC connectivity across accounts.

In an AWS application account, the company's application team has deployed a web application that uses AWS Lambda and Amazon RDS. The company's database administrators have a separate DBA account and use the account to centrally manage all the databases across the organization. The database administrators use an Amazon EC2 instance that is deployed in the DBA account to access an RDS database that is deployed in the application account.

The application team has stored the database credentials as secrets in AWS Secrets Manager in the application account. The application team is manually sharing the secrets with the database administrators. The secrets are encrypted by the default AWS managed key for Secrets Manager in the application account. A solutions architect needs to implement a solution that gives the database administrators access to the database and eliminates the need to manually share the secrets.

Which solution will meet these requirements?

- A. Use AWS Resource Access Manager (AWS RAM) to share the secrets from the application account with the DBA account. In the DBA account, create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the shared secrets. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- B. In the application account, create an IAM role that is named DBA-Secret. Grant the role the required permissions to access the secrets. In the DBA account, create an IAM role that is named DBA-Admin. Grant the DBA-Admin role the required permissions to assume the DBA-Secret role in the application account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets
- C. In the DBA account create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the secrets and the default AWS managed key in the application account. In the application account, attach resource-based policies to the key to allow access from the DBA account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- D. In the DBA account, create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the secrets in the application account. Attach an SCP to the application account to allow access to the secrets from the DBA account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.

Question #132

Topic 1

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? (Choose two.)

- A. Create an IAM role in one account under the DataOps OU. Use the ec2:InstanceType condition key in an inline policy on the role to restrict access to specific instance type.
- B. Create an IAM user in all accounts under the root OU. Use the aws:RequestedRegion condition key in an inline policy on each user to restrict access to all AWS Regions except ap-northeast-1.
- 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.
- D. Create an SCP. Use the ec2:Region condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU, the DataOps OU, and the Research 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.

Question #133

Topic 1

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 SQS queue with the Lambda function to other Regions.
- B. Subscribe the SNS topic in each Region to the SQS queue.
- C. Subscribe the SQS queue in each Region to the SNS topic.
- D. Configure the SQS queue to publish URLs to SNS topics in each Region.
- E. Deploy the SNS topic and the Lambda function to other Regions.

Question #134

Topic 1

A company runs a proprietary stateless ETL application on an Amazon EC2 Linux instances. 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?

- A. Use AWS Lambda to run the application. Use Amazon CloudWatch Logs to invoke the Lambda function every 4 hours.
- B. Use AWS Batch to run the application. Use an AWS Step Functions state machine to invoke the AWS Batch job every 4 hours.
- C. Use AWS Fargate to run the application. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke the Fargate task every 4 hours.
- D. Use Amazon EC2 Spot Instances to run the application. Use AWS CodeDeploy to deploy and run the application every 4 hours.

Question #135

Topic 1

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?

- Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Cross-Region Replication. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables.
- Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Same-Region Replication. Create a new DynamoDB table in a new Region. Configure asynchronous replication between the DynamoDB tables by using AWS Database Migration Service (AWS DMS) with change data capture (CDC).
- 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 the same Region, and configure S3 Same-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables.

Question #136

Topic 1

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?

- Use an Amazon Aurora DB cluster 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.
- Use MongoDB on Amazon EC2 instances as the database for the subscriber data. Deploy EC2 instances in an Auto Scaling group in a single Availability Zone for the Java backend application.
- Configure Amazon DocumentDB (with MongoDB compatibility) with appropriately sized instances 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.
- 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.

Question #137

Topic 1

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 Access Denied error.

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? (Choose 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.
- B. Update the `strategy_reviewer` IAM role to grant full permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key.
- C. Update the custom KMS key policy in the Creative account to grant decrypt permissions to the `strategy_reviewer` IAM role.
- D. Create a bucket policy that includes read permissions for the S3 bucket. Set the principal of the bucket policy to an anonymous user.
- E. Update the custom KMS key policy in the Creative account to grant encrypt 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.

Question #138

Topic 1

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?

- A. Use regularly scheduled AWS Snowball Edge devices to transfer the sequencing data into AWS. When AWS receives the Snowball Edge device and the data is loaded into Amazon S3, use S3 events to trigger an AWS Lambda function to process the data.
- B. Use AWS Data Pipeline to transfer the sequencing data to Amazon S3. Use S3 events to trigger an Amazon EC2 Auto Scaling group to launch custom-AMI EC2 instances running the Docker containers to process the data.
- 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.
- D. Use an AWS Storage Gateway file gateway to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Batch job that executes on Amazon EC2 instances running the Docker containers to process the data.

Question #139

Topic 1

A company runs a content management application on a single Windows Amazon EC2 instance in a development environment. The application reads and writes static content to a 2 TB Amazon Elastic Block Store (Amazon EBS) volume that is attached to the instance as the root device. The company plans to deploy this application in production as a highly available and fault-tolerant solution that runs on at least three EC2 instances across multiple Availability Zones.

A solutions architect must design a solution that joins all the instances that run the application to an Active Directory domain. The solution also must implement Windows ACLs to control access to file contents. The application always must maintain exactly the same content on all running instances at any given point in time.

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

- A. Create an Amazon Elastic File System (Amazon EFS) file share. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to install the application, join the instance to the AD domain, and mount the EFS file share.
- B. Create a new AMI from the current EC2 Instance that is running. Create an Amazon FSx for Lustre file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to join the instance to the AD domain and mount the FSx for Lustre file system.
- C. Create an Amazon FSx for Windows File Server file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to install the application and mount the FSx for Windows File Server file system. Perform a seamless domain join to join the instance to the AD domain.
- D. Create a new AMI from the current EC2 instance that is running. Create an Amazon Elastic File System (Amazon EFS) file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three Instances. Perform a seamless domain join to join the instance to the AD domain.

Question #140

Topic 1

A software as a service (SaaS) based company provides a case management solution to customers A3 part of the solution. The company uses a standalone Simple Mail Transfer Protocol (SMTP) server to send email messages from an application. The application also stores an email template for acknowledgement email messages that populate customer data before the application sends the email message to the customer.

The company plans to migrate this messaging functionality to the AWS Cloud and needs to minimize operational overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Set up an SMTP server on Amazon EC2 instances by using an AMI from the AWS Marketplace. Store the email template in an Amazon S3 bucket. Create an AWS Lambda function to retrieve the template from the S3 bucket and to merge the customer data from the application with the template. Use an SDK in the Lambda function to send the email message.
- B. Set up Amazon Simple Email Service (Amazon SES) to send email messages. Store the email template in an Amazon S3 bucket. Create an AWS Lambda function to retrieve the template from the S3 bucket and to merge the customer data from the application with the template. Use an SDK in the Lambda function to send the email message.
- C. Set up an SMTP server on Amazon EC2 instances by using an AMI from the AWS Marketplace. Store the email template in Amazon Simple Email Service (Amazon SES) with parameters for the customer data. Create an AWS Lambda function to call the SES template and to pass customer data to replace the parameters. Use the AWS Marketplace SMTP server to send the email message.
- D. Set up Amazon Simple Email Service (Amazon SES) to send email messages. Store the email template on Amazon SES with parameters for the customer data. Create an AWS Lambda function to call the SendTemplatedEmail API operation and to pass customer data to replace the parameters and the email destination.

Question #141

Topic 1

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?

- A. Turn on termination protection for the EC2 Instances
- B. Update the visibility timeout for the SQS queue to 3 hours
- C. Configure scale-in protection for the instances during processing
- D. Update the redrive policy and set maxReceiveCount to 0.

Question #142

Topic 1

A company has developed APIs that use Amazon API Gateway with Regional endpoints. The APIs call AWS Lambda functions that use API Gateway authentication mechanisms. After a design review, a solutions architect identifies a set of APIs that do not require public access.

The solutions architect must design a solution to make the set of APIs accessible only from a VPC. All APIs need to be called with an authenticated user.

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

- A. Create an internal Application Load Balancer (ALB). Create a target group. Select the Lambda function to call. Use the ALB DNS name to call the API from the VPC.
- B. Remove the DNS entry that is associated with the API in API Gateway. Create a hosted zone in Amazon Route 53. Create a CNAME record in the hosted zone. Update the API in API Gateway with the CNAME record. Use the CNAME record to call the API from the VPC.
- C. Update the API endpoint from Regional to private in API Gateway. Create an interface VPC endpoint in the VPC. Create a resource policy, and attach it to the API. Use the VPC endpoint to call the API from the VPC.
- D. Deploy the Lambda functions inside the VPC. Provision an EC2 instance, and install an Apache server. From the Apache server, call the Lambda functions. Use the internal CNAME record of the EC2 instance to call the API from the VPC.

Question #143

Topic 1

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? (Choose two.)

- A. Configure the AWS Global Accelerator endpoint for the S3 bucket in eu-west-1. Configure endpoint groups for TCP ports 80 and 443 in us-east-1.
- 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.
- C. Use Lambda@Edge to modify requests from North America to use the S3 Transfer Acceleration endpoint in us-east-1.
- D. Use Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1.
- E. Configure the AWS Global Accelerator endpoint for us-east-1 as an origin on the CloudFront distribution. Use Lambda@Edge to modify requests from North America to use the new origin.

Question #144

Topic 1

A solutions architect is investigating an issue in which a company cannot establish new sessions in Amazon Workspaces. An initial analysis indicates that the issue involves user profiles. The Amazon Workspaces environment is configured to use Amazon FSx for Windows File Server as the profile share storage. The FSx for Windows File Server file system is configured with 10 TB of storage.

The solutions architect discovers that the file system has reached its maximum capacity. The solutions architect must ensure that users can regain access. The solution also must prevent the problem from occurring again.

Which solution will meet these requirements?

- A. Remove old user profiles to create space. Migrate the user profiles to an Amazon FSx for Lustre file system.
- B. Increase capacity by using the update-file-system command. Implement an Amazon CloudWatch metric that monitors free space. Use Amazon EventBridge to invoke an AWS Lambda function to increase capacity as required.
- C. Monitor the file system by using the FreeStorageCapacity metric in Amazon CloudWatch. Use AWS Step Functions to increase the capacity as required.
- D. Remove old user profiles to create space. Create an additional FSx for Windows File Server file system. Update the user profile redirection for 50% of the users to use the new file system.

Question #145

Topic 1

An international delivery company hosts a delivery management system on AWS. Drivers use the system to upload confirmation of delivery. Confirmation includes the recipient's signature or a photo of the package with the recipient. The driver's handheld device uploads signatures and photos through FTP to a single Amazon EC2 instance. Each handheld device saves a file in a directory based on the signed-in user, and the file name matches the delivery number. The EC2 instance then adds metadata to the file after querying a central database to pull delivery information. The file is then placed in Amazon S3 for archiving.

As the company expands, drivers report that the system is rejecting connections. The FTP server is having problems because of dropped connections and memory issues in response to these problems, a system engineer schedules a cron task to reboot the EC2 instance every 30 minutes. The billing team reports that files are not always in the archive and that the central system is not always updated.

A solutions architect needs to design a solution that maximizes scalability to ensure that the archive always receives the files and that systems are always updated. The handheld devices cannot be modified, so the company cannot deploy a new application.

Which solution will meet these requirements?

- A. Create an AMI of the existing EC2 instance. Create an Auto Scaling group of EC2 instances behind an Application Load Balancer. Configure the Auto Scaling group to have a minimum of three instances.
- B. Use AWS Transfer Family to create an FTP server that places the files in Amazon Elastic File System (Amazon EFS). Mount the EFS volume to the existing EC2 instance. Point the EC2 instance to the new path for file processing.
- C. Use AWS Transfer Family to create an FTP server that places the files in Amazon S3. Use an S3 event notification through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function. Configure the Lambda function to add the metadata and update the delivery system.
- D. Update the handheld devices to place the files directly in Amazon S3. Use an S3 event notification through Amazon Simple Queue Service (Amazon SQS) to invoke an AWS Lambda function. Configure the Lambda function to add the metadata and update the delivery system.

Question #146

Topic 1

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.
- B. Set up AWS DataSync for continuous replication of the data to a different Region.
- C. Set up AWS Database Migration Service (AWS DMS) to perform a continuous replication of the data to a different Region.
- D. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule a snapshot every 5 minutes.

Question #147

Topic 1

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?

- A. Invoke an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Invoke another Lambda function when new messages arrive in the SQS queue to process the records, writing the results to a temporary location in Amazon S3. Invoke a final Lambda function once the SQS queue is empty to transform the records into JSON format and send the results to another S3 bucket for internal processing.
- B. Invoke an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Configure an AWS Fargate container application to automatically scale to a single instance when the SQS queue contains messages. Have the application process each record, and transform the record into JSON format. When the queue is empty, send the results to another S3 bucket for internal processing and scale down the AWS Fargate instance.
- C. Create an AWS Glue crawler and custom classifier based on the data feed formats and build a table definition to match. Invoke an AWS Lambda function on file 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 ETL job send the results to another S3 bucket for internal processing.
- D. Create an AWS Glue crawler and custom classifier based upon the data feed formats and build a table definition to match. Perform an Amazon Athena query on file delivery to start an Amazon EMR ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, send the results to another S3 bucket for internal processing and scale down the EMR cluster.

Question #148

Topic 1

A company wants to use AWS to create a business continuity solution in case the company's main on-premises application fails. The application runs on physical servers that also run other applications. The on-premises application that the company is planning to migrate uses a MySQL database as a data store. All the company's on-premises applications use operating systems that are compatible with Amazon EC2.

Which solution will achieve the company's goal with the LEAST operational overhead?

- A. Install the AWS Replication Agent on the source servers, including the MySQL servers. Set up replication for all servers. Launch test instances for regular drills. Cut over to the test instances to fail over the workload in the case of a failure event.
- B. Install the AWS Replication Agent on the source servers, including the MySQL servers. Initialize AWS Elastic Disaster Recovery in the target AWS Region. Define the launch settings. Frequently perform failover and fallback from the most recent point in time.
- C. Create AWS Database Migration Service (AWS DMS) replication servers and a target Amazon Aurora MySQL DB cluster to host the database. Create a DMS replication task to copy the existing data to the target DB cluster. Create a local AWS Schema Conversion Tool (AWS SCT) change data capture (CDC) task to keep the data synchronized. Install the rest of the software on EC2 instances by starting with a compatible base AMI.
- D. Deploy an AWS Storage Gateway Volume Gateway on premises. Mount volumes on all on-premises servers. Install the application and the MySQL database on the new volumes. Take regular snapshots. Install all the software on EC2 Instances by starting with a compatible base AMI. Launch a Volume Gateway on an EC2 instance. Restore the volumes from the latest snapshot. Mount the new volumes on the EC2 instances in the case of a failure event.

Question #149

Topic 1

A company is subject to regulatory audits of its financial information. External auditors who use a single AWS account need access to the company's AWS account. A solutions architect must provide the auditors with secure, read-only access to the company's AWS account. The solution must comply with AWS security best practices.

Which solution will meet these requirements?

- A. In the company's AWS account, create resource policies for all resources in the account to grant access to the auditors' AWS account. Assign a unique external ID to the resource policy.
- B. In the company's AWS account, create an IAM role that trusts the auditors' AWS account. Create an IAM policy that has the required permissions. Attach the policy to the role. Assign a unique external ID to the role's trust policy.
- C. In the company's AWS account, create an IAM user. Attach the required IAM policies to the IAM user. Create API access keys for the IAM user. Share the access keys with the auditors.
- D. In the company's AWS account, create an IAM group that has the required permissions. Create an IAM user in the company's account for each auditor. Add the IAM users to the IAM group.

Question #150

Topic 1

A company has a latency-sensitive trading platform that uses Amazon DynamoDB as a storage backend. The company configured the DynamoDB table to use on-demand capacity mode. A solutions architect needs to design a solution to improve the performance of the trading platform. The new solution must ensure high availability for the trading platform.

Which solution will meet these requirements with the LEAST latency?

- A. Create a two-node DynamoDB Accelerator (DAX) cluster. Configure an application to read and write data by using DAX.
- B. Create a three-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.
- C. Create a three-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data directly from the DynamoDB table and to write data by using DAX.
- D. Create a single-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.

Question #151

Topic 1

A company has migrated an application from on premises to AWS. The application frontend is a static website that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB). The application backend is a Python application that runs on three EC2 instances behind another ALB. The EC2 instances are large, general purpose On-Demand Instances that were sized to meet the on-premises specifications for peak usage of the application.

The application averages hundreds of thousands of requests each month. However, the application is used mainly during lunchtime and receives minimal traffic during the rest of the day.

A solutions architect needs to optimize the infrastructure cost of the application without negatively affecting the application availability.

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

- A. Change all the EC2 instances to compute optimized instances that have the same number of cores as the existing EC2 instances.
- B. Move the application frontend to a static website that is hosted on Amazon S3.
- C. Deploy the application frontend by using AWS Elastic Beanstalk. Use the same instance type for the nodes.
- D. Change all the backend EC2 instances to Spot Instances.
- E. Deploy the backend Python application to general purpose burstable EC2 instances that have the same number of cores as the existing EC2 instances.

Question #152

Topic 1

A company is running an event ticketing platform on AWS and wants to optimize the platform's cost-effectiveness. The platform is deployed on Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 and is backed by an Amazon RDS for MySQL DB instance. The company is developing new application features to run on Amazon EKS with AWS Fargate.

The platform experiences infrequent high peaks in demand. The surges in demand depend on event dates.

Which solution will provide the MOST cost-effective setup for the platform?

- A. Purchase Standard Reserved Instances for the EC2 instances that the EKS cluster uses in its baseline load. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet predicted peak load for the year.
- B. Purchase Compute Savings Plans for the predicted medium load of the EKS cluster. Scale the cluster with On-Demand Capacity Reservations based on event dates for peaks. Purchase 1-year No Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale out database read replicas during peaks.
- C. Purchase EC2 Instance Savings Plans for the predicted base load of the EKS cluster. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale up the DB instance manually during peaks.
- D. Purchase Compute Savings Plans for the predicted base load of the EKS cluster. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale up the DB instance manually during peaks.

Question #153

Topic 1

A company has deployed an application on AWS Elastic Beanstalk. The application uses Amazon Aurora for the database layer. An Amazon CloudFront distribution serves web requests and includes the Elastic Beanstalk domain name as the origin server. The distribution is configured with an alternate domain name that visitors use when they access the application.

Each week, the company takes the application out of service for routine maintenance. During the time that the application is unavailable, the company wants visitors to receive an informational message instead of a CloudFront error message.

A solutions architect creates an Amazon S3 bucket as the first step in the process.

Which combination of steps should the solutions architect take next to meet the requirements? (Choose three.)

- A. Upload static informational content to the S3 bucket.
- B. Create a new CloudFront distribution. Set the S3 bucket as the origin.
- C. Set the S3 bucket as a second origin in the original CloudFront distribution. Configure the distribution and the S3 bucket to use an origin access identity (OAI).
- D. During the weekly maintenance, edit the default cache behavior to use the S3 origin. Revert the change when the maintenance is complete.
- E. During the weekly maintenance, create a cache behavior for the S3 origin on the new distribution. Set the path pattern to \ Set the precedence to 0. Delete the cache behavior when the maintenance is complete.
- F. During the weekly maintenance, configure Elastic Beanstalk to serve traffic from the S3 bucket.

Question #154

Topic 1

A company gives users the ability to upload images from a custom application. The upload process invokes an AWS Lambda function that processes and stores the image in an Amazon S3 bucket. The application invokes the Lambda function by using a specific function version ARN.

The Lambda function accepts image processing parameters by using environment variables. The company often adjusts the environment variables of the Lambda function to achieve optimal image processing output. The company tests different parameters and publishes a new function version with the updated environment variables after validating results. This update process also requires frequent changes to the custom application to invoke the new function version ARN. These changes cause interruptions for users.

A solutions architect needs to simplify this process to minimize disruption to users.

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

- A. Directly modify the environment variables of the published Lambda function version. Use the SLATEST version to test image processing parameters.
- B. Create an Amazon DynamoDB table to store the image processing parameters. Modify the Lambda function to retrieve the image processing parameters from the DynamoDB table.
- C. Directly code the image processing parameters within the Lambda function and remove the environment variables. Publish a new function version when the company updates the parameters.
- D. Create a Lambda function alias. Modify the client application to use the function alias ARN. Reconfigure the Lambda alias to point to new versions of the function when the company finishes testing.

Question #155

Topic 1

A global media company is planning a multi-Region deployment of an application. Amazon DynamoDB global tables will back the deployment to keep the user experience consistent across the two continents where users are concentrated. Each deployment will have a public Application Load Balancer (ALB). The company manages public DNS internally. The company wants to make the application available through an apex domain.

Which solution will meet these requirements with the LEAST effort?

- A. Migrate public DNS to Amazon Route 53. Create CNAME records for the apex domain to point to the ALB. Use a geolocation routing policy to route traffic based on user location.
- B. Place a Network Load Balancer (NLB) in front of the ALB. Migrate public DNS to Amazon Route 53. Create a CNAME record for the apex domain to point to the NLB's static IP address. Use a geolocation routing policy to route traffic based on user location.
- C. Create an AWS Global Accelerator accelerator with multiple endpoint groups that target endpoints in appropriate AWS Regions. Use the accelerator's static IP address to create a record in public DNS for the apex domain.
- D. Create an Amazon API Gateway API that is backed by AWS Lambda in one of the AWS Regions. Configure a Lambda function to route traffic to application deployments by using the round robin method. Create CNAME records for the apex domain to point to the API's URL.

Question #156

Topic 1

A company is developing a new serverless API by using Amazon API Gateway and AWS Lambda. The company integrated the Lambda functions with API Gateway to use several shared libraries and custom classes.

A solutions architect needs to simplify the deployment of the solution and optimize for code reuse.

Which solution will meet these requirements?

- A. Deploy the shared libraries and custom classes into a Docker image. Store the image in an S3 bucket. Create a Lambda layer that uses the Docker image as the source. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the Lambda layer.
- B. Deploy the shared libraries and custom classes to a Docker image. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Create a Lambda layer that uses the Docker image as the source. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the Lambda layer.
- C. Deploy the shared libraries and custom classes to a Docker container in Amazon Elastic Container Service (Amazon ECS) by using the AWS Fargate launch type. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the deployed container as a Lambda layer.
- D. Deploy the shared libraries, custom classes, and code for the API's Lambda functions to a Docker image. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Configure the API's Lambda functions to use the Docker image as the deployment package.

Question #157**Topic 1**

A manufacturing company is building an inspection solution for its factory. The company has IP cameras at the end of each assembly line. The company has used Amazon SageMaker to train a machine learning (ML) model to identify common defects from still images.

The company wants to provide local feedback to factory workers when a defect is detected. The company must be able to provide this feedback even if the factory's internet connectivity is down. The company has a local Linux server that hosts an API that provides local feedback to the workers.

How should the company deploy the ML model to meet these requirements?

- A. Set up an Amazon Kinesis video stream from each IP camera to AWS. Use Amazon EC2 instances to take still images of the streams. Upload the images to an Amazon S3 bucket. Deploy a SageMaker endpoint with the ML model. Invoke an AWS Lambda function to call the inference endpoint when new images are uploaded. Configure the Lambda function to call the local API when a defect is detected.
- B. Deploy AWS IoT Greengrass on the local server. Deploy the ML model to the Greengrass server. Create a Greengrass component to take still images from the cameras and run inference. Configure the component to call the local API when a defect is detected.
- C. Order an AWS Snowball device. Deploy a SageMaker endpoint the ML model and an Amazon EC2 instance on the Snowball device. Take still images from the cameras. Run inference from the EC2 instance. Configure the instance to call the local API when a defect is detected.
- D. Deploy Amazon Monitron devices on each IP camera. Deploy an Amazon Monitron Gateway on premises. Deploy the ML model to the Amazon Monitron devices. Use Amazon Monitron health state alarms to call the local API from an AWS Lambda function when a defect is detected.

Question #158**Topic 1**

A solutions architect must create a business case for migration of a company's on-premises data center to the AWS Cloud. The solutions architect will use a configuration management database (CMDB) export of all the company's servers to create the case.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Well-Architected Tool to import the CMDB data to perform an analysis and generate recommendations.
- B. Use Migration Evaluator to perform an analysis. Use the data import template to upload the data from the CMDB export.
- C. Implement resource matching rules. Use the CMDB export and the AWS Price List Bulk API to query CMDB data against AWS services in bulk.
- D. Use AWS Application Discovery Service to import the CMDB data to perform an analysis.

Question #159

Topic 1

A company has a website that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The ALB is associated with an AWS WAF web ACL.

The website often encounters attacks in the application layer. The attacks produce sudden and significant increases in traffic on the application server. The access logs show that each attack originates from different IP addresses. A solutions architect needs to implement a solution to mitigate these attacks.

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

- A. Create an Amazon CloudWatch alarm that monitors server access. Set a threshold based on access by IP address. Configure an alarm action that adds the IP address to the web ACL's deny list.
- B. Deploy AWS Shield Advanced in addition to AWS WAF. Add the ALB as a protected resource.
- C. Create an Amazon CloudWatch alarm that monitors user IP addresses. Set a threshold based on access by IP address. Configure the alarm to invoke an AWS Lambda function to add a deny rule in the application server's subnet route table for any IP addresses that activate the alarm.
- D. Inspect access logs to find a pattern of IP addresses that launched the attacks. Use an Amazon Route 53 geolocation routing policy to deny traffic from the countries that host those IP addresses.

Question #160

Topic 1

A company has a critical application in which the data tier is deployed in a single AWS Region. The data tier uses an Amazon DynamoDB table and an Amazon Aurora MySQL DB cluster. The current Aurora MySQL engine version supports a global database. The application tier is already deployed in two Regions.

Company policy states that critical applications must have application tier components and data tier components deployed across two Regions. The RTO and RPO must be no more than a few minutes each. A solutions architect must recommend a solution to make the data tier compliant with company policy.

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

- A. Add another Region to the Aurora MySQL DB cluster
- B. Add another Region to each table in the Aurora MySQL DB cluster
- C. Set up scheduled cross-Region backups for the DynamoDB table and the Aurora MySQL DB cluster
- D. Convert the existing DynamoDB table to a global table by adding another Region to its configuration
- E. Use Amazon Route 53 Application Recovery Controller to automate database backup and recovery to the secondary Region

Question #161

Topic 1

A telecommunications company is running an application on AWS. The company has set up an AWS Direct Connect connection between the company's on-premises data center and AWS. The company deployed the application on Amazon EC2 instances in multiple Availability Zones behind an internal Application Load Balancer (ALB). The company's clients connect from the on-premises network by using HTTPS. The TLS terminates in the ALB. The company has multiple target groups and uses path-based routing to forward requests based on the URL path.

The company is planning to deploy an on-premises firewall appliance with an allow list that is based on IP address. A solutions architect must develop a solution to allow traffic flow to AWS from the on-premises network so that the clients can continue to access the application.

Which solution will meet these requirements?

- A. Configure the existing ALB to use static IP addresses. Assign IP addresses in multiple Availability Zones to the ALB. Add the ALB IP addresses to the firewall appliance.
- B. Create a Network Load Balancer (NLB). Associate the NLB with one static IP addresses in multiple Availability Zones. Create an ALB-type target group for the NLB and add the existing ALB IP addresses to the firewall appliance. Update the clients to connect to the NLB.
- C. Create a Network Load Balancer (NLB). Associate the NLB with one static IP addresses in multiple Availability Zones. Add the existing target groups to the NLB. Update the clients to connect to the NLB. Delete the ALB. Add the NLB IP addresses to the firewall appliance.
- D. Create a Gateway Load Balancer (GWLB). Assign static IP addresses to the GWLB in multiple Availability Zones. Create an ALB-type target group for the GWLB and add the existing ALB. Add the GWLB IP addresses to the firewall appliance. Update the clients to connect to the GWLB.

Question #162

Topic 1

A company runs an application on a fleet of Amazon EC2 instances that are in private subnets behind an internet-facing Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. An AWS WAF web ACL that contains various AWS managed rules is associated with the CloudFront distribution.

The company needs a solution that will prevent internet traffic from directly accessing the ALB.

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

- A. Create a new web ACL that contains the same rules that the existing web ACL contains. Associate the new web ACL with the ALB.
- B. Associate the existing web ACL with the ALB.
- C. Add a security group rule to the ALB to allow traffic from the AWS managed prefix list for CloudFront only.
- D. Add a security group rule to the ALB to allow only the various CloudFront IP address ranges.

Question #163**Topic 1**

A company is running an application that uses an Amazon ElastiCache for Redis cluster as a caching layer. A recent security audit revealed that the company has configured encryption at rest for ElastiCache. However, the company did not configure ElastiCache to use encryption in transit. Additionally, users can access the cache without authentication.

A solutions architect must make changes to require user authentication and to ensure that the company is using end-to-end encryption.

Which solution will meet these requirements?

- A. Create an AUTH token. Store the token in AWS System Manager Parameter Store, as an encrypted parameter. Create a new cluster with AUTH, and configure encryption in transit. Update the application to retrieve the AUTH token from Parameter Store when necessary and to use the AUTH token for authentication.
- B. Create an AUTH token. Store the token in AWS Secrets Manager. Configure the existing cluster to use the AUTH token, and configure encryption in transit. Update the application to retrieve the AUTH token from Secrets Manager when necessary and to use the AUTH token for authentication.
- C. Create an SSL certificate. Store the certificate in AWS Secrets Manager. Create a new cluster, and configure encryption in transit. Update the application to retrieve the SSL certificate from Secrets Manager when necessary and to use the certificate for authentication.
- D. Create an SSL certificate. Store the certificate in AWS Systems Manager Parameter Store, as an encrypted advanced parameter. Update the existing cluster to configure encryption in transit. Update the application to retrieve the SSL certificate from Parameter Store when necessary and to use the certificate for authentication.

Question #164**Topic 1**

A company is running a compute workload by using Amazon EC2 Spot Instances that are in an Auto Scaling group. The launch template uses two placement groups and a single instance type.

Recently, a monitoring system reported Auto Scaling instance launch failures that correlated with longer wait times for system users. The company needs to improve the overall reliability of the workload.

Which solution will meet this requirement?

- A. Replace the launch template with a launch configuration to use an Auto Scaling group that uses attribute-based instance type selection.
- B. Create a new launch template version that uses attribute-based instance type selection. Configure the Auto Scaling group to use the new launch template version.
- C. Update the launch template Auto Scaling group to increase the number of placement groups.
- D. Update the launch template to use a larger instance type.

Question #165

Topic 1

A company is migrating a document processing workload to AWS. The company has updated many applications to natively use the Amazon S3 API to store, retrieve, and modify documents that a processing server generates at a rate of approximately 5 documents every second. After the document processing is finished, customers can download the documents directly from Amazon S3.

During the migration, the company discovered that it could not immediately update the processing server that generates many documents to support the S3 API. The server runs on Linux and requires fast local access to the files that the server generates and modifies. When the server finishes processing, the files must be available to the public for download within 30 minutes.

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

- A. Migrate the application to an AWS Lambda function. Use the AWS SDK for Java to generate, modify, and access the files that the company stores directly in Amazon S3.
- B. Set up an Amazon S3 File Gateway and configure a file share that is linked to the document store. Mount the file share on an Amazon EC2 instance by using NFS. When changes occur in Amazon S3, initiate a RefreshCache API call to update the S3 File Gateway.
- C. Configure Amazon FSx for Lustre with an import and export policy. Link the new file system to an S3 bucket. Install the Lustre client and mount the document store to an Amazon EC2 instance by using NFS.
- D. Configure AWS DataSync to connect to an Amazon EC2 instance. Configure a task to synchronize the generated files to and from Amazon S3.

Question #166

Topic 1

A delivery company is running a serverless solution in the AWS Cloud. The solution manages user data, delivery information, and past purchase details. The solution consists of several microservices. The central user service stores sensitive data in an Amazon DynamoDB table. Several of the other microservices store a copy of parts of the sensitive data in different storage services.

The company needs the ability to delete user information upon request. As soon as the central user service deletes a user, every other microservice must also delete its copy of the data immediately.

Which solution will meet these requirements?

- A. Activate DynamoDB Streams on the DynamoDB table. Create an AWS Lambda trigger for the DynamoDB stream that will post events about user deletion in an Amazon Simple Queue Service (Amazon SQS) queue. Configure each microservice to poll the queue and delete the user from the DynamoDB table.
- B. Set up DynamoDB event notifications on the DynamoDB table. Create an Amazon Simple Notification Service (Amazon SNS) topic as a target for the DynamoDB event notification. Configure each microservice to subscribe to the SNS topic and to delete the user from the DynamoDB table.
- C. Configure the central user service to post an event on a custom Amazon EventBridge event bus when the company deletes a user. Create an EventBridge rule for each microservice to match the user deletion event pattern and invoke logic in the microservice to delete the user from the DynamoDB table.
- D. Configure the central user service to post a message on an Amazon Simple Queue Service (Amazon SQS) queue when the company deletes a user. Configure each microservice to create an event filter on the SQS queue and to delete the user from the DynamoDB table.

Question #167

Topic 1

A company is running a web application in a VPC. The web application runs on a group of Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is using AWS WAF.

An external customer needs to connect to the web application. The company must provide IP addresses to all external customers.

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

- A. Replace the ALB with a Network Load Balancer (NLB). Assign an Elastic IP address to the NLB.
- B. Allocate an Elastic IP address. Assign the Elastic IP address to the ALB. Provide the Elastic IP address to the customer.
- C. Create an AWS Global Accelerator standard accelerator. Specify the ALB as the accelerator's endpoint. Provide the accelerator's IP addresses to the customer.
- D. Configure an Amazon CloudFront distribution. Set the ALB as the origin. Ping the distribution's DNS name to determine the distribution's public IP address. Provide the IP address to the customer.

Question #168

Topic 1

A company has a few AWS accounts for development and wants to move its production application to AWS. The company needs to enforce Amazon Elastic Block Store (Amazon EBS) encryption at rest for current production accounts and future production accounts only. The company needs a solution that includes built-in blueprints and guardrails.

Which combination of steps will meet these requirements? (Choose three.)

- A. Use AWS CloudFormation StackSets to deploy AWS Config rules on production accounts.
- B. Create a new AWS Control Tower landing zone in an existing developer account. Create OUs for accounts. Add production and development accounts to production and development OUs, respectively.
- C. Create a new AWS Control Tower landing zone in the company's management account. Add production and development accounts to production and development OUs, respectively.
- D. Invite existing accounts to join the organization in AWS Organizations. Create SCPs to ensure compliance.
- E. Create a guardrail from the management account to detect EBS encryption.
- F. Create a guardrail for the production OU to detect EBS encryption.

Question #169

Topic 1

A company is running a critical stateful web application on two Linux Amazon EC2 instances behind an Application Load Balancer (ALB) with an Amazon RDS for MySQL database. The company hosts the DNS records for the application in Amazon Route 53. A solutions architect must recommend a solution to improve the resiliency of the application.

The solution must meet the following objectives:

- Application tier: RPO of 2 minutes. RTO of 30 minutes
- Database tier: RPO of 5 minutes. RTO of 30 minutes

The company does not want to make significant changes to the existing application architecture. The company must ensure optimal latency after a failover.

Which solution will meet these requirements?

- A. Configure the EC2 instances to use AWS Elastic Disaster Recovery. Create a cross-Region read replica for the RDS DB instance. Create an ALB in a second AWS Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs. Update DNS records to point to the Global Accelerator endpoint.
- B. Configure the EC2 instances to use Amazon Data Lifecycle Manager (Amazon DLM) to take snapshots of the EBS volumes. Configure RDS automated backups. Configure backup replication to a second AWS Region. Create an ALB in the second Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs. Update DNS records to point to the Global Accelerator endpoint.
- C. Create a backup plan in AWS Backup for the EC2 instances and RDS DB instance. Configure backup replication to a second AWS Region. Create an ALB in the second Region. Configure an Amazon CloudFront distribution in front of the ALB. Update DNS records to point to CloudFront.
- D. Configure the EC2 instances to use Amazon Data Lifecycle Manager (Amazon DLM) to take snapshots of the EBS volumes. Create a cross-Region read replica for the RDS DB instance. Create an ALB in a second AWS Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs.

Question #170

Topic 1

A solutions architect wants to cost-optimize and appropriately size Amazon EC2 instances in a single AWS account. The solutions architect wants to ensure that the instances are optimized based on CPU, memory, and network metrics.

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

- A. Purchase AWS Business Support or AWS Enterprise Support for the account.
- B. Turn on AWS Trusted Advisor and review any “Low Utilization Amazon EC2 Instances” recommendations.
- C. Install the Amazon CloudWatch agent and configure memory metric collection on the EC2 instances.
- D. Configure AWS Compute Optimizer in the AWS account to receive findings and optimization recommendations.
- E. Create an EC2 Instance Savings Plan for the AWS Regions, instance families, and operating systems of interest.

Question #171**Topic 1**

A company uses an AWS CodeCommit repository. The company must store a backup copy of the data that is in the repository in a second AWS Region.

Which solution will meet these requirements?

- A. Configure AWS Elastic Disaster Recovery to replicate the CodeCommit repository data to the second Region.
- B. Use AWS Backup to back up the CodeCommit repository on an hourly schedule. Create a cross-Region copy in the second Region.
- C. Create an Amazon EventBridge rule to invoke AWS CodeBuild when the company pushes code to the repository. Use CodeBuild to clone the repository. Create a .zip file of the content. Copy the file to an S3 bucket in the second Region.
- D. Create an AWS Step Functions workflow on an hourly schedule to take a snapshot of the CodeCommit repository. Configure the workflow to copy the snapshot to an S3 bucket in the second Region

Question #172**Topic 1**

A company has multiple business units that each have separate accounts on AWS. Each business unit manages its own network with several VPCs that have CIDR ranges that overlap. The company's marketing team has created a new internal application and wants to make the application accessible to all the other business units. The solution must use private IP addresses only.

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

- A. Instruct each business unit to add a unique secondary CIDR range to the business unit's VPC. Peer the VPCs and use a private NAT gateway in the secondary range to route traffic to the marketing team.
- B. Create an Amazon EC2 instance to serve as a virtual appliance in the marketing account's VPC. Create an AWS Site-to-Site VPN connection between the marketing team and each business unit's VPC. Perform NAT where necessary.
- C. Create an AWS PrivateLink endpoint service to share the marketing application. Grant permission to specific AWS accounts to connect to the service. Create interface VPC endpoints in other accounts to access the application by using private IP addresses.
- D. Create a Network Load Balancer (NLB) in front of the marketing application in a private subnet. Create an API Gateway API. Use the Amazon API Gateway private integration to connect the API to the NLB. Activate IAM authorization for the API. Grant access to the accounts of the other business units.

Question #173**Topic 1**

A company needs to audit the security posture of a newly acquired AWS account. The company's data security team requires a notification only when an Amazon S3 bucket becomes publicly exposed. The company has already established an Amazon Simple Notification Service (Amazon SNS) topic that has the data security team's email address subscribed.

Which solution will meet these requirements?

