



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

⚙ Custom View Settings

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 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 VPC. Associate 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.

← Previous Questions

Next Questions →

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