100% Pass Quiz Latest SCS-C02 - New AWS Certified Security - Specialty Test Papers

P.S. Free & New SCS-C02 dumps are available on Google Drive shared by Actual4Cert: https://drive.google.com/open?id=1HIDuL-4PcJ4tpYIiD6VBuBr8I9u1nxzM

To keep with such an era, when new knowledge is emerging, you need to pursue latest news and grasp the direction of entire development tendency, our SCS-C02 training questions have been constantly improving our performance. Our working staff regards checking update of our SCS-C02 preparation exam as a daily routine. After you purchase our SCS-C02 Study Materials, we will provide one-year free update for you. Within one year, we will send the latest version to your mailbox with no charge if we have a new version of SCS-C02 learning materials.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• Data Protection: AWS Security specialists learn to ensure data confidentiality and integrity for data in transit and at rest. Topics include lifecycle management of data at rest, credential protection, and cryptographic key management. These capabilities are central to managing sensitive data securely, reflecting the exam's focus on advanced data protection strategies.
Topic 2	• Infrastructure Security: Aspiring AWS Security specialists are trained to implement and troubleshoot security controls for edge services, networks, and compute workloads under this topic. Emphasis is placed on ensuring resilience and mitigating risks across AWS infrastructure. This section aligns closely with the exam's focus on safeguarding critical AWS services and environments.
Topic 3	• Management and Security Governance: This topic teaches AWS Security specialists to develop centralized strategies for AWS account management and secure resource deployment. It includes evaluating compliance and identifying security gaps through architectural reviews and cost analysis, essential for implementing governance aligned with certification standards.
Topic 4	• Threat Detection and Incident Response: In this topic, AWS Security specialists gain expertise in crafting incident response plans and detecting security threats and anomalies using AWS services. It delves into effective strategies for responding to compromised resources and workloads, ensuring readiness to manage security incidents. Mastering these concepts is critical for handling scenarios assessed in the SCS-C02 Exam.

100% Pass Quiz 2026 Amazon Newest New SCS-C02 Test Papers

If you want to get promotions or high-paying jobs in the Amazon sector, then it is important for you to crack the AWS Certified Security - Specialty (SCS-C02) certification exam. The Amazon SCS-C02 certification has become the best way to validate your skills and accelerate your tech career. SCS-C02 Exam applicants who are doing jobs or busy with their other matters usually don't have enough time to study for the test.

Amazon AWS Certified Security - Specialty Sample Questions (Q221-Q226):

NEW QUESTION # 221
A company uses SAML federation to grant users access to AWS accounts. A company workload that is in an isolated AWS account runs on immutable infrastructure with no human access to Amazon EC2. The company requires a specialized user known as a break glass user to have access to the workload AWS account and instances in the case of SAML errors. A recent audit discovered that the company did not create the break glass user for the AWS account that contains the workload.
The company must create the break glass user. The company must log any activities of the break glass user and send the logs to a security team.
Which combination of solutions will meet these requirements? (Select TWO.)

- A. Create a break glass IAM role for the account. Allow security team members to perform the AssumeRoleWithSAML operation. Create an AWS Cloud Trail trail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor security team activities.
- B. Create a local individual break glass IAM user for the security team. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor local user activities.
- C. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS Cloud Trail filter based on Session Manager. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic.
- D. Create a local individual break glass IAM user on the operating system level of each workload instance. Configure unrestricted security groups on the instances to grant access to the break glass IAM users.
- E. Create a break glass EC2 key pair for the AWS account. Provide the key pair to the security team. Use AWS CloudTrail to monitor key pair activity. Send notifications to the security team by using Amazon Simple Notification Service (Amazon SNS).

