



Free Questions for SAP-C02

Shared by Peterson on 19-12-2022

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)



Question 1

Question Type: MultipleChoice

A company wants to use Amazon Workspaces in combination with thin client devices to replace aging desktops. Employees use the desktops to access applications that work with clinical trial data.

a. Corporate security policy states that access to the applications must be restricted to only company branch office locations. The company is considering adding an additional branch office in the next 6 months.

Which solution meets these requirements with the MOST operational efficiency?

Options:

- A- Create an IP access control group rule with the list of public addresses from the branch offices. Associate the IP access control group with the Workspaces directory.
- B- Use AWS Firewall Manager to create a web ACL rule with an IPSet with the list of public addresses from the branch office Locations-Associate the web ACL with the Workspaces directory.
- C- Use AWS Certificate Manager (ACM) to issue trusted device certificates to the machines deployed in the branch office locations. Enable restricted access on the Workspaces directory.
- D- Create a custom Workspace image with Windows Firewall configured to restrict access to the public addresses of the branch offices. Use the image to deploy the Workspaces.

Answer:

A

Explanation:

Utilizing an IP access control group rule with the list of public addresses from branch offices and associating it with the Amazon WorkSpaces directory is the most operationally efficient solution. This method ensures that access to WorkSpaces is restricted to specified locations, aligning with the corporate security policy. This approach offers simplicity and flexibility, especially with the potential addition of a new branch office, as updating the IP access control group is straightforward.

Question 2

Question Type: MultipleChoice

A software development company has multiple engineers who are working remotely. The company is running Active Directory Domain Services (AD DS) on an Amazon EC2 instance. The company's security policy states that all internal, nonpublic services that are deployed in a VPC must be accessible through a VPN. Multi-factor authentication (MFA) must be used for access to a VPN.

What should a solutions architect do to meet these requirements?

Options:

- A- Create an AWS Site-to-Site VPN connection. Configure integration between a VPN and AD DS. Use an Amazon Workspaces client with MFA support enabled to establish a VPN connection.
- B- Create an AWS Client VPN endpoint. Create an AD Connector directory for integration with AD DS. Enable MFA for AD Connector. Use AWS Client VPN to establish a VPN connection.
- C- Create multiple AWS Site-to-Site VPN connections by using AWS VPN CloudHub. Configure integration between AWS VPN CloudHub and AD DS. Use AWS Copilot to establish a VPN connection.
- D- Create an Amazon WorkLink endpoint. Configure integration between Amazon WorkLink and AD DS. Enable MFA in Amazon WorkLink. Use AWS Client VPN to establish a VPN connection.

Answer:

B

Explanation:

Setting up an AWS Client VPN endpoint and integrating it with Active Directory Domain Services (AD DS) using an AD Connector directory enables secure remote access to internal services deployed in a VPC. Enabling multi-factor authentication (MFA) for AD Connector enhances security by adding an additional layer of authentication. This solution meets the company's requirements for secure remote access through a VPN with MFA, ensuring that the security policy is adhered to while providing a seamless experience for the remote engineers.

Question 3

Question Type: MultipleChoice

A company wants to migrate virtual Microsoft workloads from an on-premises data center to AWS. The company has successfully tested a few sample workloads on AWS. The company also has created an AWS Site-to-Site VPN connection to a VPC. A solutions architect needs to generate a total cost of ownership (TCO) report for the migration of all the workloads from the data center.

Simple Network Management Protocol (SNMP) has been enabled on each VM in the data center. The company cannot add more VMs in the data center and cannot install additional software on the VMs. The discovery data must be automatically imported into AWS Migration Hub.

Which solution will meet these requirements?

Options:

- A- Use the AWS Application Migration Service agentless service and the AWS Migration Hub Strategy Recommendations to generate the TCO report.
- B- Launch a Windows Amazon EC2 instance. Install the Migration Evaluator agentless collector on the EC2 instance. Configure Migration Evaluator to generate the TCO report.
- C- Launch a Windows Amazon EC2 instance. Install the Migration Evaluator agentless collector on the EC2 instance. Configure Migration Hub to generate the TCO report.
- D- Use the AWS Migration Readiness Assessment tool inside the VPC. Configure Migration Evaluator to generate the TCO report.

Answer:

A

Explanation:

AWS Application Migration Service:

AWS Application Migration Service (MGN) facilitates the migration of virtual machines (VMs) to AWS without installing additional software on the VMs. This agentless service helps in seamlessly migrating workloads to AWS.

AWS Migration Hub Strategy Recommendations:

AWS Migration Hub Strategy Recommendations offer insights and guidance for planning and implementing migration strategies. It helps in generating a Total Cost of Ownership (TCO) report by automatically importing discovery data from the VMs.

Generating the TCO Report:

The combined use of AWS Application Migration Service and Migration Hub Strategy Recommendations enables the automatic import of discovery data and the generation of an accurate TCO report, ensuring a smooth and cost-effective migration process.

Reference

[AWS Migration Hub Strategy Recommendations \(AWS Documentation\)](#).

Question 4

Question Type: MultipleChoice

A company is using an on-premises Active Directory service for user authentication. The company wants to use the same authentication service to sign in to the company's AWS accounts, which are using AWS Organizations. AWS Site-to-Site VPN connectivity already exists between the on-premises environment and all the company's AWS accounts.

The company's security policy requires conditional access to the accounts based on user groups and roles. User identities must be managed in a single location.

Which solution will meet these requirements?

Options:

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

Answer:

D

Explanation:

<https://aws.amazon.com/blogs/aws/new-attributes-based-access-control-with-aws-single-sign-on/>

Question 5

Question Type: MultipleChoice

A company is planning to migrate its on-premises transaction-processing application to AWS. The application runs inside Docker containers that are hosted on VMS in the company's data center. The Docker containers have shared storage where the application records transaction data.

The transactions are time sensitive. The volume of transactions inside the application is unpredictable. The company must implement a low-latency storage solution that will automatically scale throughput to meet increased demand. The company cannot develop the application further and cannot continue to administer the Docker hosting environment.

How should the company migrate the application to AWS to meet these requirements?

Options:

- A- Migrate the containers that run the application to Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon S3 to store the transaction data that the containers share.
- B- Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic File System (Amazon EFS) file system. Create a Fargate task definition. Add a volume to the task definition to point to the EFS file system
- C- Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic Block Store (Amazon EBS) volume. Create a Fargate task definition. Attach the EBS volume to each running task.
- D- Launch Amazon EC2 instances. Install Docker on the EC2 instances. Migrate the containers to the EC2 instances. Create an Amazon Elastic File System (Amazon EFS) file system. Add a mount point to the EC2 instances for the EFS file system.

Answer:

B

Explanation:

Migrating the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS) will meet the requirement of not administering the Docker hosting environment. AWS Fargate is a serverless compute engine that runs containers without requiring any infrastructure management³. Creating an Amazon Elastic File System (Amazon EFS) file

system and adding a volume to the Fargate task definition to point to the EFS file system will meet the requirement of low-latency storage that will automatically scale throughput to meet increased demand. Amazon EFS is a fully managed file system service that provides shared access to data from multiple containers, supports NFSv4 protocol, and offers consistent performance and high availability⁴. Amazon EFS also supports automatic scaling of throughput based on the amount of data stored in the file system⁵.

Question 6

Question Type: MultipleChoice

A company is planning a migration from an on-premises data center to the AWS cloud. The company plans to use multiple AWS accounts that are managed in an organization in AWS organizations. The company will cost a small number of accounts initially and will add accounts as needed. A solution architect must design a solution that turns on AWS accounts.

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

Options:

- A- Create an AWS Lambda function that creates a new cloudTrail trail in all AWS account in the organization. Invoke the Lambda function dally by using a scheduled action in Amazon EventBridge.
- B- Create a new CloudTrail trail in the organizations management account. Configure the trail to log all events for all AYYs accounts in the organization.
- C- Create a new CloudTrail trail in all AWS accounts in the organization. Create new trails whenever a new account is created.
- D- Create an AWS systems Manager Automaton runbook that creates a cloud trail in all AWS accounts in the organization. Invoke the automation by using Systems Manager State Manager.

Answer:

B

Explanation:

The most operationally efficient solution for turning on AWS CloudTrail across multiple AWS accounts managed within an AWS Organization is to create a single CloudTrail trail in the organization's management account and configure it to log events for all accounts within the organization. This approach leverages CloudTrail's ability to consolidate logs from all accounts in an organization, thereby simplifying management, reducing overhead, and ensuring consistent

logging across accounts. This method eliminates the need for manual intervention in each account, making it an operationally efficient choice for organizations planning to scale their AWS usage.

AWS CloudTrail Documentation: Provides detailed instructions on setting up CloudTrail, including how to configure it for an organization.

AWS Organizations Documentation: Offers insights into best practices for managing multiple AWS accounts and how services like CloudTrail integrate with AWS Organizations.

AWS Best Practices for Security and Governance: Guides on how to effectively use AWS services to maintain a secure and well-governed AWS environment, with a focus on centralized logging and monitoring.



To Get Premium Files for SAP-C02 Visit

<https://www.p2pexams.com/products/sap-c02>

For More Free Questions Visit

<https://www.p2pexams.com/amazon/pdf/sap-c02>

20%
DISCOUNT

P2P
exams