- A. Create an S3 event notification on all S3 buckets for the isPublic event. Select the SNS topic as the target for the event notifications.
- B. Create an analyzer in AWS Identity and Access Management Access Analyzer. Create an Amazon EventBridge rule for the event type "Access Analyzer Finding" with a filter for "isPublic: true." Select the SNS topic as the EventBridge rule target.
- C. Create an Amazon EventBridge rule for the event type "Bucket-Level API Call via CloudTrail" with a filter for "PutBucketPolicy." Select the SNS topic as the EventBridge rule target.
- D. Activate AWS Config and add the clouptrail-s3-dataevents-enabled rule. Create an Amazon EventBridge rule for the event type "Config Rules Re-evaluation Status" with a filter for "NON_COMPLIANT." Select the SNS topic as the EventBridge rule target.

Question #174

Topic 1

A solutions architect needs to assess a newly acquired company's portfolio of applications and databases. The solutions architect must create a business case to migrate the portfolio to AWS. The newly acquired company runs applications in an on-premises data center. The data center is not well documented. The solutions architect cannot immediately determine how many applications and databases exist. Traffic for the applications is variable. Some applications are batch processes that run at the end of each month.

The solutions architect must gain a better understanding of the portfolio before a migration to AWS can begin.

Which solution will meet these requirements?

- A. Use AWS Server Migration Service (AWS SMS) and AWS Database Migration Service (AWS DMS) to evaluate migration. Use AWS Service Catalog to understand application and database dependencies.
- B. Use AWS Application Migration Service. Run agents on the on-premises infrastructure. Manage the agents by using AWS Migration Hub. Use AWS Storage Gateway to assess local storage needs and database dependencies.
- C. Use Migration Evaluator to generate a list of servers. Build a report for a business case. Use AWS Migration Hub to view the portfolio. Use AWS Application Discovery Service to gain an understanding of application dependencies.
- D. Use AWS Control Tower in the destination account to generate an application portfolio. Use AWS Server Migration Service (AWS SMS) to generate deeper reports and a business case. Use a landing zone for core accounts and resources.

Question #175

Topic 1

A company has an application that runs as a ReplicaSet of multiple pods in an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster has nodes in multiple Availability Zones. The application generates many small files that must be accessible across all running instances of the application. The company needs to back up the files and retain the backups for 1 year.

Which solution will meet these requirements while providing the FASTEST storage performance?

- A. Create an Amazon Elastic File System (Amazon EFS) file system and a mount target for each subnet that contains nodes in the EKS cluster. Configure the ReplicaSet to mount the file system. Direct the application to store files in the file system. Configure AWS Backup to back up and retain copies of the data for 1 year.
- B. Create an Amazon Elastic Block Store (Amazon EBS) volume. Enable the EBS Multi-Attach feature. Configure the ReplicaSet to mount the EBS volume. Direct the application to store files in the EBS volume. Configure AWS Backup to back up and retain copies of the data for 1 year.
- C. Create an Amazon S3 bucket. Configure the ReplicaSet to mount the S3 bucket. Direct the application to store files in the S3 bucket. Configure S3 Versioning to retain copies of the data. Configure an S3 Lifecycle policy to delete objects after 1 year.
- D. Configure the ReplicaSet to use the storage available on each of the running application pods to store the files locally. Use a third-party tool to back up the EKS cluster for 1 year.

Question #176

Topic 1

A company runs a customer service center that accepts calls and automatically sends all customers a managed, interactive, two-way experience survey by text message. The applications that support the customer service center run on machines that the company hosts in an on-premises data center. The hardware that the company uses is old, and the company is experiencing downtime with the system. The company wants to migrate the system to AWS to improve reliability.

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

- A. Use Amazon Connect to replace the old call center hardware. Use Amazon Pinpoint to send text message surveys to customers.
- B. Use Amazon Connect to replace the old call center hardware. Use Amazon Simple Notification Service (Amazon SNS) to send text message surveys to customers.
- C. Migrate the call center software to Amazon EC2 instances that are in an Auto Scaling group. Use the EC2 instances to send text message surveys to customers.
- D. Use Amazon Pinpoint to replace the old call center hardware and to send text message surveys to customers.

Question #177

Topic 1

A company is building a call center by using Amazon Connect. The company's operations team is defining a disaster recovery (DR) strategy across AWS Regions. The contact center has dozens of contact flows, hundreds of users, and dozens of claimed phone numbers.

Which solution will provide DR with the LOWEST RTO?

- A. Create an AWS Lambda function to check the availability of the Amazon Connect instance and to send a notification to the operations team in case of unavailability. Create an Amazon EventBridge rule to invoke the Lambda function every 5 minutes. After notification, instruct the operations team to use the AWS Management Console to provision a new Amazon Connect instance in a second Region. Deploy the contact flows, users, and claimed phone numbers by using an AWS CloudFormation template.
- B. Provision a new Amazon Connect instance with all existing users in a second Region. Create an AWS Lambda function to check the availability of the Amazon Connect instance. Create an Amazon EventBridge rule to invoke the Lambda function every 5 minutes. In the event of an issue, configure the Lambda function to deploy an AWS CloudFormation template that provisions contact flows and claimed numbers in the second Region.
- C. Provision a new Amazon Connect instance with all existing contact flows and claimed phone numbers in a second Region. Create an Amazon Route 53 health check for the URL of the Amazon Connect instance. Create an Amazon CloudWatch alarm for failed health checks. Create an AWS Lambda function to deploy an AWS CloudFormation template that provisions all users. Configure the alarm to invoke the Lambda function.
- D. Provision a new Amazon Connect instance with all existing users and contact flows in a second Region. Create an Amazon Route 53 health check for the URL of the Amazon Connect instance. Create an Amazon CloudWatch alarm for failed health checks. Create an AWS Lambda function to deploy an AWS CloudFormation template that provisions claimed phone numbers. Configure the alarm to invoke the Lambda function.

Question #178

Topic 1

A company runs an application on AWS. The company curates data from several different sources. The company uses proprietary algorithms to perform data transformations and aggregations. After the company performs ETL processes, the company stores the results in Amazon Redshift tables. The company sells this data to other companies. The company downloads the data as files from the Amazon Redshift tables and transmits the files to several data customers by using FTP. The number of data customers has grown significantly. Management of the data customers has become difficult.

The company will use AWS Data Exchange to create a data product that the company can use to share data with customers. The company wants to confirm the identities of the customers before the company shares data. The customers also need access to the most recent data when the company publishes the data.

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

- A. Use AWS Data Exchange for APIs to share data with customers. Configure subscription verification. In the AWS account of the company that produces the data, create an Amazon API Gateway Data API service integration with Amazon Redshift. Require the data customers to subscribe to the data product.
- B. In the AWS account of the company that produces the data, create an AWS Data Exchange datashare by connecting AWS Data Exchange to the Redshift cluster. Configure subscription verification. Require the data customers to subscribe to the data product.
- C. Download the data from the Amazon Redshift tables to an Amazon S3 bucket periodically. Use AWS Data Exchange for S3 to share data with customers. Configure subscription verification. Require the data customers to subscribe to the data product.
- D. Publish the Amazon Redshift data to an Open Data on AWS Data Exchange. Require the customers to subscribe to the data product in AWS Data Exchange. In the AWS account of the company that produces the data, attach IAM resource-based policies to the Amazon Redshift tables to allow access only to verified AWS accounts.

Question #179

Topic 1

A solutions architect is designing a solution to process events. The solution must have the ability to scale in and out based on the number of events that the solution receives. If a processing error occurs, the event must move into a separate queue for review.

Which solution will meet these requirements?

- A. Send event details to an Amazon Simple Notification Service (Amazon SNS) topic. Configure an AWS Lambda function as a subscriber to the SNS topic to process the events. Add an on-failure destination to the function. Set an Amazon Simple Queue Service (Amazon SQS) queue as the target.
- B. Publish events to an Amazon Simple Queue Service (Amazon SQS) queue. Create an Amazon EC2 Auto Scaling group. Configure the Auto Scaling group to scale in and out based on the ApproximateAgeOfOldestMessage metric of the queue. Configure the application to write failed messages to a dead-letter queue.
- C. Write events to an Amazon DynamoDB table. Configure a DynamoDB stream for the table. Configure the stream to invoke an AWS Lambda function. Configure the Lambda function to process the events.
- D. Publish events to an Amazon EventBridge event bus. Create and run an application on an Amazon EC2 instance with an Auto Scaling group that is behind an Application Load Balancer (ALB). Set the ALB as the event bus target. Configure the event bus to retry events. Write messages to a dead-letter queue if the application cannot process the messages.

Question #180

Topic 1

A company runs a processing engine in the AWS Cloud. The engine processes environmental data from logistics centers to calculate a sustainability index. The company has millions of devices in logistics centers that are spread across Europe. The devices send information to the processing engine through a RESTful API.

The API experiences unpredictable bursts of traffic. The company must implement a solution to process all data that the devices send to the processing engine. Data loss is unacceptable.

Which solution will meet these requirements?

- A. Create an Application Load Balancer (ALB) for the RESTful API. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create a listener and a target group for the ALB Add the SQS queue as the target. Use a container that runs in Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to process messages in the queue.
- B. Create an Amazon API Gateway HTTP API that implements the RESTful API. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create an API Gateway service integration with the SQS queue. Create an AWS Lambda function to process messages in the SQS queue.
- C. Create an Amazon API Gateway REST API that implements the RESTful API. Create a fleet of Amazon EC2 instances in an Auto Scaling group. Create an API Gateway Auto Scaling group proxy integration. Use the EC2 instances to process incoming data.
- D. Create an Amazon CloudFront distribution for the RESTful API. Create a data stream in Amazon Kinesis Data Streams. Set the data stream as the origin for the distribution. Create an AWS Lambda function to consume and process data in the data stream.

Question #181

Topic 1

A company is designing its network configuration in the AWS Cloud. The company uses AWS Organizations to manage a multi-account setup. The company has three OUs. Each OU contains more than 100 AWS accounts. Each account has a single VPC, and all the VPCs in each OU are in the same AWS Region.

The CIDR ranges for all the AWS accounts do not overlap. The company needs to implement a solution in which VPCs in the same OU can communicate with each other but cannot communicate with VPCs in other OUs.

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

- A. Create an AWS CloudFormation stack set that establishes VPC peering between accounts in each OU. Provision the stack set in each OU.
- B. In each OU, create a dedicated networking account that has a single VPC. Share this VPC with all the other accounts in the OU by using AWS Resource Access Manager (AWS RAM). Create a VPC peering connection between the networking account and each account in the OU.
- C. Provision a transit gateway in an account in each OU. Share the transit gateway across the organization by using AWS Resource Access Manager (AWS RAM). Create transit gateway VPC attachments for each VPC.
- D. In each OU, create a dedicated networking account that has a single VPC. Establish a VPN connection between the networking account and the other accounts in the OU. Use third-party routing software to route transitive traffic between the VPCs.

Question #182

Topic 1

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:

1. The data must be highly durable and available
2. The data must always be encrypted at rest and in transit
3. The encryption key must be managed by the company and rotated periodically

Which of the following solutions should the solutions architect recommend?

- A. Deploy the storage gateway to AWS in file gateway mode. Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes.
- B. Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.
- C. Use Amazon DynamoDB with SSL to connect to DynamoDB. Use an AWS KMS key to encrypt DynamoDB objects at rest.
- D. Deploy instances with Amazon EBS volumes attached to store this data. Use EBS volume encryption using an AWS KMS key to encrypt the data.

Question #183

Topic 1

A company's public API runs as tasks on Amazon Elastic Container Service (Amazon ECS). The tasks run on AWS Fargate behind an Application Load Balancer (ALB) and are configured with Service Auto Scaling for the tasks based on CPU utilization. This service has been running well for several months.

Recently, API performance slowed down and made the application unusable. The company discovered that a significant number of SQL injection attacks had occurred against the API and that the API service had scaled to its maximum amount.

A solutions architect needs to implement a solution that prevents SQL injection attacks from reaching the ECS API service. The solution must allow legitimate traffic through and must maximize operational efficiency.

Which solution meets these requirements?

- A. Create a new AWS WAF web ACL to monitor the HTTP requests and HTTPS requests that are forwarded to the ALB in front of the ECS tasks.
- B. Create a new AWS WAF Bot Control implementation. Add a rule in the AWS WAF Bot Control managed rule group to monitor traffic and allow only legitimate traffic to the ALB in front of the ECS tasks.
- C. Create a new AWS WAF web ACL. Add a new rule that blocks requests that match the SQL database rule group. Set the web ACL to allow all other traffic that does not match those rules. Attach the web ACL to the ALB in front of the ECS tasks.
- D. Create a new AWS WAF web ACL. Create a new empty IP set in AWS WAF. Add a new rule to the web ACL to block requests that originate from IP addresses in the new IP set. Create an AWS Lambda function that scrapes the API logs for IP addresses that send SQL injection attacks, and add those IP addresses to the IP set. Attach the web ACL to the ALB in front of the ECS tasks.

Question #184

Topic 1

An environmental company is deploying sensors in major cities throughout a country to measure air quality. The sensors connect to AWS IoT Core to ingest timeseries data readings. The company stores the data in Amazon DynamoDB.

For business continuity, the company must have the ability to ingest and store data in two AWS Regions.

Which solution will meet these requirements?

- A. Create an Amazon Route 53 alias failover routing policy with values for AWS IoT Core data endpoints in both Regions. Migrate data to Amazon Aurora global tables.
- B. Create a domain configuration for AWS IoT Core in each Region. Create an Amazon Route 53 latency-based routing policy. Use AWS IoT Core data endpoints in both Regions as values. Migrate the data to Amazon MemoryDB for Redis and configure cross-Region replication.
- C. Create a domain configuration for AWS IoT Core in each Region. Create an Amazon Route 53 health check that evaluates domain configuration health. Create a failover routing policy with values for the domain name from the AWS IoT Core domain configurations. Update the DynamoDB table to a global table.
- D. Create an Amazon Route 53 latency-based routing policy. Use AWS IoT Core data endpoints in both Regions as values. Configure DynamoDB streams and cross-Region data replication.

Question #185

Topic 1

A company uses AWS Organizations for a multi-account setup in the AWS Cloud. The company's finance team has a data processing application that uses AWS Lambda and Amazon DynamoDB. The company's marketing team wants to access the data that is stored in the DynamoDB table.

The DynamoDB table contains confidential data. The marketing team can have access to only specific attributes of data in the DynamoDB table. The finance team and the marketing team have separate AWS accounts.

What should a solutions architect do to provide the marketing team with the appropriate access to the DynamoDB table?

- A. Create an SCP to grant the marketing team's AWS account access to the specific attributes of the DynamoDB table. Attach the SCP to the OU of the finance team.
- B. Create an IAM role in the finance team's account by using IAM policy conditions for specific DynamoDB attributes (fine-grained access control). Establish trust with the marketing team's account. In the marketing team's account, create an IAM role that has permissions to assume the IAM role in the finance team's account.
- C. Create a resource-based IAM policy that includes conditions for specific DynamoDB attributes (fine-grained access control). Attach the policy to the DynamoDB table. In the marketing team's account, create an IAM role that has permissions to access the DynamoDB table in the finance team's account.
- D. Create an IAM role in the finance team's account to access the DynamoDB table. Use an IAM permissions boundary to limit the access to the specific attributes. In the marketing team's account, create an IAM role that has permissions to assume the IAM role in the finance team's account.

Question #186

Topic 1

A solutions architect is creating an application that stores objects in an Amazon S3 bucket. The solutions architect must deploy the application in two AWS Regions that will be used simultaneously. The objects in the two S3 buckets must remain synchronized with each other.

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

- A. Create an S3 Multi-Region Access Point Change the application to refer to the Multi-Region Access Point
- B. Configure two-way S3 Cross-Region Replication (CRR) between the two S3 buckets
- C. Modify the application to store objects in each S3 bucket
- D. Create an S3 Lifecycle rule for each S3 bucket to copy objects from one S3 bucket to the other S3 bucket
- E. Enable S3 Versioning for each S3 bucket
- F. Configure an event notification for each S3 bucket to invoke an AWS Lambda function to copy objects from one S3 bucket to the other S3 bucket

Question #187

Topic 1

A company has an IoT platform that runs in an on-premises environment. The platform consists of a server that connects to IoT devices by using the MQTT protocol. The platform collects telemetry data from the devices at least once every 5 minutes. The platform also stores device metadata in a MongoDB cluster.

An application that is installed on an on-premises machine runs periodic jobs to aggregate and transform the telemetry and device metadata. The application creates reports that users view by using another web application that runs on the same on-premises machine. The periodic jobs take 120-600 seconds to run. However, the web application is always running.

The company is moving the platform to AWS and must reduce the operational overhead of the stack.

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

- A. Use AWS Lambda functions to connect to the IoT devices
- B. Configure the IoT devices to publish to AWS IoT Core
- C. Write the metadata to a self-managed MongoDB database on an Amazon EC2 instance
- D. Write the metadata to Amazon DocumentDB (with MongoDB compatibility)
- E. Use AWS Step Functions state machines with AWS Lambda tasks to prepare the reports and to write the reports to Amazon S3. Use Amazon CloudFront with an S3 origin to serve the reports
- F. Use an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with Amazon EC2 instances to prepare the reports. Use an ingress controller in the EKS cluster to serve the reports

Question #188**Topic 1**

A global manufacturing company plans to migrate the majority of its applications to AWS. However, the company is concerned about applications that need to remain within a specific country or in the company's central on-premises data center because of data regulatory requirements or requirements for latency of single-digit milliseconds. The company also is concerned about the applications that it hosts in some of its factory sites, where limited network infrastructure exists.

The company wants a consistent developer experience so that its developers can build applications once and deploy on premises, in the cloud, or in a hybrid architecture. The developers must be able to use the same tools, APIs, and services that are familiar to them.

Which solution will provide a consistent hybrid experience to meet these requirements?

- A. Migrate all applications to the closest AWS Region that is compliant. Set up an AWS Direct Connect connection between the central on-premises data center and AWS. Deploy a Direct Connect gateway.
- B. Use AWS Snowball Edge Storage Optimized devices for the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds. Retain the devices on premises. Deploy AWS Wavelength to host the workloads in the factory sites.
- C. Install AWS Outposts for the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds. Use AWS Snowball Edge Compute Optimized devices to host the workloads in the factory sites.
- D. Migrate the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds to an AWS Local Zone. Deploy AWS Wavelength to host the workloads in the factory sites.

Question #189**Topic 1**

A company is updating an application that customers use to make online orders. The number of attacks on the application by bad actors has increased recently.

The company will host the updated application on an Amazon Elastic Container Service (Amazon ECS) cluster. The company will use Amazon DynamoDB to store application data. A public Application Load Balancer (ALB) will provide end users with access to the application. The company must prevent attacks and ensure business continuity with minimal service interruptions during an ongoing attack.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Create an Amazon CloudFront distribution with the ALB as the origin. Add a custom header and random value on the CloudFront domain. Configure the ALB to conditionally forward traffic if the header and value match.
- B. Deploy the application in two AWS Regions. Configure Amazon Route 53 to route to both Regions with equal weight.
- C. Configure auto scaling for Amazon ECS tasks Create a DynamoDB Accelerator (DAX) cluster.
- D. Configure Amazon ElastiCache to reduce overhead on DynamoDB.
- E. Deploy an AWS WAF web ACL that includes an appropriate rule group. Associate the web ACL with the Amazon CloudFront distribution.

Question #190

Topic 1

A company runs a web application on AWS. The web application delivers static content from an Amazon S3 bucket that is behind an Amazon CloudFront distribution. The application serves dynamic content by using an Application Load Balancer (ALB) that distributes requests to a fleet of Amazon EC2 instances in Auto Scaling groups. The application uses a domain name setup in Amazon Route 53.

Some users reported occasional issues when the users attempted to access the website during peak hours. An operations team found that the ALB sometimes returned HTTP 503 Service Unavailable errors. The company wants to display a custom error message page when these errors occur. The page should be displayed immediately for this error code.

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

- A. Set up a Route 53 failover routing policy. Configure a health check to determine the status of the ALB endpoint and to fail over to the failover S3 bucket endpoint.
- B. Create a second CloudFront distribution and an S3 static website to host the custom error page. Set up a Route 53 failover routing policy. Use an active-passive configuration between the two distributions.
- C. Create a CloudFront origin group that has two origins. Set the ALB endpoint as the primary origin. For the secondary origin, set an S3 bucket that is configured to host a static website. Set up origin failover for the CloudFront distribution. Update the S3 static website to incorporate the custom error page.
- D. Create a CloudFront function that validates each HTTP response code that the ALB returns. Create an S3 static website in an S3 bucket. Upload the custom error page to the S3 bucket as a failover. Update the function to read the S3 bucket and to serve the error page to the end users.

Question #191

Topic 1

A company is planning to migrate an application to AWS. The application runs as a Docker container and uses an NFS version 4 file share.

A solutions architect must design a secure and scalable containerized solution that does not require provisioning or management of the underlying infrastructure.

Which solution will meet these requirements?

- A. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. Use Amazon Elastic File System (Amazon EFS) for shared storage. Reference the EFS file system ID, container mount point, and EFS authorization IAM role in the ECS task definition.
- B. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. Use Amazon FSx for Lustre for shared storage. Reference the FSx for Lustre file system ID, container mount point, and FSx for Lustre authorization IAM role in the ECS task definition.
- C. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type and auto scaling turned on. Use Amazon Elastic File System (Amazon EFS) for shared storage. Mount the EFS file system on the ECS container instances. Add the EFS authorization IAM role to the EC2 instance profile.
- D. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type and auto scaling turned on. Use Amazon Elastic Block Store (Amazon EBS) volumes with Multi-Attach enabled for shared storage. Attach the EBS volumes to ECS container instances. Add the EBS authorization IAM role to an EC2 instance profile.

Question #192

Topic 1

A company is running an application in the AWS Cloud. The core business logic is running on a set of Amazon EC2 instances in an Auto Scaling group. An Application Load Balancer (ALB) distributes traffic to the EC2 instances. Amazon Route 53 record api.example.com is pointing to the ALB.

The company's development team makes major updates to the business logic. The company has a rule that when changes are deployed, only 10% of customers can receive the new logic during a testing window. A customer must use the same version of the business logic during the testing window.

How should the company deploy the updates to meet these requirements?

- A. Create a second ALB, and deploy the new logic to a set of EC2 instances in a new Auto Scaling group. Configure the ALB to distribute traffic to the EC2 instances. Update the Route 53 record to use weighted routing, and point the record to both of the ALBs.
- B. Create a second target group that is referenced by the ALB. Deploy the new logic to EC2 instances in this new target group. Update the ALB listener rule to use weighted target groups. Configure ALB target group stickiness.
- C. Create a new launch configuration for the Auto Scaling group. Specify the launch configuration to use the AutoScalingRollingUpdate policy, and set the MaxBatchSize option to 10. Replace the launch configuration on the Auto Scaling group. Deploy the changes.
- D. Create a second Auto Scaling group that is referenced by the ALB. Deploy the new logic on a set of EC2 instances in this new Auto Scaling group. Change the ALB routing algorithm to least outstanding requests (LOR). Configure ALB session stickiness.

Question #193

Topic 1

A large education company recently introduced Amazon Workspaces to provide access to internal applications across multiple universities. The company is storing user profiles on an Amazon FSx for Windows File Server file system. The file 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?

- A. Use AWS Backup to create a point-in-time backup of the file system. Restore the backup to a new FSx for Windows File Server file system. Select SSD as the storage type. Select 32 MBps as the throughput capacity. When the backup and restore process is completed, adjust the DNS alias accordingly. Delete the original file system.
- B. Disconnect users from the file system. In the Amazon FSx console, update the throughput capacity to 32 MBps. Update the storage type to SSD. Reconnect users to the file system.
- C. Deploy an AWS DataSync agent onto a new Amazon EC2 instance. Create a task. Configure the existing file system as the source location. Configure a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput as the target location. Schedule the task. When the task is completed, adjust the DNS alias accordingly. Delete the original file system.
- 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.

Question #194

Topic 1

A company hosts an application on AWS. The application reads and writes objects that are stored in a single Amazon S3 bucket. The company must modify the application to deploy the application in two AWS Regions.

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

- A. Set up an Amazon CloudFront distribution with the S3 bucket as an origin. Deploy the application to a second Region. Modify the application to use the CloudFront distribution. Use AWS Global Accelerator to access the data in the S3 bucket.
- B. Create a new S3 bucket in a second Region. Set up bidirectional S3 Cross-Region Replication (CRR) between the original S3 bucket and the new S3 bucket. Configure an S3 Multi-Region Access Point that uses both S3 buckets. Deploy a modified application to both Regions.
- C. Create a new S3 bucket in a second Region. Deploy the application in the second Region. Configure the application to use the new S3 bucket. Set up S3 Cross-Region Replication (CRR) from the original S3 bucket to the new S3 bucket.
- D. Set up an S3 gateway endpoint with the S3 bucket as an origin. Deploy the application to a second Region. Modify the application to use the new S3 gateway endpoint. Use S3 Intelligent-Tiering on the S3 bucket.

Question #195

Topic 1

An online gaming company needs to rehost its gaming platform on AWS. The company's gaming application requires high performance computing (HPC) processing and has a leaderboard that changes frequently. An Ubuntu instance that is optimized for compute generation hosts a Node.js application for game display. Game state is tracked in an on-premises Redis instance.

The company needs a migration strategy that optimizes application performance.

Which solution will meet these requirements?

- A. Create an Auto Scaling group of m5.large Amazon EC2 Spot Instances behind an Application Load Balancer. Use an Amazon ElastiCache for Redis cluster to maintain the leaderboard.
- B. Create an Auto Scaling group of c5.large Amazon EC2 Spot Instances behind an Application Load Balancer. Use an Amazon OpenSearch Service cluster to maintain the leaderboard.
- C. Create an Auto Scaling group of c5.large Amazon EC2 On-Demand Instances behind an Application Load Balancer. Use an Amazon ElastiCache for Redis cluster to maintain the leaderboard.
- D. Create an Auto Scaling group of m5.large Amazon EC2 On-Demand Instances behind an Application Load Balancer. Use an Amazon DynamoDB table to maintain the leaderboard.

Question #196

Topic 1

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? (Choose two.)

- A. Deploy the application to Amazon EC2 On-Demand Instances with load balancing across multiple Availability Zones. Use scheduled Amazon EC2 Auto Scaling to add capacity before the high volume of submissions on Fridays.
- 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.
- C. Deploy the application front end to an Amazon S3 bucket served by Amazon CloudFront. Deploy the application backend using Amazon API Gateway with an AWS Lambda proxy integration.
- D. Store the timesheet submission data in Amazon Redshift. Use Amazon QuickSight to generate the reports using Amazon Redshift as the data source.
- E. Store the timesheet submission data in Amazon S3. Use Amazon Athena and Amazon QuickSight to generate the reports using Amazon S3 as the data source.

Question #197

Topic 1

A company is storing sensitive data in an Amazon S3 bucket. The company must log all activities for objects in the S3 bucket and must keep the logs for 5 years. The company's security team also must receive an email notification every time there is an attempt to delete data in the S3 bucket.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

- A. Configure AWS CloudTrail to log S3 data events.
- B. Configure S3 server access logging for the S3 bucket.
- C. Configure Amazon S3 to send object deletion events to Amazon Simple Email Service (Amazon SES).
- D. Configure Amazon S3 to send object deletion events to an Amazon EventBridge event bus that publishes to an Amazon Simple Notification Service (Amazon SNS) topic.
- E. Configure Amazon S3 to send the logs to Amazon Timestream with data storage tiering.
- F. Configure a new S3 bucket to store the logs with an S3 Lifecycle policy.

Question #198

Topic 1

A company is building a hybrid environment that includes servers in an on-premises data center and in the AWS Cloud. The company has deployed Amazon EC2 instances in three VPCs. Each VPC is in a different AWS Region. The company has established an AWS Direct Connect connection to the data center from the Region that is closest to the data center.

The company needs the servers in the on-premises data center to have access to the EC2 instances in all three VPCs. The servers in the on-premises data center also must have access to AWS public services.

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

- A. Create a Direct Connect gateway in the Region that is closest to the data center. Attach the Direct Connect connection to the Direct Connect gateway. Use the Direct Connect gateway to connect the VPCs in the other two Regions.
- B. Set up additional Direct Connect connections from the on-premises data center to the other two Regions.
- C. Create a private VIF. Establish an AWS Site-to-Site VPN connection over the private VIF to the VPCs in the other two Regions.
- D. Create a public VIF. Establish an AWS Site-to-Site VPN connection over the public VIF to the VPCs in the other two Regions.
- E. Use VPC peering to establish a connection between the VPCs across the Regions. Create a private VIF with the existing Direct Connect connection to connect to the peered VPCs.

Question #199

Topic 1

A company is using an organization in AWS Organizations to manage hundreds of AWS accounts. A solutions architect is working on a solution to provide baseline protection for the Open Web Application Security Project (OWASP) top 10 web application vulnerabilities. The solutions architect is using AWS WAF for all existing and new Amazon CloudFront distributions that are deployed within the organization.

Which combination of steps should the solutions architect take to provide the baseline protection? (Choose three.)

- A. Enable AWS Config in all accounts
- B. Enable Amazon GuardDuty in all accounts
- C. Enable all features for the organization
- D. Use AWS Firewall Manager to deploy AWS WAF rules in all accounts for all CloudFront distributions
- E. Use AWS Shield Advanced to deploy AWS WAF rules in all accounts for all CloudFront distributions
- F. Use AWS Security Hub to deploy AWS WAF rules in all accounts for all CloudFront distributions

Question #200

Topic 1

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.)

- A. The IAM user's permissions policy has allowed the use of SAML federation for that user.
- B. The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.
- B. Test users are not in the AWSFederatedUsers group in the company's IdP.
- C. 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.
- D. The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs.
- E. The company's IdP defines SAML assertions that properly map users or groups. In the company to IAM roles with appropriate permissions.

Question #201

Topic 1

A solutions architect needs to improve an application that is hosted in the AWS Cloud. The application uses an Amazon Aurora MySQL DB instance that is experiencing overloaded connections. Most of the application's operations insert records into the database. The application currently stores credentials in a text-based configuration file.

The solutions architect needs to implement a solution so that the application can handle the current connection load. The solution must keep the credentials secure and must provide the ability to rotate the credentials automatically on a regular basis.

Which solution will meet these requirements?

- A. Deploy an Amazon RDS Proxy layer. In front of the DB instance. Store the connection credentials as a secret in AWS Secrets Manager.
- B. Deploy an Amazon RDS Proxy layer in front of the DB instance. Store the connection credentials in AWS Systems Manager Parameter Store
- C. Create an Aurora Replica. Store the connection credentials as a secret in AWS Secrets Manager
- D. Create an Aurora Replica. Store the connection credentials in AWS Systems Manager Parameter Store.

Question #202

Topic 1

A company needs to build a disaster recovery (DR) solution for its ecommerce website. The web application is hosted on a fleet of t3.large Amazon EC2 instances and uses an Amazon RDS for MySQL DB instance. The EC2 instances are in an Auto Scaling group that extends across multiple Availability Zones.

In the event of a disaster, the web application must fail over to the secondary environment with an RPO of 30 seconds and an RTO of 10 minutes.

Which solution will meet these requirements MOST cost-effectively?

- A. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create a cross-Region read replica for the DB instance. Set up a backup plan in AWS Backup to create cross-Region backups for the EC2 instances and the DB instance. Create a cron expression to back up the EC2 instances and the DB instance every 30 seconds to the DR Region. Recover the EC2 instances from the latest EC2 backup. Use an Amazon Route 53 geolocation routing policy to automatically fail over to the DR Region in the event of a disaster.
- B. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create a cross-Region read replica for the DB instance. Set up AWS Elastic Disaster Recovery to continuously replicate the EC2 instances to the DR Region. Run the EC2 instances at the minimum capacity in the DR Region. Use an Amazon Route 53 failover routing policy to automatically fail over to the DR Region in the event of a disaster. Increase the desired capacity of the Auto Scaling group.
- C. Set up a backup plan in AWS Backup to create cross-Region backups for the EC2 instances and the DB instance. Create a cron expression to back up the EC2 instances and the DB instance every 30 seconds to the DR Region. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Manually restore the backed-up data on new instances. Use an Amazon Route 53 simple routing policy to automatically fail over to the DR Region in the event of a disaster.
- D. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create an Amazon Aurora global database. Set up AWS Elastic Disaster Recovery to continuously replicate the EC2 instances to the DR Region. Run the Auto Scaling group of EC2 instances at full capacity in the DR Region. Use an Amazon Route 53 failover routing policy to automatically fail over to the DR Region in the event of a disaster.

Question #203

Topic 1

A company is planning a one-time migration of an on-premises MySQL database to Amazon Aurora MySQL in the us-east-1 Region. The company's current internet connection has limited bandwidth. The on-premises MySQL database is 60 TB in size. The company estimates that it will take a month to transfer the data to AWS over the current internet connection. The company needs a migration solution that will migrate the database more quickly.

Which solution will migrate the database in the LEAST amount of time?

- A. Request a 1 Gbps AWS Direct Connect connection between the on-premises data center and AWS. Use AWS Database Migration Service (AWS DMS) to migrate the on-premises MySQL database to Aurora MySQL.
- B. Use AWS DataSync with the current internet connection to accelerate the data transfer between the on-premises data center and AWS. Use AWS Application Migration Service to migrate the on-premises MySQL database to Aurora MySQL.
- C. Order an AWS Snowball Edge device. Load the data into an Amazon S3 bucket by using the S3 interface. Use AWS Database Migration Service (AWS DMS) to migrate the data from Amazon S3 to Aurora MySQL.
- D. Order an AWS Snowball device. Load the data into an Amazon S3 bucket by using the S3 Adapter for Snowball. Use AWS Application Migration Service to migrate the data from Amazon S3 to Aurora MySQL.

Question #204

Topic 1

A company has an application in the AWS Cloud. The application runs on a fleet of 20 Amazon EC2 instances. The EC2 instances are persistent and store data on multiple attached Amazon Elastic Block Store (Amazon EBS) volumes.

The company must maintain backups in a separate AWS Region. The company must be able to recover the EC2 instances and their configuration within 1 business day, with loss of no more than 1 day's worth of data. The company has limited staff and needs a backup solution that optimizes operational efficiency and cost. The company already has created an AWS CloudFormation template that can deploy the required network configuration in a secondary Region.

Which solution will meet these requirements?

- A. Create a second CloudFormation template that can recreate the EC2 instances in the secondary Region. Run daily multivolume snapshots by using AWS Systems Manager Automation runbooks. Copy the snapshots to the secondary Region. In the event of a failure launch the CloudFormation templates, restore the EBS volumes from snapshots, and transfer usage to the secondary Region.
- B. Use Amazon Data Lifecycle Manager (Amazon DLM) to create daily multivolume snapshots of the EBS volumes. In the event of a failure, launch the CloudFormation template and use Amazon DLM to restore the EBS volumes and transfer usage to the secondary Region.
- C. Use AWS Backup to create a scheduled daily backup plan for the EC2 instances. Configure the backup task to copy the backups to a vault in the secondary Region. In the event of a failure, launch the CloudFormation template, restore the instance volumes and configurations from the backup vault, and transfer usage to the secondary Region.
- D. Deploy EC2 instances of the same size and configuration to the secondary Region. Configure AWS DataSync daily to copy data from the primary Region to the secondary Region. In the event of a failure, launch the CloudFormation template and transfer usage to the secondary Region.

Question #205

Topic 1

A company is designing a new website that hosts static content. The website will give users the ability to upload and download large files. According to company requirements, all data must be encrypted in transit and at rest. A solutions architect is building the solution by using Amazon S3 and Amazon CloudFront.

Which combination of steps will meet the encryption requirements? (Choose three.)

- A. Turn on S3 server-side encryption for the S3 bucket that the web application uses.
- B. Add a policy attribute of "aws:SecureTransport": "true" for read and write operations in the S3 ACLs.
- C. Create a bucket policy that denies any unencrypted operations in the S3 bucket that the web application uses.
- D. Configure encryption at rest on CloudFront by using server-side encryption with AWS KMS keys (SSE-KMS).
- E. Configure redirection of HTTP requests to HTTPS requests in CloudFront.
- F. Use the RequireSSL option in the creation of presigned URLs for the S3 bucket that the web application uses.

Question #206

Topic 1

A company is implementing a serverless architecture by using AWS Lambda functions that need to access a Microsoft SQL Server DB instance on Amazon RDS. The company has separate environments for development and production, including a clone of the database system.

The company's developers are allowed to access the credentials for the development database. However, the credentials for the production database must be encrypted with a key that only members of the IT security team's IAM user group can access. This key must be rotated on a regular basis.

What should a solutions architect do in the production environment to meet these requirements?

- A. Store the database credentials in AWS Systems Manager Parameter Store by using a SecureString parameter that is encrypted by an AWS Key Management Service (AWS KMS) customer managed key. Attach a role to each Lambda function to provide access to the SecureString parameter. Restrict access to the SecureString parameter and the customer managed key so that only the IT security team can access the parameter and the key.
- B. Encrypt the database credentials by using the AWS Key Management Service (AWS KMS) default Lambda key. Store the credentials in the environment variables of each Lambda function. Load the credentials from the environment variables in the Lambda code. Restrict access to the KMS key so that only the IT security team can access the key.
- C. Store the database credentials in the environment variables of each Lambda function. Encrypt the environment variables by using an AWS Key Management Service (AWS KMS) customer managed key. Restrict access to the customer managed key so that only the IT security team can access the key.
- D. Store the database credentials in AWS Secrets Manager as a secret that is associated with an AWS Key Management Service (AWS KMS) customer managed key. Attach a role to each Lambda function to provide access to the secret. Restrict access to the secret and the customer managed key so that only the IT security team can access the secret and the key.

Question #207

Topic 1

An online retail company is migrating its legacy on-premises .NET application to AWS. The application runs on load-balanced frontend web servers, load-balanced application servers, and a Microsoft SQL Server database.

The company wants to use AWS managed services where possible and does not want to rewrite the application. A solutions architect needs to implement a solution to resolve scaling issues and minimize licensing costs as the application scales.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer for the web tier and for the application tier. Use Amazon Aurora PostgreSQL with Babelfish turned on to replatform the SQL Server database.
- B. Create images of all the servers by using AWS Database Migration Service (AWS DMS). Deploy Amazon EC2 instances that are based on the on-premises imports. Deploy the instances in an Auto Scaling group behind a Network Load Balancer for the web tier and for the application tier. Use Amazon DynamoDB as the database tier.
- C. Containerize the web frontend tier and the application tier. Provision an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Create an Auto Scaling group behind a Network Load Balancer for the web tier and for the application tier. Use Amazon RDS for SQL Server to host the database.
- D. Separate the application functions into AWS Lambda functions. Use Amazon API Gateway for the web frontend tier and the application tier. Migrate the data to Amazon S3. Use Amazon Athena to query the data.

Question #208

Topic 1

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-1 Region. 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?

- A. Add an Amazon CloudFront distribution. Configure the ALB as the origin.
- B. Add an Amazon API Gateway edge-optimized API endpoint to expose the APIs. Configure the ALB as the target.
- C. Add an accelerator in AWS Global Accelerator. Configure the ALB as the origin.
- D. Deploy the APIs to two additional AWS Regions: eu-west-1 and ap-southeast-2. Add latency-based routing records in Amazon Route 53.

