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.passapply.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 recently deployed an application on AWS. The application uses Amazon DynamoDB. The company measured the application load and configured the RCUs and WCUs on the DynamoDB table to match the expected peak load. The peak load occurs once a week for a 4-hour period and is double the average load. The application load is close to the average load tor the rest of the week. The access pattern includes many more writes to the table than reads of the table.

A solutions architect needs to implement a solution to minimize the cost of the table.

Which solution will meet these requirements?

A. Use AWS Application Auto Scaling to increase capacity during the peak period. Purchase reserved RCUs and WCUs to match the average load.

B. Configure on-demand capacity mode for the table.

C. Configure DynamoDB Accelerator (DAX) in front of the table. Reduce the provisioned read capacity to match the new peak load on the table.

D. Configure DynamoDB Accelerator (DAX) in front of the table. Configure on-demand capacity mode for the table.

Correct Answer: A

on-demand prices can be 7 times higher, given the options it is better to have reserved WCU and RCU and auto scale in the given schedule

QUESTION 2

A company wants to use AWS to create a business continuity solution in case the company\\'s main on-premises application fails.

The application runs on physical servers that also run other applications. The on-premises application that the company is planning to migrate uses a MySQL database as a data store. All the company\\'s on-premises applications use operating systems that are compatible with Amazon EC2.

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

A. Install the AWS Replication Agent on the source servers, including the MySQL servers. Set up replication for all servers. Launch test instances for regular drills. Cut over to the test instances to fail over the workload in the case of a failure event.

B. Install the AWS Replication Agent on the source servers, including the MySQL servers. Initialize AWS Elastic Disaster Recovery in the target AWS Region. Define the launch settings. Frequently perform failover and fallback from the most recent point in time.

C. Create AWS Database Migration Service (AWS DMS) replication servers and a target Amazon Aurora MySQL DB cluster to host the database. Create a DMS replication task to copy the existing data to the target DB cluster. Create a local AWS Schema Conversion Tool (AWS SCT) change data capture (CDC) task to keep the data synchronized. Install the rest of the software on EC2 instances by starting with a compatible base AMI.

D. Deploy an AWS Storage Gateway Volume Gateway on premises. Mount volumes on all on-premises servers. Install the application and the MySQL database on the new volumes. Take regular snapshots. Install all the software on EC2

Instances by starting with a compatible base AMI. Launch a Volume Gateway on an EC2 instance. Restore the volumes from the latest snapshot. Mount the new volumes on the EC2 instances in the case of a failure event.

Correct Answer: B

This is not an on premise migration use case which prompts for answer C. Its a current situation of on premise application which the company wants to continue its state in the requirement of using AWS as DR solution.

https://docs.aws.amazon.com/images/drs/latest/userguide/images/drs-failback-arc.png
https://docs.aws.amazon.com/drs/latest/userguide/what-is-drs.html

QUESTION 3

A retail company needs to provide a series of data files to another company. which is its business partner. These files are saved in an Amazon S3 bucket under Account A. which belongs to the retail company. The business partner company wants one of its IAM users User_DataProcessor to access the files from its own AWS account (Account B)

Which combination of steps must the companies take so that User_DataProcessor can access the S3 bucket successfully? (Select TWO.)

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

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

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

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

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

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

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

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

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

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Correct Answer: CD

https://aws.amazon.com/premiumsupport/knowledge-center/cross-account- access-s3/

QUESTION 4

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

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

A. Create an Amazon Elastic File System (Amazon EFS) file system and a mount target for each subnet that contains nodes in the EKS cluster. Configure the ReplicaSet to mount the file system. Direct the application to store files in the file system. Configure AWS Backup to back up and retain copies of the data for 1 year.

B. Create an Amazon Elastic Block Store (Amazon EBS) volume. Enable the EBS Multi- Attach feature. Configure the ReplicaSet to mount the EBS volume. Direct the application to store files in the EBS volume. Configure AWS Backup to back up and retain copies of the data for 1 year.

C. Create an Amazon S3 bucket. Configure the ReplicaSet to mount the S3 bucket. Direct the application to store files in the S3 bucket. Configure S3 Versioning to retain copies of the data. Configure an S3 Lifecycle policy to delete objects after 1 year.

