DUMPSsheet

Free Questions for SCS-C01 by dumpssheet

Shared by Simpson on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A security engineer receives a notice from the AWS Abuse team about suspicious activity from a Linux-based Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS>-based storage The instance is making connections to known malicious addresses

The instance is in a development account within a VPC that is in the us-east-1 Region The VPC contains an internet gateway and has a subnet in us-east-1a and us-easMb Each subnet is associate with a route table that uses the internet gateway as a default route Each subnet also uses the default network ACL The suspicious EC2 instance runs within the us-east-1 b subnet. During an initial investigation a security engineer discovers that the suspicious instance is the only instance that runs in the subnet

Which response will immediately mitigate the attack and help investigate the root cause?

Options:

A- Log in to the suspicious instance and use the netstat command to identify remote connections Use the IP addresses from these remote connections to create deny rules in the security group of the instance Install diagnostic tools on the instance for investigation Update the outbound network ACL for the subnet in us-east- lb to explicitly deny all connections as the first rule during the investigation of the instance

B- Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule Replace the security group with a new security group that allows connections only from a diagnostics security group Update the outbound network ACL for the us-east-1b subnet to remove the deny all rule Launch a new EC2 instance that has diagnostic tools Assign the new security group to the new EC2 instance Use the new EC2 instance to investigate the suspicious instance

B- Ensure that the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the suspicious EC2 instance will not delete upon termination Terminate the instance Launch a new EC2 instance in us-east-1a that has diagnostic tools Mount the EBS volumes from the terminated instance for investigation

D- Create an AWS WAF web ACL that denies traffic to and from the suspicious instance Attach the AWS WAF web ACL to the instance to mitigate the attack Log in to the instance and install diagnostic tools to investigate the instance

Answer:

B, B

Explanation:

This option suggests updating the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule, replacing the security group with a new one that only allows connections from a diagnostics security group, and launching a new EC2 instance with diagnostic tools to investigate the suspicious instance. This option will immediately mitigate the attack and provide the necessary tools for investigation.

Question 2

Question Type: MultipleChoice

A company hosts an end user application on AWS Currently the company deploys the application on Amazon EC2 instances behind an Elastic Load Balancer The company wants to configure end-to-end encryption between the Elastic Load Balancer and the EC2 instances.

Which solution will meet this requirement with the LEAST operational effort?

Options:

A- Use Amazon issued AWS Certificate Manager (ACM) certificates on the EC2 instances and the Elastic Load Balancer to configure end-to-end encryption

B- Import a third-party SSL certificate to AWS Certificate Manager (ACM) Install the third-party certificate on the EC2 instances Associate the ACM imported third-party certificate with the Elastic Load Balancer

C- Deploy AWS CloudHSM Import a third-party certificate Configure the EC2 instances and the Elastic Load Balancer to use the CloudHSM imported certificate

D- Import a third-party certificate bundle to AWS Certificate Manager (ACM) Install the third-party certificate on the EC2 instances Associate the ACM imported third-party certificate with the Elastic Load Balancer.

Answer:

A

Explanation:

To configure end-to-end encryption between the Elastic Load Balancer and the EC2 instances with the least operational effort, the most appropriate solution would be to use Amazon issued AWS Certificate Manager (ACM) certificates on the EC2 instances and the Elastic Load Balancer to configure end-to-end encryption.

AWS Certificate Manager - Amazon Web Services:Elastic Load Balancing - Amazon Web Services:Amazon Elastic Compute Cloud - Amazon Web Services:AWS Certificate Manager - Amazon Web Services

Question 3

Question Type: **MultipleChoice**

A company has two VPCs in the same AWS Region and in the same AWS account Each VPC uses a CIDR block that does not overlap with the CIDR block of the other VPC One VPC contains AWS Lambda functions that run inside a subnet that accesses the internet through a NAT gateway. The Lambda functions require access to a publicly accessible Amazon Aurora MySQL database that is running in the other VPC

A security engineer determines that the Aurora database uses a security group rule that allows connections from the NAT gateway IP address that the Lambda functions use. The company's security policy states that no database should be publicly accessible.

What is the MOST secure way that the security engineer can provide the Lambda functions with access to the Aurora database?

Options:

A- Move the Aurora database into a private subnet that has no internet access routes in the database's current VPC Configure the Lambda functions to use the Aurora
database's new private IP address to access the database Configure the Aurora databases security group to allow access from the private IP addresses of the Lambda functions

B- Establish a VPC endpoint between the two VPCs in the Aurora database's VPC configure a service VPC endpoint for Amazon RDS In the Lambda functions' VPC.
configure an interface VPC endpoint that uses the service endpoint in the Aurora database's VPC Configure the service endpoint to allow connections from the Lambda functions.