Answer: B,C

Explanation:
The combination of solutions that will meet the requirements are:
* A. Create a local individual break glass IAM user for the security team. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor local user activities. This is a valid solution because it allows the security team to access the workload AWS account and instances using a local IAM user that does not depend on SAML federation. It also enables logging and monitoring of the break glass user activities using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon EventBridge123.
* E. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS CloudTrail filter based on Session Manager. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic. This is a valid solution because it allows the security team to access the workload instances without opening any inbound ports or managing SSH keys or bastion hosts. It also enables logging and notification of the break glass user activities using AWS CloudTrail, Session Manager, and Amazon SNS456.
The other options are incorrect because:
* B. Creating a break glass EC2 key pair for the AWS account and providing it to the security team is not a valid solution, because it requires opening inbound ports on the instances and managing SSH keys, which increases the security risk and complexity7.
* C. Creating a break glass IAM role for the account and allowing security team members to perform the AssumeRoleWithSAML operation is not a valid solution, because it still depends on SAML federation, which might not work in case of SAML errors8.
* D. Creating a local individual break glass IAM user on the operating system level of each workload instance and configuring unrestricted security groups on the instances to grant access to the break glass IAM users is not a valid solution, because it requires opening inbound ports on the instances and managing multiple local users, which increases the security risk and complexity9.
References:
1: Creating an IAM User in Your AWS Account 2: Creating a Trail - AWS CloudTrail 3: Using Amazon EventBridge with AWS CloudTrail 4: Setting up Session Manager - AWS Systems Manager 5: Logging Session Manager sessions - AWS Systems Manager 6: Amazon Simple Notification Service 7: Connecting to your Linux instance using SSH - Amazon Elastic Compute Cloud 8: AssumeRoleWithSAML - AWS Security Token Service 9: IAM Users - AWS Identity and Access Management

NEW QUESTION # 222
A company uses an organization in AWS Organizations to manage its AWS accounts. The company has implemented an SCP in the root account to prevent resources from being shared with external accounts.
The company now needs to allow applications in its marketing team's AWS account to share resources with external accounts. The company must continue to prevent all the other accounts in the organization from sharing resources with external accounts. All the accounts in the organization are members of the same OU.
Which solution will meet these requirements?

- A. Edit the existing SCP to add a Condition statement that excludes the marketing team's account.
- B. Create an IAM permissions boundary policy to explicitly allow resource sharing Attach the policy to IAM users in the marketing team's account.
- C. Create a new SCP in the marketing team's account Configure the SCP to explicitly allow resource sharing.
- D. Edit the existing SCP to include an Allow statement that specifies the marketing team's account.

Answer: A

Explanation:
The SCP continues to prevent resource sharing with external accounts for all other accounts in the organization.
The marketing team's account is specifically exempted from this restriction, allowing them to share resources as needed.
Here's an example of a Condition statement that could be used:
JSON
{
"Condition": {
"StringEquals": {
"aws:PrincipalOrgID": "<marketing-team-account-id>"
}
}
}

NEW QUESTION # 223
A company is using Amazon Elastic Container Service (Amazon ECS) to run its container-based application on AWS. The company needs to ensure that the container images contain no severe vulnerabilities. The company also must ensure that only specific IAM roles and specific AWS accounts can access the container images.
Which solution will meet these requirements with the LEAST management overhead?

- A. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity- based policies to restrict access to which IAM principals and accounts can access the images.
- B. Pull images from the public container registry. Publish the images to AWS CodeArtifact repositories in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.
- C. Pull images from the public container registry. Publish the images to a private container registry that is hosted on Amazon EC2 instances in a centralized AWS account. Deploy host-based container scanning tools to EC2 instances that run Amazon ECS. Restrict access to the container images by using basic authentication over HTTPS.
- D. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account.Use a CI/CD pipeline to deploy the images to different AWS accounts. Use identity-based policies to restrict access to which IAM principals can access the images.

Answer: A

Explanation:
The correct answer is C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account.
Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity- based policies to restrict access to which IAM principals and accounts can access the images.
This solution meets the requirements because:
Amazon ECR is a fully managed container registry service that supports Docker and OCI images and artifacts1. It integrates with Amazon ECS and other AWS services to simplify the development and deployment of container-based applications.