D. Configure the ReplicaSet to use the storage available on each of the running application pods to store the files locally. Use a third-party tool to back up the EKS cluster for 1 year.

Correct Answer: A

In the past, EBS can be attached only to one ec2 instance but not anymore but there are limitations like - it works only on io1/io2 instance types and many others as described here. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ ebs-volumes-multi.html EFS has shareable storage In terms of performance, Amazon EFS is optimized for workloads that require high levels of aggregate throughput and IOPS, whereas EBS is optimized for low- latency, random access I/O operations. Amazon EFS is designed to scale throughput and capacity automatically as your storage needs grow, while EBS volumes can be resized on demand.

QUESTION 5

A company operates an on-premises software-as-a-service (SaaS) solution that ingests several files daily. The company provides multiple public SFTP endpoints to its customers to facilitate the file transfers. The customers add the SFTP endpoint IP addresses to their firewall allow list for outbound traffic. Changes to the SFTP endmost IP addresses are not permitted.

The company wants to migrate the SaaS solution to AWS and decrease the operational overhead of the file transfer service.

Which solution meets these requirements?

A. Register the customer-owned block of IP addresses in the company\\'s AWS account. Create Elastic IP addresses from the address pool and assign them to an AWS Transfer for SFTP endpoint. Use AWS Transfer to store the files in Amazon S3.

B. Add a subnet containing the customer-owned block of IP addresses to a VPC Create Elastic IP addresses from the address pool and assign them to an Application Load Balancer (ALB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the ALB. Store the files in attached Amazon Elastic Block Store (Amazon EBS) volumes.

C. Register the customer-owned block of IP addresses with Amazon Route 53. Create alias records in Route 53 that point to a Network Load Balancer (NLB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the NLB. Store the files in Amazon S3.

D. Register the customer-owned block of IP addresses in the company\\'s AWS account. Create Elastic IP addresses from the address pool and assign them to an Amazon S3 VPC endpoint. Enable SFTP support on the S3 bucket.

Correct Answer: A

Bring your own IP addresses (BYOIP) You can bring part or all of your publicly routable IPv4 or IPv6 address range from your on-premises network to your AWS account. You continue to own the address range, but AWS advertises it on

the internet by default. After you bring the address range to AWS, it appears in your AWS account as an address pool. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-byoip.html AWS Transfer for SFTP enables you to easily move your file transfer workloads that use the Secure Shell File Transfer Protocol (SFTP) to AWS without needing to modify your applications or manage any SFTP servers. https://aws.amazon.com/about-aws/whats-new/2018/11/aws-transfer-for-sftp-fully-managed-sftp-for-s3/

QUESTION 6

A company has an application that sells tickets online and experiences bursts of demand every 7 days. The application has a stateless presentation layer running on Amazon EC2. an Oracle database to store unstructured data catalog information, and a backend API layer. The front-end layer uses an Elastic Load Balancer to distribute the load across nine On-Demand Instances over three Availability Zones (AZs). The Oracle database is running on a single EC2 instance. The company is experiencing performance issues when running more than two concurrent campaigns. A solutions architect must design a solution that meets the following requirements:

Address scalability issues. Increase the level of concurrency. Eliminate licensing costs. Improve reliability.

Which set of steps should the solutions architect take?

A. Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs. Convert the Oracle database into a single Amazon RDS reserved DB instance.

B. Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs. Create two additional copies of the database instance, then distribute the databases in separate AZs.

C. Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs. Convert the tables in the Oracle database into Amazon DynamoDB tables.

D. Convert the On-Demand Instances into Spot Instances to reduce costs for the front end. Convert the tables in the Oracle database into Amazon DynamoDB tables.

Correct Answer: C

Combination of On-Demand and Spot Instances + DynamoDB.

QUESTION 7

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

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

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

A. Create an Amazon CloudWatch alarm that monitors server access. Set a threshold based on access by IP address. Configure an alarm action that adds the IP address to the web ACL\\'s deny list.

B. Deploy AWS Shield Advanced in addition to AWS WAF. Add the ALB as a protected resource.

C. Create an Amazon CloudWatch alarm that monitors user IP addresses. Set a threshold based on access by IP address. Configure the alarm to invoke an AWS Lambda function to add a deny rule in the application server\\'s subnet

route table for any IP addresses that activate the alarm.