Question #209

Topic 1

A company runs an IoT application in the AWS Cloud. The company has millions of sensors that collect data from houses in the United States. The sensors use the MQTT protocol to connect and send data to a custom MQTT broker. The MQTT broker stores the data on a single Amazon EC2 instance. The sensors connect to the broker through the domain named `iot.example.com`. The company uses Amazon Route 53 as its DNS service. The company stores the data in Amazon DynamoDB.

On several occasions, the amount of data has overloaded the MQTT broker and has resulted in lost sensor data. The company must improve the reliability of the solution.

Which solution will meet these requirements?

- A. Create an Application Load Balancer (ALB) and an Auto Scaling group for the MQTT broker. Use the Auto Scaling group as the target for the ALB. Update the DNS record in Route 53 to an alias record. Point the alias record to the ALB. Use the MQTT broker to store the data.
- B. Set up AWS IoT Core to receive the sensor data. Create and configure a custom domain to connect to AWS IoT Core. Update the DNS record in Route 53 to point to the AWS IoT Core Data-ATS endpoint. Configure an AWS IoT rule to store the data.
- C. Create a Network Load Balancer (NLB). Set the MQTT broker as the target. Create an AWS Global Accelerator accelerator. Set the NLB as the endpoint for the accelerator. Update the DNS record in Route 53 to a multivalue answer record. Set the Global Accelerator IP addresses as values. Use the MQTT broker to store the data.
- D. Set up AWS IoT Greengrass to receive the sensor data. Update the DNS record in Route 53 to point to the AWS IoT Greengrass endpoint. Configure an AWS IoT rule to invoke an AWS Lambda function to store the data.

Question #210

Topic 1

A company has Linux-based Amazon EC2 instances. Users must access the instances by using SSH with EC2 SSH key pairs. Each machine requires a unique EC2 key pair.

The company wants to implement a key rotation policy that will, upon request, automatically rotate all the EC2 key pairs and keep the keys in a securely encrypted place. The company will accept less than 1 minute of downtime during key rotation.

Which solution will meet these requirements?

- A. Store all the keys in AWS Secrets Manager. Define a Secrets Manager rotation schedule to invoke an AWS Lambda function to generate new key pairs. Replace public keys on EC2 instances. Update the private keys in Secrets Manager.
- B. Store all the keys in Parameter Store, a capability of AWS Systems Manager, as a string. Define a Systems Manager maintenance window to invoke an AWS Lambda function to generate new key pairs. Replace public keys on EC2 instances. Update the private keys in Parameter Store.
- C. Import the EC2 key pairs into AWS Key Management Service (AWS KMS). Configure automatic key rotation for these key pairs. Create an Amazon EventBridge scheduled rule to invoke an AWS Lambda function to initiate the key rotation in AWS KMS.
- D. Add all the EC2 instances to Fleet Manager, a capability of AWS Systems Manager. Define a Systems Manager maintenance window to issue a Systems Manager Run Command document to generate new key pairs and to rotate public keys to all the instances in Fleet Manager.

Question #211

Topic 1

A company wants to migrate to AWS. The company is running thousands of VMs in a VMware ESXi environment. The company has no configuration management database and has little knowledge about the utilization of the VMware portfolio.

A solutions architect must provide the company with an accurate inventory so that the company can plan for a cost-effective migration.

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

- A. Use AWS Systems Manager Patch Manager to deploy Migration Evaluator to each VM. Review the collected data in Amazon QuickSight. Identify servers that have high utilization. Remove the servers that have high utilization from the migration list. Import the data to AWS Migration Hub.
- B. Export the VMware portfolio to a .csv file. Check the disk utilization for each server. Remove servers that have high utilization. Export the data to AWS Application Migration Service. Use AWS Server Migration Service (AWS SMS) to migrate the remaining servers.
- C. Deploy the Migration Evaluator agentless collector to the ESXi hypervisor. Review the collected data in Migration Evaluator. Identify inactive servers. Remove the inactive servers from the migration list. Import the data to AWS Migration Hub.
- D. Deploy the AWS Application Migration Service Agent to each VM. When the data is collected, use Amazon Redshift to import and analyze the data. Use Amazon QuickSight for data visualization.

Question #212

Topic 1

A company runs a microservice as an AWS Lambda function. The microservice writes data to an on-premises SQL database that supports a limited number of concurrent connections. When the number of Lambda function invocations is too high, the database crashes and causes application downtime. The company has an AWS Direct Connect connection between the company's VPC and the on-premises data center. The company wants to protect the database from crashes.

Which solution will meet these requirements?

- A. Write the data to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda function to read from the queue and write to the existing database. Set a reserved concurrency limit on the Lambda function that is less than the number of connections that the database supports.
- B. Create a new Amazon Aurora Serverless DB cluster. Use AWS DataSync to migrate the data from the existing database to Aurora Serverless. Reconfigure the Lambda function to write to Aurora.
- C. Create an Amazon RDS Proxy DB instance. Attach the RDS Proxy DB instance to the Amazon RDS DB instance. Reconfigure the Lambda function to write to the RDS Proxy DB instance.
- D. Write the data to an Amazon Simple Notification Service (Amazon SNS) topic. Invoke the Lambda function to write to the existing database when the topic receives new messages. Configure provisioned concurrency for the Lambda function to be equal to the number of connections that the database supports.

Question #213

Topic 1

A company uses a Grafana data visualization solution that runs on a single Amazon EC2 instance to monitor the health of the company's AWS workloads. The company has invested time and effort to create dashboards that the company wants to preserve. The dashboards need to be highly available and cannot be down for longer than 10 minutes. The company needs to minimize ongoing maintenance.

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

- A. Migrate to Amazon CloudWatch dashboards. Recreate the dashboards to match the existing Grafana dashboards. Use automatic dashboards where possible.
- B. Create an Amazon Managed Grafana workspace. Configure a new Amazon CloudWatch data source. Export dashboards from the existing Grafana instance. Import the dashboards into the new workspace.
- C. Create an AMI that has Grafana pre-installed. Store the existing dashboards in Amazon Elastic File System (Amazon EFS). Create an Auto Scaling group that uses the new AMI. Set the Auto Scaling group's minimum, desired, and maximum number of instances to one. Create an Application Load Balancer that serves at least two Availability Zones.
- D. Configure AWS Backup to back up the EC2 instance that runs Grafana once each hour. Restore the EC2 instance from the most recent snapshot in an alternate Availability Zone when required.

Question #214

Topic 1

A company needs to migrate its customer transactions database from on premises to AWS. The database resides on an Oracle DB instance that runs on a Linux server. According to a new security requirement, the company must rotate the database password each year.

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

- A. Convert the database to Amazon DynamoDB by using the AWS Schema Conversion Tool (AWS SCT). Store the password in AWS Systems Manager Parameter Store. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function for yearly password rotation.
- B. Migrate the database to Amazon RDS for Oracle. Store the password in AWS Secrets Manager. Turn on automatic rotation. Configure a yearly rotation schedule.
- C. Migrate the database to an Amazon EC2 instance. Use AWS Systems Manager Parameter Store to keep and rotate the connection string by using an AWS Lambda function on a yearly schedule.
- D. Migrate the database to Amazon Neptune by using the AWS Schema Conversion Tool (AWS SCT). Create an Amazon CloudWatch alarm to invoke an AWS Lambda function for yearly password rotation.

Question #215

Topic 1

A solutions architect is designing an AWS account structure for a company that consists of multiple teams. All the teams 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 traffic to and from the on-premises network.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Create an AWS CloudFormation template that provisions a VPC and the required subnets. Deploy the template to each AWS account.
- 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.
- C. Use AWS Transit Gateway along with an AWS Site-to-Site VPN for connectivity to the on-premises network. Share the transit gateway by using AWS Resource Access Manager.
- D. Use AWS Site-to-Site VPN for connectivity to the on-premises network.
- E. Use AWS Direct Connect for connectivity to the on-premises network.

Question #216

Topic 1

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 NAT gateway 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?

- A. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Create an Auto Scaling group of Amazon EC2 instances that run an open-source internet proxy for rule-based filtering across all Availability Zones in the Region. Modify all default routes to point to the proxy's Auto Scaling group.
- 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.
- C. Create an AWS Network Firewall firewall for rule-based filtering in each AWS account. Modify all default routes to point to the Network Firewall firewalls in each account.
- D. In each AWS account, create an Auto Scaling group of network-optimized Amazon EC2 instances that run an open-source internet proxy for rule-based filtering. Modify all default routes to point to the proxy's Auto Scaling group.

Question #217

Topic 1

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?

- A. 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. Use Amazon Inspector to monitor traffic to the ALB and EC2 instances. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB. Use an AWS Lambda function to frequently push the Amazon Inspector report to the third-party auditing application.
- B. Configure an Application Load Balancer (ALB) and add the EC2 instances as targets. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB name and enable logging with Amazon CloudWatch Logs. Use an AWS Lambda function to frequently push the logs to the third-party auditing application.
- C. Configure an Application Load Balancer (ALB) along with a target group adding the EC2 instances as targets. Create an Amazon Kinesis Data Firehose with the destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the web ACL 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.
- 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.

Question #218

Topic 1

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?

- A. Create an AWS Site-to-Site VPN connection between the VPC and the API Gateway. Use API Gateway to generate a unique API Key for each microservice. Configure the API methods to require the key.
- 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.
- C. Modify the API Gateway to use IAM authentication. Update the IAM policy for the IAM role that is assigned to the EC2 instances to allow access to the API Gateway. Move the API Gateway into a new VPDeploy a transit gateway and connect the VPCs.
- D. Create an accelerator in AWS Global Accelerator, and connect the accelerator to the API Gateway. Update the route table for all VPC subnets with a route to the created Global Accelerator endpoint IP address. Add an API key for each service to use for authentication.

Question #219

Topic 1

A company has set up its entire infrastructure on AWS. The company uses Amazon EC2 instances 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?

- A. Set up AWS Organizations for the company. Apply SCPs to govern and track noncompliant security group changes that are made to the AWS account.
- B. Enable AWS CloudTrail to capture the changes to EC2 security groups. Enable Amazon CloudWatch rules to provide alerts when noncompliant security settings are detected.
- C. Enable SCPs on the AWS account to provide alerts when noncompliant security group changes are made to the environment.
- 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.

Question #220

Topic 1

A company has IoT 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 IoT 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? (Choose three.)

- A. Reshard the stream to increase the number of shards in the stream.
- B. Use the Kinesis Producer Library (KPL). Adjust the polling frequency.
- C. Use consumers with the enhanced fan-out feature.
- D. Reshard the stream to reduce the number of shards in the stream.
- E. Use an error retry and exponential backoff mechanism in the consumer logic.
- F. Configure the stream to use dynamic partitioning.

Question #221

Topic 1

A company uses AWS Organizations to manage its AWS accounts. The company needs a list of all its Amazon EC2 instances that have underutilized CPU or memory usage. The company also needs recommendations for how to downsize these underutilized instances.

Which solution will meet these requirements with the LEAST effort?

- A. Install a CPU and memory monitoring tool from AWS Marketplace on all the EC2 instances. Store the findings in Amazon S3. Implement a Python script to identify underutilized instances. Reference EC2 instance pricing information for recommendations about downsizing options.
- B. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in the organization's management account. Use the recommendations to downsize underutilized instances in all accounts of the organization.
- C. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in each account of the organization. Use the recommendations to downsize underutilized instances in all accounts of the organization.
- D. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Create an AWS Lambda function to extract CPU and memory usage from all the EC2 instances. Store the findings as files in Amazon S3. Use Amazon Athena to find underutilized instances. Reference EC2 instance pricing information for recommendations about downsizing options.

Question #222

Topic 1

A company wants to run a custom network analysis software package to inspect traffic as traffic leaves and enters a VPC. The company has deployed the solution by using AWS CloudFormation on three Amazon EC2 instances in an Auto Scaling group. All network routing has been established to direct traffic to the EC2 instances.

Whenever the analysis software stops working, the Auto Scaling group replaces an instance. The network routes are not updated when the instance replacement occurs.

Which combination of steps will resolve this issue? (Choose three.)

- A. Create alarms based on EC2 status check metrics that will cause the Auto Scaling group to replace the failed instance.
- B. Update the CloudFormation template to install the Amazon CloudWatch agent on the EC2 instances. Configure the CloudWatch agent to send process metrics for the application.
- C. Update the CloudFormation template to install AWS Systems Manager Agent on the EC2 instances. Configure Systems Manager Agent to send process metrics for the application.
- D. Create an alarm for the custom metric in Amazon CloudWatch for the failure scenarios. Configure the alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
- E. Create an AWS Lambda function that responds to the Amazon Simple Notification Service (Amazon SNS) message to take the instance out of service. Update the network routes to point to the replacement instance.
- F. In the CloudFormation template, write a condition that updates the network routes when a replacement instance is launched.

Question #223

Topic 1

A company is developing a new on-demand video application that is based on microservices. The application will have 5 million users at launch and will have 30 million users after 6 months. The company has deployed the application on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. The company developed the application by using ECS services that use the HTTPS protocol.

A solutions architect needs to implement updates to the application by using blue/green deployments. The solution must distribute traffic to each ECS service through a load balancer. The application must automatically adjust the number of tasks in response to an Amazon CloudWatch alarm.

Which solution will meet these requirements?

- A. Configure the ECS services to use the blue/green deployment type and a Network Load Balancer. Request increases to the service quota for tasks per service to meet the demand.
- B. Configure the ECS services to use the blue/green deployment type and a Network Load Balancer. Implement Auto Scaling group for each ECS service by using the Cluster Autoscaler.
- C. Configure the ECS services to use the blue/green deployment type and an Application Load Balancer. Implement an Auto Scaling group for each ECS service by using the Cluster Autoscaler.
- D. Configure the ECS services to use the blue/green deployment type and an Application Load Balancer. Implement Service Auto Scaling for each ECS service.

Question #224

Topic 1

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 of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group.

The company uses Amazon Elastic Container Registry (Amazon ECR) 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 EventBridge 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).
- B. Configure scan on push on the repository. Configure scan results to be pushed to an Amazon Simple Queue Service (Amazon SQS) queue. Invoke an AWS Lambda function when a new message is added to the SQS queue. Use the Lambda function to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).
- C. Schedule an AWS Lambda function to start a manual image scan every hour. Configure Amazon EventBridge to invoke another Lambda function when a scan is complete. Use the second Lambda function to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- D. Configure periodic image scan on the repository. Configure scan results to be added to an Amazon Simple Queue Service (Amazon SQS) queue. Invoke an AWS Step Functions state machine when a new message is added to the SQS queue. Use the Step Functions state machine to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).

Question #225

Topic 1

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?

- A. Purchase Reserved Instances for the organization to match the size and number of the most common EC2 instances from the member accounts.
- B. Purchase a Compute Savings Plan for the organization from the management account by using the recommendation at the management account level.
- C. Purchase Reserved Instances for each member account that had high EC2 usage according to the data from the last 6 months.
- D. Purchase an EC2 Instance Savings Plan for each member account from the management account based on EC2 usage data from the last 6 months.

Question #226

Topic 1

A company has hundreds of AWS accounts. The company uses an organization in AWS Organizations to manage all the accounts. The company has turned on all features.

A finance team has allocated a daily budget for AWS costs. The finance team must receive an email notification if the organization's AWS costs exceed 80% of the allocated budget. A solutions architect needs to implement a solution to track the costs and deliver the notifications.

Which solution will meet these requirements?

- A. In the organization's management account, use AWS Budgets to create a budget that has a daily period. Add an alert threshold and set the value to 80%. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.
- B. In the organization's management account, set up the organizational view feature for AWS Trusted Advisor. Create an organizational view report for cost optimization. Set an alert threshold of 80%. Configure notification preferences. Add the email addresses of the finance team.
- C. Register the organization with AWS Control Tower. Activate the optional cost control (guardrail). Set a control (guardrail) parameter of 80%. Configure control (guardrail) notification preferences. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.
- D. Configure the member accounts to save a daily AWS Cost and Usage Report to an Amazon S3 bucket in the organization's management account. Use Amazon EventBridge to schedule a daily Amazon Athena query to calculate the organization's costs. Configure Athena to send an Amazon CloudWatch alert if the total costs are more than 80% of the allocated budget. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.

Question #227

Topic 1

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?

- A. Redeploy the application to use S3 multipart uploads.
- B. Create an Amazon CloudFront distribution and point to the application as a custom origin.
- C. Configure the buckets to use S3 Transfer Acceleration.
- D. Create an Auto Scaling group for the EC2 instances and create a scaling policy.

Question #228

Topic 1

A company wants to containerize a multi-tier web application and move the application from an on-premises data center to AWS. The application includes web, application, and database tiers. The company needs to make the application fault tolerant and scalable. Some frequently accessed data must always be available across application servers. Frontend web servers need session persistence and must scale to meet increases in traffic.

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

- A. Run the application on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. Use Amazon Elastic File System (Amazon EFS) for data that is frequently accessed between the web and application tiers. Store the frontend web server session data in Amazon Simple Queue Service (Amazon SQS).
- B. Run the application on Amazon Elastic Container Service (Amazon ECS) on Amazon EC2. Use Amazon ElastiCache for Redis to cache frontend web server session data. Use Amazon Elastic Block Store (Amazon EBS) with Multi-Attach on EC2 instances that are distributed across multiple Availability Zones.
- C. Run the application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure Amazon EKS to use managed node groups. Use ReplicaSets to run the web servers and applications. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system across all EKS pods to store frontend web server session data.
- D. Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure Amazon EKS to use managed node groups. Run the web servers and application as Kubernetes deployments in the EKS cluster. Store the frontend web server session data in an Amazon DynamoDB table. Create an Amazon Elastic File System (Amazon EFS) volume that all applications will mount at the time of deployment.

Question #229

Topic 1

A solutions architect is planning to migrate critical Microsoft SQL Server databases to AWS. Because the databases are legacy systems, the solutions architect will move the databases to a modern data architecture. The solutions architect must migrate the databases with near-zero downtime.

Which solution will meet these requirements?

- A. Use AWS Application Migration Service and the AWS Schema Conversion Tool (AWS SCT). Perform an in-place upgrade before the migration. Export the migrated data to Amazon Aurora Serverless after cutover. Repoint the applications to Amazon Aurora.
- B. Use AWS Database Migration Service (AWS DMS) to rehost the database. Set Amazon S3 as a target. Set up change data capture (CDC) replication. When the source and destination are fully synchronized, load the data from Amazon S3 into an Amazon RDS for Microsoft SQL Server DB instance.
- C. Use native database high availability tools. Connect the source system to an Amazon RDS for Microsoft SQL Server DB instance. Configure replication accordingly. When data replication is finished, transition the workload to an Amazon RDS for Microsoft SQL Server DB instance.
- D. Use AWS Application Migration Service. Rehost the database server on Amazon EC2. When data replication is finished, detach the database and move the database to an Amazon RDS for Microsoft SQL Server DB instance. Reattach the database and then cut over all networking.

Question #230

Topic 1

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.)

- A. Use AWS Resource Access Manager to share the subnets that host the service provider applications with other accounts in the organization.
- B. Place the service provider applications and the service consumer applications in AWS accounts in the same organization.
- C. Turn off cross-zone load balancing for the Network Load Balancer in all service provider application deployments.
- D. Ensure that service consumer compute resources use the Availability Zone-specific endpoint service by using the endpoint's local DNS name.
- E. Create a Savings Plan that provides adequate coverage for the organization's planned inter-Availability Zone data transfer usage.

Question #231

Topic 1

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.
- B. Create an Amazon FSx for Windows File Server Single-AZ file system within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system. Enable nightly backups.
- C. Create an Amazon FSx for Windows File Server Multi-AZ file system within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system. Enable nightly backups.
- D. Create a new S3 bucket. Deploy an AWS Storage Gateway volume 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 on the volume gateway, and automate copies of this data to an S3 bucket.

Question #232

Topic 1

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?

- A. Create an AWS Site-to-Site VPN connection between the on-premises data center and a new central VPC. Create VPC peering connections that initiate from the central VPC to all other VPCs.
- 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.
- C. Create an AWS Site-to-Site VPN connection between the on-premises data center and a new central VPC. Use a transit gateway with dynamic routing. Connect the transit gateway to all other VPCs.
- D. Create an AWS Direct Connect connection between the on-premises data center and AWS. Establish an AWS Site-to-Site VPN connection between all VPCs in each Region. Create VPC peering connections that initiate from the central VPC to all other VPCs.

Question #233

Topic 1

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.
- B. Create an IAM user in each member account. In the management account, create a cross-account role that has least privilege access. Grant the IAM users access to the cross-account role by using a trust policy.
- C. Create an IAM user in the management account. In the member accounts, create an IAM group that has least privilege access. Add the IAM user from the management account to each IAM group in the member accounts.
- D. Create an IAM user in the management account. In the member accounts, create cross-account roles that have least privilege access. Grant the IAM user access to the roles by using a trust policy.

Question #234

Topic 1

A company wants to use AWS for disaster recovery for an on-premises application. The company has hundreds of Windows-based servers that run the application. All the servers mount a common share.

The company has an RTO of 15 minutes and an RPO of 5 minutes. The solution must support native failover and fallback capabilities.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an AWS Storage Gateway File Gateway. Schedule daily Windows server backups. Save the data to Amazon S3. During a disaster, recover the on-premises servers from the backup. During failback, run the on-premises servers on Amazon EC2 instances.
- B. Create a set of AWS CloudFormation templates to create infrastructure. Replicate all data to Amazon Elastic File System (Amazon EFS) by using AWS DataSync. During a disaster, use AWS CodePipeline to deploy the templates to restore the on-premises servers. Fail back the data by using DataSync.
- C. Create an AWS Cloud Development Kit (AWS CDK) pipeline to stand up a multi-site active-active environment on AWS. Replicate data into Amazon S3 by using the s3 sync command. During a disaster, swap DNS endpoints to point to AWS. Fail back the data by using the s3 sync command.
- D. Use AWS Elastic Disaster Recovery to replicate the on-premises servers. Replicate data to an Amazon FSx for Windows File Server file system by using AWS DataSync. Mount the file system to AWS servers. During a disaster, fail over the on-premises servers to AWS. Fail back to new or existing servers by using Elastic Disaster Recovery.

Question #235

Topic 1

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.
- B. Launch the EC2 instances and attach elastic network interfaces in multiples of four.
- C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled.
- D. Ensure the cluster is launched across multiple Availability Zones.
- E. Replace Amazon EFS with multiple Amazon EBS volumes in a RAID array.
- F. Replace Amazon EFS with Amazon FSx for Lustre.

Question #236

Topic 1

A company is designing an AWS Organizations structure. The company wants to standardize a process to apply tags across the entire organization. The company will require tags with specific values when a user creates a new resource. Each of the company's OUs will have unique tag values.

Which solution will meet these requirements?

- A. Use an SCP to deny the creation of resources that do not have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the OUs.
- B. Use an SCP to deny the creation of resources that do not have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the organization's management account.
- C. Use an SCP to allow the creation of resources only when the resources have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the OUs.
- D. Use an SCP to deny the creation of resources that do not have the required tags. Define the list of tags. Attach the SCP to the OUs.

Question #237

Topic 1

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?

- A. Launch two Amazon EC2 instances to host the Kafka server in an active/standby configuration across two Availability Zones. Create a domain name in Amazon Route 53. Create a Route 53 failover policy. Route the sensors to send the data to the domain name.
- 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.
- C. Deploy AWS IoT Core, and connect it to an Amazon Kinesis Data Firehose delivery stream. Use an AWS Lambda function to handle data transformation. Route the sensors to send the data to AWS IoT Core.
- D. Deploy AWS IoT Core, and launch an Amazon EC2 instance to host the Kafka server. Configure AWS IoT Core to send the data to the EC2 instance. Route the sensors to send the data to AWS IoT Core.

Question #238

Topic 1

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? (Choose 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.
- C. Create an AWS Lambda function to replicate backups to another Region and send notification if a failure occurs.
- 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.
- E. Create an Amazon Data Lifecycle Manager (Amazon DLM) snapshot lifecycle policy for each of the retention requirements.
- F. Set up RDS snapshots on each database.

Question #239

Topic 1

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?

- A. Use Amazon Kinesis Data Firehose to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon RDS instance.
- B. Use Amazon Kinesis Data Streams to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon Redshift cluster using Amazon EMR.
- C. Use Amazon S3 to collect the inbound device data, analyze the data from Amazon SQS with Kinesis, and save the results to an Amazon Redshift cluster.
- D. Use an Amazon API Gateway to put requests into an Amazon SQS queue, analyze the data with an AWS Lambda function, and save the results to an Amazon Redshift cluster using Amazon EMR.

Question #240

Topic 1

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.)

- A. Use an Amazon Route 53 weighted routing policy set to 100/0 across the two selected Regions. Set Time to Live (TTL) to 1 hour.
- 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.
- D. Back up data from an Amazon DynamoDB table in the primary Region every 60 minutes and then write the data to Amazon S3. Use S3 cross-Region replication to copy the data from the primary Region to the disaster recovery Region. Have a script import the data into DynamoDB in a disaster recovery scenario.
- 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.
- F. Use Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use Spot Instances for the required resources.

Question #241

Topic 1

A company manufactures smart vehicles. The company uses a custom application to collect vehicle data. The vehicles use the MQTT protocol to connect to the application. The company processes the data in 5-minute intervals. The company then copies vehicle telematics data to on-premises storage. Custom applications analyze this data to detect anomalies.

The number of vehicles that send data grows constantly. Newer vehicles generate high volumes of data. The on-premises storage solution is not able to scale for peak traffic, which results in data loss. The company must modernize the solution and migrate the solution to AWS to resolve the scaling challenges.

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

- A. Use AWS IoT Greengrass to send the vehicle data to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Create an Apache Kafka application to store the data in Amazon S3. Use a pretrained model in Amazon SageMaker to detect anomalies.
- B. Use AWS IoT Core to receive the vehicle data. Configure rules to route data to an Amazon Kinesis Data Firehose delivery stream that stores the data in Amazon S3. Create an Amazon Kinesis Data Analytics application that reads from the delivery stream to detect anomalies.
- C. Use AWS IoT FleetWise to collect the vehicle data. Send the data to an Amazon Kinesis data stream. Use an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use the built-in machine learning transforms in AWS Glue to detect anomalies.
- D. Use Amazon MQ for RabbitMQ to collect the vehicle data. Send the data to an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use Amazon Lookout for Metrics to detect anomalies.

Question #242

Topic 1

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 CodeCommit repository. The security team wants to automatically find and remediate instances of this security vulnerability.

Which solution will ensure that the credentials are appropriately secured automatically?

- A. Run a script nightly using AWS Systems Manager Run Command to search for credentials on the development instances. If found, use AWS Secrets Manager to rotate the credentials.
- B. Use a scheduled AWS Lambda function to download and scan the application code from CodeCommit. If credentials are found, generate new credentials and store them in AWS KMS.
- C. Configure Amazon Macie to scan for credentials in CodeCommit repositories. If credentials are found, trigger an AWS Lambda function to disable the credentials and notify the user.
- D. Configure a CodeCommit 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.

Question #243

Topic 1

A company has a data lake 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 solutions 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.
- B. Create an interface endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Create a VPC gateway attachment for the S3 endpoint.
- 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.
- D. Create an S3 access point for each application in each AWS account and attach the access points to 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.
- E. Create a gateway endpoint for Amazon S3 in the data lake's VPC. Attach an endpoint policy to allow access to the S3 bucket. Specify the route table that is used to access the bucket.

Question #244

Topic 1

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?

- A. Enable VPC flows logs, and send them to CloudWatch. Create an AWS Lambda function to periodically export the CloudWatch logs to an Amazon S3 bucket by using the pre-defined export function. Generate ACCESS_KEY and SECRET_KEY AWS credentials. Configure Splunk to pull the logs from the S3 bucket by using those credentials.
- 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 flows logs, and send them to CloudWatch. Create a CloudWatch Logs subscription that sends log events to the Kinesis Data Firehose delivery stream.
- C. Ask the company to log every request that is made to the databases along with the EC2 instance IP address. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs grouped by database name. Export Athena results to another S3 bucket. Invoke an AWS Lambda function to automatically send any new file that is put in the S3 bucket to Splunk.
- D. Send the CloudWatch logs to an Amazon Kinesis data stream with Amazon Kinesis Data Analytics for SQL Applications. Configure a 1-minute sliding window to collect the events. Create a SQL query that uses the anomaly detection template to monitor any networking traffic anomalies in near-real time. Send the result to an Amazon Kinesis Data Firehose delivery stream with Splunk as the destination.

Question #245

Topic 1

A company has five development teams that have each created five AWS accounts to develop and host applications. To track spending, the development teams log in to each account every month, record the current cost from the AWS Billing and Cost Management console, and provide the information to the company's finance team.

The company has strict compliance requirements and needs to ensure that resources are created only in AWS Regions in the United States. However, some resources have been created in other Regions.

A solutions architect needs to implement a solution that gives the finance team the ability to track and consolidate expenditures for all the accounts. The solution also must ensure that the company can create resources only in Regions in the United States.

Which combination of steps will meet these requirements in the MOST operationally efficient way? (Choose three.)

- A. Create a new account to serve as a management account. Create an Amazon S3 bucket for the finance team. Use AWS Cost and Usage Reports to create monthly reports and to store the data in the finance team's S3 bucket.
- B. Create a new account to serve as a management account. Deploy an organization in AWS Organizations with all features enabled. Invite all the existing accounts to the organization. Ensure that each account accepts the invitation.
- C. Create an OU that includes all the development teams. Create an SCP that allows the creation of resources only in Regions that are in the United States. Apply the SCP to the OU.
- D. Create an OU that includes all the development teams. Create an SCP that denies the creation of resources in Regions that are outside the United States. Apply the SCP to the OU.
- E. Create an IAM role in the management account. Attach a policy that includes permissions to view the Billing and Cost Management console. Allow the finance team users to assume the role. Use AWS Cost Explorer and the Billing and Cost Management console to analyze cost.
- F. Create an IAM role in each AWS account. Attach a policy that includes permissions to view the Billing and Cost Management console. Allow the finance team users to assume the role.

Question #246

Topic 1

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?

- A. Use the OrganizationAccountAccessRole IAM role to create a new IAM policy with read-only access in each member account. Establish a trust relationship between the IAM policy in each member account and the security account. Ask the security team to use the IAM policy to gain access.
- B. Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team to use the IAM role to gain access.
- C. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the management account from the security account. Use the generated temporary credentials to gain access.
- 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.

Question #247

Topic 1

A large company runs workloads in VPCs that are deployed across hundreds of AWS accounts. Each VPC consists of public subnets and private subnets that span across multiple Availability Zones. NAT gateways are deployed in the public subnets and allow outbound connectivity to the internet from the private subnets.

A solutions architect is working on a hub-and-spoke design. All private subnets in the spoke VPCs must route traffic to the internet through an egress VPC. The solutions architect already has deployed a NAT gateway in an egress VPC in a central AWS account.

Which set of additional steps should the solutions architect take to meet these requirements?

- A. Create peering connections between the egress VPC and the spoke VPCs. Configure the required routing to allow access to the internet.
- B. Create a transit gateway, and share it with the existing AWS accounts. Attach existing VPCs to the transit gateway. Configure the required routing to allow access to the internet.
- C. Create a transit gateway in every account. Attach the NAT gateway to the transit gateways. Configure the required routing to allow access to the internet.
- D. Create an AWS PrivateLink connection between the egress VPC and the spoke VPCs. Configure the required routing to allow access to the internet.

Question #248

Topic 1

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 failed login attempts originate from about 500 different IP addresses that change each week. A solutions architect must prevent the failed login attempts from overwhelming the authentication service.

Which solution meets these requirements with the MOST operational efficiency?

- A. Use AWS Firewall Manager to create a security group and security group policy to deny access from the IP addresses.
- 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.
- C. Use AWS Firewall Manager to create a security group and security group policy to allow access only to specific CIDR ranges.
- D. Create an AWS WAF web ACL with an IP set match rule, and set the rule action to Block. Connect the web ACL to the ALB.

Question #249

Topic 1

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 in Amazon S3.
- B. Add a subnet containing the customer-owned block of IP addresses to a VPC. Create Elastic IP addresses from the address pool and assign them to an Application Load Balancer (ALB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the ALB. Store the files in attached Amazon Elastic Block Store (Amazon EBS) volumes.
- C. Register the customer-owned block of IP addresses with Amazon Route 53. Create alias records in Route 53 that point to a Network Load Balancer (NLB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the NLB. Store the files in Amazon S3.
- D. 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 Amazon S3 VPC endpoint. Enable SFTP support on the S3 bucket.

Question #250

Topic 1

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.
- B. Launch five new EC2 instances into an Auto Scaling group in the same Availability Zone. Attach an extra elastic network interface to each EC2 instance.
- C. Launch five new EC2 instances into a partition placement group. Ensure that the EC2 instance type supports enhanced networking.
- D. Launch five new EC2 instances into a spread placement group. Attach an extra elastic network interface to each EC2 instance.

Question #251**Topic 1**

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?

- A. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Configure CloudFront with an origin access identity (OAI) and associate it with the distribution. Configure API Gateway to ensure only the OAI can run the POST method.
- B. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Add a custom header to the CloudFront distribution populated with an API key. Configure the API to require an API key on the POST method.
- C. 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 resource policy with a request limit and associate it with the API. Configure the API to require an API key on the POST method.
- 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 the usage plan.

Question #252**Topic 1**

A company uses an Amazon Aurora PostgreSQL DB cluster for applications in a single AWS Region. The company's database team must monitor all data activity on all the databases.

Which solution will achieve this goal?

- A. Set up an AWS Database Migration Service (AWS DMS) change data capture (CDC) task. Specify the Aurora DB cluster as the source. Specify Amazon Kinesis Data Firehose as the target. Use Kinesis Data Firehose to upload the data into an Amazon OpenSearch Service cluster for further analysis.
- B. Start a database activity stream on the Aurora DB cluster to capture the activity stream in Amazon EventBridge. Define an AWS Lambda function as a target for EventBridge. Program the Lambda function to decrypt the messages from EventBridge and to publish all database activity to Amazon S3 for further analysis.
- C. Start a database activity stream on the Aurora DB cluster to push the activity stream to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to consume the Kinesis data stream and to deliver the data to Amazon S3 for further analysis.
- D. Set up an AWS Database Migration Service (AWS DMS) change data capture (CDC) task. Specify the Aurora DB cluster as the source. Specify Amazon Kinesis Data Firehose as the target. Use Kinesis Data Firehose to upload the data into an Amazon Redshift cluster. Run queries on the Amazon Redshift data to determine database activities on the Aurora database.

Question #253

Topic 1

An entertainment company recently launched a new game. To ensure a good experience for players during the launch period, the company deployed a static quantity of 12 r6g.16xlarge (memory optimized) Amazon EC2 instances behind a Network Load Balancer. The company's operations team used the Amazon CloudWatch agent and a custom metric to include memory utilization in its monitoring strategy.

Analysis of the CloudWatch metrics from the launch period showed consumption at about one quarter of the CPU and memory that the company expected. Initial demand for the game has subsided and has become more variable. The company decides to use an Auto Scaling group that monitors the CPU and memory consumption to dynamically scale the instance fleet. A solutions architect needs to configure the Auto Scaling group to meet demand in the most cost-effective way.

Which solution will meet these requirements?

- A. Configure the Auto Scaling group to deploy c6g.4xlarge (compute optimized) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- B. Configure the Auto Scaling group to deploy m6g.4xlarge (general purpose) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- C. Configure the Auto Scaling group to deploy r6g.4xlarge (memory optimized) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- D. Configure the Auto Scaling group to deploy r6g.8xlarge (memory optimized) instances. Configure a minimum capacity of 2, a desired capacity of 2, and a maximum capacity of 6.

Question #254

Topic 1

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 read activity against the table happens in bursts throughout the day, and a limited set of keys are repeatedly looked up. The company needs to reduce costs associated with DynamoDB.

Which strategy should a solutions architect recommend to meet this requirement?

- A. Deploy an Amazon ElastiCache cluster in front of the DynamoDB table
- B. Deploy DynamoDB Accelerator (DAX). Configure DynamoDB auto scaling. Purchase Savings Plans in Cost Explorer.
- C. Use provisioned capacity mode. Purchase Savings Plans in Cost Explorer.
- D. Deploy DynamoDB Accelerator (DAX). Use provisioned capacity mode. Configure DynamoDB auto scaling.

Question #255

Topic 1

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.
- B. Check that the NACL is attached to the logging service subnets to allow communications to and from the interface endpoint subnets. Check that the NACL is attached to the interface endpoint 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.
- D. Check the security group for the logging service running on EC2 instances to ensure it allows ingress from the clients.
- E. Check the security group for the NLB to ensure it allows ingress from the interface endpoint subnets.

Question #256

Topic 1

A company has millions of objects in an Amazon S3 bucket. The objects are in the S3 Standard storage class. All the S3 objects are accessed frequently. The number of users and applications that access the objects is increasing rapidly. The objects are encrypted with server-side encryption with AWS KMS keys (SSE-KMS).

A solutions architect reviews the company's monthly AWS invoice and notices that AWS KMS costs are increasing because of the high number of requests from Amazon S3. The solutions architect needs to optimize costs with minimal changes to the application.

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

- A. Create a new S3 bucket that has server-side encryption with customer-provided keys (SSE-C) as the encryption type. Copy the existing objects to the new S3 bucket. Specify SSE-C.
- B. Create a new S3 bucket that has server-side encryption with Amazon S3 managed keys (SSE-S3) as the encryption type. Use S3 Batch Operations to copy the existing objects to the new S3 bucket. Specify SSE-S3.
- C. Use AWS CloudHSM to store the encryption keys. Create a new S3 bucket. Use S3 Batch Operations to copy the existing objects to the new S3 bucket. Encrypt the objects by using the keys from CloudHSM.
- D. Use the S3 Intelligent-Tiering storage class for the S3 bucket. Create an S3 Intelligent-Tiering archive configuration to transition objects that are not accessed for 90 days to S3 Glacier Deep Archive.

Question #257

Topic 1

A media storage application uploads user photos to Amazon S3 for processing by AWS Lambda functions. Application state is stored in Amazon DynamoDB tables. Users are reporting that some uploaded photos are not being processed properly. The application developers trace the logs and find that Lambda is experiencing photo processing issues when thousands of users upload photos simultaneously. The issues are the result of Lambda concurrency limits and the performance of DynamoDB when data is saved.

Which combination of actions should a solutions architect take to increase the performance and reliability of the application? (Choose two.)

- A. Evaluate and adjust the RCUs for the DynamoDB tables.
- B. Evaluate and adjust the WCUs for the DynamoDB tables.
- C. Add an Amazon ElastiCache layer to increase the performance of Lambda functions.
- D. Add an Amazon Simple Queue Service (Amazon SQS) queue and reprocessing logic between Amazon S3 and the Lambda functions.
- E. Use S3 Transfer Acceleration to provide lower latency to users.

Question #258

Topic 1

A company runs an application in an on-premises data center. The application gives users the ability to upload media files. The files persist in a file server. The web application has many users. The application server is overutilized, which causes data uploads to fail occasionally. The company frequently adds new storage to the file server. The company wants to resolve these challenges by migrating the application to AWS.

Users from across the United States and Canada access the application. Only authenticated users should have the ability to access the application to upload files. The company will consider a solution that refactors the application, and the company needs to accelerate application development.

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

- A. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instances. Use an Application Load Balancer to distribute the requests. Modify the application to use Amazon S3 to persist the files. Use Amazon Cognito to authenticate users.
- B. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instances. Use an Application Load Balancer to distribute the requests. Set up AWS IAM Identity Center (AWS Single Sign-On) to give users the ability to sign in to the application. Modify the application to use Amazon S3 to persist the files.
- C. Create a static website for uploads of media files. Store the static assets in Amazon S3. Use AWS AppSync to create an API. Use AWS Lambda resolvers to upload the media files to Amazon S3. Use Amazon Cognito to authenticate users.
- D. Use AWS Amplify to create a static website for uploads of media files. Use Amplify Hosting to serve the website through Amazon CloudFront. Use Amazon S3 to store the uploaded media files. Use Amazon Cognito to authenticate users.

Question #259

Topic 1

A company has an application that is deployed on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are part of an Auto Scaling group. The application has unpredictable workloads and frequently scales out and in. The company's development team wants to analyze application logs to find ways to improve the application's performance. However, the logs are no longer available after instances scale in.

Which solution will give the development team the ability to view the application logs after a scale-in event?

- A. Enable access logs for the ALB. Store the logs in an Amazon S3 bucket.
- B. Configure the EC2 instances to publish logs to Amazon CloudWatch Logs by using the unified CloudWatch agent.
- C. Modify the Auto Scaling group to use a step scaling policy.
- D. Instrument the application with AWS X-Ray tracing.

Question #260

Topic 1

A company runs an unauthenticated static website (www.example.com) that includes a registration form for users. The website uses Amazon S3 for hosting and uses Amazon CloudFront as the content delivery network with AWS WAF configured. When the registration form is submitted, the website calls an Amazon API Gateway API endpoint that invokes an AWS Lambda function to process the payload and forward the payload to an external API call.

During testing, a solutions architect encounters a cross-origin resource sharing (CORS) error. The solutions architect confirms that the CloudFront distribution origin has the Access-Control-Allow-Origin header set to www.example.com.

What should the solutions architect do to resolve the error?

- A. Change the CORS configuration on the S3 bucket. Add rules for CORS to the AllowedOrigin element for www.example.com.
- B. Enable the CORS setting in AWS WAF. Create a web ACL rule in which the Access-Control-Allow-Origin header is set to www.example.com.
- C. Enable the CORS setting on the API Gateway API endpoint. Ensure that the API endpoint is configured to return all responses that have the Access-Control-Allow-Origin header set to www.example.com.
- D. Enable the CORS setting on the Lambda function. Ensure that the return code of the function has the Access-Control-Allow-Origin header set to www.example.com.

Question #261

Topic 1

A company has many separate AWS accounts and uses no central billing or management. Each AWS account hosts services for different departments in the company. The company has a Microsoft Azure Active Directory that is deployed.

A solutions architect needs to centralize billing and management of the company's AWS accounts. The company wants to start using identity federation instead of manual user management. The company also wants to use temporary credentials instead of long-lived access keys.

Which combination of steps will meet these requirements? (Choose three.)

- A. Create a new AWS account to serve as a management account. Deploy an organization in AWS Organizations. Invite each existing AWS account to join the organization. Ensure that each account accepts the invitation.
- B. Configure each AWS account's email address to be aws+@example.com so that account management email messages and invoices are sent to the same place.
- C. Deploy AWS IAM Identity Center (AWS Single Sign-On) in the management account. Connect IAM Identity Center to the Azure Active Directory. Configure IAM Identity Center for automatic synchronization of users and groups.
- D. Deploy an AWS Managed Microsoft AD directory in the management account. Share the directory with all other accounts in the organization by using AWS Resource Access Manager (AWS RAM).
- E. Create AWS IAM Identity Center (AWS Single Sign-On) permission sets. Attach the permission sets to the appropriate IAM Identity Center groups and AWS accounts.
- F. Configure AWS Identity and Access Management (IAM) in each AWS account to use AWS Managed Microsoft AD for authentication and authorization.

Question #262

Topic 1

A company wants to manage the costs associated with a group of 20 applications that are infrequently used, but are still business-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 runs for several hours.

Which is the MOST cost-effective solution?

- A. Deploy a separate AWS Lambda function for each application. Use AWS CloudTrail logs and Amazon CloudWatch alarms to verify completion of critical jobs.
- 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 CloudWatch.
- C. Deploy AWS Elastic Beanstalk for each application with Auto Scaling to ensure that all requests have sufficient resources. Monitor each AWS Elastic Beanstalk deployment by using CloudWatch alarms.
- D. Deploy a new Amazon EC2 instance cluster that co-hosts all applications by using EC2 Auto Scaling and Application Load Balancers. Scale cluster size based on a custom metric set on instance memory utilization. Purchase 3-year Reserved Instance reservations equal to the GroupMaxSize parameter of the Auto Scaling group.

Question #263

Topic 1

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, primary, 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?

- A. Launch all task, primary, and core nodes on Spot Instances in an instance fleet. Terminate the cluster, including all instances, when the processing is completed.
- B. Launch the primary 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.
- C. Continue to launch all nodes on On-Demand Instances. Terminate the cluster, including all instances, when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.
- D. Launch the primary and core nodes on On-Demand Instances. Launch the task nodes on Spot Instances in an instance fleet. Terminate only the task node instances when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.

Question #264

Topic 1

A company has migrated a legacy application to the AWS Cloud. The application runs on three Amazon EC2 instances that are spread across three Availability Zones. One EC2 instance is in each Availability Zone. The EC2 instances are running in three private subnets of the VPC and are set up as targets for an Application Load Balancer (ALB) that is associated with three public subnets.

The application needs to communicate with on-premises systems. Only traffic from IP addresses in the company's IP address range are allowed to access the on-premises systems. The company's security team is bringing only one IP address from its internal IP address range to the cloud. The company has added this IP address to the allow list for the company firewall. The company also has created an Elastic IP address for this IP address.

A solutions architect needs to create a solution that gives the application the ability to communicate with the on-premises systems. The solution also must be able to mitigate failures automatically.

Which solution will meet these requirements?

- A. Deploy three NAT gateways, one in each public subnet. Assign the Elastic IP address to the NAT gateways. Turn on health checks for the NAT gateways. If a NAT gateway fails a health check, recreate the NAT gateway and assign the Elastic IP address to the new NAT gateway.
- B. Replace the ALB with a Network Load Balancer (NLB). Assign the Elastic IP address to the NLB. Turn on health checks for the NLB. In the case of a failed health check, redeploy the NLB in different subnets.
- C. Deploy a single NAT gateway in a public subnet. Assign the Elastic IP address to the NAT gateway. Use Amazon CloudWatch with a custom metric to monitor the NAT gateway. If the NAT gateway is unhealthy, invoke an AWS Lambda function to create a new NAT gateway in a different subnet. Assign the Elastic IP address to the new NAT gateway.
- D. Assign the Elastic IP address to the ALB. Create an Amazon Route 53 simple record with the Elastic IP address as the value. Create a Route 53 health check. In the case of a failed health check, recreate the ALB in different subnets.

Question #265**Topic 1**

A company uses AWS Organizations to manage more than 1,000 AWS accounts. The company has created a new developer organization. There are 540 developer member accounts 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? (Choose three.)

- A. Call the MoveAccount operation in the Organizations API from the old organization's management account to migrate the developer accounts to the new developer organization.
- B. From the management account, remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.
- C. From each developer account, remove the account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.
- D. Sign in to the new developer organization's management account and create a placeholder member account that acts as a target for the developer account migration.
- E. Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's management 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.

Question #266**Topic 1**

A company's interactive web application uses an Amazon CloudFront distribution to serve images from an Amazon S3 bucket. Occasionally, third-party tools ingest corrupted images into the S3 bucket. This image corruption causes a poor user experience in the application later. The company has successfully implemented and tested Python logic to detect corrupt images.

A solutions architect must recommend a solution to integrate the detection logic with minimal latency between the ingestion and serving.

Which solution will meet these requirements?

- A. Use a Lambda@Edge function that is invoked by a viewer-response event.
- B. Use a Lambda@Edge function that is invoked by an origin-response event.
- C. Use an S3 event notification that invokes an AWS Lambda function.
- D. Use an S3 event notification that invokes an AWS Step Functions state machine.

Question #267

Topic 1

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?

- A. Configure Amazon EventBridge to invoke an AWS Lambda function when a new EC2 instance is launched into the Auto Scaling group. Code the Lambda function to associate the EC2 instances with the CodeDeploy deployment group.
- B. Write a script to suspend Amazon EC2 Auto Scaling operations before the deployment of new code. When the deployment is complete, create a new AMI and configure the Auto Scaling group's launch template to use the new AMI for new launches. Resume Amazon EC2 Auto Scaling operations.
- C. Create a new AWS CodeBuild project that creates a new AMI that contains the new code. Configure CodeBuild to update the Auto Scaling group's launch template to the new AMI. Run an Amazon EC2 Auto Scaling instance refresh operation.
- 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.

Question #268

Topic 1

A company has a website that runs on four Amazon EC2 instances that are behind an Application Load Balancer (ALB). When the ALB detects that an EC2 instance is no longer available, an Amazon CloudWatch alarm enters the ALARM state. A member of the company's operations team then manually adds a new EC2 instance behind the ALB.

A solutions architect needs to design a highly available solution that automatically handles the replacement of EC2 instances. The company needs to minimize downtime during the switch to the new solution.

Which set of steps should the solutions architect take to meet these requirements?

- A. Delete the existing ALB. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Create a new ALB. Attach the Auto Scaling group to the new ALB. Attach the existing EC2 instances to the Auto Scaling group.
- B. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Attach the Auto Scaling group to the existing ALB. Attach the existing EC2 instances to the Auto Scaling group.
- C. Delete the existing ALB and the EC2 instances. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Create a new ALB. Attach the Auto Scaling group to the new ALB. Wait for the Auto Scaling group to launch the minimum number of EC2 instances.
- D. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Attach the Auto Scaling group to the existing ALB. Wait for the existing ALB to register the existing EC2 instances with the Auto Scaling group.

Question #269

Topic 1

A company wants to optimize AWS data-transfer costs and compute costs across developer accounts within the company's organization in AWS Organizations. Developers can configure VPCs and launch Amazon EC2 instances in a single AWS Region. The EC2 instances retrieve approximately 1 TB of data each day from Amazon S3.

The developer activity leads to excessive monthly data-transfer charges and NAT gateway processing charges between EC2 instances and S3 buckets, along with high compute costs. The company wants to proactively enforce approved architectural patterns for any EC2 instance and VPC infrastructure that developers deploy within the AWS accounts. The company does not want this enforcement to negatively affect the speed at which the developers can perform their tasks.

Which solution will meet these requirements MOST cost-effectively?

- A. Create SCPs to prevent developers from launching unapproved EC2 instance types. Provide the developers with an AWS CloudFormation template to deploy an approved VPC configuration with S3 interface endpoints. Scope the developers' IAM permissions so that the developers can launch VPC resources only with CloudFormation.
- B. Create a daily forecasted budget with AWS Budgets to monitor EC2 compute costs and S3 data-transfer costs across the developer accounts. When the forecasted cost is 75% of the actual budget cost, send an alert to the developer teams. If the actual budget cost is 100%, create a budget action to terminate the developers' EC2 instances and VPC infrastructure.
- C. Create an AWS Service Catalog portfolio that users can use to create an approved VPC configuration with S3 gateway endpoints and approved EC2 instances. Share the portfolio with the developer accounts. Configure an AWS Service Catalog launch constraint to use an approved IAM role. Scope the developers' IAM permissions to allow access only to AWS Service Catalog.
- D. Create and deploy AWS Config rules to monitor the compliance of EC2 and VPC resources in the developer AWS accounts. If developers launch unapproved EC2 instances or if developers create VPCs without S3 gateway endpoints, perform a remediation action to terminate the unapproved resources.

Question #270

Topic 1

A company is expanding. The company plans to separate its resources into hundreds of different AWS accounts in multiple AWS Regions. A solutions architect must recommend a solution that denies access to any operations outside of specifically designated Regions.

Which solution will meet these requirements?

- A. Create IAM roles for each account. Create IAM policies with conditional allow permissions that include only approved Regions for the accounts.
- B. Create an organization in AWS Organizations. Create IAM users for each account. Attach a policy to each user to block access to Regions where an account cannot deploy infrastructure.
- C. Launch an AWS Control Tower landing zone. Create OUs and attach SCPs that deny access to run services outside of the approved Regions.
- D. Enable AWS Security Hub in each account. Create controls to specify the Regions where an account can deploy infrastructure.

Question #271

Topic 1

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?

- A. Use Amazon S3 for web hosting with Amazon API Gateway for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use Amazon Elastic Container Service (Amazon ECS) for business logic with Amazon SQS long polling for retaining failed orders.
- B. Use AWS Elastic Beanstalk for web hosting with Amazon API Gateway for database API services. Use Amazon MQ for order queuing. Use AWS Step Functions for business logic with Amazon S3 Glacier Deep Archive for retaining failed orders.
- 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.
- D. Use Amazon Lightsail for web hosting with AWS AppSync for database API services. Use Amazon Simple Email Service (Amazon SES) for order queuing. Use Amazon Elastic Kubernetes Service (Amazon EKS) for business logic with Amazon OpenSearch Service for retaining failed orders.

Question #272

Topic 1

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?

- A. Migrate the database to an Amazon RDS for MySQL instance with a cross-Region read replica in us-west-2.
- B. Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2.
- C. Migrate the database to an Amazon RDS for MySQL instance with a Multi-AZ deployment.
- D. Create a MySQL standby database on an Amazon EC2 instance in us-west-2.

Question #273

Topic 1

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?

- A. Create an AWS Config rule in the specific member accounts to limit Regions and apply a tag policy.
- B. From the AWS Billing and Cost Management console, in the management account, disable Regions for the specific member accounts and apply a tag policy on the root.
- C. Associate the specific member accounts with the root. Apply a tag policy and an SCP using conditions to limit Regions.
- D. Associate the specific member accounts with a new OU. Apply a tag policy and an SCP using conditions to limit Regions.

Question #274

Topic 1

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?

- A. Create an AWS Lambda function that applies a deny all policy for users who are not authenticated. Create a scheduled event to invoke the Lambda function.
- B. Review the AWS Trusted Advisor bucket permissions check and implement the recommended actions.
- C. Run a script that puts a private ACL on all of the objects in the bucket.
- D. Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket.

Question #275

Topic 1

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? (Choose three.)

- A. Create a new RDS for PostgreSQL DB instance in the target account. Use the AWS Schema Conversion Tool (AWS SCT) to migrate the database schema from the source database to the target database.
- 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.
- D. Temporarily allow the source DB instance to be publicly accessible to provide connectivity from the VPC in 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.
- F. Use AWS Database Migration Service (AWS DMS) in the target account to perform a 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.

Question #276

Topic 1

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?

- A. Increase the backend processing timeout to 30 seconds to match the visibility timeout.
- B. Reduce the visibility timeout of the queue to automatically remove the faulty message.
- C. Configure a new SQS FIFO queue as a dead-letter queue to isolate the faulty messages.
- D. Configure a new SQS standard queue as a dead-letter queue to isolate the faulty messages.

Question #277

Topic 1

A company has automated the nightly retraining of 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? (Choose 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".
- D. Add a new email address to Amazon Simple Email Service (Amazon SES). Verify the email address.
- E. Create a task named "Email" that forwards the input arguments to the SES email address.
- F. Add a Catch field to all Task, Map, and Parallel states that have a statement of "ErrorEquals": ["States.Runtime"] and "Next": "Email".

Question #278

Topic 1

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?

- A. Create an empty private zone in Amazon Route 53 for company.example. Add an additional NS record to the company's on-premises company.example zone that points to the authoritative name servers for the new private zone in Route 53.
- 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.
- C. Turn on DNS hostnames for the VPC. Configure a new inbound resolver endpoint with Amazon Route 53 Resolver. Configure the on-premises DNS server to forward requests for company.example to the new resolver.
- D. Use AWS Systems Manager to configure a run document that will install a hosts file that contains any required hostnames. Use an Amazon EventBridge rule to run the document when an instance is entering the running state.

Question #279

Topic 1

A company uses AWS CloudFormation 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?

- A. Update the network ACL of each subnet within a VPC to allow outbound traffic only to the authorized VPCs. Remove all deny rules except the default deny rule.
- B. Update all the security groups that are used within a VPC to deny outbound traffic to security groups that are used within the unauthorized VPCs.
- C. Create a dedicated transit gateway route table for each VPC attachment. Route traffic only to the authorized VPCs.
- D. Update the main route table of each VPC to route traffic only to the authorized VPCs through the transit gateway.

Question #280

Topic 1

A company has a Windows-based desktop application that is packaged and deployed to the users' Windows machines. The company recently acquired another company that has employees who primarily use machines with a Linux operating system. The acquiring company has decided to migrate and rehost the Windows-based desktop application to AWS.

All employees must be authenticated before they use the application. The acquiring company uses Active Directory on premises but wants a simplified way to manage access to the application on AWS for all the employees.

Which solution will rehost the application on AWS with the LEAST development effort?

- A. Set up and provision an Amazon Workspaces virtual desktop for every employee. Implement authentication by using Amazon Cognito identity pools. Instruct employees to run the application from their provisioned Workspaces virtual desktops.
- B. Create an Auto Scaling group of Windows-based Amazon EC2 instances. Join each EC2 instance to the company's Active Directory domain. Implement authentication by using the Active Directory that is running on premises. Instruct employees to run the application by using a Windows remote desktop.
- C. Use an Amazon AppStream 2.0 image builder to create an image that includes the application and the required configurations. Provision an AppStream 2.0 On-Demand fleet with dynamic Fleet Auto Scaling policies for running the image. Implement authentication by using AppStream 2.0 user pools. Instruct the employees to access the application by starting browser-based AppStream 2.0 streaming sessions.
- D. Refactor and containerize the application to run as a web-based application. Run the application in Amazon Elastic Container Service (Amazon ECS) on AWS Fargate with step scaling policies. Implement authentication by using Amazon Cognito user pools. Instruct the employees to run the application from their browsers.

Question #281

Topic 1

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 solutions architect must propose the most cost-effective solution that will allow SQL data queries.

Which solution will meet these requirements?

- A. Store data in Amazon S3. Use Amazon Redshift Spectrum to query data.
- B. Store data in Amazon S3. Use the AWS Glue Data Catalog and Amazon Athena to query data.
- C. Store data in EMR File System (EMRFS). Use Presto in Amazon EMR to query data.
- D. Store data in Amazon Redshift. Use Amazon Redshift to query data.

Question #282

Topic 1

A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into details 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 instances.

Which strategy should the solutions architect provide to meet these requirements?

- A. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources.
- B. Use an AWS Config rule to alert the finance team of untagged resources. Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoDB resources every hour using a cross-account role.
- 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.
- D. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources. Update existing federated roles to restrict privileges to provision resources that do not include the cost center and project ID on the resource.

Question #283

Topic 1

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? (Choose 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.
- B. 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 public VIF between the on-premises environment and the private VPC.
- C. Create an Amazon S3 interface endpoint in the networking account.
- D. Create an Amazon S3 gateway endpoint in the networking account.
- E. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Peer VPCs from the accounts that host the S3 buckets with the VPC in the network account.

Question #284

Topic 1

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 RCU and 80,000 WCU 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?

- A. Reduce the provisioned RCU and WCU.
- B. Change the DynamoDB table to use on-demand capacity.
- C. Enable Dynamo DB auto scaling for the table.
- D. Purchase 1-year reserved capacity that is sufficient to cover the peak load for 4 hours each day.

Question #285

Topic 1

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 making the comments appear in real time.

Which design should be used to reduce comment latency and improve user experience?

- A. Use edge-optimized API with Amazon CloudFront to cache API responses.
- B. Modify the blog application code to request GET/comments/{commentId} every 10 seconds.
- C. Use AWS AppSync and leverage WebSockets to deliver comments.
- D. Change the concurrency limit of the Lambda functions to lower the API response time.

Question #286

Topic 1

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?

- A. Set the S3 access point resource policy to deny the s3>CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- 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.
- C. Use AWS CloudFormation StackSets to create a new IAM policy in each AWS account that allows the s3>CreateAccessPoint action only if the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- D. Set the S3 bucket policy to deny the s3>CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.

Question #287

Topic 1

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?

- A. Redirect to the new environment using Amazon Route 53.
- B. Select the Swap Environment URLs option.
- C. Replace the Auto Scaling launch configuration.
- D. Update the DNS records to point to the green environment.

Question #288

Topic 1

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 will then overlay text on the uploaded images, which will then be published on the company website.

Which design should a solutions architect implement?

- A. Store the uploaded images in Amazon Elastic File System (Amazon EFS). Send application log information about each image to Amazon CloudWatch Logs. Create a fleet of Amazon EC2 instances that use CloudWatch Logs to determine which images need to be processed. Place processed images in another directory in Amazon EFS. Enable Amazon CloudFront and configure the origin to be the one of the EC2 instances in the fleet.
- B. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to Amazon Simple Notification Service (Amazon SNS). Create a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) to pull messages from Amazon SNS to process the images and place them in Amazon Elastic File System (Amazon EFS). Use Amazon CloudWatch metrics for the SNS message volume to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the ALB in front of the EC2 instances.
- 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.
- D. Store the uploaded images on a shared Amazon Elastic Block Store (Amazon EBS) volume mounted to a fleet of Amazon EC2 Spot instances. Create an Amazon DynamoDB table that contains information about each uploaded image and whether it has been processed. Use an Amazon EventBridge rule to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to reference an Elastic Load Balancer in front of the fleet of EC2 instances.

Question #289

Topic 1

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 DB 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.
- B. Add a cross-Region replica in eu-west-1 for the RDS for MySQL DB instance. Configure the replica to replicate write queries back to the primary DB instance. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.
- C. Copy the most recent snapshot from the RDS for MySQL DB instance to eu-west-1. Create a new RDS for MySQL DB instance in eu-west-1 from the snapshot. Configure MySQL logical replication from us-east-1 to eu-west-1. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.
- D. Convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster. Add eu-west-1 as a secondary Region to the DB 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.

Question #290

Topic 1

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?

- A. 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 publicly accessible endpoint. Associate the SFTP Elastic IP address with the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.
- 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.
- C. Disassociate the Elastic IP address from the EC2 instance. Create a new Amazon Elastic File System (Amazon EFS) file system to be used for SFTP file hosting. Create an AWS Fargate task definition to run an SFTP server. Specify the EFS file system as a mount in the task definition. Create a Fargate service by using the task definition, and place a Network Load Balancer (NLB) in front of the service. When configuring the service, attach the security group with customer IP addresses to the tasks that run the SFTP server. Associate the Elastic IP address with the NLB. Sync all files from the SFTP server to the S3 bucket.
- D. Disassociate the Elastic IP address from the EC2 instance. Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used for SFTP file hosting. Create a Network Load Balancer (NLB) with the Elastic IP address attached. Create an Auto Scaling group with EC2 instances that run an SFTP server. Define in the Auto Scaling group that instances that are launched should attach the new multi-attach EBS volume. Configure the Auto Scaling group to automatically add instances behind the NLB. Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launches. Sync all files from the SFTP server to the new multi-attach EBS volume.

Question #291

Topic 1

A company ingests and processes streaming market data. The data rate is constant. A nightly process that calculates aggregate statistics takes 4 hours to complete. The statistical analysis is not critical to the business, and data points are processed during the next iteration if a particular run fails.

The current architecture uses a pool of Amazon EC2 Reserved Instances with 1-year reservations. These EC2 instances run full time to ingest and store the streaming data in attached Amazon Elastic Block Store (Amazon EBS) volumes. A scheduled script launches EC2 On-Demand Instances each night to perform the nightly processing. The instances access the stored data from NFS shares on the ingestion servers. The script terminates the instances when the processing is complete.

The Reserved Instance reservations are expiring. The company needs to determine whether to purchase new reservations or implement a new design.

Which solution will meet these requirements MOST cost-effectively?

- A. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use a scheduled script to launch a fleet of EC2 On-Demand Instances each night to perform the batch processing of the S3 data. Configure the script to terminate the instances when the processing is complete.
- B. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use AWS Batch with Spot Instances to perform nightly processing with a maximum Spot price that is 50% of the On-Demand price.
- C. Update the ingestion process to use a fleet of EC2 Reserved Instances with 3-year reservations behind a Network LoadBalancer. Use AWS Batch with Spot Instances to perform nightly processing with a maximum Spot price that is 50% of the On-Demand price.
- D. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon Redshift. Use Amazon EventBridge to schedule an AWS Lambda function to run nightly to query Amazon Redshift to generate the daily statistics.

Question #292

Topic 1

A company needs to migrate an on-premises SFTP site to AWS. The SFTP site currently runs on a Linux VM. Uploaded files are made available to downstream applications through an NFS share.

As part of the migration to AWS, a solutions architect must implement high availability. The solution must provide external vendors with a set of static public IP addresses that the vendors can allow. The company has set up an AWS Direct Connect connection between its on-premises data center and its VPC.

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

- A. Create an AWS Transfer Family server. Configure an internet-facing VPC endpoint for the Transfer Family server. Specify an Elastic IP address for each subnet. Configure the Transfer Family server to place files into an Amazon Elastic File System (Amazon EFS) file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.
- B. Create an AWS Transfer Family server. Configure a publicly accessible endpoint for the Transfer Family server. Configure the Transfer Family server to place files into an Amazon Elastic File System (Amazon EFS) file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.
- C. Use AWS Application Migration Service to migrate the existing Linux VM to an Amazon EC2 instance. Assign an Elastic IP address to the EC2 instance. Mount an Amazon Elastic File System (Amazon EFS) file system to the EC2 instance. Configure the SFTP server to place files in the EFS file system. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.
- D. Use AWS Application Migration Service to migrate the existing Linux VM to an AWS Transfer Family server. Configure a publicly accessible endpoint for the Transfer Family server. Configure the Transfer Family server to place files into an Amazon FSx for Lustre file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the FSx for Lustre endpoint instead.

Question #293

Topic 1

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 IPv4 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 AZ1 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.
- B. Terminate the EC2 instances in the AZ1 subnet. Delete and re-create the AZ1 subnet using half the address space. Update the Auto Scaling group to use this new subnet. Repeat this for the second AZ. Define a new subnet in AZ3, then update the Auto Scaling group to target all three new subnets.
- C. Create a new VPC with the same IPv4 address space and define three subnets, with one for each AZ. Update the existing Auto Scaling group to target the new subnets in the new VPC.
- D. Update the Auto Scaling group to use the AZ2 subnet only. Update the AZ1 subnet to have half the previous address space. Adjust the Auto Scaling group to also use the AZ1 subnet again. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Update the current AZ2 subnet and assign 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.

Question #294

Topic 1

A company uses an organization in AWS Organizations to manage the company's AWS accounts. The company uses AWS CloudFormation to deploy all infrastructure. A finance team wants to build a chargeback model. The finance team asked each business unit to tag resources by using a predefined list of project values.

When the finance team used the AWS Cost and Usage Report in AWS Cost Explorer and filtered based on project, the team noticed noncompliant project values. The company wants to enforce the use of project tags for new resources.

Which solution will meet these requirements with the LEAST effort?

- A. Create a tag policy that contains the allowed project tag values in the organization's management account. Create an SCP that denies the clouformation:CreateStack API operation unless a project tag is added. Attach the SCP to each OU.
- B. Create a tag policy that contains the allowed project tag values in each OU. Create an SCP that denies the clouformation:CreateStack API operation unless a project tag is added. Attach the SCP to each OU.
- C. Create a tag policy that contains the allowed project tag values in the AWS management account. Create an IAM policy that denies the clouformation:CreateStack API operation unless a project tag is added. Assign the policy to each user.
- D. Use AWS Service Catalog to manage the CloudFormation stacks as products. Use a TagOptions library to control project tag values. Share the portfolio with all OUs that are in the organization.

Question #295

Topic 1

An application is deployed on Amazon EC2 instances that run in an Auto Scaling group. The Auto Scaling group configuration uses only one type of instance.

CPU and memory utilization metrics show that the instances are underutilized. A solutions architect needs to implement a solution to permanently reduce the EC2 cost and increase the utilization.

Which solution will meet these requirements with the LEAST number of configuration changes in the future?

- A. List instance types that have properties that are similar to the properties that the current instances have. Modify the Auto Scaling group's launch template configuration to use multiple instance types from the list.
- B. Use the information about the application's CPU and memory utilization to select an instance type that matches the requirements. Modify the Auto Scaling group's configuration by adding the new instance type. Remove the current instance type from the configuration.
- C. Use the information about the application's CPU and memory utilization to specify CPU and memory requirements in a new revision of the Auto Scaling group's launch template. Remove the current instance type from the configuration.
- D. Create a script that selects the appropriate instance types from the AWS Price List Bulk API. Use the selected instance types to create a new revision of the Auto Scaling group's launch template.

Question #296

Topic 1

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 automates 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?

- A. Set up an Aurora global database and DynamoDB global tables to replicate the databases to a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon CloudFront with origin failover to route traffic to the secondary Region during a DR scenario.
- B. Use AWS Database Migration Service (AWS DMS), Amazon EventBridge, and AWS Lambda to replicate the Aurora databases to a secondary AWS Region. Use DynamoDB Streams, EventBridge, and Lambda to replicate the DynamoDB databases to the secondary 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.
- 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.
- D. Set up an Aurora global database and DynamoDB global tables to replicate the databases to 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.

Question #297

Topic 1

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. The 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.
- B. Update the CloudFront distribution to disable caching based on query string parameters.
- C. Deploy a reverse proxy after the load balancer to post-process the emitted URLs in the application to force the URL strings to be lowercase.
- D. Update the CloudFront distribution to specify casing-insensitive query string processing.

Question #298

Topic 1

A company runs an ecommerce application in a single AWS Region. The application uses a five-node Amazon Aurora MySQL DB cluster to store information about customers and their recent orders. The DB cluster experiences a large number of write transactions throughout the day.

The company needs to replicate the data in the Aurora database to another Region to meet disaster recovery requirements. The company has an RPO of 1 hour.

Which solution will meet these requirements with the **LOWEST** cost?

- A. Modify the Aurora database to be an Aurora global database. Create a second Aurora database in another Region.
- B. Enable the Backtrack feature for the Aurora database. Create an AWS Lambda function that runs daily to copy the snapshots of the database to a backup Region.
- C. Use AWS Database Migration Service (AWS DMS). Create a DMS change data capture (CDC) task that replicates the ongoing changes from the Aurora database to an Amazon S3 bucket in another Region.
- D. Turn off automated Aurora backups. Configure Aurora backups with a backup frequency of 1 hour. Specify another Region as the destination Region. Select the Aurora database as the resource assignment.

Question #299

Topic 1

A company's solutions architect is evaluating an AWS workload that was deployed several years ago. The application tier is stateless and runs on a single large Amazon EC2 instance that was launched from an AMI. The application stores data in a MySQL database that runs on a single EC2 instance.

The CPU utilization on the application server EC2 instance often reaches 100% and causes the application to stop responding. The company manually installs patches on the instances. Patching has caused downtime in the past. The company needs to make the application highly available.

Which solution will meet these requirements with the LEAST development me?

- A. Move the application tier to AWS Lambda functions in the existing VPC. Create an Application Load Balancer to distribute traffic across the Lambda functions. Use Amazon GuardDuty to scan the Lambda functions. Migrate the database to Amazon DocumentDB (with MongoDB compatibility).
- B. Change the EC2 instance type to a smaller Graviton powered instance type. Use the existing AMI to create a launch template for an Auto Scaling group. Create an Application Load Balancer to distribute traffic across the instances in the Auto Scaling group. Set the Auto Scaling group to scale based on CPU utilization. Migrate the database to Amazon DynamoDB.
- C. Move the application tier to containers by using Docker. Run the containers on Amazon Elastic Container Service (Amazon ECS) with EC2 instances. Create an Application Load Balancer to distribute traffic across the ECS cluster. Configure the ECS cluster to scale based on CPU utilization. Migrate the database to Amazon Neptune.
- D. Create a new AMI that is configured with AWS Systems Manager Agent (SSM Agent). Use the new AMI to create a launch template for an Auto Scaling group. Use smaller instances in the Auto Scaling group. Create an Application Load Balancer to distribute traffic across the instances in the Auto Scaling group. Set the Auto Scaling group to scale based on CPU utilization. Migrate the database to Amazon Aurora MySQL.

Question #300

Topic 1

A company is planning to migrate several applications to AWS. The company does not have a good understanding of its entire application estate. The estate consists of a mixture of physical machines and VMs.

One application that the company will migrate has many dependencies that are sensitive to latency. The company is unsure what all the dependencies are. However the company knows that the low-latency communications use a custom IP-based protocol that runs on port 1000. The company wants to migrate the application and these dependencies together to move all the low-latency interfaces to AWS at the same time.

The company has installed the AWS Application Discovery Agent and has been collecting data for several months.

What should the company do to identify the dependencies that need to be migrated in the same phase as the application?

- A. Use AWS Migration Hub and select the servers that host the application. Visualize the network graph to find servers that interact with the application. Turn on data exploration in Amazon Athena. Query the data that is transferred between the servers to identify the servers that communicate on port 1000. Return to Migration Hub. Create a move group that is based on the findings from the Athena queries.
- B. Use AWS Application Migration Service and select the servers that host the application. Visualize the network graph to find servers that interact with the application. Configure Application Migration Service to launch test instances for all the servers that interact with the application. Perform acceptance tests on the test instances. If no issues are identified, create a move group that is based on the tested servers.
- C. Use AWS Migration Hub and select the servers that host the application. Turn on data exploration in Network Access Analyzer. Use the Network Access Analyzer console to select the servers that host the application. Select a Network Access Scope of port 1000 and note the matching servers. Return to Migration Hub. Create a move group that is based on the findings from Network Access Analyzer.
- D. Use AWS Migration Hub and select the servers that host the application. Push the Amazon CloudWatch agent to the identified servers by using the AWS Application Discovery Agent. Export the CloudWatch logs that the agents collect to Amazon S3. Use Amazon Athena to query the logs to find servers that communicate on port 1000. Return to Migration Hub. Create a move group that is based on the findings from the Athena queries.

Question #301

Topic 1

A company is building an application that will run on an AWS Lambda function. Hundreds of customers will use the application. The company wants to give each customer a quota of requests for a specific time period. The quotas must match customer usage patterns. Some customers must receive a higher quota for a shorter time period.

Which solution will meet these requirements?

- A. Create an Amazon API Gateway REST API with a proxy integration to invoke the Lambda function. For each customer, configure an API Gateway usage plan that includes an appropriate request quota. Create an API key from the usage plan for each user that the customer needs.
- B. Create an Amazon API Gateway HTTP API with a proxy integration to invoke the Lambda function. For each customer configure an API Gateway usage plan that includes an appropriate request quota. Configure route-level throttling for each usage plan. Create an API Key from the usage plan for each user that the customer needs.
- C. Create a Lambda function alias for each customer. Include a concurrency limit with an appropriate request quota. Create a Lambda function URL for each function alias. Share the Lambda function URL for each alias with the relevant customer.
- D. Create an Application Load Balancer (ALB) in a VPC. Configure the Lambda function as a target for the ALB. Configure an AWS WAF web ACL for the ALB. For each customer configure a rate-based rule that includes an appropriate request quota.

Question #302

Topic 1

A company is planning to migrate its on-premises VMware cluster of 120 VMs to AWS. The VMs have many different operating systems and many custom software packages installed. The company also has an on-premises NFS server that is 10 TB in size. The company has set up a 10 Gbps AWS Direct Connect connection to AWS for the migration.

Which solution will complete the migration to AWS in the LEAST amount of time?

- A. Export the on-premises VMs and copy them to an Amazon S3 bucket. Use VM Import/Export to create AMIs from the VM images that are stored in Amazon S3. Order an AWS Snowball Edge device. Copy the NFS server data to the device. Restore the NFS server data to an Amazon EC2 instance that has NFS configured.
- B. Configure AWS Application Migration Service with a connection to the VMware cluster. Create a replication job for the VMS. Create an Amazon Elastic File System (Amazon EFS) file system. Configure AWS DataSync to copy the NFS server data to the EFS file system over the Direct Connect connection.
- C. Recreate the VMs on AWS as Amazon EC2 instances. Install all the required software packages. Create an Amazon FSx for Lustre file system. Configure AWS DataSync to copy the NFS server data to the FSx for Lustre file system over the Direct Connect connection.
- D. Order two AWS Snowball Edge devices. Copy the VMs and the NFS server data to the devices. Run VM Import/Export after the data from the devices is loaded to an Amazon S3 bucket. Create an Amazon Elastic File System (Amazon EFS) file system. Copy the NFS server data from Amazon S3 to the EFS file system.

Question #303

Topic 1

An online survey company runs its application in the AWS Cloud. The application is distributed and consists of microservices that run in an automatically scaled Amazon Elastic Container Service (Amazon ECS) cluster. The ECS cluster is a target for an Application Load Balancer (ALB). The ALB is a custom origin for an Amazon CloudFront distribution.

The company has a survey that contains sensitive data. The sensitive data must be encrypted when it moves through the application. The application's data-handling microservice is the only microservice that should be able to decrypt the data.

Which solution will meet these requirements?

- A. Create a symmetric AWS Key Management Service (AWS KMS) key that is dedicated to the data-handling microservice. Create a field-level encryption profile and a configuration. Associate the KMS key and the configuration with the CloudFront cache behavior.
- B. Create an RSA key pair that is dedicated to the data-handling microservice. Upload the public key to the CloudFront distribution. Create a field-level encryption profile and a configuration. Add the configuration to the CloudFront cache behavior.
- C. Create a symmetric AWS Key Management Service (AWS KMS) key that is dedicated to the data-handling microservice. Create a Lambda@Edge function. Program the function to use the KMS key to encrypt the sensitive data.
- D. Create an RSA key pair that is dedicated to the data-handling microservice. Create a Lambda@Edge function. Program the function to use the private key of the RSA key pair to encrypt the sensitive data.

Question #304

Topic 1

A solutions architect is determining the DNS strategy for an existing VPC. The VPC is provisioned to use the 10.24.34.0/24 CIDR block. The VPC also uses Amazon Route 53 Resolver for DNS. New requirements mandate that DNS queries must use private hosted zones. Additionally instances that have public IP addresses must receive corresponding public hostnames

Which solution will meet these requirements to ensure that the domain names are correctly resolved within the VPC?

- A. Create a private hosted zone. Activate the enableDnsSupport attribute and the enableDnsHostnames attribute for the VPC. Update the VPC DHCP options set to include domain-name-servers=10.24.34.2.
- B. Create a private hosted zone Associate the private hosted zone with the VPC. Activate the enableDnsSupport attribute and the enableDnsHostnames attribute for the VPC. Create a new VPC DHCP options set, and configure domain-name-servers=AmazonProvidedDNS. Associate the new DHCP options set with the VPC.
- C. Deactivate the enableDnsSupport attribute for the VPCActivate the enableDnsHostnames attribute for the VPCCreate a new VPC DHCP options set, and configure domain-name-servers=10.24.34.2. Associate the new DHCP options set with the VPC.
- D. Create a private hosted zone. Associate the private hosted zone with the VPC. Activate the enableDnsSupport attribute for the VPC. Deactivate the enableDnsHostnames attribute for the VPC. Update the VPC DHCP options set to include domain-name-servers=AmazonProvidedDNS.

