SCS-C02 Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

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

https://www.leads4pass.com/scs-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 Security Engineer has been tasked with enabling IAM Security Hub to monitor Amazon EC2 instances fix CVE in a single IAM account The Engineer has already enabled IAM Security Hub and Amazon Inspector m the IAM Management Console and has installed me Amazon Inspector agent on an EC2 instances that need to be monitored.

Which additional steps should the Security Engineer lake 10 meet this requirement?

A. Configure the Amazon inspector agent to use the CVE rule package

B. Configure the Amazon Inspector agent to use the CVE rule package Configure Security Hub to ingest from IAM inspector by writing a custom resource policy

C. Configure the Security Hub agent to use the CVE rule package Configure IAM Inspector lo ingest from Security Hub by writing a custom resource policy

D. Configure the Amazon Inspector agent to use the CVE rule package Install an additional Integration library Allow the Amazon Inspector agent to communicate with Security Hub

Correct Answer: D

you need to configure the Amazon Inspector agent to use the CVE rule package, which is a set of rules that check for vulnerabilities and exposures on your EC2 instances. You also need to install an additional integration library that enables communication between the Amazon Inspector agent and Security Hub. Security Hub is a service that provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices. The other options are either incorrect or incomplete for meeting the requirement.

QUESTION 2

Auditors for a health care company have mandated that all data volumes be encrypted at rest Infrastructure is deployed mainly via IAM CloudFormation however third-party frameworks and manual deployment are required on some legacy systems

What is the BEST way to monitor, on a recurring basis, whether all EBS volumes are encrypted?

A. On a recurring basis, update an IAM user policies to require that EC2 instances are created with an encrypted volume

B. Configure an IAM Config rule lo run on a recurring basis \\'or volume encryption

C. Set up Amazon Inspector rules tor volume encryption to run on a recurring schedule

D. Use CloudWatch Logs to determine whether instances were created with an encrypted volume

Correct Answer: B

https://d1.IAMstatic.com/whitepapers/IAM-security-whitepaper.pdf "For example, IAM Config provides a managed IAM Config Rules to ensure that encryption is turned on for all EBS volumes in your account."

QUESTION 3

A security engineer must troubleshoot an administrator\\'s inability to make an existing Amazon S3 bucket public in an account that is part of an organization n IAM Organizations. The administrator switched the role from the master account to a member account and then attempted to make one S3 bucket public. This action was immediately denied

Which actions should the security engineer take to troubleshoot the permissions issue? (Select TWO.)

A. Review the cross-account role permissions and the S3 bucket policy Verify that the Amazon S3 block public access option in the member account is deactivated.

B. Review the role permissions m the master account and ensure it has sufficient privileges to perform S3 operations

C. Filter IAM CloudTrail logs for the master account to find the original deny event and update the cross-account role m the member account accordingly Verify that the Amazon S3 block public access option in the master account is deactivated.

D. Evaluate the SCPs covering the member account and the permissions boundary of the role in the member account for missing permissions and explicit denies.

E. Ensure the S3 bucket policy explicitly allows the s3 PutBucketPublicAccess action for the role m the member account

Correct Answer: DE

A is incorrect because reviewing the cross-account role permissions and the S3 bucket policy is not enough to troubleshoot the permissions issue. You also need to verify that the Amazon S3 block public access option in the member account

is deactivated, as well as the permissions boundary and the SCPs of the role in the member account.

D is correct because evaluating the SCPs and the permissions boundary of the role in the member account can help you identify any missing permissions or explicit denies that could prevent the administrator from making the S3 bucket

public.

E is correct because ensuring that the S3 bucket policy explicitly allows the s3 PutBucketPublicAccess action for the role in the member account can help you override any block public access settings that could prevent the administrator from

making the S3 bucket public.

QUESTION 4

A company is using AWS Organizations to manage multiple accounts. The company needs to allow an IAM user to use a role to access resources that are in another organization\\'s AWS account.

Which combination of steps must the company perform to meet this requirement? (Select TWO.)

A. Create an identity policy that allows the sts: AssumeRole action in the AWS account that contains the resources. Attach the identity policy to the IAM user.

B. Ensure that the sts: AssumeRole action is allowed by the SCPs of the organization that owns the resources that the IAM user needs to access.

C. Create a role in the AWS account that contains the resources. Create an entry in the role\\'s trust policy that allows the IAM user to assume the role. Attach the trust policy to the role.

D. Establish a trust relationship between the IAM user and the AWS account that contains the resources.

E. Create a role in the IAM user\\'s AWS account. Create an identity policy that allows the sts: AssumeRole action. Attach the identity policy to the role.

Correct Answer: BC

To allow cross-account access to resources using IAM roles, the following steps are required: Create a role in the AWS account that contains the resources (the trusting account) and specify the AWS account that contains the IAM user (the trusted account) as a trusted entity in the role\\'s trust policy. This allows users from the trusted account to assume the role and access resources in the trusting account. Ensure that the IAM user has permission to assume the role in their own AWS account. This can be done by creating an identity policy that allows the sts:AssumeRole action and attaching it to the IAM user or their group. Ensure that there are no service control policies (SCPs) in the organization that owns the resources that deny or restrict access to the sts:AssumeRole action or the role itself. SCPs are applied to all accounts in an organization and can override any permissions granted by IAM policies.

Verified References: https://repost.aws/knowledge-center/cross-account-access-iam
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accou nts_access.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

---

QUESTION 5

A company accidentally deleted the private key for an Amazon Elastic Block Store (Amazon EBS)-backed Amazon EC2 instance. A security engineer needs to regain access to the instance.

Which combination of steps will meet this requirement? (Choose two.)

A. Stop the instance. Detach the root volume. Generate a new key pair.

B. Keep the instance running. Detach the root volume. Generate a new key pair.

C. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new public key. Move the volume back to the original instance. Start the instance.

D. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new private key. Move the volume back to the original instance. Start the instance.

E. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new public key. Move the volume back to the original instance that is running.

Correct Answer: AC

If you lose the private key for an EBS-backed instance, you can regain access to your instance. You must stop the instance, detach its root volume and attach it to another instance as a data volume, modify the authorized_keys file with a new public key, move the volume back to the original instance, and restart the instance.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConne cting.html#replacing-lost-key-pai