D. Inspect access logs to find a pattern of IP addresses that launched the attacks. Use an Amazon Route 53 geolocation routing policy to deny traffic from the countries that host those IP addresses.

Correct Answer: C

"The AWS WAF API supports security automation such as blacklisting IP addresses that exceed request limits, which can be useful for mitigating HTTP flood attacks." > https://aws.amazon.com/blogs/security/how-to-protect-dynamic-webapplications-against- ddos-attacks-by-using-amazon-cloudfront-and-amazon-route-53/

QUESTION 8

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 tie system on premises, and the application servers connect to the shared We system through SMB.

A solutions architect must implement a solution that uses an Amazon S3 bucket tor shared storage Until the application Is fully migrated and code is rewritten to use native Amazon S3 APIs, the application must continue to have access to the data through SMB The solutions architect must migrate the application data to AWS to its new location while still allowing the on-premises application to access the data.

Which solution will meet these requirements?

A. Create a new Amazon FSx for Windows File Server fie system Configure AWS DataSync with one location tor 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 Me gateway on an on-premises VM. Create a new file share that stores data in the S3 bucket and is associated with the tie gateway. Copy the data from the on-premises storage to the new file gateway endpoint.

Correct Answer: A

QUESTION 9

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

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

Which solution will meet these requirements?

A. Create an AWS Cost and Usage Report for the organization. Define tags and cost categories in the report. Create a table in Amazon Athena. Create an Amazon QuickSight dataset based on the Athena table. Share the dataset with the

finance team.

B. Create an AWS Cost and Usage Report for the organization. Define tags and cost categories in the report. Create a specialized template in AWS Cost Explorer that the finance department will use to build reports.

C. Create an Amazon QuickSight dataset that receives spending information from the AWS Price List Query API. Share the dataset with the finance team.

D. Use the AWS Price List Query API to collect account spending information. Create a specialized template in AWS Cost Explorer that the finance department will use to build reports.

Correct Answer: A

Creating an AWS Cost and Usage Report for the organization and defining tags and cost categories in the report will allow for detailed cost reporting for the different companies that have been consolidated into one organization. By creating a table in Amazon Athena and an Amazon QuickSight dataset based on the Athena table, the finance team will be able to easily query and generate reports on the costs for all the companies. The dataset can then be shared with the finance team for them to use for their reporting needs.

Option B is not correct because it does not provide a way to query and generate reports on the costs for all the companies.

Option C is not correct because it only provides spending information from the AWS Price List Query API and does not provide detailed cost reporting for the different companies.

Option D is not correct because it only uses the AWS Price List Query API and does not provide a way to query and generate reports on the costs for all the companies.

QUESTION 10

A company that tracks medical devices in hospitals wants to migrate its existing storage solution to the AWS Cloud. The company equips all of its devices with sensors that collect location and usage information. This sensor data is sent in unpredictable patterns with large spikes. The data is stored in a MySQL database running on premises at each hospital. The company wants the cloud storage solution to scale with usage.

The company\\'s analytics team uses the sensor data to calculate usage by device type and hospital. The team needs to keep analysis tools running locally while fetching data from the cloud. The team also needs to use existing Java application and SQL queries with as few changes as possible.

How should a solutions architect meet these requirements while ensuring the sensor data is secure?

A. Store the data in an Amazon Aurora Serverless database. Serve the data through a Network Load Balancer (NLB). Authenticate users using the NLB with credentials stored in AWS Secrets Manager.

B. Store the data in an Amazon S3 bucket. Serve the data through Amazon QuickSight using an IAM user authorized with AWS Identity and Access Management (IAM) with the S3 bucket as the data source.

C. Store the data in an Amazon Aurora Serverless database. Serve the data through the Aurora Data API using an IAM user authorized with AWS Identity and Access Management (IAM) and the AWS Secrets Manager ARN.

D. Store the data in an Amazon S3 bucket. Serve the data through Amazon Athena using AWS PrivateLink to secure the data in transit.