Question #305

Topic 1

A data analytics company has an Amazon Redshift cluster that consists of several reserved nodes. The cluster 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 all times. A solutions architect must devise a solution that accommodates the bursts of usage.

Which solution meets these requirements MOST cost-effectively?

- A. Provision an Amazon EMR cluster Offload the complex data processing tasks.
- B. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using a classic resize operation when the cluster's CPU metrics in Amazon CloudWatch reach 80%.
- C. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using an elastic resize operation when the cluster's CPU metrics in Amazon CloudWatch reach 80%.
- D. Turn on the Concurrency Scaling feature for the Amazon Redshift cluster.

Question #306

Topic 1

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 `$(aws:username)`. Apply the policy on the scientists' IAM user group.
- B. Configure a trail with AWS CloudTrail to capture all object-level events in the S3 bucket. Store the trail output in another S3 bucket. Use Amazon Athena to query the logs and generate reports.
- 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.
- D. Create an S3 bucket policy that grants read and write access to users in the scientists' IAM user group.
- E. Configure a trail with AWS CloudTrail to capture all object-level events in the S3 bucket and write the events to Amazon CloudWatch. Use the Amazon Athena CloudWatch connector to query the logs and generate reports.

Question #307

Topic 1

A company uses AWS Organizations to manage a multi-account structure. The company has hundreds of AWS accounts and expects the number of accounts to increase. The company is building a new application that uses Docker images. The company will push the Docker images to Amazon Elastic Container Registry (Amazon ECR). Only accounts that are within the company's organization should have access to the images.

The company has a CI/CD process that runs frequently. The company wants to retain all the tagged images. However, the company wants to retain only the five most recent untagged images.

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

- A. Create a private repository in Amazon ECR. Create a permissions policy for the repository that allows only required ECR operations. Include a condition to allow the ECR operations if the value of the `aws:PrincipalOrgID` condition key is equal to the ID of the company's organization. Add a lifecycle rule to the ECR repository that deletes all untagged images over the count of five.
- B. Create a public repository in Amazon ECR. Create an IAM role in the ECR account. Set permissions so that any account can assume the role if the value of the `aws:PrincipalOrgID` condition key is equal to the ID of the company's organization. Add a lifecycle rule to the ECR repository that deletes all untagged images over the count of five.
- C. Create a private repository in Amazon ECR. Create a permissions policy for the repository that includes only required ECR operations. Include a condition to allow the ECR operations for all account IDs in the organization. Schedule a daily Amazon EventBridge rule to invoke an AWS Lambda function that deletes all untagged images over the count of five.
- D. Create a public repository in Amazon ECR. Configure Amazon ECR to use an interface VPC endpoint with an endpoint policy that includes the required permissions for images that the company needs to pull. Include a condition to allow the ECR operations for all account IDs in the company's organization. Schedule a daily Amazon EventBridge rule to invoke an AWS Lambda function that deletes all untagged images over the count of five.

Question #308

Topic 1

A solutions architect is reviewing a company's process for taking snapshots of Amazon RDS DB instances. The company takes automatic snapshots every day and retains the snapshots for 7 days.

The solutions architect needs to recommend a solution that takes snapshots every 6 hours and retains the snapshots for 30 days. The company uses AWS Organizations to manage all of its AWS accounts. The company needs a consolidated view of the health of the RDS snapshots.

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

- A. Turn on the cross-account management feature in AWS Backup. Create a backup plan that specifies the frequency and retention requirements. Add a tag to the DB instances. Apply the backup plan by using tags. Use AWS Backup to monitor the status of the backups.
- B. Turn on the cross-account management feature in Amazon RDS. Create a snapshot global policy that specifies the frequency and retention requirements. Use the RDS console in the management account to monitor the status of the backups.
- C. Turn on the cross-account management feature in AWS CloudFormation. From the management account, deploy a CloudFormation stack set that contains a backup plan from AWS Backup that specifies the frequency and retention requirements. Create an AWS Lambda function in the management account to monitor the status of the backups. Create an Amazon EventBridge rule in each account to run the Lambda function on a schedule.
- D. Configure AWS Backup in each account. Create an Amazon Data Lifecycle Manager lifecycle policy that specifies the frequency and retention requirements. Specify the DB instances as the target resource. Use the Amazon Data Lifecycle Manager console in each member account to monitor the status of the backups.

Question #309

Topic 1

A company is using AWS Organizations with a multi-account architecture. The company's current security configuration for the account architecture includes SCPs, resource-based policies, identity-based policies, trust policies, and session policies.

A solutions architect needs to allow an IAM user in Account A to assume a role in Account B.

Which combination of steps must the solutions architect take to meet this requirement? (Choose three.)

- A. Configure the SCP for Account A to allow the action.
- B. Configure the resource-based policies to allow the action.
- C. Configure the identity-based policy on the user in Account A to allow the action.
- D. Configure the identity-based policy on the user in Account B to allow the action.
- E. Configure the trust policy on the target role in Account B to allow the action.
- F. Configure the session policy to allow the action and to be passed programmatically by the GetSessionToken API operation.

Question #310

Topic 1

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?

- A. 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 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- B. Deploy an AWS Storage Gateway volume gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the volume gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.
- C. Deploy an AWS Storage Gateway tape gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the tape gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- D. 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.

Question #311

Topic 1

A company runs its application on Amazon EC2 instances and AWS Lambda functions. The EC2 instances experience a continuous and stable load. The Lambda functions experience a varied and unpredictable load. The application includes a caching layer that uses an Amazon MemoryDB for Redis cluster.

A solutions architect must recommend a solution to minimize the company's overall monthly costs.

Which solution will meet these requirements?

- A. Purchase an EC2 instance Savings Plan to cover the EC2 instances. Purchase a Compute Savings Plan for Lambda to cover the minimum expected consumption of the Lambda functions. Purchase reserved nodes to cover the MemoryDB cache nodes.
- B. Purchase a Compute Savings Plan to cover the EC2 instances. Purchase Lambda reserved concurrency to cover the expected Lambda usage. Purchase reserved nodes to cover the MemoryDB cache nodes.
- C. Purchase a Compute Savings Plan to cover the entire expected cost of the EC2 instances, Lambda functions, and MemoryDB cache nodes.
- D. Purchase a Compute Savings Plan to cover the EC2 instances and the MemoryDB cache nodes. Purchase Lambda reserved concurrency to cover the expected Lambda usage.

Question #312

Topic 1

A company is launching a new online game on Amazon EC2 instances. The game must be available globally. The company plans to run the game in three AWS Regions us-east-1, eu-west-1, and ap-southeast-1. The game's leaderboards, player inventory and event status must be available across Regions.

A solutions architect must design a solution that will give any Region the ability to scale to handle the load of all Regions. Additionally, users must automatically connect to the Region that provides the least latency.

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

- A. Create an EC2 Spot Fleet. Attach the Spot Fleet to a Network Load Balancer (NLB) in each Region. Create an AWS Global Accelerator IP address that points to the NLB. Create an Amazon Route 53 latency-based routing entry for the Global Accelerator IP address. Save the game metadata to an Amazon RDS for MySQL DB instance in each Region. Set up a read replica in the other Regions.
- B. Create an Auto Scaling group for the EC2 instances. Attach the Auto Scaling group to a Network Load Balancer (NLB) in each Region. For each Region, create an Amazon Route 53 entry that uses geoproximity routing and points to the NLB in that Region. Save the game metadata to MySQL databases on EC2 instances in each Region. Set up replication between the database EC2 instances in each Region.
- C. Create an Auto Scaling group for the EC2 instances. Attach the Auto Scaling group to a Network Load Balancer (NLB) in each Region. For each Region, create an Amazon Route 53 entry that uses latency-based routing and points to the NLB in that Region. Save the game metadata to an Amazon DynamoDB global table.
- D. Use EC2 Global View. Deploy the EC2 instances to each Region. Attach the instances to a Network Load Balancer (NLB). Deploy a DNS server on an EC2 instance in each Region. Set up custom logic on each DNS server to redirect the user to the Region that provides the lowest latency. Save the game metadata to an Amazon Aurora global database.

Question #313

Topic 1

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.
- B. Create a new Network Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Network Load Balancer. Add each of the firewall appliance instances to the target group.
- 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.
- D. Create a VPC interface 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.
- E. Deploy two firewall appliances into the shared services VPC, each in the same Availability Zone.
- 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.

Question #314

Topic 1

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.

Given these requirements, which combination of steps should be taken to implement highly available architecture for the application servers in AWS? (Choose 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.
- B. Create a pool of ENIs. Request license files from the vendor for the pool, store the license files on an Amazon EC2 instance. Create an AMI from the instance and use this AMI for all future EC2 instances.
- C. Create a bootstrap automation script to request a new license file from the vendor. When the response is received, apply the license file 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.
- E. Edit an Amazon EC2 instance to include the database server IP address in the configuration files and re-create the AMI to use for all future EC2 stances.

Question #315

Topic 1

A company runs its sales reporting application in an AWS Region in the United States. The application uses an Amazon API Gateway Regional API and AWS Lambda functions to generate on-demand reports from data in an Amazon RDS for MySQL database. The frontend of the application is hosted on Amazon S3 and is accessed by users through an Amazon CloudFront distribution. The company is using Amazon Route 53 as the DNS service for the domain. Route 53 is configured with a simple routing policy to route traffic to the API Gateway API.

In the next 6 months, the company plans to expand operations to Europe. More than 90% of the database traffic is read-only traffic. The company has already deployed an API Gateway API and Lambda functions in the new Region.

A solutions architect must design a solution that minimizes latency for users who download reports.

Which solution will meet these requirements?

- A. Use an AWS Database Migration Service (AWS DMS) task with full load to replicate the primary database in the original Region to the database in the new Region. Change the Route 53 record to latency-based routing to connect to the API Gateway API.
- B. Use an AWS Database Migration Service (AWS DMS) task with full load plus change data capture (CDC) to replicate the primary database in the original Region to the database in the new Region. Change the Route 53 record to geolocation routing to connect to the API Gateway API.
- C. Configure a cross-Region read replica for the RDS database in the new Region. Change the Route 53 record to latency-based routing to connect to the API Gateway API.
- D. Configure a cross-Region read replica for the RDS database in the new Region. Change the Route 53 record to geolocation routing to connect to the API Gateway API.

Question #316

Topic 1

A software company needs to create short-lived test environments to test pull requests as part of its development process. Each test environment consists of a single Amazon EC2 instance that is in an Auto Scaling group.

The test environments must be able to communicate with a central server to report test results. The central server is located in an on-premises data center. A solutions architect must implement a solution so that the company can create and delete test environments without any manual intervention. The company has created a transit gateway with a VPN attachment to the on-premises network.

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

- A. Create an AWS CloudFormation template that contains a transit gateway attachment and related routing configurations. Create a CloudFormation stack set that includes this template. Use CloudFormation StackSets to deploy a new stack for each VPC in the account. Deploy a new VPC for each test environment.
- B. Create a single VPC for the test environments. Include a transit gateway attachment and related routing configurations. Use AWS CloudFormation to deploy all test environments into the VPC.
- C. Create a new OU in AWS Organizations for testing. Create an AWS CloudFormation template that contains a VPC, necessary networking resources, a transit gateway attachment, and related routing configurations. Create a CloudFormation stack set that includes this template. Use CloudFormation StackSets for deployments into each account under the testing OU. Create a new account for each test environment.
- D. Convert the test environment EC2 instances into Docker images. Use AWS CloudFormation to configure an Amazon Elastic Kubernetes Service (Amazon EKS) cluster in a new VPC, create a transit gateway attachment, and create related routing configurations. Use Kubernetes to manage the deployment and lifecycle of the test environments.

Question #317

Topic 1

A company is deploying a new API to AWS. The API uses Amazon API Gateway with a Regional API endpoint and an AWS Lambda function for hosting. The API retrieves data from an external vendor API, stores data in an Amazon DynamoDB global table, and retrieves data from the DynamoDB global table. The API key for the vendor's API is stored in AWS Secrets Manager and is encrypted with a customer managed key in AWS Key Management Service (AWS KMS). The company has deployed its own API into a single AWS Region.

A solutions architect needs to change the API components of the company's API to ensure that the components can run across multiple Regions in an active-active configuration.

Which combination of changes will meet this requirement with the LEAST operational overhead? (Choose three.)

- A. Deploy the API to multiple Regions. Configure Amazon Route 53 with custom domain names that route traffic to each Regional API endpoint. Implement a Route 53 multivalue answer routing policy.
- B. Create a new KMS multi-Region customer managed key. Create a new KMS customer managed replica key in each in-scope Region.
- C. Replicate the existing Secrets Manager secret to other Regions. For each in-scope Region's replicated secret, select the appropriate KMS key.
- D. Create a new AWS managed KMS key in each in-scope Region. Convert an existing key to a multiRegion key. Use the multi-Region key in other Regions.
- E. Create a new Secrets Manager secret in each in-scope Region. Copy the secret value from the existing Region to the new secret in each in-scope Region.
- F. Modify the deployment process for the Lambda function to repeat the deployment across in-scope Regions. Turn on the multi-Region option for the existing API. Select the Lambda function that is deployed in each Region as the backend for the multi-Region API.

Question #318

Topic 1

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?

- A. Migrate the database to an Amazon RDS MySQL Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon Neptune
- 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.
- C. Migrate the database to Amazon DocumentDB (with MongoDB compatibility). Deploy the application in an Auto Scaling group on Amazon EC2 instances behind a Network Load Balancer. Store sessions in Amazon Kinesis Data Firehose.
- D. Migrate the database to an Amazon RDS MariaDB Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon ElastiCache for Memcached.

Question #319

Topic 1

A company's solutions architect needs to provide secure Remote Desktop connectivity to users for Amazon EC2 Windows instances that are hosted in a VPC. The solution must integrate centralized user management with the company's on-premises Active Directory. Connectivity to the VPC is through the internet. The company has hardware that can be used to establish an AWS Site-to-Site VPN connection.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy a managed Active Directory by using AWS Directory Service for Microsoft Active Directory. Establish a trust with the on-premises Active Directory. Deploy an EC2 instance as a bastion host in the VPC. Ensure that the EC2 instance is joined to the domain. Use the bastion host to access the target instances through RDP.
- B. Configure AWS IAM Identity Center (AWS Single Sign-On) to integrate with the on-premises Active Directory by using the AWS Directory Service for Microsoft Active Directory AD Connector. Configure permission sets against user groups for access to AWS Systems Manager. Use Systems Manager Fleet Manager to access the target instances through RDP.
- C. Implement a VPN between the on-premises environment and the target VPEnsure that the target instances are joined to the on-premises Active Directory domain over the VPN connection. Configure RDP access through the VPN. Connect from the company's network to the target instances.
- D. Deploy a managed Active Directory by using AWS Directory Service for Microsoft Active Directory. Establish a trust with the on-premises Active Directory. Deploy a Remote Desktop Gateway on AWS by using an AWS Quick Start. Ensure that the Remote Desktop Gateway is joined to the domain. Use the Remote Desktop Gateway to access the target instances through RDP.

Question #320

Topic 1

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?

- A. Create an Amazon EventBridge rule to detect the creation of unencrypted EBS volumes. Invoke an AWS Lambda function to delete noncompliant volumes.
- B. Use AWS Audit Manager with data encryption.
- C. Create an AWS Config rule to detect the creation of a new EBS volume. Encrypt the volume by using AWS Systems Manager Automation.
- D. Turn on EBS encryption by default in all AWS Regions.

Question #321

Topic 1

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?

- A. Launch new EC2 instances, and generate an individual SSH key for each instance. Store the SSH key in AWS Secrets Manager. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement for the GetSecretValue action. Instruct the engineers to fetch the SSH key from Secrets Manager when they connect through any SSH client.
- B. Create an AWS Systems Manager document to run commands on EC2 instances to set a new unique SSH key. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement to run Systems Manager documents. Instruct the engineers to run the document to set an SSH key and to connect through any SSH client.
- C. Launch new EC2 instances without setting up any SSH key for the instances. Set up EC2 Instance Connect on each instance. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement for the SendSSHPublicKey action. Instruct the engineers to connect to the instance by using a browser-based SSH client from the EC2 console.
- 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 call 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.

Question #322

Topic 1

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?

- A. Provision a set of EC2 instances across two Availability Zones in the VPC as caching DNS servers to resolve DNS queries from the application servers within the VPC.
- B. Provision an Amazon Route 53 private hosted zone. Configure NS records that point to on-premises DNS servers.
- 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.
- D. Provision a new Active Directory domain controller in the VPC with a bidirectional trust between this new domain and the on-premises Active Directory domain.

Question #323

Topic 1

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?

- A. Use Amazon Kinesis Data Firehose to send the data to Amazon Redshift.
- B. Use Amazon Kinesis Data Streams to send the data to Amazon DynamoDB.
- C. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to send the data to Amazon Aurora.
- D. Use Amazon Kinesis Data Firehose to send the data to Amazon Keyspaces (for Apache Cassandra).

Question #324

Topic 1

A company is migrating a legacy application from an on-premises data center to AWS. The application uses MongoDB 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?

- A. Create new Amazon DocumentDB (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes. Use the instance endpoint to connect to Amazon DocumentDB.
- B. Create new Amazon DynamoDB tables for the application with on-demand capacity. Use a gateway VPC endpoint for DynamoDB to connect to the DynamoDB tables.
- C. Create new Amazon DynamoDB tables for the application with on-demand capacity. Use an interface VPC endpoint for DynamoDB to connect to the DynamoDB tables.
- D. Create new Amazon DocumentDB (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes. Use the cluster endpoint to connect to Amazon DocumentDB.

Question #325

Topic 1

A company is running an application on Amazon EC2 instances in the AWS Cloud. The application is using a MongoDB database with a replica set as its data tier. The MongoDB database is installed on systems in the company's on-premises data center and is accessible through an AWS Direct Connect connection to the data center environment.

A solutions architect must migrate the on-premises MongoDB database to Amazon DocumentDB (with MongoDB compatibility).

Which strategy should the solutions architect choose to perform this migration?

- A. Create a fleet of EC2 instances. Install MongoDB Community Edition on the EC2 instances, and create a database. Configure continuous synchronous replication with the database that is running in the on-premises data center.
- B. Create an AWS Database Migration Service (AWS DMS) replication instance. Create a source endpoint for the on-premises MongoDB database by using change data capture (CDC). Create a target endpoint for the Amazon DocumentDB database. Create and run a DMS migration task.
- C. Create a data migration pipeline by using AWS Data Pipeline. Define data nodes for the on-premises MongoDB database and the Amazon DocumentDB database. Create a scheduled task to run the data pipeline.
- D. Create a source endpoint for the on-premises MongoDB database by using AWS Glue crawlers. Configure continuous asynchronous replication between the MongoDB database and the Amazon DocumentDB database.

Question #326

Topic 1

A company is rearchitecting its applications to run on AWS. The company's infrastructure includes multiple Amazon EC2 instances. The company's development team needs different levels of access. The company wants to implement a policy that requires all Windows EC2 instances to be joined to an Active Directory domain on AWS. The company also wants to implement enhanced security processes such as multi-factor authentication (MFA). The company wants to use managed AWS services wherever possible.

Which solution will meet these requirements?

- A. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.
- B. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.
- C. Create an AWS Directory Service Simple AD implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.
- D. Create an AWS Directory Service Simple AD implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.

Question #327

Topic 1

A company wants to migrate its on-premises application to AWS. The database for the application stores structured product data and temporary user session data. The company needs to decouple the product data from the user session data. The company also needs to implement replication in another AWS Region for disaster recovery.

Which solution will meet these requirements with the HIGHEST performance?

- A. Create an Amazon RDS DB instance with separate schemas to host the product data and the user session data. Configure a read replica for the DB instance in another Region.
- B. Create an Amazon RDS DB instance to host the product data. Configure a read replica for the DB instance in another Region. Create a global datastore in Amazon ElastiCache for Memcached to host the user session data.
- C. Create two Amazon DynamoDB global tables. Use one global table to host the product data. Use the other global table to host the user session data. Use DynamoDB Accelerator (DAX) for caching.
- D. Create an Amazon RDS DB instance to host the product data. Configure a read replica for the DB instance in another Region. Create an Amazon DynamoDB global table to host the user session data.

Question #328

Topic 1

A company orchestrates a multi-account structure on AWS by using AWS Control Tower. The company is using AWS Organizations, AWS Config, and AWS Trusted Advisor. The company has a specific OU for development accounts that developers use to experiment on AWS. The company has hundreds of developers, and each developer has an individual development account.

The company wants to optimize costs in these development accounts. Amazon EC2 instances and Amazon RDS instances in these accounts must be burstable. The company wants to disallow the use of other services that are not relevant.

What should a solutions architect recommend to meet these requirements?

- A. Create a custom SCP in AWS Organizations to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the SCP to the development OU.
- B. Create a custom detective control (guardrail) in AWS Control Tower. Configure the control (guardrail) to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the control (guardrail) to the development OU.
- C. Create a custom preventive control (guardrail) in AWS Control Tower. Configure the control (guardrail) to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the control (guardrail) to the development OU.
- D. Create an AWS Config rule in the AWS Control Tower account. Configure the AWS Config rule to allow the deployment of only burstable instances and to disallow services that are not relevant. Deploy the AWS Config rule to the development OU by using AWS CloudFormation StackSets.

Question #329

Topic 1

A financial services company runs a complex, multi-tier application on Amazon EC2 instances and AWS Lambda functions. The application stores temporary data in Amazon S3. The S3 objects are valid for only 45 minutes and are deleted after 24 hours.

The company deploys each version of the application by launching an AWS CloudFormation stack. The stack creates all resources that are required to run the application. When the company deploys and validates a new application version, the company deletes the CloudFormation stack of the old version.

The company recently tried to delete the CloudFormation stack of an old application version, but the operation failed. An analysis shows that CloudFormation failed to delete an existing S3 bucket. A solutions architect needs to resolve this issue without making major changes to the application's architecture.

Which solution meets these requirements?

- A. Implement a Lambda function that deletes all files from a given S3 bucket. Integrate this Lambda function as a custom resource into the CloudFormation stack. Ensure that the custom resource has a DependsOn attribute that points to the S3 bucket's resource.
- B. Modify the CloudFormation template to provision an Amazon Elastic File System (Amazon EFS) file system to store the temporary files there instead of in Amazon S3. Configure the Lambda functions to run in the same VPC as the file system. Mount the file system to the EC2 instances and Lambda functions.
- C. Modify the CloudFormation stack to create an S3 Lifecycle rule that expires all objects 45 minutes after creation. Add a DependsOn attribute that points to the S3 bucket's resource.
- D. Modify the CloudFormation stack to attach a DeletionPolicy attribute with a value of Delete to the S3 bucket.

Question #330

Topic 1

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 in central 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 session data. Management has asked a solutions architect to present a cloud architecture that can handle the game's varying load and provide low-latency data access. The API model should not be changed.

Which solution meets these requirements?

- A. Implement the REST API using a Network Load Balancer (NLB). Run the business logic on an Amazon EC2 instance behind the NLB. Store player session data in Amazon Aurora Serverless.
- B. Implement the REST API using an Application Load Balancer (ALB). Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.
- 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.
- D. Implement the REST API using AWS AppSync. Run the business logic in AWS Lambda. Store player session data in Amazon Aurora Serverless.

Question #331

Topic 1

A company is migrating an application to the AWS Cloud. The application 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?

- A. Configure a periodic process to run the aws s3 sync command from the on-premises file system to Amazon S3. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system.
- B. Deploy an AWS Storage Gateway file gateway with an NFS mount point. Mount the file gateway file system on the on-premises server. Configure a process to periodically copy the images to the mount point.
- C. 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 S3 bucket by using a public VIF. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system.
- 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.

Question #332

Topic 1

A company recently migrated a web application from an on-premises data center to the AWS Cloud. The web application infrastructure consists of an Amazon CloudFront distribution that routes to an Application Load Balancer (ALB), with Amazon Elastic Container Service (Amazon ECS) to process requests. A recent security audit revealed that the web application is accessible by using both CloudFront and ALB endpoints. However, the company requires that the web application must be accessible only by using the CloudFront endpoint.

Which solution will meet this requirement with the LEAST amount of effort?

- A. Create a new security group and attach it to the CloudFront distribution. Update the ALB security group ingress to allow access only from the CloudFront security group.
- B. Update ALB security group ingress to allow access only from the com.amazonaws.global.cloudfront.origin-facing CloudFront managed prefix list.
- C. Create a com.amazonaws.region.elasticloadbalancing VPC interface endpoint for Elastic Load Balancing. Update the ALB scheme from internet-facing to internal.
- D. Extract CloudFront IPs from the AWS provided ip-ranges.json document. Update ALB security group ingress to allow access only from CloudFront IPs.

Question #333

Topic 1

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?

- A. Use AWS CloudFormation to deploy identical ALB, EC2, ECS and RDS resources in two regions. Schedule RDS snapshots every 8 hours. Use RDS multi-region replication to update the secondary region's copy of the database. In the event of a failure, restore from the latest snapshot, and use an Amazon Route 53 DNS failover policy to automatically redirect customers to the ALB in the secondary region.
- 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.
- C. Use AWS CloudFormation to deploy identical ALB, EC2, ECS, and RDS resources in a secondary region. Schedule hourly RDS MySQL backups to Amazon S3 and use cross-region replication to replicate data to a bucket in the secondary region. In the event of a failure, import the latest Docker image to Amazon ECR in the secondary region, deploy to the EC2 instance, restore the latest MySQL backup, and update the DNS record to point to the ALB in the secondary region.
- D. Deploy a pilot light environment in a secondary region with an ALB and a minimal resource EC2 deployment for Docker in an AWS Auto Scaling group with a scaling policy to increase instance size and number of nodes. Create a cross-region read replica of the RDS data. In the event of a failure, promote the replica to primary, and update the DNS record to point to the ALB in the secondary region.

Question #334

Topic 1

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 for federation with the on-premises AD FS server. Configure a central logging 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.
- B. Create an organization in AWS Organizations. Enable AWS Control Tower on the organization. Review included controls (guardrails) for SCPs. Check AWS Config for areas that require additions. Add OUs as necessary. Connect AWS IAM Identity Center (AWS Single Sign-On) to the on-premises AD FS server.
- C. Create an organization in AWS Organizations. Create SCPs for least privilege access. Create an OU structure, and use it to group AWS accounts. Connect AWS IAM Identity Center (AWS Single Sign-On) to the on-premises AD FS server. Configure a central logging 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 aggregators and conformance packs.
- D. Create an organization in AWS Organizations. Enable AWS Control Tower on the organization. Review included controls (guardrails) for SCPs. Check AWS Config for areas that require additions. Configure an IAM identity provider for federation with the on-premises AD FS server.

Question #335

Topic 1

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.

The magazine is expecting 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? (Choose two.)

- A. Use logical cross-Region replication to replicate the Aurora MySQL database to a secondary Region. Replace the web servers with Amazon S3. Deploy S3 buckets in cross-Region replication mode.
- B. Ensure the web and application tiers are each in Auto Scaling groups. Introduce an AWS Direct Connect connection. Deploy the web and application tiers in Regions across the world.
- C. Migrate the database from Amazon Aurora to Amazon RDS for MySQL. Ensure all three of the application tiers – web, application, and database – are in private subnets.
- 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-based routing and Amazon CloudFront distributions. Ensure the web and application tiers are each in Auto Scaling groups.

Question #336

Topic 1

An online gaming company needs to optimize the cost of its workloads on AWS. The company uses a dedicated account to host the production environment for its online gaming application and an analytics application.

Amazon EC2 instances host the gaming application and must always be available. The EC2 instances run all year. The analytics application uses data that is stored in Amazon S3. The analytics application can be interrupted and resumed without issue.

Which solution will meet these requirements MOST cost-effectively?

- A. Purchase an EC2 Instance Savings Plan for the online gaming application instances. Use On-Demand Instances for the analytics application.
- B. Purchase an EC2 Instance Savings Plan for the online gaming application instances. Use Spot Instances for the analytics application.
- C. Use Spot Instances for the online gaming application and the analytics application. Set up a catalog in AWS Service Catalog to provision services at a discount.
- D. Use On-Demand Instances for the online gaming application. Use Spot Instances for the analytics application. Set up a catalog in AWS Service Catalog to provision services at a discount.

Question #337

Topic 1

A company runs applications in hundreds of production AWS accounts. The company uses AWS Organizations with all features enabled and has a centralized backup operation that uses AWS Backup.

The company is concerned about ransomware attacks. To address this concern, the company has created a new policy that all backups must be resilient to breaches of privileged-user credentials in any production account.

Which combination of steps will meet this new requirement? (Choose three.)

- A. Implement cross-account backup with AWS Backup vaults in designated non-production accounts.
- B. Add an SCP that restricts the modification of AWS Backup vaults.
- C. Implement AWS Backup Vault Lock in compliance mode.
- C. Implement least privilege access for the IAM service role that is assigned to AWS Backup.
- D. Configure the backup frequency, lifecycle, and retention period to ensure that at least one backup always exists in the cold tier.
- E. Configure AWS Backup to write all backups to an Amazon S3 bucket in a designated non-production account. Ensure that the S3 bucket has S3 Object Lock enabled.

Question #338

Topic 1

A company needs to aggregate Amazon CloudWatch logs from its AWS accounts into one central logging account. The collected logs must remain in the AWS Region of creation. The central logging account will then process the logs, normalize the logs into standard output format, and stream the output logs to a security tool for more processing.

A solutions architect must design a solution that can handle a large volume of logging data that needs to be ingested. Less logging will occur outside normal business hours than during normal business hours. The logging solution must scale with the anticipated load. The solutions architect has decided to use an AWS Control Tower design to handle the multi-account logging process.

Which combination of steps should the solutions architect take to meet the requirements? (Choose three.)

- A. Create a destination Amazon Kinesis data stream in the central logging account.
- B. Create a destination Amazon Simple Queue Service (Amazon SQS) queue in the central logging account.
- C. Create an IAM role that grants Amazon CloudWatch Logs the permission to add data to the Amazon Kinesis data stream. Create a trust policy. Specify the trust policy in the IAM role. In each member account, create a subscription filter for each log group to send data to the Kinesis data stream.
- D. Create an IAM role that grants Amazon CloudWatch Logs the permission to add data to the Amazon Simple Queue Service (Amazon SQS) queue. Create a trust policy. Specify the trust policy in the IAM role. In each member account, create a single subscription filter for all log groups to send data to the SQS queue.
- E. Create an AWS Lambda function. Program the Lambda function to normalize the logs in the central logging account and to write the logs to the security tool.
- F. Create an AWS Lambda function. Program the Lambda function to normalize the logs in the member accounts and to write the logs to the security tool.

Question #339

Topic 1

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.)

- A. Use an AWS Server Migration Service (AWS SMS) replication job to migrate the database server VM to AWS.
- B. Use VM Import/Export to import the application server VM.
- C. Export the VM images to an AWS Snowball Edge Storage Optimized device.
- 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.

Question #340

Topic 1

A company operates a fleet of servers on premises and operates a fleet of Amazon EC2 instances in its organization in AWS Organizations. The company's AWS accounts contain hundreds of VPCs. The company wants to connect its AWS accounts to its on-premises network. AWS Site-to-Site VPN connections are already established to a single AWS account. The company wants to control which VPCs can communicate with other VPCs.

Which combination of steps will achieve this level of control with the LEAST operational effort? (Choose three.)

- A. Create a transit gateway in an AWS account. Share the transit gateway across accounts by using AWS Resource Access Manager (AWS RAM).
- B. Configure attachments to all VPCs and VPNs.
- C. Setup transit gateway route tables. Associate the VPCs and VPNs with the route tables.
- D. Configure VPC peering between the VPCs.
- E. Configure attachments between the VPCs and VPNs.
- F. Setup route tables on the VPCs and VPNs.

Question #341

Topic 1

A company needs to optimize the cost of its application on AWS. The application uses AWS Lambda functions and Amazon Elastic Container Service (Amazon ECS) containers that run on AWS Fargate. The application is write-heavy and stores data in an Amazon Aurora MySQL database.

The load on the application is not consistent. The application experiences long periods of no usage, followed by sudden and significant increases and decreases in traffic. The database runs on a memory optimized DB instance that cannot handle the load.

A solutions architect must design a solution that can scale to handle the changes in traffic.

Which solution will meet these requirements MOST cost-effectively?

- A. Add additional read replicas to the database. Purchase Instance Savings Plans and RDS Reserved Instances.
- B. Migrate the database to an Aurora DB cluster that has multiple writer instances. Purchase Instance Savings Plans.
- C. Migrate the database to an Aurora global database. Purchase Compute Savings Plans and RDS Reserved instances.
- D. Migrate the database to Aurora Serverless v1. Purchase Compute Savings Plans.

Question #342

Topic 1

A company migrated an application to the AWS Cloud. The application runs on two Amazon EC2 instances behind an Application Load Balancer (ALB).

Application data is stored in a MySQL database that runs on an additional EC2 instance. The application's use of the database is read-heavy.

The application loads static content from Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. The static content is updated frequently and must be copied to each EBS volume.

The load on the application changes throughout the day. During peak hours, the application cannot handle all the incoming requests. Trace data shows that the database cannot handle the read load during peak hours.

Which solution will improve the reliability of the application?

- A. Migrate the application to a set of AWS Lambda functions. Set the Lambda functions as targets for the ALB. Create a new single EBS volume for the static content. Configure the Lambda functions to read from the new EBS volume. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB cluster.
- B. Migrate the application to a set of AWS Step Functions state machines. Set the state machines as targets for the ALB. Create an Amazon Elastic File System (Amazon EFS) file system for the static content. Configure the state machines to read from the EFS file system. Migrate the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance.
- C. Containerize the application. Migrate the application to an Amazon Elastic Container Service (Amazon ECS) cluster. Use the AWS Fargate launch type for the tasks that host the application. Create a new single EBS volume for the static content. Mount the new EBS volume on the ECS cluster. Configure AWS Application Auto Scaling on the ECS cluster. Set the ECS service as a target for the ALB. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB cluster.
- D. Containerize the application. Migrate the application to an Amazon Elastic Container Service (Amazon ECS) cluster. Use the AWS Fargate launch type for the tasks that host the application. Create an Amazon Elastic File System (Amazon EFS) file system for the static content. Mount the EFS file system to each container. Configure AWS Application Auto Scaling on the ECS cluster. Set the ECS service as a target for the ALB. Migrate the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance.

Question #343

Topic 1

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.
- B. For the API Gateway resource, set CORS to enabled and only return the company's domain in Access-Control-Allow-Origin headers. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.
- C. Create an AWS Lambda function as the custom authorizer, ask the API client to pass the key and secret when making the call, and then use Lambda to validate the key/secret pair against the IAM system. Use AWS X-Ray to trace and analyze user requests to API Gateway.
- D. Create a client certificate for API Gateway. Distribute the certificate to the AWS users and roles that need to access the endpoint. Enable the API caller to pass the client certificate when accessing the endpoint. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.

Question #344

Topic 1

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?

- A. Adapt the deployment scripts to detect and report CloudFormation error conditions when performing deployments. Write test plans for a testing team to run in a non-production environment before approving the change for production.
- 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.
- C. Use plugins for the integrated development environment (IDE) to check the templates for errors, and use the AWS CLI to validate that the templates are correct. Adapt the deployment code to check for error conditions and generate notifications on errors. Deploy to a test environment and run a manual test plan before approving the change for production.
- D. Use AWS CodeDeploy and a blue/green deployment pattern with CloudFormation to replace the user data deployment scripts. Have the operators log in to running instances and go through a manual test plan to verify the application is running as expected.

Question #345

Topic 1

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?

- A. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. 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 in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB.
- 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.
- C. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) that spans both VPCs. Deploy EC2 instances across multiple Availability Zones as part of an Auto Scaling group in each VPC served by the ALB. Create an Amazon Route 53 record that points to the ALB.
- D. 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 separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions.

Question #346

Topic 1

A company has a legacy application that runs on multiple .NET Framework components. The components share the same Microsoft SQL Server database and communicate with each other asynchronously by using Microsoft Message Queueing (MSMQ).

The company is starting a migration to containerized .NET Core components and wants to refactor the application to run on AWS. The .NET Core components require complex orchestration. The company must have full control over networking and host configuration. The application's database model is strongly relational.

Which solution will meet these requirements?

- A. Host the .NET Core components on AWS App Runner. Host the database on Amazon RDS for SQL Server. Use Amazon EventBridge for asynchronous messaging.
- B. Host the .NET Core components on Amazon Elastic Container Service (Amazon ECS) with the AWS Fargate launch type. Host the database on Amazon DynamoDB. Use Amazon Simple Notification Service (Amazon SNS) for asynchronous messaging.
- C. Host the .NET Core components on AWS Elastic Beanstalk. Host the database on Amazon Aurora PostgreSQL Serverless v2. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) for asynchronous messaging.
- D. Host the .NET Core components on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. Host the database on Amazon Aurora MySQL Serverless v2. Use Amazon Simple Queue Service (Amazon SQS) for asynchronous messaging.

Question #347

Topic 1

A solutions architect has launched multiple Amazon EC2 instances in a placement group within a single Availability Zone. Because of additional load on the system, the solutions architect attempts to add new instances to the placement group. However, the solutions architect receives an insufficient capacity error.

What should the solutions architect do to troubleshoot this issue?

- A. Use a spread placement group. Set a minimum of eight instances for each Availability Zone.
- B. Stop and start all the instances in the placement group. Try the launch again.
- C. Create a new placement group. Merge the new placement group with the original placement group.
- D. Launch the additional instances as Dedicated Hosts in the placement groups.

Question #348

Topic 1

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 solutions architect recommend to avoid a recurrence of this issue? (Choose two.)

- A. Modify the Auto Scaling group by setting the Update policy to target the oldest launch configuration for replacement.
- B. Create a new Auto Scaling group before the next patch maintenance. During the maintenance window, patch both groups and reboot the instances.
- C. Create an Elastic Load Balancer in front of the Auto Scaling group. Configure monitoring to ensure that target group health checks return healthy after the Auto Scaling group replaces the terminated instances.
- D. Create automation scripts to patch an AMI, update the launch configuration, and invoke an Auto Scaling instance refresh.
- E. Create an Elastic Load Balancer in front of the Auto Scaling group. Configure termination protection on the instances.

Question #349**Topic 1**

A team of data scientists is using Amazon SageMaker instances and SageMaker APIs to train machine learning (ML) models. The SageMaker instances are deployed in a VPC that does not have access to or from the internet. Datasets for ML model training are stored in an Amazon S3 bucket. Interface VPC endpoints provide access to Amazon S3 and the SageMaker APIs.

Occasionally, the data scientists require access to the Python Package Index (PyPI) repository to update Python packages that they use as part of their workflow. A solutions architect must provide access to the PyPI repository while ensuring that the SageMaker instances remain isolated from the internet.

