2026 100% Free SAP-C02–Accurate 100% Free Exam Preparation | Reliable SAP-C02 Exam Pattern

The Amazon SAP-C02 PDF dumps format is the most simple and easy version, specially designed by the PassTorrent to provide value to its consumers. It is also compatible with all smart devices. Thus it is portable, which will help you practice the Amazon SAP-C02 Exam without the barrier of time and place.

Achieving the AWS Certified Solutions Architect - Professional certification demonstrates a high level of technical expertise and knowledge in designing and deploying AWS-based systems and applications. It is a valuable credential that can help IT professionals to advance their careers and gain recognition as an expert in the field of cloud computing.

>> SAP-C02 Exam Preparation <<

Pass Guaranteed 2026 Amazon SAP-C02: Marvelous AWS Certified Solutions Architect - Professional (SAP-C02) Exam Preparation

All these three Prepare for your AWS Certified Solutions Architect - Professional (SAP-C02) (SAP-C02) exam questions formats are specifically designed for quick and complete Amazon SAP-C02 exam preparation. The SAP-C02 PDF Dumps file is the collection of real, valid, and updated Prepare for your AWS Certified Solutions Architect - Professional (SAP-C02) (SAP-C02) exam practice test questions that are being presented in PDF format. This AWS Certified Solutions Architect - Professional (SAP-C02) (SAP-C02) PDF file comes with some top features such as being very easy to download and use.

The SAP-C02 Exam covers a broad range of topics, including designing and deploying applications on AWS, managing security and compliance, optimizing cost and performance, and implementing continuous deployment and delivery. It is a rigorous exam that tests the candidate's ability to design, deploy and manage complex applications on the AWS platform.

Amazon AWS Certified Solutions Architect - Professional (SAP-C02) Sample Questions (Q583-Q588):

NEW QUESTION # 583
A company runs a Java application that has complex dependencies on VMs that are in the company's data center. The application is stable. but the company wants to modernize the technology stack. The company wants to migrate the application to AWS and minimize the administrative overhead to maintain the servers.
Which solution will meet these requirements with the LEAST code changes?

- A. Migrate the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate by using AWS App2Container. Store container images in Amazon Elastic Container Registry (Amazon ECR). Grant the ECS task execution role permission 10 access the ECR image repository. Configure Amazon ECS to use an Application Load Balancer (ALB). Use the ALB to interact with the application.
- B. Migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) on EKS managed node groups by using

AWS App2Container. Store container images in Amazon Elastic Container Registry (Amazon ECR). Give the EKS nodes permission to access the ECR image repository.
Use Amazon API Gateway to interact with the application.

- C. Migrate the application code to a container that runs in AWS Lambda. Build an Amazon API Gateway REST API with Lambda integration. Use API Gateway to interact with the application.
- D. Migrate the application code to a container that runs in AWS Lambda. Configure Lambda to use an Application Load Balancer (ALB). Use the ALB to interact with the application.

Answer: A

Explanation:
By using AWS App2Container to migrate the application to Amazon ECS, the company can make the migration process easier. Additionally, using Amazon ECR to store the container images and granting the ECS task execution role permission to access the ECR image repository will minimize the administrative overhead to maintain the servers. Finally, configuring Amazon ECS to use an ALB and using the ALB to interact with the application will reduce the amount of code changes needed. This solution will allow the company to modernize their technology stack while minimizing the amount of code changes needed.
You can refer to the AWS App2Container documentation for more information on how to use this service:
https://aws.amazon.com/app2container/
You can refer to the AWS Fargate documentation for more information on how to use this service:
https://aws.amazon.com/fargate/
You can refer to the AWS Elastic Container Service documentation for more information on how to use this service:
https://aws.amazon.com/ecs/
You can refer to the Amazon Elastic Container Registry documentation for more information on how to use this service:
https://aws.amazon.com/ecr/
You can refer to the Application Load Balancer documentation for more information on how to use this service:
https://aws.amazon.com/elasticloadbalancing/applicationloadbalancer/

NEW QUESTION # 584
A company is planning to host a web application on AWS and works to load balance the traffic across a group of Amazon EC2 instances.
One of the security requirements is to enable end-to-end encryption in transit between the client and the web server.
Which solution will meet this requirement?

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

Answer: B

Explanation:
They can place the EC2 instances behind an Application Load Balancer (ALB), provision an SSL certificate using AWS Certificate Manager (ACM), and associate the SSL certificate with the ALB.
They can also provision a third-party SSL certificate and install it on each EC2 instance. Finally, they can configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances. This will ensure that traffic is encrypted both between the client and the ALB, and between the ALB and the EC2 instances.

NEW QUESTION # 585

A company has developed a hybrid solution between its data center and AWS. The company uses Amazon VPC and Amazon EC2 instances that send application logs to Amazon CloudWatch. The EC2 instances read data from multiple relational databases that are hosted on premises.

The company wants to monitor which EC2 instances are connected to the databases in near-real time. The company already has a monitoring solution that uses Splunk on premises. A solutions architect needs to determine how to send networking traffic to Splunk. How should the solutions architect meet these requirements?

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

Answer: B

Explanation:
https://docs.aws.amazon.com/firehose/latest/dev/creating-the-stream-to-splunk.html

NEW QUESTION # 586

Question:
A company mandates that all internal AWS communications use private IPs. A solutions architect created interface VPC endpoints for public AWS services like S3. However, service names are still resolving to public IP addresses, and the internal apps cannot connect.
What should the architect do to resolve this issue?

- A. Enable the private DNS option on the VPC attributes.
- B. Configure a private hosted zone with conditional forwarding.
- C. Update the subnet route table with a route to the interface endpoint.
- D. Configure the security group on the interface endpoint to allow access.

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
B is correct. When Private DNS is enabled for an interface endpoint, AWS automatically updates the public service DNS names (e.g., s3.amazonaws.com) to resolve to private IPs inside the VPC. This ensures all traffic stays within the AWS network and complies with the private IP policy.
* A is not necessary - VPC endpoints already route via local network.
* C only affects security group rules, not DNS resolution.
* D is unnecessary unless using custom DNS resolution systems.
References:
VPC Endpoints and Private DNS

NEW QUESTION # 587

A company wants to migrate its workloads from on premises to AWS. The workloads run on Linux and Windows. The company has a large on-premises infrastructure that consists of physical machines and VMs that host numerous applications.

The company must capture details about the system configuration, system performance, running processes, and network connections

of its on-premises workloads. The company also must divide the on-premises applications into groups for AWS migrations. The company needs recommendations for Amazon EC2 instance types so that the company can run its workloads on AWS in the most cost-effective manner.

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

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

Answer: A,B,C

Explanation:
https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-agent.html
https://docs.aws.amazon.com/migrationhub/latest/ug/ec2-recommendations.html

NEW QUESTION # 588
......