AWS Certified Security - Specialty

1. You have an S3 bucket defined in IAM. You want to ensure that you encrypt the data before sending it across the wire.
What is the best way to achieve this.

A. Enable server side encryption for the S3 bucket. This request will ensure that the data is encrypted first.

B. Use the IAM Encryption CLI to encrypt the data first.

C. Use a Lambda function to encrypt the data before sending it to the S3 bucket.

D. Enable client encryption for the bucket.

Answer(s): B

---

2. Your company has a set of EC2 Instances defined in IAM. These Ec2 Instances have strict security groups attached to them. You need to ensure that changes to the Security groups are noted and acted on accordingly. How can you achieve this?

A. Use Cloudwatch logs to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS for the notification.

B. Use Cloudwatch metrics to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS for the notification.

C. Use IAM inspector to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS f the notification.

D. Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well.

Answer(s): D

---

3. Your company has just set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server.
Which of the below options is best suited to achieve this requirement.

A. Set up VPC peering between the central server VPC and each of the teams VPCs.

B. Set up IAM DirectConnect between the central server VPC and each of the teams VPCs.

C. Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.

D. None of the above options will work.

Answer(s): A

---

4. There is a requirement for a company to transfer large amounts of data between IAM and an on- premise location. There is an additional requirement for low latency and high consistency traffic to IAM. Given these requirements how would you design a hybrid architecture?
Choose the correct answer from the options below.

A. Provision a Direct Connect connection to an IAM region using a Direct Connect partner.

B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.

C. Create an iPSec tunnel for private connectivity, which increases network consistency and reduces latency.

D. Create a VPC peering connection between IAM and the Customer gateway.

Answer(s): A

---

5. Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.

A.

B.

C.

D.

Answer(s): A

---

6. A company's IAM account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?

A. Create a new role and add each user to the IAM role.

B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group.

C. Create a policy and apply it to multiple users using a JSON script.

D. Create an S3 bucket policy with unlimited access which includes each user's IAM account ID

Answer(s): B

---

7. You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?

A. Add an IAM managed policy for the user.

B. Add a service policy for the user.

C. Add an IAM role for the user.

D. Add an inline policy for the user.

Answer(s): D

---

8. Your company is planning on using bastion hosts for administering the servers in IAM. Which of the following is the best description of a bastion host from a security perspective?

A. A Bastion host should be on a private subnet and never a public subnet due to security concerns.

B. A Bastion host sits on the outside of an internal network and is used as a gateway into the private network and is considered the critical strong point of the network.

C. Bastion hosts allow users to log in using RDP or SSH and use that session to S5H into internal network to access private subnet resources.

D. A Bastion host should maintain extremely tight security and monitoring as it is available to the public.

Answer(s): C

---

9. Your company uses IAM to host its resources. They have the following requirements.
1) Record all API calls and Transitions.
2) Help in understanding what resources are there in the account.
3) Facility to allow auditing credentials and logins Which services would suffice the above requirements.

A. IAM Inspector, CloudTrail, IAM Credential Reports.

B. CloudTrail. IAM Credential Reports, IAM SNS

C. CloudTrail, IAM Config, IAM Credential Reports.

D. IAM SQS, IAM Credential Reports, CloudTrail.

Answer(s): C

---

10. Your CTO is very worried about the security of your IAM account. How best can you prevent hackers from completely hijacking your account?

A. Use short but complex password on the root account and any administrators.

B. Use IAM IAM Geo-Lock and disallow anyone from logging in except for in your city.

C. Use MFA on all users and accounts, especially on the root account.

D. Don't write down or remember the root account password after creating the IAM account.

Answer(s): C

---

11. Your CTO thinks your IAM account was hacked.
What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated IAM engineers and doing everything they can to cover their tracks?

A. Use CloudTrail Log File Integrity Validation.

B. Use IAM Config SNS Subscriptions and process events in real time.

C. Use CloudTrail backed up to IAM S3 and Glacier.

D. Use IAM Config Timeline forensics.

Answer(s): A

---

12. Your development team is using access keys to develop an application that has access to S3 and DynamoDB. A new security policy has outlined that the credentials should not be older than 2 months, and should be rotated. How can you achieve this?

A. Use the application to rotate the keys in every 2 months via the SDK

B. Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.

