SAP-C02 Q&As

AWS Certified Solutions Architect - Professional

Pass Amazon SAP-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/sap-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company needs to improve the reliability of its ticketing application. The application runs on an Amazon Elastic Container Service (Amazon ECS) cluster. The company uses Amazon CloudFront to serve the application. A single ECS service of the ECS cluster is the CloudFront distribution\\'s origin.

The application allows only a specific number of active users to enter a ticket purchasing flow. These users are identified by an encrypted attribute in their JSON Web Token (JWT). All other users are redirected to a waiting room module until there is available capacity for purchasing.

The application is experiencing high loads. The waiting room module is working as designed, but load on the waiting room is disrupting the applications availability. This disruption is negatively affecting the application\\'s ticket sale transactions.

Which solution will provide the MOST reliability for ticket sale transactions during periods of high load?

A. Create a separate service in the ECS cluster for the waiting room. Use a separate scaling configuration. Ensure that the ticketing service uses the JWT information and appropriately forwards requests to the waiting room service.

B. Move the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Split the waiting room module into a pod that is separate from the ticketing pod. Make the ticketing pod part of a StatefulSet. Ensure that the ticketing pod uses the JWT information and appropriately forwards requests to the waiting room pod.

C. Create a separate service in the ECS cluster for the waiting room. Use a separate scaling configuration. Create a CloudFront function that inspects the JWT information and appropriately forwards requests to the ticketing service or the waiting room service.

D. Move the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Split the waiting room module into a pod that is separate from the ticketing pod. Use AWS App Mesh by provisioning the App Mesh controller for Kubernetes. Enable mTLS authentication and service-to-service authentication for communication between the ticketing pod and the waiting room pod. Ensure that the ticketing pod uses the JWT information and appropriately forwards requests to the waiting room pod.

Correct Answer: C

QUESTION 2

A company has many AWS accounts and uses AWS Organizations to manage all of them. A solutions architect must implement a solution that the company can use to share a common network across multiple accounts.

The company\\'s infrastructure team has a dedicated infrastructure account that has a VPC. The infrastructure team must use this account to manage the network. Individual accounts cannot have the ability to manage their own networks. However, individual accounts must be able to create AWS resources within subnets.

Which combination of actions should the solutions architect perform to meet these requirements? (Select TWO.)

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.

Correct Answer: BD

https://docs.aws.amazon.com/vpc/latest/userguide/sharing-managed-prefix- lists.html

QUESTION 3

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.

Correct Answer: D

QUESTION 4

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 a low developers the possibilityy 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 SCPs 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 StrmgEquals condition for the DevelopmentUnit resource tag and aws Principal Tag \\'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

Correct Answer: B

This option allows the solutions architect to use session tags to pass additional information about the federated user, such as the development unit name, to AWS1. Session tags are key-value pairs that you can define in your identity provider (IdP) and pass in your SAML assertion1. By using a deny action and a StringNotEquals condition in the IAM policy, you can prevent developers from accessing or modifying EC2 instances that belong to a different development unit2. This way, you can enforce fine-grained access control and prevent accidental or malicious incidents. References: Passing session tags in SAML assertions Using tags for attribute-based access control

QUESTION 5

A company\\'s solutions architect is reviewing a new internally developed application in a sandbox AWS account The application uses an AWS Auto Scaling group of Amazon EC2 instances that have an IAM instance profile attached Part of the application logic creates and accesses secrets from AWS Secrets Manager The company has an AWS Lambda function that calls the application API to test the functionality The company also has created an AWS CloudTrail trail in the account

The application\\'s developer has attached the SecretsManagerReadWnte AWS managed IAM policy to an IAM role The IAM role is associated with the instance profile that is attached to the EC2 instances The solutions architect has invoked the Lambda function for testing

The solutions architect must replace the SecretsManagerReadWnte policy with a new policy that provides least privilege access to the Secrets Manager actions that the application requires

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

A. Generate a policy based on CloudTrail events for the IAM role Use the generated policy output to create a new IAM policy Use the newly generated IAM policy to replace the SecretsManagerReadWnte policy that is attached to the IAM role

B. Create an analyzer in AWS Identity and Access Management Access Analyzer Use the IAM role\\'s Access Advisor findings to create a new IAM policy Use the newly created IAM policy to replace the SecretsManagerReadWnte policy that is attached to the IAM role

C. Use the aws cloudtrail lookup-events AWS CLI command to filter and export CloudTrail events that are related to Secrets Manager Use a new IAM policy that contains the actions from CloudTrail to replace the

SecretsManagerReadWnte policy that is attached to the IAM role

D. Use the IAM policy simulator to generate an IAM policy for the IAM role Use the newly generated IAM policy to replace the SecretsManagerReadWnte policy that is attached to the IAM role

Correct Answer: D

The IAM policy simulator will generate a policy that contains only the necessary permissions for the application to access Secrets Manager, providing the least privilege necessary to get the job done. This is the most efficient solution as it will not require additional steps such as analyzing CloudTrail events or manually creating and testing an IAM policy. You can use the IAM policy simulator to generate an IAM policy for an IAM role by specifying the role and the API actions and resources that the application or service requires. The simulator will then generate an IAM policy that grants the least privilege access to those actions and resources. Once you have generated an IAM policy using the simulator, you can replace the existing SecretsManagerReadWnte policy that is attached to the IAM role with the newly generated policy. This will ensure that the application or service has the least privilege access to the Secrets Manager actions that it requires. You can access the IAM policy simulator through the IAM console, AWS CLI, and AWS SDKs. Here is the link for more information:https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_simulator.html

QUESTION 6

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.

Correct Answer: A

QUESTION 7

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.