C- Establish an AWS Direct Connect interface between the VPCs Configure the Lambda functions to use a new route table that accesses the Aurora database through the Direct Connect interface Configure the Aurora database's security group to allow access from the Direct Connect interface IP address

D- Move the Lambda functions into a public subnet in their VPC Move the Aurora database into a private subnet in its VPC Configure the Lambda functions to use the Aurora database's new private IP address to access the database Configure the Aurora database to allow access from the public IP addresses of the Lambda functions

Answer:

B

Explanation:

This option involves creating a VPC Endpoint between the two VPCs that allows private communication between them without going through the internet or exposing any public IP addresses. In this option, a VPC endpoint for Amazon RDS will be established, and an interface VPC endpoint will be created that points to the service endpoint in the Aurora database's VPC. This way, the Lambda functions can use the private IP address of the Aurora database to access it through the VPC endpoint without exposing any public IP addresses or allowing public internet access to the database.

Question 4

Question Type: **MultipleChoice**

A company wants to remove all SSH keys permanently from a specific subset of its Amazon Linux 2 Amazon EC2 instances that are using the same 1AM instance profile However three individuals who have IAM user accounts will need to access these instances by using an SSH session to perform critical duties

How can a security engineer provide the access to meet these requirements'?

Options:

A- Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager Provide the 1AM user accounts with permission to use Systems Manager Remove the SSH keys from the EC2 instances Use Systems Manager Inventory to select the EC2 instance and connect

B- Assign an 1AM policy to the 1AM user accounts to provide permission to use AWS Systems Manager Run Command Remove the SSH keys from the EC2 instances Use Run Command to open an SSH connection to the EC2 instance

C- Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager Provide the 1AM user accounts with permission to use Systems Manager Remove the SSH keys from the EC2 instances Use Systems Manager Session Manager to select the EC2 instance and connect

D- Assign an 1AM policy to the 1AM user accounts to provide permission to use the EC2 service in the AWS Management Console Remove the SSH keys from the EC2 instances Connect to the EC2 instance as the ec2-user through the AWS Management Console's EC2 SSH client method

Answer:

C

Explanation:

To provide access to the three individuals who have IAM user accounts to access the Amazon Linux 2 Amazon EC2 instances that are using the same IAM instance profile, the most appropriate solution would be to assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager, provide the IAM user accounts with permission to use Systems Manager, remove the SSH keys from the EC2 instances, and use Systems Manager Session Manager to select the EC2 instance and connect.

Question 5

Question Type: **MultipleChoice**

A company is using an AWS Key Management Service (AWS KMS) AWS owned key in its application to encrypt files in an AWS account The company's security team wants the ability to change to new key material for new files whenever a potential key breach occurs A security engineer must implement a solution that gives the security team the ability to change the key whenever the team wants to do so

Which solution will meet these requirements?

Options:

A- Create a new customer managed key Add a key rotation schedule to the key Invoke the key rotation schedule every time the security team requests a key change

B- Create a new AWS managed key Add a key rotation schedule to the key Invoke the key rotation schedule every time the security team requests a key change

C- Create a key alias Create a new customer managed key every time the security team requests a key change Associate the alias with the new key

D- Create a key alias Create a new AWS managed key every time the security team requests a key change Associate the alias with the new key

Answer:

A

Explanation:

To meet the requirement of changing the key material for new files whenever a potential key breach occurs, the most appropriate solution would be to create a new customer managed key, add a key rotation schedule to the key, and invoke the key rotation schedule every time the security team requests a key change.

Question 6

Question Type: MultipleChoice

A company has an AWS Key Management Service (AWS KMS) customer managed key with imported key material Company policy requires all encryption keys to be rotated every year

What should a security engineer do to meet this requirement for this customer managed key?

Options:

A- Enable automatic key rotation annually for the existing customer managed key

B- Use the AWS CLI to create an AWS Lambda function to rotate the existing customer managed key annually

C- Import new key material to the existing customer managed key Manually rotate the key

D- Create a new customer managed key Import new key material to the new key Point the key alias to the new key

Answer:

A

Explanation:

To meet the requirement of rotating the AWS KMS customer managed key every year, the most appropriate solution would be to enable automatic key rotation annually for the existing customer managed key. This will ensure that AWS KMS generates new cryptographic material for the CMK every year. AWS KMS also saves the CMK's older cryptographic material in perpetuity so it can be used to decrypt data that it encrypted. AWS KMS does not delete any rotated key material until you delete the CMK.

Question 7

Question Type: MultipleChoice

A company usesAWS Organizations to run workloads in multiple AWS accounts Currently the individual team members at the company access all Amazon EC2 instances remotely by using SSH or Remote Desktop Protocol (RDP) The company does not have any audit trails and security groups are occasionally open The company must secure access management and implement a centralized togging solution

Which solution will meet these requirements MOST securely?