C. Delete the user associated with the keys after every 2 months. Then recreate the user again.

D. Delete the IAM Role associated with the keys after every 2 months. Then recreate the IAM Role again.

Answer(s): B

---

13. You work at a company that makes use of IAM resources. One of the key security policies is to ensure that all data i encrypted both at rest and in transit.
Which of the following is one of the right ways to implement this.

A. Use S3 SSE and use SSL for data in transit.

B. SSL termination on the ELB

C. Enabling Proxy Protocol.

D. Enabling sticky sessions on your load balancer.

Answer(s): A

---

14. There are currently multiple applications hosted in a VPC. During monitoring it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours.
Which of the following is the best method to quickly and temporarily deny access from the specified IP Address's.

A. Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.

B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.

C. Add a rule to all of the VPC Security Groups to deny access from the IP Address block.

D. Modify the Windows Firewall settings on all AMI'S that your organization uses in that VPC to deny access from the IP address block.

Answer(s): B

---

15. A company has a set of EC2 Instances hosted in IAM. The EC2 Instances have EBS volumes which is used to store critical information. There is a business continuity requirement to ensure high availability for the EBS volumes. How can you achieve this?

A. Use lifecycle policies for the EBS volumes.

B. Use EBS Snapshots.

C. Use EBS volume replication.

D. Use EBS volume encryption.

Answer(s): B

---

16. A company is developing a highly resilient application to be hosted on multiple Amazon EC2 instances . The application will store highly sensitive user data in Amazon RDS tables.
The application must.
- Include migration to a different IAM Region in the application disaster recovery plan.
- Provide a full audit trail of encryption key administration events.
- Allow only company administrators to administer keys.
- Protect data at rest using application layer encryption.
A Security Engineer is evaluating options for encryption key management.
Why should the Security Engineer choose IAM CloudHSM over IAM KMS for encryption key management in this situation?

A. The key administration event logging generated by CloudHSM is significantly more extensive than IAM KMS.

B. CloudHSM ensures that only company support staff can administer encryption keys, whereas IAM KMS allows IAM staff to administer keys.

C. The ciphertext produced by CloudHSM provides more robust protection against brute force decryption attacks than the ciphertext produced by IAM KMS

D. CloudHSM provides the ability to copy keys to a different Region, whereas IAM KMS does not.

Answer(s): B

---

17. A company has multiple Amazon S3 buckets encrypted with customer-managed CMKs Due to regulatory requirements the keys must be rotated every year. The company's Security Engineer has enabled automatic key rotation for the CMKs; however the company wants to verity that the rotation has occurred.
What should the Security Engineer do to accomplish this?

A. Filter IAM CloudTrail logs for KeyRotaton events.

B. Monitor Amazon CloudWatcn Events for any IAM KMS CMK rotation events.

C. Using the IAM CLI. run the IAM kms gel-key-relation-status operation with the --key-id parameter to check the CMK rotation date.

D. Use Amazon Athena to query IAM CloudTrail logs saved in an S3 bucket to filter Generate New Key events.

Answer(s): C

---

18. A company needs a forensic-logging solution for hundreds of applications running in Docker on Amazon EC2 The solution must perform real-time analytics on the togs must support the replay of messages and must persist the logs.
Which IAM services should be used to meet these requirements? (Select TWO)

☐ A. Amazon Athena.

☐ B. Amazon Kinesis.

☐ C. Amazon SQS

☐ D. Amazon Elasticsearch.

☐ E. Amazon EMR

Answer(s): B D

---

19. 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.

Answer(s): B

---

20. A company became aware that one of its access keys was exposed on a code sharing website 11 days ago. A Security Engineer must review all use of the exposed access keys to determine the extent of the exposure. The company enabled IAM CloudTrail m an regions when it opened the account.
Which of the following will allow (he Security Engineer 10 complete the task?

A. Filter the event history on the exposed access key in the CloudTrail console Examine the data from the past 11 days.

B. Use the IAM CLI lo generate an IAM credential report Extract all the data from the past 11 days.

C. Use Amazon Athena to query the CloudTrail logs from Amazon S3 Retrieve the rows for the exposed access key tor the past 11 days.

D. Use the Access Advisor tab in the IAM console to view all of the access key activity for the past 11 days.

Answer(s): C