Which solution will meet these requirements?

- A. Create an AWS CodeCommit repository for each package that the data scientists need to access. Configure code synchronization between the PyPI repository and the CodeCommit repository. Create a VPC endpoint for CodeCommit.
- B. Create a NAT gateway in the VPC. Configure VPC routes to allow access to the internet with a network ACL that allows access to only the PyPI repository endpoint.
- C. Create a NAT instance in the VPC. Configure VPC routes to allow access to the internet. Configure SageMaker notebook instance firewall rules that allow access to only the PyPI repository endpoint.
- D. Create an AWS CodeArtifact domain and repository. Add an external connection for public:pypi to the CodeArtifact repository. Configure the Python client to use the CodeArtifact repository. Create a VPC endpoint for CodeArtifact.

Question #350**Topic 1**

A solutions architect works for a government agency that has strict disaster 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 daily to copy the EBS snapshots to the additional Regions.
- B. Use Amazon EventBridge to schedule an AWS Lambda function to copy the EBS snapshots to the additional Regions.
- C. Setup AWS Backup to create the EBS snapshots. Configure Amazon S3 Cross-Region Replication to copy the EBS snapshots to the additional Regions.
- D. Schedule Amazon EC2 Image Builder to run once daily to create an AMI and copy the AMI to the additional Regions.

Question #351

Topic 1

A company has a project that is launching Amazon EC2 instances that are 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?

- A. Create a new developer account. Move all EC2 instances, users, and assets into us-east-2. Add the account to the company's organization in AWS Organizations. Enforce a tagging policy that denotes Region affinity.
- B. Create an SCP that denies the launch of all EC2 instances except t3.small EC2 instances in us-east-2. Attach the SCP to the project's account.
- C. Create and purchase a t3.small EC2 Reserved Instance for each developer in us-east-2. Assign each developer a specific EC2 instance with their name as the tag.
- 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 project's account.

Question #352

Topic 1

A scientific company needs to process text and image data from an Amazon S3 bucket. The data is collected from several radar stations 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?

- A. Setup an AWS DataSync agent to replicate the prefixed data from the source S3 bucket to the destination S3 bucket. Select to use all available bandwidth on the task, and monitor the task to ensure that it is in the TRANSFERRING status. Create an Amazon EventBridge rule to initiate an alert if this status changes.
- B. In the second account, create another S3 bucket to receive data from the radar station with the most accurate data. Set up a new replication rule for this new S3 bucket to separate the replication from the other radar stations. Monitor the maximum replication time to the destination. Create an Amazon EventBridge rule to initiate an alert when the time exceeds the desired threshold.
- C. Enable Amazon S3 Transfer Acceleration on the source S3 bucket, and configure the radar station with the most accurate data to use the new endpoint. Monitor the S3 destination bucket's TotalRequestLatency metric. Create an Amazon EventBridge rule to initiate an alert if this status changes.
- 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 rule to initiate an alert when the time exceeds the desired threshold.

Question #353

Topic 1

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 dependent 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 the solutions architect use to plan the cloud migration? (Choose three.)

- A. AWS Application Discovery Service
- B. AWS SMS
- C. AWS X-Ray
- D. AWS Cloud Adoption Readiness Tool (CART)
- E. Amazon Inspector
- F. AWS Migration Hub

Question #354

Topic 1

A solutions architect is reviewing an application's resilience before launch. The application runs on an Amazon EC2 instance that is deployed in a private subnet of a VPC. The EC2 instance is provisioned by an Auto Scaling group that has a minimum capacity of 1 and a maximum capacity of 1. The application stores data on an Amazon RDS for MySQL DB instance. The VPC has subnets configured in three Availability Zones and is configured with a single NAT gateway.

The solutions architect needs to recommend a solution to ensure that the application will operate across multiple Availability Zones.

Which solution will meet this requirement?

- A. Deploy an additional NAT gateway in the other Availability Zones. Update the route tables with appropriate routes. Modify the RDS for MySQL DB instance to a Multi-AZ configuration. Configure the Auto Scaling group to launch the instances across Availability Zones. Set the minimum capacity and maximum capacity of the Auto Scaling group to 3.
- B. Replace the NAT gateway with a virtual private gateway. Replace the RDS for MySQL DB instance with an Amazon Aurora MySQL DB cluster. Configure the Auto Scaling group to launch instances across all subnets in the VPC. Set the minimum capacity and maximum capacity of the Auto Scaling group to 3.
- C. Replace the NAT gateway with a NAT instance. Migrate the RDS for MySQL DB instance to an RDS for PostgreSQL DB instance. Launch a new EC2 instance in the other Availability Zones.
- D. Deploy an additional NAT gateway in the other Availability Zones. Update the route tables with appropriate routes. Modify the RDS for MySQL DB instance to turn on automatic backups and retain the backups for 7 days. Configure the Auto Scaling group to launch instances across all subnets in the VPC. Keep the minimum capacity and the maximum capacity of the Auto Scaling group at 1.

Question #355**Topic 1**

A company is planning to migrate its on-premises transaction-processing application to AWS. The application runs inside Docker containers that are hosted on VMs in the company's data center. The Docker containers have shared storage where the application records transaction data.

The transactions are time sensitive. The volume of transactions inside the application is unpredictable. The company must implement a low-latency storage solution that will automatically scale throughput to meet increased demand. The company cannot develop the application further and cannot continue to administer the Docker hosting environment.

How should the company migrate the application to AWS to meet these requirements?

- A. Migrate the containers that run the application to Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon S3 to store the transaction data that the containers share.
- B. Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic File System (Amazon EFS) file system. Create a Fargate task definition. Add a volume to the task definition to point to the EFS file system.
- C. Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic Block Store (Amazon EBS) volume. Create a Fargate task definition. Attach the EBS volume to each running task.
- D. Launch Amazon EC2 instances. Install Docker on the EC2 instances. Migrate the containers to the EC2 instances. Create an Amazon Elastic File System (Amazon EFS) file system. Add a mount point to the EC2 instances for the EFS file system.

Question #356**Topic 1**

A company is planning to migrate to the AWS Cloud. The company hosts many applications on Windows servers and Linux servers. Some of the servers are physical, and some of the servers are virtual. The company uses several types of databases in its on-premises environment. The company does not have an accurate inventory of its on-premises servers and applications.

The company wants to rightsize its resources during migration. A solutions architect needs to obtain information about the network connections and the application relationships. The solutions architect must assess the company's current environment and develop a migration plan.

Which solution will provide the solutions architect with the required information to develop the migration plan?

- A. Use Migration Evaluator to request an evaluation of the environment from AWS. Use the AWS Application Discovery Service Agentless Collector to import the details into a Migration Evaluator Quick Insights report.
- B. Use AWS Migration Hub and install the AWS Application Discovery Agent on the servers. Deploy the Migration Hub Strategy Recommendations application data collector. Generate a report by using Migration Hub Strategy Recommendations.
- C. Use AWS Migration Hub and run the AWS Application Discovery Service Agentless Collector on the servers. Group the servers and databases by using AWS Application Migration Service. Generate a report by using Migration Hub Strategy Recommendations.
- D. Use the AWS Migration Hub import tool to load the details of the company's on-premises environment. Generate a report by using Migration Hub Strategy Recommendations.

Question #357

Topic 1

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?

- A. Create a new AWS CloudTrail trail. Use an existing Amazon S3 bucket in the organization's management account to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 bucket.
- B. Create a new AWS CloudTrail trail in each member account of the organization. Create new Amazon S3 buckets to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 buckets.
- 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.
- D. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket to store the logs. Configure Amazon Simple Notification Service (Amazon SNS) to send log-file delivery notifications to an external management system that will track the logs. Enable MFA delete and encryption on the S3 bucket.

Question #358

Topic 1

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?

- A. Launch memory optimized EC2 instances in a partition placement group.
- B. Launch compute optimized EC2 instances in a partition placement group.
- C. Launch memory optimized EC2 instances in a cluster placement group.
- D. Launch compute optimized EC2 instances in a spread placement group.

Question #359

Topic 1

A company maintains information on premises in approximately 1 million.csv files that are hosted on a VM. The data initially is 10 TB in size and grows at a rate of 1 TB each week. The company needs to automate backups of the data to the AWS Cloud.

Backups of the data must occur daily. The company needs a solution that applies custom filters to back up only a subset of the data that is located in designated source directories. The company has set up an AWS Direct Connect connection.

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

- A. Use the Amazon S3 CopyObject API operation with multipart upload to copy the existing data to Amazon S3. Use the CopyObject API operation to replicate new data to Amazon S3 daily.
- B. Create a backup plan in AWS Backup to back up the data to Amazon S3. Schedule the backup plan to run daily.
- C. Install the AWS DataSync agent as a VM that runs on the on-premises hypervisor. Configure a DataSync task to replicate the data to Amazon S3 daily.
- D. Use an AWS Snowball Edge device for the initial backup. Use AWS DataSync for incremental backups to Amazon S3 daily.

Question #360

Topic 1

A financial services company has an asset management product that thousands of customers use around the world. The customers provide feedback about the product through surveys. The company is building a new analytical solution that runs on Amazon EMR to analyze the data from these surveys. The following user personas need to access the analytical solution to perform different actions:

- Administrator: Provisions the EMR cluster for the analytics team based on the team's requirements
- Data engineer: Runs ETL scripts to process, transform, and enrich the datasets
- Data analyst: Runs SQL and Hive queries on the data

A solutions architect must ensure that all the user personas have least privilege access to only the resources that they need. The user personas must be able to launch only applications that are approved and authorized. The solution also must ensure tagging for all resources that the user personas create.

Which solution will meet these requirements?

- A. Create IAM roles for each user persona. Attach identity-based policies to define which actions the user who assumes the role can perform. Create an AWS Config rule to check for noncompliant resources. Configure the rule to notify the administrator to remediate the noncompliant resources.
- B. Setup Kerberos-based authentication for EMR clusters upon launch. Specify a Kerberos security configuration along with cluster-specific Kerberos options.
- C. Use AWS Service Catalog to control the Amazon EMR versions available for deployment, the cluster configuration, and the permissions for each user persona.
- D. Launch the EMR cluster by using AWS CloudFormation. Attach resource-based policies to the EMR cluster during cluster creation. Create an AWS Config rule to check for noncompliant clusters and noncompliant Amazon S3 buckets. Configure the rule to notify the administrator to remediate the noncompliant resources.

Question #361

Topic 1

A software as a service (SaaS) company uses AWS to host a service that is powered by AWS PrivateLink. The service consists of proprietary software that runs on three Amazon EC2 instances behind a Network Load Balancer (NLB). The instances are in private subnets in multiple Availability Zones in the eu-west-2 Region. All the company's customers are in eu-west-2.

However, the company now acquires a new customer in the us-east-1 Region. The company creates a new VPC and new subnets in us-east-1. The company establishes inter-Region VPC peering between the VPCs in the two Regions.

The company wants to give the new customer access to the SaaS service, but the company does not want to immediately deploy new EC2 resources in us-east-1.

Which solution will meet these requirements?

- A. Configure a PrivateLink endpoint service in us-east-1 to use the existing NLB that is in eu-west-2. Grant specific AWS accounts access to connect to the SaaS service.
- B. Create an NLB in us-east-1. Create an IP target group that uses the IP addresses of the company's instances in eu-west-2 that host the SaaS service. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.
- C. Create an Application Load Balancer (ALB) in front of the EC2 instances in eu-west-2. Create an NLB in us-east-1. Associate the NLB that is in us-east-1 with an ALB target group that uses the ALB that is in eu-west-2. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.
- D. Use AWS Resource Access Manager (AWS RAM) to share the EC2 instances that are in eu-west-2. In us-east-1, create an NLB and an instance target group that includes the shared EC2 instances from eu-west-2. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.

Question #362

Topic 1

A company needs to monitor a growing number of Amazon S3 buckets across two AWS Regions. The company also needs to track the percentage of objects that are encrypted in Amazon S3. The company needs a dashboard to display this information for internal compliance teams.

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

- A. Create a new Storage Lens dashboard in each Region to track bucket and encryption metrics. Aggregate data from both Region dashboards into a single dashboard in Amazon QuickSight for the compliance teams.
- B. Deploy an AWS Lambda function in each Region to list the number of buckets and the encryption status of objects. Store this data in Amazon S3. Use Amazon Athena queries to display the data on a custom dashboard in Amazon QuickSight for the compliance teams.
- C. Use the S3 Storage Lens default dashboard to track bucket and encryption metrics. Give the compliance teams access to the dashboard directly in the S3 console.
- D. Create an Amazon EventBridge rule to detect AWS CloudTrail events for S3 object creation. Configure the rule to invoke an AWS Lambda function to record encryption metrics in Amazon DynamoDB. Use Amazon QuickSight to display the metrics in a dashboard for the compliance teams.

Question #363

Topic 1

A company's CISO has asked a solutions architect to re-engineer the company's current CI/CD practices to make sure patch deployments to its application can happen as quickly as 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 web 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?

- A. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for in-place deployment. Monitor the newly deployed code, and, if there are any issues, push another code update
- B. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for blue/green deployments. Monitor the newly deployed code, and, if there are any issues, trigger a manual rollback using CodeDeploy.
- C. Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stacks. Monitor the newly deployed code, and, if there are any issues, push another code update.
- D. Configure the CodePipeline with a deploy stage using AWS OpsWorks and in-place deployments. Monitor the newly deployed code, and, if there are any issues, push another code update.

Question #364

Topic 1

A company is managing many AWS accounts by using an organization in AWS Organizations. Different business units in the company run applications on Amazon EC2 instances. All the EC2 instances must have a BusinessUnit tag so that the company can track the cost for each business unit.

A recent audit revealed that some instances were missing this tag. The company manually added the missing tag to the instances.

What should a solutions architect do to enforce the tagging requirement in the future?

- A. Enable tag policies in the organization. Create a tag policy for the BusinessUnit tag. Ensure that compliance with tag key capitalization is turned off. Implement the tag policy for the ec2:instance resource type. Attach the tag policy to the root of the organization.
- B. Enable tag policies in the organization. Create a tag policy for the BusinessUnit tag. Ensure that compliance with tag key capitalization is turned on. Implement the tag policy for the ec2:instance resource type. Attach the tag policy to the organization's management account.
- C. Create an SCP and attach the SCP to the root of the organization. Include the following statement in the SCP:

```
{  
    "Sid": "DenyEC2Creation",  
    "Effect": "Deny",  
    "Action": [  
        "ec2:RunInstances"  
    ],  
    "Resource": [  
        "arn:aws:ec2:*:*:instance/*"  
    ],  
    "Condition": {  
        "Null": {  
            "aw:RequestTag/BusinessUnit": "true"  
        }  
    }  
}
```

- D. Create an SCP and attach the SCP to the organization's management account. Include the following statement in the SCP:

```
{  
    "Sid": "DenyEC2Creation",  
    "Effect": "Deny",  
    "Action": [  
        "e2:RunInstances"  
    ],  
    "Resource": [  
        "arn:aws:ec2:*:*:instance/*"  
    ],  
    "Condition": {  
        "Null": {  
            "aws:RequestTag/BusinessUnit": "false"  
        }  
    }  
}
```

Question #365

Topic 1

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?

- A. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Update all the VPC route tables, and add a route for ::/0 to the internet gateway.
- B. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Update the VPC route tables for all private subnets, and add a route for ::/0 to the NAT gateway.
- 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.
- D. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Create a new NAT gateway, and enable IPv6 support. Update the VPC route tables for all private subnets, and add a route for ::/0 to the IPv6-enabled NAT gateway.

Question #366

Topic 1

A company is using Amazon API Gateway to deploy a private REST API that will provide access to sensitive data. The API must be accessible only from an application that is deployed in a VPC. The company deploys the API successfully. However, the API is not accessible from an Amazon EC2 instance that is deployed in the VPC.

Which solution will provide connectivity between the EC2 instance and the API?

- A. Create an interface VPC endpoint for API Gateway. Attach an endpoint policy that allows apigateway:* actions. Disable private DNS naming for the VPC endpoint. Configure an API resource policy that allows access from the VPC. Use the VPC endpoint's DNS name to access the API.
- B. Create an interface VPC endpoint for API Gateway. Attach an endpoint policy that allows the execute-api:Invoke action. Enable private DNS naming for the VPC endpoint. Configure an API resource policy that allows access from the VPC endpoint. Use the API endpoint's DNS names to access the API.
- C. Create a Network Load Balancer (NLB) and a VPC link. Configure private integration between API Gateway and the NLB. Use the API endpoint's DNS names to access the API.
- D. Create an Application Load Balancer (ALB) and a VPC Link. Configure private integration between API Gateway and the ALB. Use the ALB endpoint's DNS name to access the API.

Question #367

Topic 1

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?

- A. Create the OrganizationAccountAccess IAM group in each member account. Include the necessary IAM roles for each administrator.
- B. Create the OrganizationAccountAccessPolicy IAM policy in each member account. Connect the member accounts to the management account by using cross-account access.
- C. Create the OrganizationAccountAccessRole IAM role in each member account. Grant permission to the management account to assume the IAM role.
- D. Create the OrganizationAccountAccessRole IAM role in the management account. Attach the AdministratorAccess AWS managed policy to the IAM role. Assign the IAM role to the administrators in each member account.

Question #368

Topic 1

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?

- A. Create an EC2 Auto Scaling group behind an Application Load Balancer. Create additional read replicas for the DB instance. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.
- B. Create an EC2 Auto Scaling group behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.
- C. Deploy the application on a Kubernetes cluster created on the EC2 instances behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. 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.
- 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.

Question #369

Topic 1

A company hosts a VPN in an on-premises data center. Employees currently connect to the VPN to access files in their Windows home directories. Recently, there has been a large growth in the number of employees who work remotely. As a result, bandwidth usage for connections into the data center has begun to reach 100% during business hours.

The company must design a solution on AWS that will support the growth of the company's remote workforce, reduce the bandwidth usage for connections into the data center, and reduce operational overhead.

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

- A. Create an AWS Storage Gateway Volume Gateway. Mount a volume from the Volume Gateway to the on-premises file server.
- B. Migrate the home directories to Amazon FSx for Windows File Server.
- C. Migrate the home directories to Amazon FSx for Lustre.
- D. Migrate remote users to AWS Client VPN.
- E. Create an AWS Direct Connect connection from the on-premises data center to AWS.

Question #370

Topic 1

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 controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.
- B. Use the AWS CLI to list all the unencrypted volumes in all the AWS accounts. Run a script to encrypt all the unencrypted volumes in place.
- 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.
- D. Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the mandatory controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.
- E. Turn on AWS CloudTrail. Configure an Amazon EventBridge rule to detect and automatically encrypt unencrypted volumes.

Question #371

Topic 1

A company hosts an intranet web application on Amazon EC2 instances behind an Application Load Balancer (ALB). Currently, users authenticate to the application against an internal user database.

The company needs to authenticate users to the application by using an existing AWS Directory Service for Microsoft Active Directory directory. All users with accounts in the directory must have access to the application.

Which solution will meet these requirements?

- A. Create a new app client in the directory. Create a listener rule for the ALB. Specify the authenticate-oidc action for the listener rule. Configure the listener rule with the appropriate issuer, client ID and secret, and endpoint details for the Active Directory service. Configure the new app client with the callback URL that the ALB provides.
- B. Configure an Amazon Cognito user pool. Configure the user pool with a federated identity provider (IdP) that has metadata from the directory. Create an app client. Associate the app client with the user pool. Create a listener rule for the ALB. Specify the authenticate-cognito action for the listener rule. Configure the listener rule to use the user pool and app client.
- C. Add the directory as a new IAM identity provider (IdP). Create a new IAM role that has an entity type of SAML 2.0 federation. Configure a role policy that allows access to the ALB. Configure the new role as the default authenticated user role for the IdP. Create a listener rule for the ALB. Specify the authenticate-oidc action for the listener rule.
- D. Enable AWS IAM Identity Center (AWS Single Sign-On). Configure the directory as an external identity provider (IdP) that uses SAML. Use the automatic provisioning method. Create a new IAM role that has an entity type of SAML 2.0 federation. Configure a role policy that allows access to the ALB. Attach the new role to all groups. Create a listener rule for the ALB. Specify the authenticate-cognito action for the listener rule.

Question #372

Topic 1

A company has a website that serves many visitors. The company deploys a backend service for the website in a primary AWS Region and a disaster recovery (DR) Region.

A single Amazon CloudFront distribution is deployed for the website. The company creates an Amazon Route 53 record set with health checks and a failover routing policy for the primary Region's backend service. The company configures the Route 53 record set as an origin for the CloudFront distribution. The company configures another record set that points to the backend service's endpoint in the DR Region as a secondary failover record type. The TTL for both record sets is 60 seconds.

Currently, failover takes more than 1 minute. A solutions architect must design a solution that will provide the fastest failover time.

Which solution will achieve this goal?

- A. Deploy an additional CloudFront distribution. Create a new Route 53 failover record set with health checks for both CloudFront distributions.
- B. Set the TTL to 4 second for the existing Route 53 record sets that are used for the backend service in each Region.
- C. Create new record sets for the backend services by using a latency routing policy. Use the record sets as an origin in the CloudFront distribution.
- D. Create a CloudFront origin group that includes two origins, one for each backend service Region. Configure origin failover as a cache behavior for the CloudFront distribution.

Question #373

Topic 1

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? (Choose three.)

- A. Use a Deny list strategy.
- B. Review the Access Advisor in AWS IAM to determine services recently used
- C. Review the AWS Trusted Advisor report to determine services recently used.
- D. Remove the default FullAWSAccess SCP.
- E. Define organizational units (OUs) and place the member accounts in the OUs.
- F. Remove the default DenyAWSAccess SCP.

Question #374

Topic 1

A live-events company is designing a scaling solution for its ticket application on AWS. The application has high peaks of utilization during sale events. Each sale event is a one-time event that is scheduled. The application runs on Amazon EC2 instances that are in an Auto Scaling group. The application uses PostgreSQL for the database layer.

The company needs a scaling solution to maximize availability during the sale events.

Which solution will meet these requirements?

- A. Use a predictive scaling policy for the EC2 instances. Host the database on an Amazon Aurora PostgreSQL Serverless v2 Multi-AZ DB instance with automatically scaling read replicas. Create an AWS Step Functions state machine to run parallel AWS Lambda functions to pre-warm the database before a sale event. Create an Amazon EventBridge rule to invoke the state machine.
- B. Use a scheduled scaling policy for the EC2 instances. Host the database on an Amazon RDS for PostgreSQL Multi-AZ DB instance with automatically scaling read replicas. Create an Amazon EventBridge rule that invokes an AWS Lambda function to create a larger read replica before a sale event. Fail over to the larger read replica. Create another EventBridge rule that invokes another Lambda function to scale down the read replica after the sale event.
- C. Use a predictive scaling policy for the EC2 instances. Host the database on an Amazon RDS for PostgreSQL MultiAZ DB instance with automatically scaling read replicas. Create an AWS Step Functions state machine to run parallel AWS Lambda functions to pre-warm the database before a sale event. Create an Amazon EventBridge rule to invoke the state machine.
- D. Use a scheduled scaling policy for the EC2 instances. Host the database on an Amazon Aurora PostgreSQL Multi-AZ DB cluster. Create an Amazon EventBridge rule that invokes an AWS Lambda function to create a larger Aurora Replica before a sale event. Fail over to the larger Aurora Replica. Create another EventBridge rule that invokes another Lambda function to scale down the Aurora Replica after the sale event.

Question #375

Topic 1

A company runs an intranet application on premises. The company wants to configure a cloud backup of the application. The company has selected AWS Elastic Disaster Recovery for this solution.

The company requires that replication traffic does not travel through the public internet. The application also must not be accessible from the internet. The company does not want this solution to consume all available network bandwidth because other applications require bandwidth.

Which combination of steps will meet these requirements? (Choose three.)

- A. Create a VPC that has at least two private subnets, two NAT gateways, and a virtual private gateway.
- B. Create a VPC that has at least two public subnets, a virtual private gateway, and an internet gateway.
- C. Create an AWS Site-to-Site VPN connection between the on-premises network and the target AWS network.
- D. Create an AWS Direct Connect connection and a Direct Connect gateway between the on-premises network and the target AWS network.
- E. During configuration of the replication servers, select the option to use private IP addresses for data replication.
- F. During configuration of the launch settings for the target servers, select the option to ensure that the Recovery instance's private IP address matches the source server's private IP address.

Question #376

Topic 1

A company that provides image storage services wants to deploy a customer-facing solution to AWS. Millions of individual customers will use the solution. The solution will receive batches of large image files, resize the files, and store the files in an Amazon S3 bucket for up to 6 months.

The solution must handle significant variance in demand. The solution must also be reliable at enterprise scale and have the ability to rerun processing jobs in the event of failure.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Step Functions to process the S3 event that occurs when a user stores an image. Run an AWS Lambda function that resizes the image in place and replaces the original file in the S3 bucket. Create an S3 Lifecycle expiration policy to expire all stored images after 6 months.
- B. Use Amazon EventBridge to process the S3 event that occurs when a user uploads an image. Run an AWS Lambda function that resizes the image in place and replaces the original file in the S3 bucket. Create an S3 Lifecycle expiration policy to expire all stored images after 6 months.
- C. Use S3 Event Notifications to invoke an AWS Lambda function when a user stores an image. Use the Lambda function to resize the image in place and to store the original file in the S3 bucket. Create an S3 Lifecycle policy to move all stored images to S3 Standard-Infrequent Access (S3 Standard-IA) after 6 months.
- D. Use Amazon Simple Queue Service (Amazon SQS) to process the S3 event that occurs when a user stores an image. Run an AWS Lambda function that resizes the image and stores the resized file in an S3 bucket that uses S3 Standard-Infrequent Access (S3 Standard-IA). Create an S3 Lifecycle policy to move all stored images to S3 Glacier Deep Archive after 6 months.

Question #377

Topic 1

A company has an organization in AWS Organizations that includes a separate AWS account for each of the company's departments. Application teams from different departments develop and deploy solutions independently.

The company wants to reduce compute costs and manage costs appropriately across departments. The company also wants to improve visibility into billing for individual departments. The company does not want to lose operational flexibility when the company selects compute resources.

Which solution will meet these requirements?

- A. Use AWS Budgets for each department. Use Tag Editor to apply tags to appropriate resources. Purchase EC2 Instance Savings Plans.
- B. Configure AWS Organizations to use consolidated billing. Implement a tagging strategy that identifies departments. Use SCPs to apply tags to appropriate resources. Purchase EC2 Instance Savings Plans.
- C. Configure AWS Organizations to use consolidated billing. Implement a tagging strategy that identifies departments. Use Tag Editor to apply tags to appropriate resources. Purchase Compute Savings Plans.
- D. Use AWS Budgets for each department. Use SCPs to apply tags to appropriate resources. Purchase Compute Savings Plans.

Question #378

Topic 1

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 ensuring only authenticated users are allowed to post content?

- A. Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 PutObject operation. Secure the API Gateway using a COGNITO_USER_POOLS authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.
- B. Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 PutObject operation. Secure the API Gateway using an AWS Lambda authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.
- 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 API.
- D. Configure an Amazon CloudFront distribution for the destination S3 bucket. Enable PUT and POST methods for the CloudFront cache behavior. Update the CloudFront origin to use an origin access identity (OAI). Give the OAI user 3: PutObject permissions in the bucket policy. Have the browser interface upload objects using the CloudFront distribution.

Question #379

Topic 1

A large company is migrating its entire IT portfolio to AWS. Each business unit in the company has a standalone AWS account 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 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 meets the company's needs with the LEAST effort? (Choose two.)

- A. Use a collection of parameterized AWS CloudFormation templates defining common IAM permissions that are launched into each account. Require all new and existing accounts to launch the appropriate stacks to enforce the least privilege model.
- 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.
- C. Require each business unit to use its own AWS accounts. Tag each AWS account appropriately and enable Cost Explorer to administer chargebacks.
- D. Enable all features of AWS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts.
- E. Consolidate all of the company's AWS accounts into a single AWS account. Use tags for billing purposes and the IAM's Access Advisor feature to enforce the least privilege model.

Question #380

Topic 1

A company has a solution that analyzes weather data from thousands of weather stations. The weather stations send the data over an Amazon API Gateway REST API that has an AWS Lambda function integration. The Lambda function calls a third-party service for data pre-processing. The third-party service gets overloaded and fails the pre-processing, causing a loss of data.

A solutions architect must improve the resiliency of the solution. The solutions architect must ensure that no data is lost and that data can be processed later if failures occur.

What should the solutions architect do to meet these requirements?

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue as the dead-letter queue for the API.
- B. Create two Amazon Simple Queue Service (Amazon SQS) queues: a primary queue and a secondary queue. Configure the secondary queue as the dead-letter queue for the primary queue. Update the API to use a new integration to the primary queue. Configure the Lambda function as the invocation target for the primary queue.
- C. Create two Amazon EventBridge event buses: a primary event bus and a secondary event bus. Update the API to use a new integration to the primary event bus. Configure an EventBridge rule to react to all events on the primary event bus. Specify the Lambda function as the target of the rule. Configure the secondary event bus as the failure destination for the Lambda function.
- D. Create a custom Amazon EventBridge event bus. Configure the event bus as the failure destination for the Lambda function.

Question #381

Topic 1

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? (Choose 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 EC2 instances and implement tracing of SQL queries with the X-Ray SDK for Java.
- C. Configure the Aurora MySQL DB cluster to stream slow query and error logs to Amazon Kinesis.
- D. Install and configure an Amazon CloudWatch Logs agent on the EC2 instances to send the Apache logs to CloudWatch Logs.
- E. Enable and configure AWS CloudTrail to collect and analyze application activity from Amazon EC2 and Aurora
- F. Enable Aurora MySQL DB cluster performance benchmarking and publish the stream to AWS X-Ray.

Question #382

Topic 1

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?

- A. Migrate the backend services to AWS Lambda. Increase the read and write capacity of DynamoDB.
- B. Migrate the backend services to AWS Lambda. Configure DynamoDB to use global tables.
- C. Use Auto Scaling groups for the backend services. Use DynamoDB auto scaling.
- D. Use Auto Scaling groups for the backend services. Use Amazon Simple Queue Service (Amazon SQS) and an AWS Lambda function to write to DynamoDB.

Question #383

Topic 1

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.
- B. Configure the Amazon CloudWatch agent on all servers within the local environment and publish metrics to Amazon CloudWatch Logs.
- C. Use AWS Application Discovery Service and enable agentless discovery in the existing virtualization environment.
- D. Enable AWS Application Discovery Service in the AWS Management Console and configure the corporate firewall to allow scans over a VPN.

Question #384

Topic 1

A company provides a software as a service (SaaS) application that runs in the AWS Cloud. The application runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The instances are in an Auto Scaling group and are distributed across three Availability Zones in a single AWS Region.

The company is deploying the application into additional Regions. The company must provide static IP addresses for the application to customers so that the customers can add the IP addresses to allow lists. The solution must automatically route customers to the Region that is geographically closest to them.

Which solution will meet these requirements?

- A. Create an Amazon CloudFront distribution. Create a CloudFront origin group. Add the NLB for each additional Region to the origin group. Provide customers with the IP address ranges of the distribution's edge locations.
- B. Create an AWS Global Accelerator standard accelerator. Create a standard accelerator endpoint for the NLB in each additional Region. Provide customers with the Global Accelerator IP address.
- C. Create an Amazon CloudFront distribution. Create a custom origin for the NLB in each additional Region. Provide customers with the IP address ranges of the distribution's edge locations.
- D. Create an AWS Global Accelerator custom routing accelerator. Create a listener for the custom routing accelerator. Add the IP address and ports for the NLB in each additional Region. Provide customers with the Global Accelerator IP address.

Question #385

Topic 1

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 in 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?

- A. Create separate OUs in AWS Organizations for each development unit. Assign the created OUs to the company AWS accounts. Create separate SCP with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag that matches the development unit name. Assign the SCP to the corresponding OU.
- B. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Update the IAM policy for the developers' assumed IAM role with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit.
- C. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Create an SCP with an allow action and a StringEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit. Assign the SCP to the root OU.
- D. Create separate IAM policies for each development unit. For every IAM policy, add an allow action and a StringEquals condition for the DevelopmentUnit resource tag and the development unit name. During SAML federation, use AWS Security Token Service (AWS STS) to assign the IAM policy and match the development unit name to the assumed IAM role.

Question #386

Topic 1

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.)

- A. Develop infrastructure services using AWS CloudFormation templates. Add the templates to a central Amazon S3 bucket and add the IAM roles or users that require access to the S3 bucket policy.
- B. Develop infrastructure services using AWS CloudFormation templates. Upload each template as an AWS Service Catalog product to portfolios created in a central AWS account. Share these portfolios with the Organizations structure created for the company.
- C. Allow user IAM roles to have AWSCloudFormationFullAccess and AmazonS3ReadOnlyAccess permissions. Add an Organizations SCP at the AWS account root user level to deny all services except AWS CloudFormation and Amazon S3.
- 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.
- F. Use the AWS CloudFormation Resource Tags property to enforce the application of tags to any CloudFormation templates that will be created for users.

Question #387

Topic 1

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?

- A. Create an AWS Lambda function that consolidates each day's AWS WAF logs into one log file.
- B. Reduce the amount of data scanned by configuring AWS WAF to send logs to a different S3 bucket each day.
- C. Update the Kinesis Data Firehose configuration to partition the data in Amazon S3 by date and time. Create external tables for Amazon Redshift. Configure Amazon Redshift Spectrum to query the data source.
- 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.

Question #388

Topic 1

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?

- A. Create an IPSet containing a list of IP ranges that belong to the specified country. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from an IP range in the IPSet. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- B. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from the specified country. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- C. Configure AWS Shield to block any requests that do not originate from the specified country. Associate AWS Shield with the ALB.
- D. Create a security group rule that allows ports 80 and 443 from IP ranges that belong to the specified country. Associate the security group with the ALB.

Question #389

Topic 1

A company is migrating an application from on-premises infrastructure to the AWS Cloud. During migration design meetings, the company expressed concerns about the availability and recovery options for its legacy Windows file server. The file server contains sensitive business-critical data that cannot be recreated in the event of data corruption or data loss. According to compliance requirements, the data must not travel across the public internet. The company wants to move to AWS managed services where possible.

The company decides to store the data in an Amazon FSx for Windows File Server file system. A solutions architect must design a solution that copies the data to another AWS Region for disaster recovery (DR) purposes.

Which solution will meet these requirements?

- A. Create a destination Amazon S3 bucket in the DR Region. Establish connectivity between the FSx for Windows File Server file system in the primary Region and the S3 bucket in the DR Region by using Amazon FSx File Gateway. Configure the S3 bucket as a continuous backup source in FSx File Gateway.
- B. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using AWS Site-to-Site VPN. Configure AWS DataSync to communicate by using VPN endpoints.
- C. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using VPC peering. Configure AWS DataSync to communicate by using interface VPC endpoints with AWS PrivateLink.
- D. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using AWS Transit Gateway in each Region. Use AWS Transfer Family to copy files between the FSx for Windows File Server file system in the primary Region and the FSx for Windows File Server file system in the DR Region over the private AWS backbone network.

Question #390

Topic 1

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?

- A. Deploy an Amazon Aurora DB cluster and take snapshots of the cluster every 5 minutes. Once a snapshot is complete, copy the snapshot to a secondary Region to serve as a backup in the event of a failure.
- 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.
- C. Deploy an Amazon Aurora DB cluster in the primary Region and another in a secondary Region. Use AWS DMS to keep the secondary Region in sync.
- D. Deploy an Amazon RDS instance with a read replica in the same Region. In the event of a failure, promote the read replica to become the primary.

Question #391

Topic 1

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 Support1 from the management 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 finance1@example.com. Set up the IAM users as required.
- B. From the management account, switch roles to assume the OrganizationAccountAccessRole role with the account ID of the new member account. Set up the IAM users as required.
- C. Go to the AWS Management Console sign-in page. Choose "Sign in using root account credentials." Sign in by using the email address finance1@example.com and the management account's root password. Set up the IAM users as required.
- D. Go to the AWS Management Console sign-in page. Sign in by using the account ID of the new member account and the Support1 IAM credentials. Set up the IAM users as required.

Question #392

Topic 1

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 functions, 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.
- B. Implement an Amazon ElastiCache for Redis cache to store the results of the database calls. Modify the Lambda functions to use the cache.
- C. Modify the Aurora Serverless DB cluster configuration to increase the maximum amount of available memory.
- D. Enable throttling in the API Gateway production stage. Set the rate and burst values to limit the incoming calls.

Question #393

Topic 1

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?

- A. Perform a database backup. Copy the backup files to an AWS Snowball Edge Storage Optimized device. Import the backup 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.
- B. Use AWS Database Migration Service (AWS DMS) to migrate the data to AWS. Create a DMS replication instance in a private subnet. Create VPC endpoints for AWS DMS. Configure a DMS task to copy data from the on-premises database to the DB instance by using full load plus change data capture (CDC). Use the AWS Key Management Service (AWS KMS) default key for encryption at rest. Use TLS for encryption in transit.
- C. Perform a database backup. Use AWS DataSync to transfer 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.
- 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.

Question #394

Topic 1

Accompany 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?

- A. Provision an AWS Storage Gateway file gateway NFS file share that is attached to an Amazon S3 bucket. Mount the NFS file share on each EC2 instance in the cluster.
- B. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses General Purpose performance mode. Mount the EFS file system on each EC2 instance in the cluster.
- C. Provision a new Amazon Elastic Block Store (Amazon EBS) volume that uses the io2 volume type. Attach the EBS volume to all of the EC2 instances in the cluster.
- 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.

Question #395

Topic 1

A company hosts a software as a service (SaaS) solution on AWS. The solution has an Amazon API Gateway API that serves an HTTPS endpoint. The API uses AWS Lambda functions for compute. The Lambda functions store data in an Amazon Aurora Serverless v1 database.

The company used the AWS Serverless Application Model (AWS SAM) to deploy the solution. The solution extends across multiple Availability Zones and has no disaster recovery (DR) plan.

A solutions architect must design a DR strategy that can recover the solution in another AWS Region. The solution has an RTO of 5 minutes and an RPO of 1 minute.

What should the solutions architect do to meet these requirements?

- A. Create a read replica of the Aurora Serverless v1 database in the target Region. Use AWS SAM to create a runbook to deploy the solution to the target Region. Promote the read replica to primary in case of disaster.
- B. Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Use AWS SAM to create a runbook to deploy the solution to the target Region.
- C. Create an Aurora Serverless v1 DB cluster that has multiple writer instances in the target Region. Launch the solution in the target Region. Configure the two Regional solutions to work in an active-passive configuration.
- D. Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Launch the solution in the target Region. Configure the two Regional solutions to work in an active-passive configuration.

Question #396

Topic 1

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.
- B. Set up Amazon ElastiCache for Redis. Update the application to use ElastiCache. Create an Auto Scaling group for the EC2 instances. Create an Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distribution. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates.
- C. Set up Amazon ElastiCache for Memcached. Update the application to use ElastiCache. 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 application before the content updates.
- D. 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 Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distribution. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates.

Question #397

Topic 1

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.

Which combination of actions should a solutions architect take to ensure image processing can scale to handle the load? (Choose three.)