Correct Answer: C

https://aws.amazon.com/blogs/aws/new-data-api-for-amazon-aurora- serverless/
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/data-api.html

https://aws.amazon.com/blogs/aws/aws-privatelink-for-amazon-s3-now-available/

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/data-api.html#data- api.access The data is currently stored in a MySQL database running on-prem. Storing MySQL data in S3 doesn\\'t sound good so B and D are out. Aurora Data API "enables the SQL HTTP endpoint, a connectionless Web Service API for running SQL queries against this database. When the SQL HTTP endpoint is enabled, you can also query your database from inside the RDS console (these features are free to use)."

QUESTION 11

A company that provisions job boards for a seasonal workforce is seeing an increase in traffic and usage. The backend services run on a pair of Amazon EC2 instances behind an Application Load Balancer with Amazon DynamoDB as the datastore. Application read and write traffic is slow during peak seasons.

Which option provides a scalable application architecture to handle peak seasons with the LEAST development effort?

A. Migrate the backend services to AWS Lambda. Increase the read and write capacity of DynamoDB.

B. Migrate the backend services to AWS Lambda. Configure DynamoDB to use global tables.

C. Use Auto Scaling groups for the backend services. Use DynamoDB auto scaling.

D. Use Auto Scaling groups for the backend services. Use Amazon Simple Queue Service (Amazon SQS) and an AWS Lambda function to write to DynamoDB.

Correct Answer: C

Option C is correct because using Auto Scaling groups for the backend services allows the company to scale up or down the number of EC2 instances based on the demand and traffic. This way, the backend services can handle more requests during peak seasons without compromising performance or availability. Using DynamoDB auto scaling allows the company to adjust the provisioned read and write capacity of the table or index automatically based on the actual traffic patterns. This way, the table or index can handle sudden increases or decreases in workload without throttling or overprovisioning1. Option A is incorrect because migrating the backend services to AWS Lambda may require significant development effort to rewrite the code and test the functionality. Moreover, increasing the read and write capacity of DynamoDB manually may not be efficient or cost-effective, as it does not account for the variability of the workload. The company may end up paying for unused capacity or experiencing throttling if the workload exceeds the provisioned capacity1. Option B is incorrect because migrating the backend services to AWS Lambda may require significant development effort to rewrite the code and test the functionality. Moreover, configuring DynamoDB to use global tables may not be necessary or beneficial for the company, as global tables are mainly used for replicating data across multiple AWS Regions for fast local access and disaster recovery. Global tables do not automatically scale the provisioned capacity of each replica table; they still require manual or auto scaling settings2. Option D is incorrect because using Amazon Simple Queue Service (Amazon SQS) and an AWS Lambda function to write to DynamoDB may introduce additional complexity and latency to the application architecture. Amazon SQS is a message queue service that decouples and coordinates the components of a distributed system. AWS Lambda is a serverless compute service that runs code in response to events. Using these services may require significant development effort to integrate them with the backend services and DynamoDB. Moreover, they may not improve the read performance of DynamoDB, which may also be affected by high traffic3.

References: Auto Scaling groups DynamoDB auto scaling AWS Lambda DynamoDB global tables AWS Lambda vs EC2: Comparison of AWS Compute Resources - Simform Managing throughput capacity automatically with DynamoDB auto scaling - Amazon DynamoDB AWS Aurora Global Database vs. DynamoDB Global Tables Amazon Simple Queue Service (SQS)

QUESTION 12

A company has a web application that allows users to upload short videos. The videos are stored on Amazon EBS volumes and analyzed by custom recognition software for categorization.

The website contains stat c content that has variable traffic with peaks in certain months. The architecture consists of Amazon EC2 instances running in an Auto Scaling group for the web application and EC2 instances running in an Auto Scaling group to process an Amazon SQS queue The company wants to re-architect the application to reduce operational overhead using AWS managed services where possible and remove dependencies on third-party software.

Which solution meets these requirements?

A. Use Amazon ECS containers for the web application and Spot Instances for the Auto Scaling group that processes the SQS queue. Replace the custom software with Amazon Recognition to categorize the videos.

B. Store the uploaded videos n Amazon EFS and mount the file system to the EC2 instances for Te web application. Process the SOS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.

C. Host the web application in Amazon S3. Store the uploaded videos in Amazon S3. Use S3 event notifications to publish events to the SQS queue Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.

