Note: This is set of exam questions developed for AWS Certification—a level of Amazon Web Services cloud expertise The original questions are developed by advanced AWS professionals and edited by instructional designers for structure, clarity, accuracy, and conformity to goals and standards.

Original text	After editing pass
1. If the Security Operations Engineer receives a notify-cation suggesting possible unauthorized use of the company's AWS account root user, what investigation steps should they take as a priority to ensure that only authorised person(s) can login as the root user?(Select THREE) A. Set the status of AWS account root user in disabled mode while the unauthorized activity is being investigated. B. Review the details of the CloudTrail Event History for ConsoleLogin and other events involving the user name of root. C. Review the last activity day indicator against all defined IAM users in the AWS account to determine other suspicious activity. D. Change AWS account security credentials settings and ensure that only authorized person(s) are able to make use of them. E. Define new AWS account security challenge questions to add further protection on AWS account root user logins. F. Review AWS Config event timelines to identify and fix unauthorised configurations may have been made by the root user. Answers A. Incorrect: It is not possible to set the account root user in disabled mode in a literal sense, so this is not applicable. B. It is important to confirm the accuracy of the notification of unauthorised account root usage and compare it to company records detailing when authorised root usage was approved. C. The account root user is not defined as an IAM user, and therefore investigating other user activity is not pertinent to the task at hand. D. One of the most important aspects of regaining control of potentially compromised user credentials is to change them to new	1. You receive a notification that suggests unauthorized use of your organization's AWS account root user identity. What initial actions should you take? (Select THREE.) A. Disable the root user account. B. In the CloudTrail Event history, look for ConsoleLogin and other events with the user name *root*. C. Look for other suspicious events by reviewing the last activity day indicator for all IAM users in the AWS account. D. Change the security credentials of the AWS account root user. E. Define new AWS account security challenge questions for the root user login. F. Review AWS Config event timelines to identify and fix unauthorized configurations made by the root user. Answers and explanations: A. Incorrect: The root user account cannot be disabled. B. Correct: You should confirm that the unauthorized usage actually occurred. Compare the event to company records to see when authorized root usage was approved. C. Incorrect: Because the account root user is not defined as an IAM user, investigating this activity provides nothing useful for this situation. D. Correct: In any case of a compromised user account, you should quickly change the security credentials and make sure their use is properly controlled. This is especially true for root user credentials. E. Incorrect: The security challenge questions defined in AWS account settings are not

values and then ensure proper control thereafter of who can use them, especially for the account root credentials. E. Incorrect: The security challenge questions defined in AWS account settings have no direct relevance to the protection of AWS account root user authentication credentials. F. There is an assumption here that Config is enabled, but this AWS service is a good choice to identify AWS resource configurations and to review changes that have occurred over time, especially around the date/time of suspected unauthorized root user access.	relevant to the root user authentication credentials. F. Correct: You can use this AWS service to easily review AWS resource configurations, especially those that occurred around the date and time of suspected unauthorized root user access.

Original text	**After editing pass**
2. What are some of the key factors that the Security Architect should consider when deciding between CloudHSM and KMS to perform encryption key management? (Select THREE.) A. CloudHSM produces a much stronger form of ciphertext compared to what KMS can generate. B. There is a corporate requirement or a material risk reduction associated with an organisation directly administering the key management HSM backing appliance. C. The additional security assurance gained by integrating an application with a CloudHSM outweighs the additional complexity of doing so compared to KMS. D. There are regulatory or legal requirements mandating the use of a dedicated HSM appliance or HSM partition for encryption of sensitive data. E. The ability to extract backing keys from CloudHSM and KMS to store locally within the organization. Answers and explanations:	2. Which of the following are valid reasons to choose AWS CloudHSM instead of Amazon Key Management Service (KMS) for encryption key management? (Select THREE.) A. CloudHSM generates more robust ciphertext than KMS. B. The organization has a corporate or risk-mitigation requirement to use an HSM backup device for key management. C. The organization's risk assessment concludes that HSM poses less risk than KMS. D. A regulatory or legal requirement mandates the use of a dedicated HSM appliance or partition to encrypt sensitive data. E. CloudHSM allows the extraction of backing keys for local storage. Answers and explanations: A. Incorrect: The ciphertext produced by each option is equally robust (assuming the default option of AES-256). B. Correct: Some organizations follow a strict corporate standard or specific risk mitigation requirement to use a dedicated CloudHSM partition despite its additional cost and administration overhead.