- A. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon MQ queue.
- 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.
- D. Invoke an S3 Batch Operations job 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.
- F. Send a push notification to the mobile app by using Amazon Simple Email Service (Amazon SES) when processing is complete.

Question #398

Topic 1

A company is building an application on AWS. The application sends logs to an Amazon OpenSearch Service 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 OpenSearch Service 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.
- B. Create a transit gateway, and connect it to the VPC. Create an AWS Site-to-Site VPN. Create an attachment to the transit gateway. Instruct the developers to connect by using an OpenVPN client.
- C. Create a transit gateway, and connect it to the VPC. Create an AWS Direct Connect connection. Set up a public VIF on the Direct Connect connection. Associate the public VIF with the transit gateway. Instruct the developers to connect to the Direct Connect connection.
- D. Create and configure a bastion host in a public subnet of the VPC. Configure the bastion host security group to allow SSH access from the company CIDR ranges. Instruct the developers to connect by using SSH.

Question #399

Topic 1

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.)

- A. Create tasks using the bridge network mode.
- B. Create tasks using the awsvpc network mode.
- C. Apply security groups to Amazon EC2 instances, and use IAM roles for EC2 instances to access other resources.
- D. Apply security groups to the tasks, and pass IAM credentials into the container at launch time to access other resources.
- E. Apply security groups to the tasks, and use IAM roles for tasks to access other resources.

Question #400

Topic 1

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? (Choose two.)

- A. Create three public subnets in the Neptune VPC, and route traffic through an internet gateway. Host the Lambda functions in the three new public subnets.
- 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.
- C. Host the Lambda functions outside the VPC. Update the Neptune security group to allow access from the IP ranges of the Lambda functions.
- 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.
- E. Create three private subnets in the Neptune VPC. Host the Lambda functions in the three new isolated subnets. Create a VPC endpoint for DynamoDB, and route DynamoDB traffic to the VPC endpoint.

Question #401

Topic 1

A company wants to design a disaster recovery (DR) solution for an application that runs in the company's data center. The application writes to an SMB file share and creates a copy on a second file share. Both file shares are in the data center. The application uses two types of files: metadata files and image files.

The company wants to store the copy on AWS. The company needs the ability to use SMB to access the data from either the data center or AWS if a disaster occurs. The copy of the data is rarely accessed but must be available within 5 minutes.

- A. Deploy AWS Outposts with Amazon S3 storage. Configure a Windows Amazon EC2 instance on Outposts as a file server.
- B. Deploy an Amazon FSx File Gateway. Configure an Amazon FSx for Windows File Server Multi-AZ file system that uses SSD storage.
- C. Deploy an Amazon S3 File Gateway. Configure the S3 File Gateway to use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the metadata files and to use S3 Glacier Deep Archive for the image files.
- D. Deploy an Amazon S3 File Gateway. Configure the S3 File Gateway to use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the metadata files and image files.

Question #402

Topic 1

A company is creating a solution that can move 400 employees into a remote working environment in the event of an unexpected disaster. The user desktops have a mix of Windows and Linux operating systems. Multiple types of software, such as web browsers and mail clients, are installed on each desktop.

A solutions architect needs to implement a solution that can be integrated with the company's on-premises Active Directory to allow employees to use their existing identity credentials. The solution must provide multifactor authentication (MFA) and must replicate the user experience from the existing desktops.

Which solution will meet these requirements?

- A. Use Amazon WorkSpaces for the cloud desktop service. Set up a VPN connection to the on-premises network. Create an AD Connector, and connect to the on-premises Active Directory. Activate MFA for Amazon WorkSpaces by using the AWS Management Console.
- B. Use Amazon AppStream 2.0 as an application streaming service. Configure Desktop View for the employees. Set up a VPN connection to the on-premises network. Set up Active Directory Federation Services (AD FS) on premises. Connect the VPC network to AD FS through the VPN connection.
- C. Use Amazon WorkSpaces for the cloud desktop service. Set up a VPN connection to the on-premises network. Create an AD Connector, and connect to the on-premises Active Directory. Configure a RADIUS server for MFA.
- D. Use Amazon AppStream 2.0 as an application streaming service. Set up Active Directory Federation Services on premises. Configure MFA to grant users access on AppStream 2.0.

Question #403

Topic 1

A company has deployed an Amazon Connect contact center. Contact center agents are reporting large numbers of computer-generated calls. The company is concerned about the cost and productivity effects of these calls. The company wants a solution that will allow agents to flag the call as spam and automatically block the numbers from going to an agent in the future.

What is the MOST operationally efficient solution to meet these requirements?

- A. Customize the Contact Control Panel (CCP) by adding a flag call button that will invoke an AWS Lambda function that calls the UpdateContactAttributes API. Use an Amazon DynamoDB table to store the spam numbers. Modify the contact flows to look for the updated attribute and to use a Lambda function to read and write to the DynamoDB table.
- B. Use a Contact Lens for Amazon Connect rule that will look for spam calls. Use an Amazon DynamoDB table to store the spam numbers. Modify the contact flows to look for the rule and to invoke an AWS Lambda function to read and write to the DynamoDB table.
- C. Use an Amazon DynamoDB table to store the spam numbers. Create a quick connect that the agents can transfer the spam call to from the Contact Control Panel (CCP). Modify the quick connect contact flow to invoke an AWS Lambda function to write to the DynamoDB table.
- D. Modify the initial contact flow to ask for caller input. If the agent does not receive input, the agent should mark the caller as spam. Use an Amazon DynamoDB table to store the spam numbers. Use an AWS Lambda function to read and write to the DynamoDB table.

Question #404

Topic 1

A company has mounted sensors to collect information about environmental parameters such as humidity and light throughout all the company's factories. The company needs to stream and analyze the data in the AWS Cloud in real time. If any of the parameters fall out of acceptable ranges, the factory operations team must receive a notification immediately.

Which solution will meet these requirements?

- A. Stream the data to an Amazon Kinesis Data Firehose delivery stream. Use AWS Step Functions to consume and analyze the data in the Kinesis Data Firehose delivery stream. Use Amazon Simple Notification Service (Amazon SNS) to notify the operations team.
- B. Stream the data to an Amazon Managed Streaming for Apache Kafka (Amazon MSK) cluster. Set up a trigger in Amazon MSK to invoke an AWS Fargate task to analyze the data. Use Amazon Simple Email Service (Amazon SES) to notify the operations team.
- C. Stream the data to an Amazon Kinesis data stream. Create an AWS Lambda function to consume the Kinesis data stream and to analyze the data. Use Amazon Simple Notification Service (Amazon SNS) to notify the operations team.
- D. Stream the data to an Amazon Kinesis Data Analytics application. Use an automatically scaled and containerized service in Amazon Elastic Container Service (Amazon ECS) to consume and analyze the data. Use Amazon Simple Email Service (Amazon SES) to notify the operations team.

Question #405

Topic 1

A company is preparing to deploy an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for a workload. The company expects the cluster to support an unpredictable number of stateless pods. Many of the pods will be created during a short time period as the workload automatically scales the number of replicas that the workload uses.

Which solution will MAXIMIZE node resilience?

- A. Use a separate launch template to deploy the EKS control plane into a second cluster that is separate from the workload node groups.
- B. Update the workload node groups. Use a smaller number of node groups and larger instances in the node groups.
- C. Configure the Kubernetes Cluster Autoscaler to ensure that the compute capacity of the workload node groups stays underprovisioned.
- D. Configure the workload to use topology spread constraints that are based on Availability Zone.

Question #406

Topic 1

A company needs to implement a disaster recovery (DR) plan for a web application. The application runs in a single AWS Region.

The application uses microservices that run in containers. The containers are hosted on AWS Fargate in Amazon Elastic Container Service (Amazon ECS). The application has an Amazon RDS for MySQL DB instance as its data layer and uses Amazon Route 53 for DNS resolution. An Amazon CloudWatch alarm invokes an Amazon EventBridge rule if the application experiences a failure.

A solutions architect must design a DR solution to provide application recovery to a separate Region. The solution must minimize the time that is necessary to recover from a failure.

Which solution will meet these requirements?

- A. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Create an AWS Lambda function to perform the following actions: take a snapshot of the RDS DB instance, copy the snapshot to the separate Region, create a new RDS DB instance from the snapshot, and update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.
- B. Create an AWS Lambda function that creates a second ECS cluster and ECS service in the separate Region. Configure the Lambda function to perform the following actions: take a snapshot of the RDS DB instance, copy the snapshot to the separate Region, create a new RDS DB instance from the snapshot, and update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.
- C. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Create a cross-Region read replica of the RDS DB instance in the separate Region. Create an AWS Lambda function to promote the read replica to the primary database. Configure the Lambda function to update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.
- D. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Take a snapshot of the RDS DB instance. Convert the snapshot to an Amazon DynamoDB global table. Create an AWS Lambda function to update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.

Question #407

Topic 1

A company has AWS accounts that are in an organization in AWS Organizations. The company wants to track Amazon EC2 usage as a metric. The company's architecture team must receive a daily alert if the EC2 usage is more than 10% higher than the average EC2 usage from the last 30 days.

Which solution will meet these requirements?

- A. Configure AWS Budgets in the organization's management account. Specify a usage type of EC2 running hours. Specify a daily period. Set the budget amount to be 10% more than the reported average usage for the last 30 days from AWS Cost Explorer. Configure an alert to notify the architecture team if the usage threshold is met.
- B. Configure AWS Cost Anomaly Detection in the organization's management account. Configure a monitor type of AWS Service. Apply a filter of Amazon EC2. Configure an alert subscription to notify the architecture team if the usage is 10% more than the average usage for the last 30 days.
- C. Enable AWS Trusted Advisor in the organization's management account. Configure a cost optimization advisory alert to notify the architecture team if the EC2 usage is 10% more than the reported average usage for the last 30 days.
- D. Configure Amazon Detective in the organization's management account. Configure an EC2 usage anomaly alert to notify the architecture team if Detective identifies a usage anomaly of more than 10%.

Question #408

Topic 1

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?

- A. Receive the orders in an Amazon EC2-hosted database and use EC2 instances to process them.
- B. Receive the orders in an Amazon SQS queue and invoke an AWS Lambda function to process them.
- C. Receive the orders using the AWS Step Functions program and launch an Amazon ECS container to process them.
- D. Receive the orders in Amazon Kinesis Data Streams and use Amazon EC2 instances to process them.

Question #409

Topic 1

A company is deploying AWS Lambda functions that access an Amazon RDS for PostgreSQL database. The company needs to launch the Lambda functions in a QA environment and in a production environment.

The company must not expose credentials within application code and must rotate passwords automatically.

Which solution will meet these requirements?

- A. Store the database credentials for both environments in AWS Systems Manager Parameter Store. Encrypt the credentials by using an AWS Key Management Service (AWS KMS) key. Within the application code of the Lambda functions, pull the credentials from the Parameter Store parameter by using the AWS SDK for Python (Boto3). Add a role to the Lambda functions to provide access to the Parameter Store parameter.
- B. Store the database credentials for both environments in AWS Secrets Manager with distinct key entry for the QA environment and the production environment. Turn on rotation. Provide a reference to the Secrets Manager key as an environment variable for the Lambda functions.
- C. Store the database credentials for both environments in AWS Key Management Service (AWS KMS). Turn on rotation. Provide a reference to the credentials that are stored in AWS KMS as an environment variable for the Lambda functions.
- D. Create separate S3 buckets for the QA environment and the production environment. Turn on server-side encryption with AWS KMS keys (SSE-KMS) for the S3 buckets. Use an object naming pattern that gives each Lambda function's application code the ability to pull the correct credentials for the function's corresponding environment. Grant each Lambda function's execution role access to Amazon S3.

Question #410

Topic 1

A company is using AWS Control Tower to manage AWS accounts in an organization in AWS Organizations. The company has an OU that contains accounts. The company must prevent any new or existing Amazon EC2 instances in the OU's accounts from gaining a public IP address.

Which solution will meet these requirements?

- A. Configure all instances in each account in the OU to use AWS Systems Manager. Use a Systems Manager Automation runbook to prevent public IP addresses from being attached to the instances.
- B. Implement the AWS Control Tower proactive control to check whether instances in the OU's accounts have a public IP address. Set the AssociatePublicIpAddress property to False. Attach the proactive control to the OU.
- C. Create an SCP that prevents the launch of instances that have a public IP address. Additionally, configure the SCP to prevent the attachment of a public IP address to existing instances. Attach the SCP to the OU.
- D. Create an AWS Config custom rule that detects instances that have a public IP address. Configure a remediation action that uses an AWS Lambda function to detach the public IP addresses from the instances.

Question #411

Topic 1

A company is deploying a third-party web application on AWS. The application is packaged as a Docker image. The company has deployed the Docker image as an AWS Fargate service in Amazon Elastic Container Service (Amazon ECS). An Application Load Balancer (ALB) directs traffic to the application.

The company needs to give only a specific list of users the ability to access the application from the internet. The company cannot change the application and cannot integrate the application with an identity provider. All users must be authenticated through multi-factor authentication (MFA).

Which solution will meet these requirements?

- A. Create a user pool in Amazon Cognito. Configure the pool for the application. Populate the pool with the required users. Configure the pool to require MFA. Configure a listener rule on the ALB to require authentication through the Amazon Cognito hosted UI.
- B. Configure the users in AWS Identity and Access Management (IAM). Attach a resource policy to the Fargate service to require users to use MFA. Configure a listener rule on the ALB to require authentication through IAM.
- C. Configure the users in AWS Identity and Access Management (IAM). Enable AWS IAM Identity Center (AWS Single Sign-On). Configure resource protection for the ALB. Create a resource protection rule to require users to use MFA.
- D. Create a user pool in AWS Amplify. Configure the pool for the application. Populate the pool with the required users. Configure the pool to require MFA. Configure a listener rule on the ALB to require authentication through the Amplify hosted UI.

Question #412

Topic 1

A solutions architect is preparing to deploy a new security tool into several previously unused AWS Regions. The solutions architect will deploy the tool by using an AWS CloudFormation stack set. The stack set's template contains an IAM role that has a custom name. Upon creation of the stack set, no stack instances are created successfully.

What should the solutions architect do to deploy the stacks successfully?

- A. Enable the new Regions in all relevant accounts. Specify the CAPABILITY_NAMED_IAM capability during the creation of the stack set.
- B. Use the Service Quotas console to request a quota increase for the number of CloudFormation stacks in each new Region in all relevant accounts. Specify the CAPABILITY_IAM capability during the creation of the stack set.
- C. Specify the CAPABILITY_NAMED_IAM capability and the SELF_MANAGED permissions model during the creation of the stack set.
- D. Specify an administration role ARN and the CAPABILITY_IAM capability during the creation of the stack set.

Question #413

Topic 1

A company has an application that uses an Amazon Aurora PostgreSQL DB cluster for the application's database. The DB cluster contains one small primary instance and three larger replica instances. The application runs on an AWS Lambda function. The application makes many short-lived connections to the database's replica instances to perform read-only operations.

During periods of high traffic, the application becomes unreliable and the database reports that too many connections are being established. The frequency of high-traffic periods is unpredictable.

Which solution will improve the reliability of the application?

- A. Use Amazon RDS Proxy to create a proxy for the DB cluster. Configure a read-only endpoint for the proxy. Update the Lambda function to connect to the proxy endpoint.
- B. Increase the max_connections setting on the DB cluster's parameter group. Reboot all the instances in the DB cluster. Update the Lambda function to connect to the DB cluster endpoint.
- C. Configure instance scaling for the DB cluster to occur when the DatabaseConnections metric is close to the max connections setting. Update the Lambda function to connect to the Aurora reader endpoint.
- D. Use Amazon RDS Proxy to create a proxy for the DB cluster. Configure a read-only endpoint for the Aurora Data API on the proxy. Update the Lambda function to connect to the proxy endpoint.

Question #414

Topic 1

A retail company is mounting IoT sensors in all of its stores worldwide. During the manufacturing of each sensor, the company's private certificate authority (CA) issues an X.509 certificate that contains a unique serial number. The company then deploys each certificate to its respective sensor.

A solutions architect needs to give the sensors the ability to send data to AWS after they are installed. Sensors must not be able to send data to AWS until they are installed.

Which solution will meet these requirements?

- A. Create an AWS Lambda function that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Add the Lambda function as a pre-provisioning hook. During manufacturing, call the RegisterThing API operation and specify the template and parameters.
- B. Create an AWS Step Functions state machine that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Specify the Step Functions state machine to validate parameters. Call the StartThingRegistrationTask API operation during installation.
- C. Create an AWS Lambda function that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Add the Lambda function as a pre-provisioning hook. Register the CA with AWS IoT Core, specify the provisioning template, and set the allow-auto-registration parameter.
- D. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Include parameter validation in the template. Provision a claim certificate and a private key for each device that uses the CA. Grant AWS IoT Core service permissions to update AWS IoT things during provisioning.

Question #415

Topic 1

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 DevOps 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?

- A. Use GitHub websockets to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.
- B. Use GitHub webhooks to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.
- C. Use GitHub websockets to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.
- D. Use GitHub webhooks to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.

Question #416

Topic 1

A software as a service (SaaS) company has developed a multi-tenant environment. The company uses Amazon DynamoDB tables that the tenants share for the storage layer. The company uses AWS Lambda functions for the application services.

The company wants to offer a tiered subscription model that is based on resource consumption by each tenant. Each tenant is identified by a unique tenant ID that is sent as part of each request to the Lambda functions. The company has created an AWS Cost and Usage Report (AWS CUR) in an AWS account. The company wants to allocate the DynamoDB costs to each tenant to match that tenant's resource consumption.

Which solution will provide a granular view of the DynamoDB cost for each tenant with the LEAST operational effort?

- A. Associate a new tag that is named tenant ID with each table in DynamoDB. Activate the tag as a cost allocation tag in the AWS Billing and Cost Management console. Deploy new Lambda function code to log the tenant ID in Amazon CloudWatch Logs. Use the AWS CUR to separate DynamoDB consumption cost for each tenant ID.
- B. Configure the Lambda functions to log the tenant ID and the number of RCUs and WCUs consumed from DynamoDB for each transaction to Amazon CloudWatch Logs. Deploy another Lambda function to calculate the tenant costs by using the logged capacity units and the overall DynamoDB cost from the AWS Cost Explorer API. Create an Amazon EventBridge rule to invoke the calculation Lambda function on a schedule.
- C. Create a new partition key that associates DynamoDB items with individual tenants. Deploy a Lambda function to populate the new column as part of each transaction. Deploy another Lambda function to calculate the tenant costs by using Amazon Athena to calculate the number of tenant items from DynamoDB and the overall DynamoDB cost from the AWS CUR. Create an Amazon EventBridge rule to invoke the calculation Lambda function on a schedule.
- D. Deploy a Lambda function to log the tenant ID, the size of each response, and the duration of the transaction call as custom metrics to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the custom metrics for each tenant. Use AWS Pricing Calculator to obtain the overall DynamoDB costs and to calculate the tenant costs.

Question #417

Topic 1

A company has an application that stores data in a single Amazon S3 bucket. The company must keep all data for 1 year. The company's security team is concerned that an attacker could gain access to the AWS account through leaked long-term credentials.

Which solution will ensure that existing and future objects in the S3 bucket are protected?

- A. Create a new AWS account that is accessible only to the security team through an assumed role. Create an S3 bucket in the new account. Enable S3 Versioning and S3 Object Lock. Configure a default retention period of 1 year. Set up replication from the existing S3 bucket to the new S3 bucket. Create an S3 Batch Replication job to copy all existing data.
- B. Use the s3-bucket-versioning-enabled AWS Config managed rule. Configure an automatic remediation action that uses an AWS Lambda function to enable S3 Versioning and MFA Delete on noncompliant resources. Add an S3 Lifecycle rule to delete objects after 1 year.
- C. Explicitly deny bucket creation from all users and roles except for an AWS Service Catalog launch constraint role. Define a Service Catalog product for the creation of the S3 bucket to force S3 Versioning and MFA Delete to be enabled. Authorize users to launch the product when they need to create an S3 bucket.
- D. Enable Amazon GuardDuty with the S3 protection feature for the account and the AWS Region. Add an S3 Lifecycle rule to delete objects after 1 year.

Question #418

Topic 1

A company needs to improve the security of its web-based application on AWS. The application uses Amazon CloudFront with two custom origins. The first custom origin routes requests to an Amazon API Gateway HTTP API. The second custom origin routes traffic to an Application Load Balancer (ALB). The application integrates with an OpenID Connect (OIDC) identity provider (IdP) for user management.

A security audit shows that a JSON Web Token (JWT) authorizer provides access to the API. The security audit also shows that the ALB accepts requests from unauthenticated users.

A solutions architect must design a solution to ensure that all backend services respond to only authenticated users.

Which solution will meet this requirement?

- A. Configure the ALB to enforce authentication and authorization by integrating the ALB with the IdP. Allow only authenticated users to access the backend services.
- B. Modify the CloudFront configuration to use signed URLs. Implement a permissive signing policy that allows any request to access the backend services.
- C. Create an AWS WAF web ACL that filters out unauthenticated requests at the ALB level. Allow only authenticated traffic to reach the backend services.
- D. Enable AWS CloudTrail to log all requests that come to the ALB. Create an AWS Lambda function to analyze the logs and block any requests that come from unauthenticated users.

Question #419

Topic 1

A company creates an AWS Control Tower landing zone to manage and govern a multi-account AWS environment. The company's security team will deploy preventive controls and detective controls to monitor AWS services across all the accounts. The security team needs a centralized view of the security state of all the accounts.

Which solution will meet these requirements?

- A. From the AWS Control Tower management account, use AWS CloudFormation StackSets to deploy an AWS Config conformance pack to all accounts in the organization.
- B. Enable Amazon Detective for the organization in AWS Organizations. Designate one AWS account as the delegated administrator for Detective.
- C. From the AWS Control Tower management account, deploy an AWS CloudFormation stack set that uses the automatic deployment option to enable Amazon Detective for the organization.
- D. Enable AWS Security Hub for the organization in AWS Organizations. Designate one AWS account as the delegated administrator for Security Hub.

Question #420

Topic 1

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 ap-northeast-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.
- B. Configure Amazon Kinesis Data Firehose to transfer the images using S3 Transfer Acceleration.
- C. Use an AWS Snowball device to transfer the images with the S3 bucket as the target.
- D. Transfer the images over a Site-to-Site VPN connection using the S3 API with multipart upload.

Question #421

Topic 1

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?

- A. Increase the concurrency limit of the Lambda function.
- B. Implement DynamoDB auto scaling on the table.
- C. Increase the API Gateway throttle limit.
- D. Re-create the DynamoDB table with a better-partitioned primary index.

Question #422

Topic 1

A company has an application that has a web frontend. The application runs in the company's on-premises data center and requires access to file storage for critical data. The application runs on three Linux VMs for redundancy. The architecture includes a load balancer with HTTP request-based routing.

The company needs to migrate the application to AWS as quickly as possible. The architecture on AWS must be highly available.

Which solution will meet these requirements with the FEWEST changes to the architecture?

- A. Migrate the application to Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type in three Availability Zones. Use Amazon S3 to provide file storage for all three containers. Use a Network Load Balancer to direct traffic to the containers.
- B. Migrate the application to Amazon EC2 instances in three Availability Zones. Use Amazon Elastic File System (Amazon EFS) for file storage. Mount the file storage on all three EC2 instances. Use an Application Load Balancer to direct traffic to the EC2 instances.
- C. Migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) containers that use the Fargate launch type in three Availability Zones. Use Amazon FSx for Lustre to provide file storage for all three containers. Use a Network Load Balancer to direct traffic to the containers.
- D. Migrate the application to Amazon EC2 instances in three AWS Regions. Use Amazon Elastic Block Store (Amazon EBS) for file storage. Enable Cross-Region Replication (CRR) for all three EC2 instances. Use an Application Load Balancer to direct traffic to the EC2 instances.

Question #423

Topic 1

A company is planning to migrate an on-premises data center to AWS. The company currently hosts the data center on Linux-based VMware VMs. A solutions architect must collect information about network dependencies between the VMs. The information must be in the form of a diagram that details host IP addresses, hostnames, and network connection information.

Which solution will meet these requirements?

- A. Use AWS Application Discovery Service. Select an AWS Migration Hub home AWS Region. Install the AWS Application Discovery Agent on the on-premises servers for data collection. Grant permissions to Application Discovery Service to use the Migration Hub network diagrams.
- B. Use the AWS Application Discovery Service Agentless Collector for server data collection. Export the network diagrams from the AWS Migration Hub in .png format.
- C. Install the AWS Application Migration Service agent on the on-premises servers for data collection. Use AWS Migration Hub data in Workload Discovery on AWS to generate network diagrams.
- D. Install the AWS Application Migration Service agent on the on-premises servers for data collection. Export data from AWS Migration Hub in .csv format into an Amazon CloudWatch dashboard to generate network diagrams.

Question #424

Topic 1

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 periods because of many database connections. The company needs to improve the scalable performance and availability of the database.

Which solution meets these requirements?

- A. Create an Amazon CloudWatch alarm action that triggers a Lambda function to add an Amazon RDS for MySQL read replica when resource utilization hits a threshold.
- B. Migrate the database to Amazon Aurora, and add a read replica. Add a database connection pool outside of the Lambda handler function.
- C. Migrate the database to Amazon Aurora, and add a read replica. Use Amazon Route 53 weighted records.
- D. Migrate the database to Amazon Aurora, and add an Aurora Replica. Configure Amazon RDS Proxy to manage database connection pools.

Question #425

Topic 1

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 file system through SMB.

A solutions architect must implement a solution that uses an Amazon S3 bucket for 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?

- A. Create a new Amazon FSx for Windows File Server file system. Configure AWS DataSync with one location for the on-premises file share and one location for the new Amazon FSx file system. Create a new DataSync task to copy the data from the on-premises file share location to the Amazon FSx file system.
- B. Create an S3 bucket for the application. Copy the data from the on-premises storage to the S3 bucket.
- C. Deploy an AWS Server Migration Service (AWS SMS) VM to the on-premises environment. Use AWS SMS to migrate the file storage server from on premises to an Amazon EC2 instance.
- 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.

Question #426

Topic 1

A global company has a mobile app that displays ticket barcodes. Customers use the tickets on the mobile app to attend live events. Event scanners read the ticket barcodes and call a backend API to validate the barcode data against data in a database. After the barcode is scanned, the backend logic writes to the database's single table to mark the barcode as used.

The company needs to deploy the app on AWS with a DNS name of api.example.com. The company will host the database in three AWS Regions around the world.

Which solution will meet these requirements with the LOWEST latency?

- A. Host the database on Amazon Aurora global database clusters. Host the backend on three Amazon Elastic Container Service (Amazon ECS) clusters that are in the same Regions as the database. Create an accelerator in AWS Global Accelerator to route requests to the nearest ECS cluster. Create an Amazon Route 53 record that maps api.example.com to the accelerator endpoint
- B. Host the database on Amazon Aurora global database clusters. Host the backend on three Amazon Elastic Kubernetes Service (Amazon EKS) clusters that are in the same Regions as the database. Create an Amazon CloudFront distribution with the three clusters as origins. Route requests to the nearest EKS cluster. Create an Amazon Route 53 record that maps api.example.com to the CloudFront distribution.
- C. Host the database on Amazon DynamoDB global tables. Create an Amazon CloudFront distribution. Associate the CloudFront distribution with a CloudFront function that contains the backend logic to validate the barcodes. Create an Amazon Route 53 record that maps api.example.com to the CloudFront distribution.
- D. Host the database on Amazon DynamoDB global tables. Create an Amazon CloudFront distribution. Associate the CloudFront distribution with a Lambda@Edge function that contains the backend logic to validate the barcodes. Create an Amazon Route 53 record that maps api.example.com to the CloudFront distribution.

Question #427

Topic 1

A medical company is running a REST API on a set of Amazon EC2 instances. The EC2 instances run in 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 ALB 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 ALB.
- B. Create an AWS WAF web ACL rule with an IP match condition of the CloudFront service IP address ranges. Associate the web ACL with the ALB. Move the ALB into the three private subnets.
- C. Store a random string in AWS Systems Manager Parameter Store. Configure Parameter Store automatic rotation for the string. Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Inspect the value of the custom HTTP header, and block access in the ALB.
- D. Configure AWS Shield Advanced. Create a security group policy to allow connections from CloudFront service IP address ranges. Add the policy to AWS Shield Advanced, and attach the policy to the ALB.

Question #428

Topic 1

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 traverse the public internet.

How should the solutions architect design a highly available solution that meets the requirements and is cost-effective?

- A. Establish AWS Direct Connect connections from the company headquarters to all AWS Regions in use. Use the company WAN to send traffic over to the headquarters and then to the respective DX connection to access the data.
- B. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use inter-region VPC peering to access the data in other AWS Regions.
- C. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use an AWS transit VPC solution to access data in other AWS Regions.
- D. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use Direct Connect Gateway to access data in other AWS Regions.

Question #429

Topic 1

A company has developed an application that is running Windows Server on VMware vSphere VMs that the company hosts on 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 part of its disaster recovery plan, the company wants the ability to host its application on AWS temporarily if the 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 is 5 minutes.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Configure AWS DataSync. Replicate the data to Amazon Elastic Block Store (Amazon EBS) volumes. When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and attach the EBS volumes.
- B. Configure AWS Elastic 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 Elastic Disaster Recovery to launch EC2 instances that use the replicated volumes.
- C. Provision an AWS Storage Gateway file gateway. Replicate the data to an Amazon S3 bucket. When the on-premises environment is unavailable, use AWS Backup to restore the data to Amazon Elastic Block Store (Amazon EBS) volumes and launch Amazon EC2 instances from these EBS volumes.
- D. Provision an Amazon FSx for Windows File Server file system on AWS. Replicate the data to the file system. When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and use AWS::CloudFormation::Init commands to mount the Amazon FSx file shares.

Question #430

Topic 1

A company runs a highly available data collection application on Amazon EC2 in the eu-north-1 Region. The application collects data from end-user devices and writes records to an Amazon Kinesis data stream and a set of AWS Lambda functions that process the records. The company persists the output of the record processing to an Amazon S3 bucket in eu-north-1. The company uses the data in the S3 bucket as a data source for Amazon Athena.

The company wants to increase its global presence. A solutions architect must launch the data collection capabilities in the sa-east-1 and ap-northeast-1 Regions. The solutions architect deploys the application, the Kinesis data stream, and the Lambda functions in the two new Regions. The solutions architect keeps the S3 bucket in eu-north-1 to meet a requirement to centralize the data analysis.

During testing of the new setup, the solutions architect notices a significant lag on the arrival of data from the new Regions to the S3 bucket.

Which solution will improve this lag time the MOST?

- A. In each of the two new Regions, set up the Lambda functions to run in a VPC. Set up an S3 gateway endpoint in that VPC.
- B. Turn on S3 Transfer Acceleration on the S3 bucket in eu-north-1. Change the application to use the new S3 accelerated endpoint when the application uploads data to the S3 bucket.
- C. Create an S3 bucket in each of the two new Regions. Set the application in each new Region to upload to its respective S3 bucket. Set up S3 Cross-Region Replication to replicate data to the S3 bucket in eu-north-1.
- D. Increase the memory requirements of the Lambda functions to ensure that they have multiple cores available. Use the multipart upload feature when the application uploads data to Amazon S3 from Lambda.

Question #431

Topic 1

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?

- A. Create an AWS Transit Gateway. Attach the shared VPC and the authorized business unit VPCs to the transit gateway. Create a single transit gateway route table and associate it with all of the attached VPCs. Allow automatic propagation of routes from the attachments into the route table. Configure VPC routing tables to send traffic to the transit gateway.
- 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.
- C. Create a VPC peering connection from each business unit VPC to the shared VPC. Accept the VPC peering connections from the shared VPC console. Configure VPC routing tables to send traffic to the VPC peering connection.
- D. Configure a virtual private gateway for the shared VPC and create customer gateways for each of the authorized business unit VPCs. Establish a Site-to-Site VPN connection from the business unit VPCs to the shared VPC. Configure VPC routing tables to send traffic to the VPN connection.

Question #432

Topic 1

A company wants to migrate its website to AWS. The website uses microservices and runs on containers that are deployed in an on-premises, self-managed Kubernetes cluster. All the manifests that define the deployments for the containers in the Kubernetes deployment are in source control.

All data for the website is stored in a PostgreSQL database. An open source container image repository runs alongside the on-premises environment.

A solutions architect needs to determine the architecture that the company will use for the website on AWS.

Which solution will meet these requirements with the LEAST effort to migrate?

- A. Create an AWS App Runner service. Connect the App Runner service to the open source container image repository. Deploy the manifests from on premises to the App Runner service. Create an Amazon RDS for PostgreSQL database.
- B. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that has managed node groups. Copy the application containers to a new Amazon Elastic Container Registry (Amazon ECR) repository. Deploy the manifests from on premises to the EKS cluster. Create an Amazon Aurora PostgreSQL DB cluster.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster that has an Amazon EC2 capacity pool. Copy the application containers to a new Amazon Elastic Container Registry (Amazon ECR) repository. Register each container image as a new task definition. Configure ECS services for each task definition to match the original Kubernetes deployments. Create an Amazon Aurora PostgreSQL DB cluster.
- D. Rebuild the on-premises Kubernetes cluster by hosting the cluster on Amazon EC2 instances. Migrate the open source container image repository to the EC2 instances. Deploy the manifests from on premises to the new cluster on AWS. Deploy an open source PostgreSQL database on the new cluster.

Question #433

Topic 1

A company uses a mobile app on AWS to run online contests. The company selects a winner at random at the end of each contest. The contests run for variable lengths of time. The company does not need to retain any data from a contest after the contest is finished.

The company uses custom code that is hosted on Amazon EC2 instances to process the contest data and select a winner. The EC2 instances run behind an Application Load Balancer and store contest entries on Amazon RDS DB instances. The company must design a new architecture to reduce the cost of running the contests.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate storage of the contest entries to Amazon DynamoDB. Create a DynamoDB Accelerator (DAX) cluster. Rewrite the code to run as Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type. At the end of the contest, delete the DynamoDB table.
- B. Migrate the storage of the contest entries to Amazon Redshift. Rewrite the code as AWS Lambda functions. At the end of the contest, delete the Redshift cluster.
- C. Add an Amazon ElastiCache for Redis cluster in front of the RDS DB instances to cache the contest entries. Rewrite the code to run as Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type. Set the ElastiCache TTL attribute on each entry to expire each entry at the end of the contest.
- D. Migrate the storage of the contest entries to Amazon DynamoDB. Rewrite the code as AWS Lambda functions. Set the DynamoDB TTL attribute on each entry to expire each entry at the end of the contest.

Question #434**Topic 1**

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.
- B. Add a rule to the security group that is assigned to the proxy EC2 instances to allow all traffic between instances that have this security group. Assign this security group to all EC2 instances in the VPC.
- C. Change the VPCs DHCP options set. Set the DNS server options to point to the addresses of the proxy EC2 instances.
- D. Assign one additional elastic network interface to each proxy EC2 instance. Ensure that one of these network interfaces has a route to the private subnets. Ensure that the other network interface has a route to the internet.

Question #435**Topic 1**

A company is running its solution on AWS in a manually created VPC. The company is using AWS CloudFormation 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?

- A. Create a new AWS Cloud Development Kit (AWS CDK) stack that strictly provisions the existing VPC resources and configuration. Use AWS CDK to import the VPC into the stack and to manage the VPC.
- B. Create a CloudFormation stack set that creates the VPC. Use the stack set to import the VPC into the stack.
- C. Create a new CloudFormation template that strictly provisions the existing VPC resources and configuration. From the CloudFormation console, create a new stack by importing the Existing resources.
- D. Create a new CloudFormation template that creates the VPC. Use the AWS Serverless Application Model (AWS SAM) CLI to import the VPC.

Question #436

Topic 1

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.

- A. Store the game files on Amazon EBS volumes mounted on Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.
- B. Store the game files on Amazon EFS volumes that are attached to Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on each of the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.
- 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.
- D. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Set Requester Pays for the S3 bucket. Publish the game download URL for users to download the package.

Question #437

Topic 1

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 in 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? (Choose three.)

- A. Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer.
- B. Provision an additional VPC peering connection.
- C. Migrate the MySQL database to Amazon Aurora with one Aurora Replica.
- D. Provision two NAT gateways in the database VPC.
- E. Move the Tomcat server to the database VPC.
- F. Create an additional public subnet in a different Availability Zone in the website VPC.

Question #438

Topic 1

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.
- B. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Target.FailedHealthChecks is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a publicly accessible web server.
- C. Modify the existing Amazon Route 53 records by adding health checks. Configure a fallback target if the health check fails. Modify DNS records to point to a publicly accessible webpage.
- D. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Elb.InternalError is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a public accessible web server.
- E. Add a custom error response by configuring a CloudFront custom error page. Modify DNS records to point to a publicly accessible web page.

Question #439

Topic 1

A company wants to migrate an Amazon Aurora MySQL DB cluster from an existing AWS account to a new AWS account in the same AWS Region. Both accounts are members of the same organization in AWS Organizations.

The company must minimize database service interruption before the company performs DNS cutover to the new database.

Which migration strategy will meet this requirement? (Choose two.)

- A. Take a snapshot of the existing Aurora database. Share the snapshot with the new AWS account. Create an Aurora DB cluster in the new account from the snapshot.
- B. Create an Aurora DB cluster in the new AWS account. Use AWS Database Migration Service (AWS DMS) to migrate data between the two Aurora DB clusters.
- C. Use AWS Backup to share an Aurora database backup from the existing AWS account to the new AWS account. Create an Aurora DB cluster in the new AWS account from the snapshot.
- D. Create an Aurora DB cluster in the new AWS account. Use AWS Application Migration Service to migrate data between the two Aurora DB clusters.

Question #440

Topic 1

A software as a service (SaaS) company provides a media software solution to customers. The solution is hosted on 50 VPCs across various AWS Regions and AWS accounts. One of the VPCs is designated as a management VPC. The compute resources in the VPCs work independently.

The company has developed a new feature that requires all 50 VPCs to be able to communicate with each other. The new feature also requires one-way access from each customer's VPC to the company's management VPC. The management VPC hosts a compute resource that validates licenses for the media software solution.

The number of VPCs that the company will use to host the solution will continue to increase as the solution grows.

Which combination of steps will provide the required VPC connectivity with the LEAST operational overhead? (Choose two.)

- A. Create a transit gateway. Attach all the company's VPCs and relevant subnets to the transit gateway.
- B. Create VPC peering connections between all the company's VPCs.
- C. Create a Network Load Balancer (NLB) that points to the compute resource for license validation. Create an AWS PrivateLink endpoint service that is available to each customer's VPAssociate the endpoint service with the NLB.
- D. Create a VPN appliance in each customer's VPC. Connect the company's management VPC to each customer's VPC by using AWS Site-to-Site VPN.
- E. Create a VPC peering connection between the company's management VPC and each customer's VPC.

Question #441

Topic 1

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.)