D. Use AWS Elastic Beanstalk to launch EC2 instances in an Auto Scaling group for the web application and launch a worker environment to process the SQS queue Replace the custom software with Amazon Rekognition to categorize the videos.

Correct Answer: C

Option C is correct because hosting the web application in Amazon S3, storing the uploaded videos in Amazon S3, and using S3 event notifications to publish events to the SQS queue reduces the operational overhead of managing EC2 instances and EBS volumes. Amazon S3 can serve static content such as HTML, CSS, JavaScript, and media files directly from S3 buckets. Amazon S3 can also trigger AWS Lambda functions through S3 event notifications when new objects are created or existing objects are updated or deleted. AWS Lambda can process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos. This solution eliminates the need for custom recognition software and third-party dependencies345

References:

1: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html

2: https://aws.amazon.com/efs/pricing/
3:https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html
4:https://docs.aws.amazon.com/AmazonS3/latest/userguide/NotificationHowTo.html
5:https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html
6:https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html

QUESTION 13

A company is deploying a third-party firewall appliance solution from AWS Marketplace to monitor and protect traffic that leaves the company\\'s AWS environments. The company wants to deploy this appliance into a shared services VPC and route all outbound internet- bound traffic through the appliances.

A solutions architect needs to recommend a deployment method that prioritizes reliability and minimizes failover time

between firewall appliances within a single AWS Region. The company has set up routing from the shared services VPC to other VPCs.

Which steps should the solutions architect recommend to meet these requirements? (Select THREE.)

A. Deploy two firewall appliances into the shared services VPC, each in a separate Availability Zone.

B. Create a new Network Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Network Load Balancer. Add each of the firewall appliance instances to the target group.

C. Create a new Gateway Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Gateway Load Balancer. Add each of the firewall appliance instances to the target group.

D. Create a VPC interface endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.

E. Deploy two firewall appliances into the shared services VPC. each in the same Availability Zone.

F. Create a VPC Gateway Load Balancer endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.

Correct Answer: ACF

QUESTION 14

A company has an application that generates reports and stores them in an Amazon S3 bucket. When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company\\'s security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved.

Which set of actions will immediately remediate the security issue without impacting the application\\'s normal workflow?

A. Create an AWS Lambda function that applies a deny all policy for users who are not authenticated. Create a scheduled event to invoke the Lambda function.

B. Review the AWS Trusted Advisor bucket permissions check and implement the recommended actions.

C. Run a script that puts a private ACL on all of the objects in the bucket.

D. Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket.

Correct Answer: D

The S3 bucket is allowing public access and this must be immediately disabled. Setting the IgnorePublicAcls option to TRUE causes Amazon S3 to ignore all public ACLs on a bucket and any objects that it contains. The other settings you can configure with the Block Public Access Feature are:

1.

BlockPublicAcls - PUT bucket ACL and PUT objects requests are blocked if granting public access.

2.

BlockPublicPolicy - Rejects requests to PUT a bucket policy if granting public access.

3.

RestrictPublicBuckets - Restricts access to principles in the bucket owners\\' AWS account.
https://aws.amazon.com/s3/features/block-public-access/

QUESTION 15

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

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

A. Enable AWS Config in all accounts.

B. Enable Amazon GuardDuty in all accounts.

C. Enable all features for the organization.

D. Use AWS Firewall Manager to deploy AWS WAF rules in all accounts for all CloudFront distributions.

E. Use AWS Shield Advanced to deploy AWS WAF rules in all accounts for all CloudFront distributions.

F. Use AWS Security Hub to deploy AWS WAF rules in all accounts for all CloudFront distributions.

Correct Answer: CDE

Enabling all features for the organization will enable using AWS Firewall Manager to centrally configure and manage firewall rules across multiple AWS accounts1. Using AWS Firewall Manager to deploy AWS WAF rules in all accounts for all CloudFront distributions will enable providing baseline protection for the OWASP top 10 web application vulnerabilities2. AWS Firewall Manager supports AWS WAF rules that can help protect against common web exploits such as SQL injection and cross-site scripting3. Configuring redirection of HTTP requests to HTTPS requests in CloudFront will enable encrypting the data in transit using SSL/TLS.