A. The ciphertext produced by CloudHSM and KMS are both equally robust when assuming the default option of AES-256. B. There should be a strict corporate standard or specific risk mitigation requirement to warrant taking on the additional cost and administration overhead associated with a dedicated CloudHSM partition. C. There should be a risk assessment that proves that the additional complexity of integrating applications with an HSM is a worthwhile investment versus the likelihood and damage that could be caused by a control failure in KMS. D. The most likely reason for choosing a AWS CloudHSM partition over the AWS managed KMS service is for legal or regulatory reasons. E. It is not possible to extract backing keys from either CloudHSM or KMS.	C. Correct: Some organizations conduct risk assessments showing that damage caused by a control failure in KMS is a greater risk than potential problems caused by the additional complexity of integrating an application with CloudHSM. D. Correct: The most common reason for choosing CloudHSM over KMS is for legal or regulatory reasons. E. Incorrect: Neither CloudHSM nor KMS supports extracting backing keys.

Original text	**After editing pass**
3. What simple and cost-effective AWS native control mechanisms could the Security Architect include in their design proposal to detect possible command-and-control malware infection on EC2 instances (Select TWO.) A. CloudTrail B. Systems Manager C. Shield D. CloudWatch Alarm E. GuardDuty Answers and Explanations A. CloudTrail will not detect operating system events or network communications occurring from inside the EC2 instance. B. Systems Manager is an operational management tool for EC2 and is not a good choice for detecting malware infection.	3. You are considering ways to detect command-and-control malware infections on Amazon Elastic Compute Cloud (EC2) instances. Your solution must be cost-effective and use an AWS native control mechanism. Which mechanisms are possible options? (Select TWO.) A. CloudTrail B. Systems Manager C. Shield D. CloudWatch Alarm E. GuardDuty Answers and explanations: A. Incorrect: CloudTrail captures API activity in your AWS account but does not detect events occurring inside the EC2 instance. B. Incorrect: Systems Manager is an operational management tool for EC2 and is not intended to detect malware infections.

C. Shield is primarily design to protect against incoming denial of service attacks and is not a good choice alone for detecting EC2 malware infection. D. Since a common option is to send VPC Flow Logs to CloudWatch Logs, then it is simple and cheap to define an Alarm to detect Flow Logs that resulted in a 'REJECT' action, which might be an indication of malware infection and subsequent outbound command and control network requests, or all manner of other unauthorised network requests. E. GuardDuty is available as a simple and cheap AWS service to detect some or all EC2 command-and-control malware infection where DNS name resolution requests and possibly outbound communication requests occur to known bad IP addresses.	C. Incorrect: Although Shield protects against incoming denial-of-service attacks, it is not a good choice for detecting EC2 malware infections. D. Correct: Because VPC Flow logs are commonly sent to CloudWatch logs, you can define an alarm for denied connections in VPC, which is a possible indication of a malware infection. E. Correct: GuardDuty is an AWS service that detects command-and-control malware infections by monitoring DNS traffic from EC2 instances.