Options:

A- Configure trusted access for AWS System Manager in Organizations Configure a bastion host from the management account Replace SSH and RDP by using Systems Manager Session Manager from the management account Configure Session Manager logging to Amazon CloudWatch Logs

B- Replace SSH and RDP with AWS Systems Manager Session Manager Install Systems Manager Agent (SSM Agent) on the instances Attach the

C- AmazonSSMManagedInstanceCore role to the instances Configure session data streaming to Amazon CloudWatch Logs Create a separate logging account that has appropriate cross-account permissions to audit the log data

C- Install a bastion host in the management account Reconfigure all SSH and RDP to allow access only from the bastion host Install AWS Systems Manager Agent (SSM Agent) on the bastion host Attach the AmazonSSMManagedInstanceCore role to the bastion host Configure session data streaming to Amazon CloudWatch Logs in a separate logging account to audit log data

D- Replace SSH and RDP with AWS Systems Manager State Manager Install Systems Manager Agent (SSM Agent) on the instances Attach the
AmazonSSMManagedInstanceCore role to the instances Configure session data streaming to Amazon CloudTrail Use CloudTrail Insights to analyze the trail data

Answer:

C, C

Explanation:

To meet the requirements of securing access management and implementing a centralized logging solution, the most secure solution would be to:

Install a bastion host in the management account.

Reconfigure all SSH and RDP to allow access only from the bastion host.

Install AWS Systems Manager Agent (SSM Agent) on the bastion host.

Attach the AmazonSSMManagedInstanceCore role to the bastion host.

Configure session data streaming to Amazon CloudWatch Logs in a separate logging account to audit log data

This solution provides the following security benefits:

It uses AWS Systems Manager Session Manager instead of traditional SSH and RDP protocols, which provides a secure method for accessing EC2 instances without requiring inbound firewall rules or open ports.

It provides audit trails by configuring Session Manager logging to Amazon CloudWatch Logs and creating a separate logging account to audit the log data.

It uses the AWS Systems Manager Agent to automate common administrative tasks and improve the security posture of the instances.

The separate logging account with cross-account permissions provides better data separation and improves security posture.

https://aws.amazon.com/solutions/implementations/centralized-logging/

Question 8

Question Type: MultipleChoice

Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

Options:

A- Default AWS Certificate Manager certificate

B- Custom SSL certificate stored in AWS KMS

C- Default CloudFront certificate

D- Custom SSL certificate stored in AWS Certificate Manager

E- Default SSL certificate stored in AWS Secrets Manager

F- Custom SSL certificate stored in AWS IAM

Answer:

A, B, C

Explanation:

The key length for an RSA certificate that you use with CloudFront is 2048 bits, even though ACM supports larger keys. If you use an imported certificate with CloudFront, your key length must be 1024 or 2048 bits and cannot exceed 2048 bits. You must import the certificate in the US East (N. Virginia) Region.You must have permission to use and import the SSL/TLS certificate

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

Question 9

Question Type: MultipleChoice

A company has launched an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume in the us-east-1 Region The volume is encrypted with an AWS Key Management Service (AWS KMS) customer managed key that the company's security team created The security team has created an 1AM key policy and has assigned the policy to the key The security team has also created an 1AM instance profile and has assigned the profile to the instance

The EC2 instance will not start and transitions from the pending state to the shutting-down state to the terminated state

Which combination of steps should a security engineer take to troubleshoot this issue? (Select TWO)

Options:

A- Verify that the KMS key policy specifies a deny statement that prevents access to the key by using the aws SourceIP condition key Check that the range includes the EC2 instance IP address that is associated with the EBS volume

B- Verify that the KMS key that is associated with the EBS volume is set to the Symmetric key type

C- Verify that the KMS key that is associated with the EBS volume is in the Enabled state

D- Verify that the EC2 role that is associated with the instance profile has the correct 1AM instance policy to launch an EC2 instance with the EBS volume

E- Verify that the key that is associated with the EBS volume has not expired and needs to be rotated
C) Verify that the KMS key that is associated with the EBS volume is in the Enabled state. If the key is not enabled, it will not function properly and could cause the EC2 instance to fail.
D) Verify that the EC2 role that is associated with the instance profile has the correct IAM instance policy to launch an EC2 instance with the EBS volume. If the instance does not have the necessary permissions, it may not be able to mount the volume and could cause the instance to fail.
Therefore, options C and D are the correct answers.

Answer:

C, D

Explanation:

To troubleshoot the issue of an EC2 instance failing to start and transitioning to a terminated state when it has an EBS volume encrypted with an AWS KMS customer managed key, a security engineer should take the following steps: