AWS Certified Security - Specialty

1. The Security Engineer implemented a new vault lock policy for 10TB of data and called initiatevault-lock 12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault. What is the MOST cost-effective way to correct this?

A. A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.

B. B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.

C. C. Update the policy, keeping the vault lock in place.

D. D. Update the policy and call initiate-vault-lock again to apply the new policy.

Answer(s): A

---

2. 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. A. AWS IAM groups

B. B. AWS IAM users

C. C. AWS IAM roles

D. D. AWS IAM access keys

Answer(s): C

---

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

B. B. The Auditor is using the incorrect password.

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

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

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

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

Answer(s): A C F

---

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

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

D. 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(s): B

---

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

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

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

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

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

Answer(s): B C

---

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

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

Answer(s): C

---

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

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

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

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

Answer(s): C

---

8. 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:

A. 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.)

Answer(s): A D

---

9. 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. 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. 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. 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. D. Create a CMK with unique imported key material for each data classification type, and rotate them annually. For the “Restricted” key material, define the MFA policy in the key policy. Use S3 SSE-KMS to encrypt the objects

Answer(s): A

---

10. An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, AWS Lambda functions must issue queries to the RDS database by using the same database credentials. The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom. What should the Security Engineer do to meet these requirements?

A. A. Store the database credentials in AWS Key Management Service (AWS KMS). Create an IAM role with access to AWS KMS by using the EC2 and Lambda service principals in the role trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances. Set up Lambda to use the new role for execution.

B. B. Store the database credentials in AWS KMS. Create an IAM role with access to KMS by using the EC2 and Lambda service principals in the role trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances and the Lambda function.

C. C. Store the database credentials in AWS Secrets Manager. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances and the Lambda function.

D. D. Store the database credentials in AWS Secrets Manager. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances. Set up Lambda to use the new role for execution.

Answer(s): D

---

11. A company has a customer master key (CMK) with imported key materials. Company policy requires that all encryption keys must be rotated every year. What can be done to implement the

above policy?

A. A. Enable automatic key rotation annually for the CMK.

B. B. Use AWS Command Line Interface to create an AWS Lambda function to rotate the existing CMK annually.

C. C. Import new key material to the existing CMK and manually rotate the CMK.

D. D. Create a new CMK, import new key material to it, and point the key alias to the new CMK.

E.

Answer(s): D

---

12. A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials. An operational safety policy requires that access to specific credentials is independently auditable. What is the MOST cost-effective way to manage the storage of credentials?

A. A. Use AWS Systems Manager to store the credentials as Secure Strings Parameters. Secure by using an AWS KMS key.

B. B. Use AWS Key Management System to store a master key, which is used to encrypt the credentials. The encrypted credentials are stored in an Amazon RDS instance.

C. C. Use AWS Secrets Manager to store the credentials.

D. D. Store the credentials in a JSON file on Amazon S3 with server-side encryption.

Answer(s): A

---

13. An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing. Which steps should be taken to troubleshoot the issue? (Choose two.)

A. A. Use an EC2 run command to confirm that the “awslogs” service is running on all instances.

B. B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.

C. C. Check whether any application log entries were rejected because of invalid time stamps by reviewing /var/cwlogs/rejects.log.

D. D. Check that the trust relationship grants the service “cwlogs.amazonaws.com” permission to write objects to the Amazon S3 staging bucket.

E. E. Verify that the time zone on the application servers is in UTC.

Answer(s): A B

---

14. A Security Engineer must design a solution that enables the Incident Response team to audit for changes to a user’s IAM permissions in the case of a security incident. How can this be accomplished?

A. A. Use AWS Config to review the IAM policy assigned to users before and after the incident.

B. B. Run the GenerateCredentialReport via the AWS CLI, and copy the output to Amazon S3 daily for auditing purposes.

C. C. Copy AWS CloudFormation templates to S3, and audit for changes from the template.

D. D. Use Amazon EC2 Systems Manager to deploy images, and review AWS CloudTrail logs for changes.

Answer(s): A

---

15. A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs). What mechanism will allow the company to implement all required network rules without incurring additional cost?

A. A. Configure AWS WAF rules to implement the required rules.

B. B. Use the operating system built-in, host-based firewall to implement the required rules.

C. C. Use a NAT gateway to control ingress and egress according to the requirements.

D. D. Launch an EC2-based firewall product from the AWS Marketplace, and implement the required rules in that product.

Answer(s): B

---

16. A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation. What should the Security Engineer use to isolate and research this event? (Choose three.)

A. A. AWS CloudTrail

B. B. Amazon Athena

C. C. AWS Key Management Service (AWS KMS)

D. D. VPC Flow Logs

E. E. AWS Firewall Manager

F. F. Security groups

Answer(s): A D F

---

17. A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements: Users may access the website by using an Amazon CloudFront distribution. Users may not access the website directly by using an Amazon S3 URL. Which configurations will support these requirements? (Choose two.)

A. A. Associate an origin access identity with the CloudFront distribution.

B. B. Implement a “Principal”: “cloudfront.amazonaws.com” condition in the S3 bucket policy.

C. C. Modify the S3 bucket permissions so that only the origin access identity can access the bucket contents.

D. D. Implement security groups so that the S3 bucket can be accessed only by using the intended CloudFront distribution.

E. E. Configure the S3 bucket policy so that it is accessible only through VPC endpoints, and place the CloudFront distribution into the specified VPC.

Answer(s): A C

---

18. A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months. What would be the BEST way to reduce the potential impact of these attacks in the future?

A. A. Use custom route tables to prevent malicious traffic from routing to the instances.

B. B. Update security groups to deny traffic from the originating source IP addresses.

C. C. Use network ACLs.

D. D. Install intrusion prevention software (IPS) on each instance.

Answer(s): D

---

19. A company requires that IP packet data be inspected for invalid or malicious content. Which of the following approaches achieve this requirement? (Choose two.)

A. A. Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through it. Perform inspection within proxy software on the EC2 instance.

B. B. Configure the host-based agent on each EC2 instance within the VPC. Perform inspection within the host-based agent.

C. C. Enable VPC Flow Logs for all subnets in the VPC. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.

D. D. Configure Elastic Load Balancing (ELB) access logs. Perform inspection from the log data within the ELB access log files.

E. E. Configure the CloudWatch Logs agent on each EC2 instance within the VPC. Perform inspection from the log data within CloudWatch Logs.

Answer(s): A B

---

20. An organization has a system in AWS that allows a large number of remote workers to submit data files. File sizes vary from a few kilobytes to several megabytes. A recent audit highlighted a concern that data files are not encrypted while in transit over untrusted networks. Which solution would remediate the audit finding while minimizing the effort required?

A. A. Upload an SSL certificate to IAM, and configure Amazon CloudFront with the passphrase for the private key.

B. B. Call KMS.Encrypt() in the client, passing in the data file contents, and call KMS.Decrypt() serverside.

C. C. Use AWS Certificate Manager to provision a certificate on an Elastic Load Balancing in front of the web service’s servers.

D. D. Create a new VPC with an Amazon VPC VPN endpoint, and update the web service’s DNS record.

Answer(s): C