Original text	**After editing pass**
4. What actions should the Security Operations Engineer generally take as initial steps when they receive an Amazon EC2 Abuse Report email that indicates host vulnerability scanning activity? (Select THREE.) A. Reply to the Amazon EC2 Abuse team and ask for more details. B. Assess whether the EC2 Instance ID indicated an application function which could be regarded by Amazon as conducting unauthorized network port scanning. C. Reboot the EC2 instance and wait to see if further abuse notices are received. D. Create an image of the EC2 running instance before making changes to enable any required forensic investigation. E. Collect a memory dump and all relevant security event log files from the EC2 instance and store them safely for possible future forensic analysis.	4. You receive an email message from the AWS Abuse team about possible host vulnerability scanning on an EC2 instance. Which of the following actions should you initially take? (Select THREE.) A. Contact the AWS Abuse team for more details. B. Assess whether the EC2 instance hosts an application function that is conducting unauthorized port scanning. C. Reboot the EC2 instance and see whether you receive another report of potential abuse. D. Before making any changes, create an image of the EC2 running instance. E. Collect a memory dump and all relevant security event log files from the EC2 instance and store them for forensic analysis.

F. Remove all defined outbound rules in the Security Group that is associated with the EC2 Instance ID indicated. A. An AWS abuse notice is primarily an informational warning to the EC2 instance owner and automatically generated. Taking an initial step of asking for more details will only delay the root cause analysis and recovery action. B. If the EC2 instance indicated is not compromised by an attacker, then a common situation is where an application running on the EC2 instance is exhibiting vulnerability scanning behavior. C. Rebooting the instance is likely not going to solve the problem since any app that runs and causes this problem will probably survive a reboot. D. If the result from the analysis in Answer B yields no explanation, then it may be necessary to perform a forensic investigation to determine if the EC2 instance has been infected with malware. E. In case the malware is not persisted to storage, it will be necessary to capture the running processes and the audit trails of security events that were previously generated. F. This will remediate the port scanning issue, but it may also block outbound communications that the EC2 instance application require to function properly.	F. Remove all outbound rules in the security group associated with the EC2 instance. Answers and explanations: A. Incorrect: The AWS Abuse team is tasked with protecting AWS customers from security threats, but they are not “first responders” for potential threats. Also, the reports should already include sufficient detail. B. Correct: An application running on the EC2 instance may be compromised by an attacker instead of the instance itself. C. Incorrect: Rebooting the instance does not stop abusive activity. D. Correct: You may need the image for a forensic investigation to determine whether the EC2 instance has been infected with malware. E. Correct: If the malware is not persisted to storage, you must capture the running processes and the audit trails of security events that were previously generated. F. Incorrect: Although removing the rules eliminates the port scanning issue, this may also block outbound communications that the EC2 instance application requires to function properly.

Original text	**After editing pass**
5. What are the easiest ways to implement a dashboard visualization of VPC Flow Logs data by using only AWS standard service offerings? (Select TWO) A. Elasticsearch Service and Kibana B. S3 and Machine Learning	5. Using only AWS standard service offerings, you must develop a dashboard visualization of VPC Flow Logs data. Which of the following combinations of services could you use? (Select TWO.) A. Elasticsearch and Kibana B. S3 and Machine Learning

C. SageMaker and DeepLens D. Athena and QuickSight E. CloudWatch Logs and X-Ray Answers and explanations: A. The preferred option for those who are most comfortable using the AWS assisted build of Elastic Stack open source products. B. It may be possible to use Machine Learning data visualization capabilities to illustrate Flow Logs data, but it is more complex and not a common solution. C. A distractor combination that is not suited to this task. D. The preferred option for those wanting to use fully AWS managed service offerings. E. A distractor combination that is not suited to this task.	C. SageMaker and DeepLens D. Athena and QuickSight E. CloudWatch Logs and X-Ray Answers and explanations: A. Correct: This option is the best choice if you want to use the AWS-assisted build of Elastic Stack open-source products. B. Incorrect: Although you can potentially create this visualization with Machine Learning, it is a complex and uncommon solution. C. Incorrect: AWS DeepLens is a programmable video camera that is often used with the SageMaker machine learning platform. D. Correct: This option is the best choice if you want to use the fully AWS-managed service offerings. E. Incorrect: These complementary services monitor and debug applications but cannot perform this task.

