Congratulation!! You have selected the best success partner to become

Exam overview

Level: Specialty

Length: 170 minutes to complete the exam

Cost: 300 USD

Visit **Exam pricing** for additional cost information.

Format: 65 questions; either multiple choice or multiple response

Delivery method: Pearson VUE and PSI; testing center or online proctored exam

https://aws.amazon.com/certification/certified-security-specialty/

QUESTION NO: 1

The Security team believes that a former employee may have gained unauthorized access to AWS resources sometime in the past 3 months by using an identified access key.

What approach would enable the Security team to find out what the former employee may have done within AWS?

A.
Use the AWS CloudTrail console to search for user activity.

B.
Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.

C.
Use AWS Config to see what actions were taken by the user.

D.
Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

Answer: A
Explanation:

QUESTION NO: 2

A company is storing data in Amazon S3 Glacier. The security engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock operation 12 hours ago. The audit team identified a typo in the policy that is allowing unintended access to the vault.

What is the MOST cost-effective way to correct this?

A.
Call the abort-vault-lock operation. Update the policy. Call the initiate-vault-lock operation again.

B.
Copy the vault data to a new S3 bucket. Delete the vault. Create a new vault with the data.

C.
Update the policy to keep the vault lock in place.

D.
Update the policy. Call initiate-vault-lock operation again to apply the new policy.

Answer: A

Explanation:

Initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. While in the in-progress state, you have 24 hours to validate your vault lock policy before the lock ID expires.

Use the lock ID to complete the lock process. If the vault lock policy doesn't work as expected, you can abort the lock and restart from the beginning. For information on how to use the S3 Glacier API to lock a vault, see Locking a Vault by Using the Amazon S3 Glacier API.

Reference: https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html

QUESTION NO: 3

A company wants to control access to its AWS resources by using identities and groups that are defined in its existing Microsoft Active Directory.

What must the company create in its AWS account to map permissions for AWS services to Active Directory user attributes?

A.
AWS IAM groups

B.
AWS IAM users

C.
AWS IAM roles

D.
AWS IAM access keys

Answer: C
Reference:

https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/

QUESTION NO: 4

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

A.
The external ID used by the Auditor is missing or incorrect.

B.
The Auditor is using the incorrect password.

C.
The Auditor has not been granted sts:AssumeRole for the role in the destination account.

D.
The Amazon EC2 role used by the Auditor must be set to the destination account role.

E.
The secret key used by the Auditor is missing or incorrect.

F.
The role ARN used by the Auditor is missing or incorrect.

Answer: C,E,F
Reference:

https://aws.amazon.com/ru/blogs/security/how-to-use-external-id-when-granting-access-to-your-aws-resources/

QUESTION NO: 5

Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.

Which of the following solutions will meet these requirements?

A.

Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.

B.
Route all traffic through a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.

C.
Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.

D.
Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer and the EC2 instances.

Answer: B
Explanation:

QUESTION NO: 6

An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.

How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

A.
Configure the application's EC2 instances to use NAT gateways for all inbound traffic.

B.
Move the web servers to private subnets without public IP addresses.

C.
Configure AWS WAF to provide DDoS attack protection for the ALB.

D.
Require all inbound network traffic to route through a bastion host in the private subnet.

E.
Require all inbound and outbound network traffic to route through an AWS Direct Connect connection.

Answer: B,C

Explanation:

QUESTION NO: 7

A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational AWS resource purposes.

How can the Administrator restrict usage of member root user accounts across the organization?

A.
Disable the use of the root user account at the organizational root. Enable multi-factor authentication of the root user account for each organizational member account.

B.
Configure IAM user policies to restrict root account capabilities for each Organizations member account.

C.
Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root user. Add all operational accounts to the new OU.

D.
Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

Answer: C
Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_about-scps.html

QUESTION NO: 8

A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards.

The mail application should be configured to connect to which of the following endpoints and

corresponding ports?

A.
email.us-east-1.amazonaws.com over port 8080

B.
email-pop3.us-east-1.amazonaws.com over port 995

C.
email-smtp.us-east-1.amazonaws.com over port 587

D.
email-imap.us-east-1.amazonaws.com over port 993

Answer: C
Reference:

https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html

QUESTION NO: 9

A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside AWS (Account 1). The threat was documented as follows:

Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an AWS account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.

Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.

Which of the following options will mitigate the threat? (Choose two.)

A.
Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.

B.
Block outbound access to public S3 endpoints on the proxy server.

C.
Configure Network ACLs on Server X to deny access to S3 endpoints.

D.
Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.

E.
Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

Answer: A,C
Explanation:

QUESTION NO: 10

A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of “Sensitive," “Confidential," and “Restricted." The security solution must meet all of the following requirements:

- Each object must be encrypted using a unique key.
- Items that are stored in the “Restricted" bucket require two-factor authentication for decryption.
- AWS KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

A.
Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annually. For the “Restricted" CMK, define the MFA policy within the key policy. Use S3 SSE-KMS to encrypt the objects.

B.
Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to true. S3 can then use the grants to encrypt each object with a unique CMK.

C.
Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA policy. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.

D.