Amazon ECR provides image scanning on push, which uses the Common Vulnerabilities and Exposures (CVEs) database from the open-source Clair project to detect software vulnerabilities in container images2.
The scan results are available in the AWS Management Console, AWS CLI, orAWS SDKs2.
Amazon ECR supports cross-account access to repositories, whichallows sharing images across multiple AWS accounts3.This can be achieved by using repository policies, which are resource-based policies that specify which IAM principals and accounts can access the repositories and what actions they can perform4.
Additionally, identity-based policies can be used to control which IAM roles in each account can access the repositories5.
The other options are incorrect because:
A: This option does not use repository policies to restrict cross-account access to the images, which is a requirement.Identity-based policies alone are not sufficient to control access to Amazon ECR repositories5.
B: This option does not use Amazon ECR, which is a fully managed service that provides image scanning and cross-account access features. Hosting a private container registry on EC2 instances would require more management overhead and additional security measures.
D:This option uses AWS CodeArtifact, which is a fully managed artifact repository service that supports Maven, npm, NuGet, PyPI, and generic package formats6. However, AWS CodeArtifact does not support Docker or OCI container images, which are required for Amazon ECS applications.

NEW QUESTION # 224
A company's AWS CloudTrail logs are all centrally stored in an Amazon S3 bucket. The security team controls the company's AWS account. The security team must prevent unauthorized access and tampering of the CloudTrail logs.
Which combination of steps should the security team take? (Choose three.)

- A. Implement least privilege access to the S3 bucket by configuring a bucket policy.
- B. Configure Access Analyzer for S3.
- C. Configure CloudTrail log file integrity validation.
- D. Compress log files with secure gzip.
- E. Create an Amazon EventBridge rule to notify the security team of any modifications on CloudTrail log files.
- F. Configure server-side encryption with AWS KMS managed encryption keys (SSE-KMS).

Answer: A,C,F

Explanation:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html

NEW QUESTION # 225
A Security Architect has been asked to review an existing security architecture and identify why the application servers cannot successfully initiate a connection to the database servers. The following summary describes the architecture:
1 An Application Load Balancer, an internet gateway, and a NAT gateway are configured in the public subnet
2. Database, application, and web servers are configured on three different private subnets.
3 The VPC has two route tables: one for the public subnet and one for all other subnets The route table for the public subnet has a 0 0 0 0/0 route to the internet gateway The route table for all other subnets has a 0 0.0.0/0 route to the NAT gateway. All private subnets can route to each other
4 Each subnet has a network ACL implemented that limits all inbound and outbound connectivity to only the required ports and protocols
5 There are 3 Security Groups (SGs) database application and web Each group limits all inbound and outbound connectivity to the minimum required Which of the following accurately reflects the access control mechanisms the Architect should verify1?

- A. Outbound SG configuration on database servers Inbound SG configuration on application servers inbound and outbound network ACL configuration on the database subnet Inbound and outbound network ACL configuration on the application server subnet
- B. Inbound SG configuration on database servers Outbound SG configuration on application servers Inbound network ACL configuration on the database subnet Outbound network ACL configuration on the application server subnet.
- C. Inbound and outbound SG configuration on database servers Inbound and outbound SG configuration on application servers Inbound network ACL configuration on the database subnet Outbound network ACL configuration on the application server subnet
- D. Inbound SG configuration on database servers
  Outbound SG configuration on application servers
  Inbound and outbound network ACL configuration on the database subnet

Inbound and outbound network ACL configuration on the application server subnet

Answer: A

Explanation:
Explanation
this is the accurate reflection of the access control mechanisms that the Architect should verify. Access control mechanisms are methods that regulate who can access what resources and how. Security groups and network ACLs are two types of access control mechanisms that can be applied to EC2 instances and subnets. Security groups are stateful, meaning they remember and return traffic that was previously allowed. Network ACLs are stateless, meaning they do not remember or return traffic that was previously allowed. Security groups and network ACLs can have inbound and outbound rules that specify the source, destination, protocol, and port of the traffic. By verifying the outbound security group configuration on database servers, the inbound security group configuration on application servers, and the inbound and outbound network ACL configuration on both the database and application server subnets, the Architect can check if there are any misconfigurations or conflicts that prevent the application servers from initiating a connection to the database servers. The other options are either inaccurate or incomplete for verifying the access control mechanisms.

NEW QUESTION # 226
.....

About some esoteric points, they illustrate with examples for you. Our SCS-C02 practice materials are the accumulation of professional knowledge worthy practicing and remembering, so you will not regret choosing our SCS-C02 practice materials. The best way to gain success is not cramming, but to master the discipline and regular exam points of question behind the tens of millions of questions. Our SCS-C02 practice materials can remove all your doubts about the exam. If you believe in our products this time, you will enjoy the happiness of success all your life.