Original text	**After editing pass**
6. An IAM user,is unable to download objects from an S3 bucket in the same AWS account using the Management Consol. The S3 bucket is configured with the default encryption option using a custom CMK in the same AWS account. Which access control policy objects must the Security Operations Engineer review and amend as a priority to resolve the problem? (Select THREE.) A. KMS CMK key policy B. VPC endpoint policy C. Organizations SCP policy D. S3 bucket policy E. S3 bucket ACL F. IAM user/group policy	6. An Identity and Access Management (IAM) user signs into a Management Console but is unable to download objects from an S3 bucket in that AWS account. The S3 bucket is configured with the default encryption option using a customer-managed key (CMK). To fix this problem, which access control policy objects must be reviewed and amended? (Select THREE.) A. KMS CMK key policy B. VPC endpoint policy C. The organization's SCP policy D. S3 bucket policy E. S3 bucket ACL F. IAM user/group policy

Answers A. Correct: Because the S3 bucket is encrypted with the default encryption option, it is important to review whether this IAM user is allowed to make calls to the kms:Decrypt action on this CMK. B. Incorrect: Although this policy might be relevant if the problem were occurring from an EC2 instance, but since the IAM user is accessing the bucket via the Management Console, it is not relevant. C. Incorrect: This policy might be relevant if it was affecting all users within the account, but it is not the priority to review during troubleshooting exercise. D. Correct: It is important to review this policy with priority to confirm whether the IAM user is granted permission to s3:GetObject in the bucket policy, else it will need to be allowed in IAM policy. E. Incorrect: The S3 bucket ACL is a legacy feature and primarily used for allowing access to bucket contents by users from other AWS account, so not relevant in this scenario. F. Correct: Confirm that the IAM user has access to s3:GetObject in the IAM user or group policy, else it will need to be allowed in the S3 bucket policy.	Answers and explanations: A. Correct: Because the S3 bucket is encrypted with the default encryption option, you must determine whether this IAM user is allowed to make calls to the kms:Decrypt action on this CMK. B. Incorrect: This policy is relevant if the problem occurs on an EC2 instance. In this case, the IAM user accessed the bucket through the Management Console. C. Incorrect: Reviewing a policy that affects all users is not relevant because the problem is limited to one user. D. Correct: You must review this policy to confirm that the IAM user is granted permission to s3:GetObject. E. Incorrect: The S3 bucket ACL is a legacy feature and primarily used for allowing access to bucket contents by users from other AWS accounts. F. Correct: Confirm that the IAM user has access to s3:GetObject in the IAM user or group policy. If not, access must be allowed in the S3 bucket policy.

Original text	**After editing pass**
7. What are the most likely reasons for a permissioned EC2 instance not being able to use a KMS CMK for decryption purposes when it is allowed the kms:Decrypt action in its IAM role against all resources? (Select THREE.) A. The EC2 IAM role also requires kms:GenerateDataKey privilege. B. The EC2 instance has no network access to the KMS endpoint via either a VPC endpoint or directly to the Internet.	7. An EC2 instance assuming an IAM role can use the kms:Decrypt action against all resources. However, it cannot gain access to the KMS customer master key (CMK) for decryption. Which of the following are mandatory for the role to have access to the CMK? (Select THREE.) A. The role has Grant kms:GenerateDataKey permission. B. The EC2 instance has network access to the KMS endpoint, either through a VPC endpoint or directly to the Internet.