Correct Answer: B

By reducing the number of data nodes in the cluster to 2 and adding UltraWarm nodes to handle the expected capacity, the company can reduce the cost of running the cluster. Additionally, configuring the indexes to transition to UltraWarm when OpenSearch Service ingests the data will ensure that the data is stored in the most cost- effective manner. Finally, transitioning the input data to S3 Glacier Deep Archive after 1 month by using an S3 Lifecycle policy will ensure that the data is retained for compliance purposes, while also reducing the ongoing costs.

QUESTION 8

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.

Correct Answer: C

to connect out from the private subnet you need an NAT gateway and since only one Elastic IP whitelisted on firewall its one NATGateway at time and if AZ failure happens Lambda creates a new NATGATEWAY in a different AZ using the Same Elastic IP ,dont be tempted to select D since application that needs to connect is on a private subnet whose outbound connections use the NATGateway Elastic IP

QUESTION 9

A company wants to migrate its website to AWS. The website uses containers that are deployed in an on-premises, self-managed Kubernetes cluster. All data for the website is stored in an on-premises PostgreSQL database.

The company has decided to migrate the on-premises Kubernetes cluster to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster will use EKS managed node groups with a static number of nodes. The company

will also migrate the on-premises database to an Amazon RDS for PostgreSQL database.

A solutions architect needs to estimate the total cost of ownership (TCO) for this workload before the migration.

Which solution will provide the required TCO information?

A. Request access to Migration Evaluator. Run the Migration Evaluator Collector and import the data. Configure a scenario. Export a Quick Insights report from Migration Evaluator.

B. Launch AWS Database Migration Service (AWS DMS) for the on-premises database. Generate an assessment report. Create an estimate in AWS Pricing Calculator for the costs of the EKS migration.

C. Initialize AWS Application Migration Service. Add the on-premises servers as source servers. Launch a test instance. Output a TCO report from Application Migration Service.

D. Access the AWS Cloud Economics Center webpage to assess the AWS Cloud Value Framework. Create an AWS Cost and Usage report from the Cloud Value Framework.

Correct Answer: A

QUESTION 10

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.

Correct Answer: AD

All features The default feature set that is available to AWS Organizations. It includes all the functionality of consolidated billing, plus advanced features that give you more control over accounts in your organization. For example, when all features are enabled the management account of the organization has full control over what member accounts can do. The management account can apply SCPs to restrict the services and actions that users (including the root user) and roles in an account can access.

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html#feature-set

QUESTION 11

A company hosts a web application that tuns on a group of Amazon EC2 instances that ate behind an Application Load Balancer (ALB) in a VPC. The company wants to analyze the network payloads lo reverse-engineer a sophisticated attack of the application.

Which approach should the company take to achieve this goal?

A. Enable VPC Flow Logs. Store the flow logs in an Amazon S3 bucket for analysis.

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

C. Create an AWS WAF web ACL. and associate it with the ALB. Configure AWS WAF logging.

D. Enable logging for the ALB. Store the logs in an Amazon S3 bucket for analysis.

Correct Answer: A

QUESTION 12

A company plans to refactor a monolithic application into a modern application designed deployed or AWS. The CLCD pipeline needs to be upgraded to support the modem design for the application with the following requirements

1.

It should allow changes to be released several times every hour.

2.

It should be able to roll back the changes as quickly as possible

Which design will meet these requirements?

A. Deploy a Cl-CD pipeline that incorporates AMIs to contain the application and their configurations Deploy the application by replacing Amazon EC2 instances

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

C. Use AWS Systems Manager to re-provision the infrastructure for each deployment Update the Amazon EC2 user data to pull the latest code art-fact from Amazon S3 and use Amazon Route 53 weighted routing to point to the new environment

D. Roll out At application updates as pan 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.

Correct Answer: B

It is the fastest when it comes to rollback and deploying changes every hour

QUESTION 13

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 getaway between the two VPCs.

Correct Answer: A

https://docs.aws.amazon.com/pt_br/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-vpn.html

Transit gateway is an AWS managed high availability and scalability regional network transit hub used to interconnect VPCs and customer networks. AWS Transit Gateway + VPN, using the Transit Gateway VPN Attachment, provides the

option of creating an IPsec VPN connection between your remote network and the Transit Gateway over the internet, as shown in the following picture.

https://docs.aws.amazon.com/images/whitepapers/latest/aws-vpc-connectivity-options/images/image4.png

Option A is the correct answer since the transit gateway will allow both VPCs to connect to the on premises network.

Option B suggests the same feature but is using the Transit Gateway in a incorrect way. The soul purpose of the gateway is to have point for interconnectivity.

QUESTION 14

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 myservice.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

Correct Answer: C

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html

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. As it uses the NLB as the resource in the A-record, traffic will be routed through the NLB, and it will automatically route the traffic to the healthy instances based on the health checks and also it provides the fixed address assignments as the other companies can add the NLB\\'s Elastic IP addresses to their allow lists.

QUESTION 15

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. Trigger an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Trigger 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. Trigger 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. Trigger 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. Trigger 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.

Correct Answer: C

You can use a Glue crawler to populate the AWS Glue Data Catalog with tables. The Lambda function can be triggered using S3 event notifications when object create events occur. The Lambda function will then trigger the Glue ETL job to transform the records masking the sensitive data and modifying the output format to JSON. This solution meets all requirements.

Create an AWS Glue crawler and custom classifier based on the data feed formats and build a table definition to match. Trigger an AWS Lambda function 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. https://docs.aws.amazon.com/glue/latest/dg/trigger-job.html https://d1.awsstatic.com/Products/product-name/diagrams/product-page-diagram_Glue_Event-driven-ETL-Pipelines.e24d59bb79a9e24cdba7f43ffd234ec0482a60e2.png

SAP-C02 PDF Dumps SAP-C02 VCE Dumps SAP-C02 Practice Test