- A. Use AWS Organizations to create an organization in the parent account for each LOB. Then invite each LOB account to the appropriate organization.
- B. Use AWS Organizations to create a single organization in the parent account. Then, invite each LOB's AWS account to join the organization.
- C. Implement service quotas to define the services and features that are permitted and apply the quotas to each LOB. as appropriate.
- D. Create an SCP that allows only approved services and features, then apply the policy to the LOB accounts.
- E. Enable consolidated billing in the parent account's billing console and link the LOB accounts.

Question #442

Topic 1

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? (Choose two.)

- A. The weight for the Region where the web servers were stopped is higher than the weight for the other Region.
- B. One of the web servers in the secondary Region did not pass its HTTP health check.
- C. Latency resource record sets cannot be used in combination with weighted resource record sets.
- D. The setting to evaluate target health is not turned on for the latency alias resource record set that is associated with the domain in the Region where the web servers were stopped.
- 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.

Question #443

Topic 1

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 1 MB 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 remaining servers 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?

- A. Send the sensor data to Amazon Kinesis Data Firehose. Use an AWS Lambda function to read the Kinesis Data Firehose data, convert it to .csv format, and insert it into an Amazon Aurora MySQL DB instance. Instruct the data analysts to query the data directly from the DB instance.
- 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.
- C. Send the sensor data to an Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) application to convert the data to .csv format and store it in an Amazon S3 bucket. Import the data into an Amazon Aurora MySQL DB instance. Instruct the data analysts to query the data directly from the DB instance.
- D. Send the sensor data to an Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) application to convert the data to Apache Parquet format and store it in an Amazon S3 bucket. Instruct the data analysts to query the data by using Amazon Athena.

Question #444

Topic 1

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 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? (Choose two.)

- A. Configure read replicas for Amazon RDS MySQL and use the single reader endpoint in the web application to reduce the load on the backend database tier.
- 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 CloudWatch alarms to notify administrators when the site fails.
- C. Configure the target group health check to use a TCP check of the Amazon EC2 web server and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- D. Configure an Amazon CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the database tier.
- E. Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySQL instances to reduce the load on the backend database tier.

Question #445

Topic 1

A company has an on-premises data center and is using Kubernetes to develop a new solution on AWS. The company uses Amazon Elastic Kubernetes Service (Amazon EKS) clusters for its development and test environments.

The EKS control plane and data plane for production workloads must reside on premises. The company needs an AWS managed solution for Kubernetes management.

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

- A. Install an AWS Outposts server in the on-premises data center. Deploy Amazon EKS by using a local cluster configuration on the Outposts server for the production workloads.
- B. Install Amazon EKS Anywhere on the company's hardware in the on-premises data center. Deploy the production workloads on an EKS Anywhere cluster.
- C. Install an AWS Outposts server in the on-premises data center. Deploy Amazon EKS by using an extended cluster configuration on the Outposts server for the production workloads.
- D. Install an AWS Outposts server in the on-premises data center. Install Amazon EKS Anywhere on the Outposts server. Deploy the production workloads on an EKS Anywhere cluster.

Question #446

Topic 1

A company uses AWS Organizations to manage its development environment. Each development team at the company has its own AWS account. Each account has a single VPC and CIDR blocks that do not overlap.

The company has an Amazon Aurora DB cluster in a shared services account. All the development teams need to work with live data from the DB cluster.

Which solution will provide the required connectivity to the DB cluster with the LEAST operational overhead?

- A. Create an AWS Resource Access Manager (AWS RAM) resource share for the DB cluster. Share the DB cluster with all the development accounts.
- B. Create a transit gateway in the shared services account. Create an AWS Resource Access Manager (AWS RAM) resource share for the transit gateway. Share the transit gateway with all the development accounts. Instruct the developers to accept the resource share. Configure networking.
- C. Create an Application Load Balancer (ALB) that points to the IP address of the DB cluster. Create an AWS PrivateLink endpoint service that uses the ALB. Add permissions to allow each development account to connect to the endpoint service.
- D. Create an AWS Site-to-Site VPN connection in the shared services account. Configure networking. Use AWS Marketplace VPN software in each development account to connect to the Site-to-Site VPN connection.

Question #447

Topic 1

A company used AWS CloudFormation to create all new infrastructure in its AWS member accounts. The resources rarely change and are properly sized for the expected load. The monthly AWS bill is consistent.

Occasionally, a developer creates a new resource for testing and forgets to remove the resource when the test is complete. Most of these tests last a few days before the resources are no longer needed.

The company wants to automate the process of finding unused resources. A solutions architect needs to design a solution that determines whether the cost in the AWS bill is increasing. The solution must help identify resources that cause an increase in cost and must automatically notify the company's operations team.

Which solution will meet these requirements?

- A. Turn on billing alerts. Use AWS Cost Explorer to determine the costs for the past month. Create an Amazon CloudWatch alarm for total estimated charges. Specify a cost threshold that is higher than the costs that Cost Explorer determined. Add a notification to alert the operations team if the alarm threshold is breached.
- B. Turn on billing alerts. Use AWS Cost Explorer to determine the average monthly costs for the past 3 months. Create an Amazon CloudWatch alarm for total estimated charges. Specify a cost threshold that is higher than the costs that Cost Explorer determined. Add a notification to alert the operations team if the alarm threshold is breached.
- C. Use AWS Cost Anomaly Detection to create a cost monitor that has a monitor type of Linked account. Create a subscription to send daily AWS cost summaries to the operations team. Specify a threshold for cost variance.
- D. Use AWS Cost Anomaly Detection to create a cost monitor that has a monitor type of AWS services. Create a subscription to send daily AWS cost summaries to the operations team. Specify a threshold for cost variance.

Question #448

Topic 1

A company is deploying a new web-based application and needs a storage solution for the Linux application servers. The company wants to create a single location for updates to application data for all instances. The active dataset will be up to 100 GB in size. A solutions architect has determined that peak operations will occur for 3 hours daily and will require a total of 225 MiBps of read throughput.

The solutions architect must design a Multi-AZ solution that makes a copy of the data available in another AWS Region for disaster recovery (DR). The DR copy has an RPO of less than 1 hour.

Which solution will meet these requirements?

- A. Deploy a new Amazon Elastic File System (Amazon EFS) Multi-AZ file system. Configure the file system for 75 MiBps of provisioned throughput. Implement replication to a file system in the DR Region.
- B. Deploy a new Amazon FSx for Lustre file system. Configure Bursting Throughput mode for the file system. Use AWS Backup to back up the file system to the DR Region.
- C. Deploy a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume with 225 MiBps of throughput. Enable Multi-Attach for the EBS volume. Use AWS Elastic Disaster Recovery to replicate the EBS volume to the DR Region.
- D. Deploy an Amazon FSx for OpenZFS file system in both the production Region and the DR Region. Create an AWS DataSync scheduled task to replicate the data from the production file system to the DR file system every 10 minutes.

Question #449

Topic 1

A company needs to gather data from an experiment in a remote location that does not have internet connectivity. During the experiment, sensors that are connected to a local network will generate 6 TB of data in a proprietary format over the course of 1 week. The sensors can be configured to upload their data files to an FTP server periodically, but the sensors do not have their own FTP server. The sensors also do not support other protocols. The company needs to collect the data centrally and move the data to object storage in the AWS Cloud as soon as possible after the experiment.

Which solution will meet these requirements?

- A. Order an AWS Snowball Edge Compute Optimized device. Connect the device to the local network. Configure AWS DataSync with a target bucket name, and unload the data over NFS to the device. After the experiment, return the device to AWS so that the data can be loaded into Amazon S3.
- B. Order an AWS Snowcone device, including an Amazon Linux 2 AMI. Connect the device to the local network. Launch an Amazon EC2 instance on the device. Create a shell script that periodically downloads data from each sensor. After the experiment, return the device to AWS so that the data can be loaded as an Amazon Elastic Block Store (Amazon EBS) volume.
- C. Order an AWS Snowcone device, including an Amazon Linux 2 AMI. Connect the device to the local network. Launch an Amazon EC2 instance on the device. Install and configure an FTP server on the EC2 instance. Configure the sensors to upload data to the EC2 instance. After the experiment, return the device to AWS so that the data can be loaded into Amazon S3.
- D. Order an AWS Snowcone device. Connect the device to the local network. Configure the device to use Amazon FSx. Configure the sensors to upload data to the device. Configure AWS DataSync on the device to synchronize the uploaded data with an Amazon S3 bucket. Return the device to AWS so that the data can be loaded as an Amazon Elastic Block Store (Amazon EBS) volume.

Question #450

Topic 1

A company that has multiple business units is using AWS Organizations with all features enabled. The company has implemented an account structure in which each business unit has its own AWS account. Administrators in each AWS account need to view detailed cost and utilization data for their account by using Amazon Athena.

Each business unit can have access to only its own cost and utilization data. The IAM policies that govern the ability to set up AWS Cost and Usage Reports are in place. A central Cost and Usage Report that contains all data for the organization is already available in an Amazon S3 bucket.

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

- A. In the organization's management account, use AWS Resource Access Manager (AWS RAM) to share the Cost and Usage Report data with each member account.
- B. In the organization's management account, configure an S3 event to invoke an AWS Lambda function each time a new file arrives in the S3 bucket that contains the central Cost and Usage Report. Configure the Lambda function to extract each member account's data and to place the data in Amazon S3 under a separate prefix. Modify the S3 bucket policy to allow each member account to access its own prefix.
- C. In each member account, access AWS Cost Explorer. Create a new report that contains relevant cost information for the account. Save the report in Cost Explorer. Provide instructions that the account administrators can use to access the saved report.
- D. In each member account, create a new S3 bucket to store Cost and Usage Report data. Set up a Cost and Usage Report to deliver the data to the new S3 bucket.

Question #451

Topic 1

A company is designing an AWS environment for a manufacturing application. The application has been successful with customers, and the application's user base has increased. The company has connected the AWS environment to the company's on-premises data center through a 1 Gbps AWS Direct Connect connection. The company has configured BGP for the connection.

The company must update the existing network connectivity solution to ensure that the solution is highly available, fault tolerant, and secure.

Which solution will meet these requirements MOST cost-effectively?

- A. Add a dynamic private IP AWS Site-to-Site VPN as a secondary path to secure data in transit and provide resilience for the Direct Connect connection. Configure MACsec to encrypt traffic inside the Direct Connect connection.
- B. Provision another Direct Connect connection between the company's on-premises data center and AWS to increase the transfer speed and provide resilience. Configure MACsec to encrypt traffic inside the Direct Connect connection.
- C. Configure multiple private VIFs. Load balance data across the VIFs between the on-premises data center and AWS to provide resilience.
- D. Add a static AWS Site-to-Site VPN as a secondary path to secure data in transit and to provide resilience for the Direct Connect connection.

Question #452**Topic 1**

A company needs to modernize an application and migrate the application to AWS. The application stores user profile data as text in a single table in an on-premises MySQL database.

After the modernization, users will use the application to upload video files that are up to 4 GB in size. Other users must be able to download the video files from the application. The company needs a video storage solution that provides rapid scaling. The solution must not affect application performance.

Which solution will meet these requirements?

- A. Migrate the database to Amazon Aurora PostgreSQL by using AWS Database Migration Service (AWS DMS). Store the videos as base64-encoded strings in a TEXT column in the database.
- B. Migrate the database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as objects in Amazon S3. Store the S3 key in the corresponding DynamoDB item.
- C. Migrate the database to Amazon Keyspaces (for Apache Cassandra) by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as objects in Amazon S3. Store the S3 object identifier in the corresponding Amazon Keyspaces entry.
- D. Migrate the database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as base64-encoded strings in the corresponding DynamoDB item.

Question #453**Topic 1**

A company stores and manages documents in an Amazon Elastic File System (Amazon EFS) file system. The file system is encrypted with an AWS Key Management Service (AWS KMS) key. The file system is mounted to an Amazon EC2 instance that runs proprietary software.

The company has enabled automatic backups for the file system. The automatic backups use the AWS Backup default backup plan.

A solutions architect must ensure that deleted documents can be recovered within an RPO of 100 minutes.

Which solution will meet these requirements?

- A. Create a new IAM role. Create a new backup plan. Use the new IAM role to create backups. Update the KMS key policy to allow the new IAM role to use the key. Implement an hourly backup schedule for the file system.
- B. Create a new backup plan. Update the KMS key policy to allow the AWSServiceRoleForBackup IAM role to use the key. Implement a custom cron expression to run a backup of the file system every 30 minutes.
- C. Create a new IAM role. Use the existing backup plan. Update the KMS key policy to allow the new IAM role to use the key. Enable continuous backups for point-in-time recovery.
- D. Use the existing backup plan. Update the KMS key policy to allow the AWSServiceRoleForBackup IAM role to use the key. Enable Cross-Region Replication for the file system.

Question #454**Topic 1**

A solutions architect must provide a secure way for a team of cloud engineers to use the AWS CLI to upload objects into an Amazon S3 bucket. Each cloud engineer has an IAM user, IAM access keys, and a virtual multi-factor authentication (MFA) device. The IAM users for the cloud engineers are in a group that is named S3-access. The cloud engineers must use MFA to perform any actions in Amazon S3.

Which solution will meet these requirements?

- A. Attach a policy to the S3 bucket to prompt the IAM user for an MFA code when the IAM user performs actions on the S3 bucket. Use IAM access keys with the AWS CLI to call Amazon S3.
- B. Update the trust policy for the S3-access group to require principals to use MFA when principals assume the group. Use IAM access keys with the AWS CLI to call Amazon S3.
- C. Attach a policy to the S3-access group to deny all S3 actions unless MFA is present. Use IAM access keys with the AWS CLI to call Amazon S3.
- D. Attach a policy to the S3-access group to deny all S3 actions unless MFA is present. Request temporary credentials from AWS Security Token Service (AWS STS). Attach the temporary credentials in a profile that Amazon S3 will reference when the user performs actions in Amazon S3.

Question #455**Topic 1**

A company needs to migrate 60 on-premises legacy applications to AWS. The applications are based on the .NET Framework and run on Windows.

The company needs a solution that minimizes migration time and requires no application code changes. The company also does not want to manage the infrastructure.

Which solution will meet these requirements?

- A. Refactor the applications and containerize them by using AWS Toolkit for .NET Refactoring. Use Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to host the containerized applications.
- B. Use the Windows Web Application Migration Assistant to migrate the applications to AWS Elastic Beanstalk. Use Elastic Beanstalk to deploy and manage the applications.
- C. Use the Windows Web Application Migration Assistant to migrate the applications to Amazon EC2 instances. Use the EC2 instances to deploy and manage the applications.
- D. Refactor the applications and containerize them by using AWS Toolkit for .NET Refactoring. Use Amazon Elastic Kubernetes Service (Amazon EKS) with the Fargate launch type to host the containerized applications.

Question #456

Topic 1

A company needs to run large batch-processing jobs on data that is stored in an Amazon S3 bucket. The jobs perform simulations. The results of the jobs are not time sensitive, and the process can withstand interruptions.

Each job must process 15-20 GB of data when the data is stored in the S3 bucket. The company will store the output from the jobs in a different Amazon S3 bucket for further analysis.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a serverless data pipeline. Use AWS Step Functions for orchestration. Use AWS Lambda functions with provisioned capacity to process the data.
- B. Create an AWS Batch compute environment that includes Amazon EC2 Spot Instances. Specify the SPOT_CAPACITY_OPTIMIZED allocation strategy.
- C. Create an AWS Batch compute environment that includes Amazon EC2 On-Demand Instances and Spot Instances. Specify the SPOT_CAPACITY_OPTIMIZED allocation strategy for the Spot Instances.
- D. Use Amazon Elastic Kubernetes Service (Amazon EKS) to run the processing jobs. Use managed node groups that contain a combination of Amazon EC2 On-Demand Instances and Spot Instances.

Question #457

Topic 1

A company has an application that analyzes and stores image data on premises. The application receives millions of new image files every day. Files are an average of 1 MB in size. The files are analyzed in batches of 1 GB. When the application analyzes a batch, the application zips the images together. The application then archives the images as a single file in an on-premises NFS server for long-term storage.

The company has a Microsoft Hyper-V environment on premises and has compute capacity available. The company does not have storage capacity and wants to archive the images on AWS. The company needs the ability to retrieve archived data within 1 week of a request.

The company has a 10 Gbps AWS Direct Connect connection between its on-premises data center and AWS. The company needs to set bandwidth limits and schedule archived images to be copied to AWS during non-business hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy an AWS DataSync agent on a new GPU-based Amazon EC2 instance. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Glacier Instant Retrieval. After the successful copy, delete the data from the on-premises storage.
- B. Deploy an AWS DataSync agent as a Hyper-V VM on premises. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Glacier Deep Archive. After the successful copy, delete the data from the on-premises storage.
- C. Deploy an AWS DataSync agent on a new general purpose Amazon EC2 instance. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Standard. After the successful copy, delete the data from the on-premises storage. Create an S3 Lifecycle rule to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 day.
- D. Deploy an AWS Storage Gateway Tape Gateway on premises in the Hyper-V environment. Connect the Tape Gateway to AWS. Use automatic tape creation. Specify an Amazon S3 Glacier Deep Archive pool. Eject the tape after the batch of images is copied.

Question #458

Topic 1

A company wants to record key performance indicators (KPIs) from its application as part of a strategy to convert to a user-based licensing schema. The application is a multi-tier application with a web-based UI. The company saves all log files to Amazon CloudWatch by using the CloudWatch agent. All logins to the application are saved in a log file.

As part of the new license schema, the company needs to find out how many unique users each client has on a daily basis, weekly basis, and monthly basis.

Which solution will provide this information with the LEAST change to the application?

- A. Configure an Amazon CloudWatch Logs metric filter that saves each successful login as a metric. Configure the user name and client name as dimensions for the metric.
- B. Change the application logic to make each successful login generate a call to the AWS SDK to increment a custom metric that records user name and client name dimensions in CloudWatch.
- C. Configure the CloudWatch agent to extract successful login metrics from the logs. Additionally, configure the CloudWatch agent to save the successful login metrics as a custom metric that uses the user name and client name as dimensions for the metric.
- D. Configure an AWS Lambda function to consume an Amazon CloudWatch Logs stream of the application logs. Additionally, configure the Lambda function to increment a custom metric in CloudWatch that uses the user name and client name as dimensions for the metric.

Question #459

Topic 1

A company is using GitHub Actions to run a CI/CD pipeline that accesses resources on AWS. The company has an IAM user that uses a secret key in the pipeline to authenticate to AWS. An existing IAM role with an attached policy grants the required permissions to deploy resources.

The company's security team implements a new requirement that pipelines can no longer use long-lived secret keys. A solutions architect must replace the secret key with a short-lived solution.

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

- A. Create an IAM SAML 2.0 identity provider (IdP) in AWS Identity and Access Management (IAM). Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRole API call. Attach the existing IAM policy to the new IAM role. Update GitHub to use SAML authentication for the pipeline.
- B. Create an IAM OpenID Connect (OIDC) identity provider (IdP) in AWS Identity and Access Management (IAM). Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRoleWithWebIdentity API call from the GitHub OIDC IdP. Update GitHub to assume the role for the pipeline.
- C. Create an Amazon Cognito identity pool. Configure the authentication provider to use GitHub. Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRoleWithWebIdentity API call from the GitHub authentication provider. Configure the pipeline to use Cognito as its authentication provider.
- D. Create a trust anchor to AWS Private Certificate Authority. Generate a client certificate to use with AWS IAM Roles Anywhere. Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRole API call. Attach the existing IAM policy to the new IAM role. Configure the pipeline to use the credential helper tool and to reference the client certificate public key to assume the new IAM role.

Question #460

Topic 1

A company is running a web-crawling process on a list of target URLs to obtain training documents for machine learning training algorithms. A fleet of Amazon EC2 t2.micro instances pulls the target URLs from an Amazon Simple Queue Service (Amazon SQS) queue. The instances then write the result of the crawling algorithm as a .csv file to an Amazon Elastic File System (Amazon EFS) volume. The EFS volume is mounted on all instances of the fleet.

A separate system adds the URLs to the SQS queue at infrequent rates. The instances crawl each URL in 10 seconds or less.

Metrics indicate that some instances are idle when no URLs are in the SQS queue. A solutions architect needs to redesign the architecture to optimize costs.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Use m5.8xlarge instances instead of t2.micro instances for the web-crawling process. Reduce the number of instances in the fleet by 50%.
- B. Convert the web-crawling process into an AWS Lambda function. Configure the Lambda function to pull URLs from the SQS queue.
- C. Modify the web-crawling process to store results in Amazon Neptune.
- D. Modify the web-crawling process to store results in an Amazon Aurora Serverless MySQL instance.
- E. Modify the web-crawling process to store results in Amazon S3.

Question #461

Topic 1

A company needs to migrate its website from an on-premises data center to AWS. The website consists of a load balancer, a content management system (CMS) that runs on a Linux operating system, and a MySQL database.

The CMS requires persistent NFS-compatible storage for a file system. The new solution on AWS must be able to scale from 2 Amazon EC2 instances to 30 EC2 instances in response to unpredictable traffic increases. The new solution also must require no changes to the website and must prevent data loss.

Which solution will meet these requirements?

- A. Create an Amazon Elastic File System (Amazon EFS) file system. Deploy the CMS to AWS Elastic Beanstalk with an Application Load Balancer and an Auto Scaling group. Use .ebextensions to mount the EFS file system to the EC2 instances. Create an Amazon Aurora MySQL database that is separate from the Elastic Beanstalk environment.
- B. Create an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume. Deploy the CMS to AWS Elastic Beanstalk with a Network Load Balancer and an Auto Scaling group. Use .ebextensions to mount the EBS volume to the EC2 instances. Create an Amazon RDS for MySQL database in the Elastic Beanstalk environment.
- C. Create an Amazon Elastic File System (Amazon EFS) file system. Create a launch template and an Auto Scaling group to launch EC2 instances to support the CMS. Create a Network Load Balancer to distribute traffic. Create an Amazon Aurora MySQL database. Use an EC2 Auto Scaling scale-in lifecycle hook to mount the EFS file system to the EC2 instances.
- D. Create an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume. Create a launch template and an Auto Scaling group to launch EC2 instances to support the CMS. Create an Application Load Balancer to distribute traffic. Create an Amazon ElastiCache for Redis cluster to support the MySQL database. Use EC2 user data to attach the EBS volume to the EC2 instances.

Question #462

Topic 1

A company needs to implement disaster recovery for a critical application that runs in a single AWS Region. The application's users interact with a web frontend that is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The application writes to an Amazon RDS for MySQL DB instance. The application also outputs processed documents that are stored in an Amazon S3 bucket.

The company's finance team directly queries the database to run reports. During busy periods, these queries consume resources and negatively affect application performance.

A solutions architect must design a solution that will provide resiliency during a disaster. The solution must minimize data loss and must resolve the performance problems that result from the finance team's queries.

Which solution will meet these requirements?

- A. Migrate the database to Amazon DynamoDB and use DynamoDB global tables. Instruct the finance team to query a global table in a separate Region. Create an AWS Lambda function to periodically synchronize the contents of the original S3 bucket to a new S3 bucket in the separate Region. Launch EC2 instances and create an ALB in the separate Region. Configure the application to point to the new S3 bucket.
- B. Launch additional EC2 instances that host the application in a separate Region. Add the additional instances to the existing ALB in the separate Region, create a read replica of the RDS DB instance. Instruct the finance team to run queries against the read replica. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, promote the read replica to a standalone DB instance. Configure the application to point to the new S3 bucket and to the newly promoted read replica.
- C. Create a read replica of the RDS DB instance in a separate Region. Instruct the finance team to run queries against the read replica. Create AMIs of the EC2 instances that host the application frontend. Copy the AMIs to the separate Region. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, promote the read replica to a standalone DB instance. Launch EC2 instances from the AMIs and create an ALB to present the application to end users. Configure the application to point to the new S3 bucket.
- D. Create hourly snapshots of the RDS DB instance. Copy the snapshots to a separate Region. Add an Amazon ElastiCache cluster in front of the existing RDS database. Create AMIs of the EC2 instances that host the application frontend. Copy the AMIs to the separate Region. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, restore the database from the latest RDS snapshot. Launch EC2 instances from the AMIs and create an ALB to present the application to end users. Configure the application to point to the new S3 bucket.

Question #463

Topic 1

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.
- B. Create a VPC Endpoint Service that accepts HTTP or HTTPS traffic, host it behind an Application Load Balancer, and make the service available over DX.
- C. Attach an internet gateway to the VPC, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.
- D. Attach a NAT gateway to the VPC, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.

Question #464

Topic 1

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?

- A. Create an SCP that applies to all the AWS accounts to allow IAM actions only for administrator roles. Apply the SCP to the root OU.
- B. Configure AWS CloudTrail to invoke an AWS Lambda function for each event that is related to IAM actions. Configure the function to deny the action if the user who invoked the action is not an administrator.
- 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.
- D. Set an IAM permissions boundary that allows IAM actions. Attach the permissions boundary to every administrator role across all the AWS accounts.

Question #465

Topic 1

A company uses an organization in AWS Organizations to manage multiple AWS accounts. The company hosts some applications in a VPC in the company's shared services account.

The company has attached a transit gateway to the VPC in the shared services account.

The company is developing a new capability and has created a development environment that requires access to the applications that are in the shared services account. The company intends to delete and recreate resources frequently in the development account. The company also wants to give a development team the ability to recreate the team's connection to the shared services account as required.

Which solution will meet these requirements?

- A. Create a transit gateway in the development account. Create a transit gateway peering request to the shared services account. Configure the shared services transit gateway to automatically accept peering connections.
- B. Turn on automatic acceptance for the transit gateway in the shared services account. Use AWS Resource Access Manager (AWS RAM) to share the transit gateway resource in the shared services account with the development account. Accept the resource in the development account. Create a transit gateway attachment in the development account.
- C. Turn on automatic acceptance for the transit gateway in the shared services account. Create a VPC endpoint. Use the endpoint policy to grant permissions on the VPC endpoint for the development account. Configure the endpoint service to automatically accept connection requests. Provide the endpoint details to the development team.
- D. Create an Amazon EventBridge rule to invoke an AWS Lambda function that accepts the transit gateway attachment when the development account makes an attachment request. Use AWS Network Manager to share the transit gateway in the shared services account with the development account. Accept the transit gateway in the development account.

Question #466

Topic 1

A company wants to migrate virtual Microsoft workloads from an on-premises data center to AWS. The company has successfully tested a few sample workloads on AWS. The company also has created an AWS Site-to-Site VPN connection to a VPC. A solutions architect needs to generate a total cost of ownership (TCO) report for the migration of all the workloads from the data center.

Simple Network Management Protocol (SNMP) has been enabled on each VM in the data center. The company cannot add more VMs in the data center and cannot install additional software on the VMs. The discovery data must be automatically imported into AWS Migration Hub.

Which solution will meet these requirements?

- A. Use the AWS Application Migration Service agentless service and the AWS Migration Hub Strategy Recommendations to generate the TCO report.
- B. Launch a Windows Amazon EC2 instance. Install the Migration Evaluator agentless collector on the EC2 instance. Configure Migration Evaluator to generate the TCO report.
- C. Launch a Windows Amazon EC2 instance. Install the Migration Evaluator agentless collector on the EC2 instance. Configure Migration Hub to generate the TCO report.
- D. Use the AWS Migration Readiness Assessment tool inside the VPC. Configure Migration Evaluator to generate the TCO report.

Question #467

Topic 1

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?

- A. Create an Amazon CloudFront distribution. Create an origin group with one origin for each ALB. Set one of the origins as primary.
- B. Create an Amazon Route 53 health check for each ALB. Create a Route 53 failover routing record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.
- C. Create two Amazon CloudFront distributions, each with one ALB as the origin. Create an Amazon Route 53 failover routing record pointing to the two CloudFront distributions. Set the Evaluate Target Health value to Yes.
- 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.

Question #468

Topic 1

A company deploys workloads in multiple AWS accounts. Each account has a VPC with VPC flow logs published in text log format to a centralized Amazon S3 bucket. Each log file is compressed with gzip compression. The company must retain the log files indefinitely.

A security engineer occasionally analyzes the logs by using Amazon Athena to query the VPC flow logs. The query performance is degrading over time as the number of ingested logs is growing. A solutions architect must improve the performance of the log analysis and reduce the storage space that the VPC flow logs use.

Which solution will meet these requirements with the LARGEST performance improvement?

- A. Create an AWS Lambda function to decompress the gzip files and to compress the files with bzip2 compression. Subscribe the Lambda function to an s3:ObjectCreated:Put S3 event notification for the S3 bucket.
- B. Enable S3 Transfer Acceleration for the S3 bucket. Create an S3 Lifecycle configuration to move files to the S3 Intelligent-Tiering storage class as soon as the files are uploaded.
- C. Update the VPC flow log configuration to store the files in Apache Parquet format. Specify hourly partitions for the log files.
- D. Create a new Athena workgroup without data usage control limits. Use Athena engine version 2.

Question #469

Topic 1

A company wants to establish a dedicated connection between its on-premises infrastructure and AWS. The company is setting up a 1 Gbps AWS Direct Connect connection to its account VPC. The architecture includes a transit gateway and a Direct Connect gateway to connect multiple VPCs and the on-premises infrastructure.

The company must connect to VPC resources over a transit VIF by using the Direct Connect connection.

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

- A. Update the 1 Gbps Direct Connect connection to 10 Gbps.
- B. Advertise the on-premises network prefixes over the transit VIF.
- C. Advertise the VPC prefixes from the Direct Connect gateway to the on-premises network over the transit VIF.
- D. Update the Direct Connect connection's MACsec encryption mode attribute to must_encrypt.
- E. Associate a MACsec Connection Key Name/Connectivity Association Key (CKN/CAK) pair with the Direct Connect connection.

Question #470

Topic 1

A company wants to use Amazon WorkSpaces in combination with thin 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 office in the next 6 months.

Which solution meets these requirements with the MOST operational efficiency?

- A. Create an IP access control group rule with the list of public addresses from the branch offices. Associate the IP access control group with the WorkSpaces directory.
- B. Use AWS Firewall Manager to create a web ACL rule with an IPSet with the list of public addresses from the branch office locations. Associate the web ACL with the WorkSpaces directory.
- C. Use AWS Certificate Manager (ACM) to issue trusted device certificates to the machines deployed in the branch office locations. Enable restricted access on the WorkSpaces directory.
- D. Create a custom WorkSpace image with Windows Firewall configured to restrict access to the public addresses of the branch offices. Use the image to deploy the WorkSpaces.

Question #471

Topic 1

A company uses AWS Organizations. The company runs two firewall appliances in a centralized networking account. Each firewall appliance runs on a manually configured highly available Amazon EC2 instance. A transit gateway connects the VPC from the centralized networking account to VPCs of member accounts. Each firewall appliance uses a static private IP address that is then used to route traffic from the member accounts to the internet.

During a recent incident, a badly configured script initiated the termination of both firewall appliances. During the rebuild of the firewall appliances, the company wrote a new script to configure the firewall appliances at startup.

The company wants to modernize the deployment of the firewall appliances. The firewall appliances need the ability to scale horizontally to handle increased traffic when the network expands. The company must continue to use the firewall appliances to comply with company policy. The provider of the firewall appliances has confirmed that the latest version of the firewall code will work with all AWS services.

Which combination of steps should the solutions architect recommend to meet these requirements MOST cost-effectively? (Choose three.)

- A. Deploy a Gateway Load Balancer in the centralized networking account. Set up an endpoint service that uses AWS PrivateLink.
- B. Deploy a Network Load Balancer in the centralized networking account. Set up an endpoint service that uses AWS PrivateLink.
- C. Create an Auto Scaling group and a launch template that uses the new script as user data to configure the firewall appliances. Create a target group that uses the instance target type.
- D. Create an Auto Scaling group. Configure an AWS Launch Wizard deployment that uses the new script as user data to configure the firewall appliances. Create a target group that uses the IP target type.
- E. Create VPC endpoints in each member account. Update the route tables to point to the VPC endpoints.
- F. Create VPC endpoints in the centralized networking account. Update the route tables in each member account to point to the VPC endpoints.

Question #472

Topic 1

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 a failover event.
- B. In the primary Region, create a health check on the database that will invoke an AWS Lambda function when a failure is detected. Program the Lambda function to recreate the database from the latest database snapshot in the secondary Region and update the Route 53 host records for the database.
- C. Create an AWS Lambda function to copy the latest automated backup to the secondary Region every 2 hours.
- 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.
- E. Create a hot standby database in the secondary Region. Use an AWS Lambda function to restore the secondary database to the latest RDS automatic backup in the event that the primary database fails.

Question #473

Topic 1

An ecommerce company runs an application on AWS. The application has an Amazon API Gateway API that invokes an AWS Lambda function. The data is stored in an Amazon RDS for PostgreSQL DB instance.

During the company's most recent flash sale, a sudden increase in API calls negatively affected the application's performance. A solutions architect reviewed the Amazon CloudWatch metrics during that time and noticed a significant increase in Lambda invocations and database connections. The CPU utilization also was high on the DB instance.

What should the solutions architect recommend to optimize the application's performance?

- A. Increase the memory of the Lambda function. Modify the Lambda function to close the database connections when the data is retrieved.
- B. Add an Amazon ElastiCache for Redis cluster to store the frequently accessed data from the RDS database.
- C. Create an RDS proxy by using the Lambda console. Modify the Lambda function to use the proxy endpoint.
- D. Modify the Lambda function to connect to the database outside of the function's handler. Check for an existing database connection before creating a new connection.

Question #474

Topic 1

A retail company wants to improve its application architecture. The company's applications register new orders, handle returns of merchandise, and provide analytics. The applications store retail data in a MySQL database and an Oracle OLAP analytics database. All the applications and databases are hosted on Amazon EC2 instances.

Each application consists of several components that handle different parts of the order process. These components use incoming data from different sources. A separate ETL job runs every week and copies data from each application to the analytics database.

A solutions architect must redesign the architecture into an event-driven solution that uses serverless services. The solution must provide updated analytics in near real time.

Which solution will meet these requirements?

- A. Migrate the individual applications as microservices to Amazon Elastic Container Service (Amazon ECS) containers that use AWS Fargate. Keep the retail MySQL database on Amazon EC2. Move the analytics database to Amazon Neptune. Use Amazon Simple Queue Service (Amazon SQS) to send all the incoming data to the microservices and the analytics database.
- B. Create an Auto Scaling group for each application. Specify the necessary number of EC2 instances in each Auto Scaling group. Migrate the retail MySQL database and the analytics database to Amazon Aurora MySQL. Use Amazon Simple Notification Service (Amazon SNS) to send all the incoming data to the correct EC2 instances and the analytics database.
- C. Migrate the individual applications as microservices to Amazon Elastic Kubernetes Service (Amazon EKS) containers that use AWS Fargate. Migrate the retail MySQL database to Amazon Aurora Serverless MySQL. Migrate the analytics database to Amazon Redshift Serverless. Use Amazon EventBridge to send all the incoming data to the microservices and the analytics database.
- D. Migrate the individual applications as microservices to Amazon AppStream 2.0. Migrate the retail MySQL database to Amazon Aurora MySQL. Migrate the analytics database to Amazon Redshift Serverless. Use AWS IoT Core to send all the incoming data to the microservices and the analytics database.

Question #475

Topic 1

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?

- A. Create an AWS Lambda function that creates a new CloudTrail trail in all AWS accounts in the organization. Invoke the Lambda function daily by using a scheduled action in Amazon EventBridge.
- 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.
- C. Create a new CloudTrail trail in all AWS accounts in the organization. Create new trails whenever a new account is created. Define an SCP that prevents deletion or modification of trails. Apply the SCP to the root OU.
- D. Create an AWS Systems Manager Automation runbook that creates a CloudTrail trail in all AWS accounts in the organization. Invoke the automation by using Systems Manager State Manager.

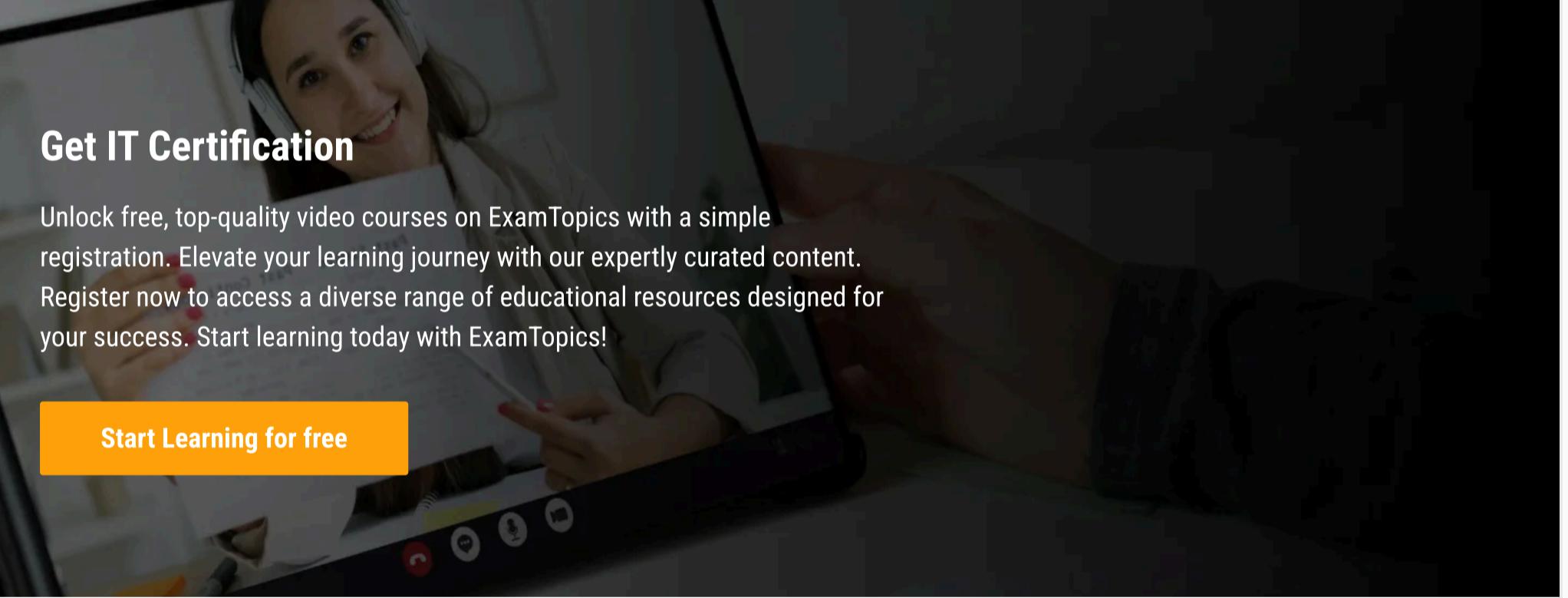
Question #476

Topic 1

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?

- A. Create an AWS Site-to-Site VPN connection. Configure integration between a VPN and AD DS. Use an Amazon WorkSpaces client with MFA support enabled to establish a VPN connection.
- 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.
- C. Create multiple AWS Site-to-Site VPN connections by using AWS VPN CloudHub. Configure integration between AWS VPN CloudHub and AD DS. Use AWS Copilot to establish a VPN connection.
- D. Create an Amazon WorkLink endpoint. Configure integration between Amazon WorkLink and AD DS. Enable MFA in Amazon WorkLink. Use AWS Client VPN to establish a VPN connection.



Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)