C. The KMS CMK does not have a tag defined with the ARN of the EC2 instance. D. The EC2 IAM role also requires kms:Encrypt privilege as a matching pair. E. The default CMK key policy statement Sid of “Enable IAM User Permissions” has been removed. F. The KMS CMK is set in Disabled status. Answers A. The EC2 IAM role does not require kms:GenerateDataKey permission to use KMS for data decryption actions. B. The EC2 instance needs to be able to communicate with the KMS service endpoint, either via VPC endpoint (com.amazonaws.{region}.kms) or directly to the Internet. C. There is no requirement for tags to be defined on a KMS CMK in order to use it. D. The EC2 IAM role does not require kms:Encrypt permission to use KMS for data decryption actions. E. This KMS CMK key policy statement needs to be defined in order to delegate permissions assignment via IAM. F. The KMS CMK needs to be in Enabled status in order to use it for kms:Decrypt actions.	C. The KMS CMK has a tag defined with the Amazon Resource Name (ARN) of the EC2 instance. D. The role has kms:Encrypt permission. E. The CMK policy grants permission to the role. F. The KMS CMK is enabled. Answers and explanations: A. Incorrect: The EC2 IAM role does not require kms:GenerateDataKey permission to use KMS for data decryption. B. Correct: The EC2 instance must be able to communicate with the KMS service endpoint, either through a VPC endpoint (com.amazonaws.{region}.kms) or directly to the Internet. C. Incorrect: There is no requirement for tags to be defined on a KMS CMK in order to use it. D. Incorrect: The EC2 IAM role does not require kms:Encrypt permission to use KMS for data decryption. E. Correct: The key policy must allow access. IAM policies alone cannot grant access to a KMS key. F. Correct: To perform kms:Decrypt actions, the KMS CMK must be enabled.

Original text	**After editing pass**
8. The Security Architect is given the requirement to design a system in AWS that ensures the secrecy of user supplied passwords. Which of the following design options is the most secure approach? A. Store the passwords in DynamoDB and configure table encryption plus fine-grained IAM access control to restrict read access on the password column to the application only.	8. You must design a system that maintains the security of an organization’s user-supplied passwords. What is the best approach? A. Store the passwords in DynamoDB. Use table encryption and fine-grained IAM access control to restrict read access on the password column to the application only.

B. Encrypt the passwords with a kms:Encrypt action against a custom defined KMS CMK, and then store them in an RDS database table.

C. Run the passwords through a modern hashing algorithm and store them in an RDS database table.

D. Encrypt the passwords through application calls to a CloudHSM and use the largest key type and size of RSA 4096-bit.Store the encrypted passwords in an RDS database table.

Answer and explanations:

A. This will result in plain-text passwords stored in an Internet facing data store. If there are weaknesses with the application, there is a risk that all user passwords may be exposed.

B. Using a symmetric password encryption technique has the disadvantage that all passwords can be decrypted by those who have permission to call the kms:Decrypt action.

C. Using a strong hashing technique (e.g. PBKDF2, bcrypt or Argon2) is the most secure form of password protection as the stored value is non-reversible and can only be used to compare a further user password submission against the stored version.

D. While some may regard the CloudHSM service as the most protected form of encryption key management, it suffers from the fact that encrypted passwords are reversible by the application or any other user who has the privilege to make decryption calls to the HSM.

B. Encrypt the passwords with a kms:Encrypt action against a custom-defined KMS CMK, and then store them in an RDS database table.

C. Run the passwords through a strong hashing algorithm and store them in an RDS database table.

D. Encrypt the passwords through application calls to a CloudHSM and use the largest key type and size of RSA 4096-bit. Store the encrypted passwords in an RDS database table.

Answer and explanations:

A. Incorrect: This method results in plain-text passwords stored in an Internet-facing data store. Any weaknesses with the application could lead to the exposure of all user passwords.

B. Incorrect: This is not a secure option because any user with permission to call the kms:Decrypt action can decrypt all passwords.

C. Correct: Use of a strong hashing technique (such as PBKDF2, bcrypt, or Argon2) is the most secure form of password protection. The stored value is non-reversible and can be used only to compare a future user password submission against the stored version.

D. Incorrect: Encrypted passwords are reversible by the application or any other user who has the privilege to make decryption calls to the HSM.