AWS Certified Security – Specialty ( Security Engineering on AWS ) Quiz Questions and Answers – part 2 of 3

How does the analogy of a ship navigating through stormy seas relate to responding to threats in AWS environments?

Answer :

* It emphasizes the need for continuous monitoring for threats

Explanation :

The analogy of a ship navigating through stormy seas highlights the importance of continuous monitoring for threats in AWS environments to ensure security.

Which AWS service provides temporary security credentials to applications to facilitate integration with an external identity provider?

Answer :

* AWS STS

Explanation :

AWS STS (Security Token Service) provides temporary security credentials to applications, facilitating secure integration with external identity providers.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527234)

Which AWS service should be used for automated security assessments of applications and continuous monitoring for vulnerabilities?

Answer :

* Amazon Inspector

Explanation :

Amazon Inspector provides automated security assessments, continuous monitoring for vulnerabilities and capability to improve security and compliance.

What is the core principle of the AWS Shared Responsibility Model that differentiates services responsibility between AWS and customers?

Answer :

* Physical infrastructure

Explanation :

AWS is responsible for the physical infrastructure while customers manage their data. This division is the essence of the Shared Responsibility Model.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527155)

Which AWS service allows secure storing and managing of encryption keys along with centralized key management?

Answer :

* AWS Key Management Service (KMS)

Explanation :

AWS Key Management Service (KMS) is designed for secure management, storage, and handling of encryption keys with centralized key management features.

Why would you choose to deploy AWS WAF at the CloudFront edge locations instead of directly on an EC2 instance?

Answer :

* To enhance global performance and protection

Explanation :

Deploying AWS WAF at CloudFront edge locations enhances performance and protection because it can block threats closer to the user and reduce latency.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527294)

What is the key objective of understanding incident response dynamics within AWS environments?

Answer :

* To identify and mitigate security incidents promptly

Explanation :

Understanding incident response dynamics in AWS environments aims to identify and mitigate security incidents promptly to minimize potential damage.

Which AWS service would you primarily use to set alarms for baseline deviations in application performance metrics?

Answer :

* Amazon CloudWatch

Explanation :

Amazon CloudWatch is designed to monitor and set alarms on metrics, making it suitable for detecting baseline deviations in application performance.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527242)

Which formula correctly describes the cost implication if a key is replicated in 3 Regions with the known cost C for a single key?

Answer :

* 3C

Explanation :

Replicating a KMS key across 3 Regions means you are essentially paying for 3 instances of the key, so the cost would be 3 times a single key price.

When configuring Amazon Macie, what is the first step to take in order to scan a new dataset for sensitive information?

Answer :

* Enable Macie and create a classification job

Explanation :

To scan a new dataset, you need to enable Macie and create a classification job which specifies the S3 buckets and other parameters to be monitored.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527193)

Which AWS service provides a cost-effective and automated way to analyze large-scale log data to assist in infrastructure edge protection?

Answer :

* Amazon GuardDuty

Explanation :

Amazon GuardDuty provides threat detection services that continuously monitor your AWS environment for malicious activity and unauthorized behavior.

When setting up a development and production environment using AWS Control Tower, which of the following ensures compliance across accounts?

Answer :

* Implementing Service Control Policies (SCPs) to enforce specific actions.

Explanation :

Service Control Policies (SCPs) are used within AWS Control Tower to enforce constraints and compliance across multiple accounts in an organization.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527203)

When setting up guardrails in AWS Control Tower, how would you enforce the use of encryption across all S3 buckets in your AWS accounts?

Answer :

* By configuring a guardrail in AWS Control Tower

Explanation :

AWS Control Tower guardrails help enforce compliance and security policies across your AWS accounts, including the use of encryption for S3 buckets.

To monitor and protect against suspicious activity in your VPC, which AWS service would you employ to analyze network traffic for potential threats?

Answer :

* AWS GuardDuty

Explanation :

AWS GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior within your AWS environment.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527145)

Which AWS service is most suitable for protecting API endpoints from malicious traffic and maintaining the integrity of API communications?

Answer :

* AWS WAF

Explanation :

AWS WAF is well-suited for protecting API endpoints by filtering and monitoring HTTP and HTTPS requests against known and custom threat signatures.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527224)

Why is it important to integrate AWS CloudFront with AWS Shield for content delivery during a large-scale attack?

Answer :

* CloudFront provides a global network to absorb attacks

Explanation :

AWS CloudFront, when integrated with AWS Shield, uses its global edge locations to absorb and mitigate attacks, ensuring reliable content delivery.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527279)

How would enabling multi-region replication improve the security of archived data stored in S3?

Answer :

* Enhances data availability and durability

Explanation :

Multi-region replication improves security by enhancing data availability and durability, ensuring data is accessible even if one region goes down.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527095)

Which of the following best describes the role of Multi-Factor Authentication (MFA) in securing AWS accounts?

Answer :

* MFA adds an extra security layer by using a second form of authentication.

Explanation :

MFA adds an extra layer of protection by requiring a second form of authentication, such as a physical device or app, in addition to the password.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527259)

Which of the following best describes the primary function of Amazon Macie in the context of AWS data security?

Answer :

* Monitoring data for sensitive information using machine learning

Explanation :

Amazon Macie uses machine learning to discover, classify, and protect sensitive data stored in AWS. It helps identify PII and other critical data.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527258)

What is the primary function of AWS Organizations in managing multiple AWS accounts?

Answer :

* To provide central governance across multiple AWS accounts

Explanation :

AWS Organizations helps in centrally managing policies, access, and compliance across multiple AWS accounts, thereby providing central governance.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527174)

Given an RPO (Recovery Point Objective) of 1 hour, which AWS service should be used to back up a relational database every 30 minutes and why?

Answer :

* AWS RDS Snapshots

Explanation :

AWS RDS Snapshots allow you to back up your relational database at regular intervals to meet specific RPO requirements, such as every 30 minutes.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527069)

Which AWS service integration is exclusive to AWS Shield Advanced for additional protection against DDoS attacks?

Answer :

* AWS Web Application Firewall (WAF)

Explanation :

AWS Shield Advanced integrates with AWS Web Application Firewall (WAF) to provide advanced protection and rate-based rules against DDoS attacks.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527223)

When setting up guardrails in AWS Control Tower, how would you enforce the use of encryption across all S3 buckets in your AWS accounts?

Answer :

* By configuring a guardrail in AWS Control Tower

Explanation :

AWS Control Tower guardrails help enforce compliance and security policies across your AWS accounts, including the use of encryption for S3 buckets.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527206)

To monitor and protect against suspicious activity in your VPC, which AWS service would you employ to analyze network traffic for potential threats?

Answer :

* AWS GuardDuty

Explanation :

AWS GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior within your AWS environment.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527145)

Which AWS service is most suitable for protecting API endpoints from malicious traffic and maintaining the integrity of API communications?

Answer :

* AWS WAF

Explanation :

AWS WAF is well-suited for protecting API endpoints by filtering and monitoring HTTP and HTTPS requests against known and custom threat signatures.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527224)

Why is it important to integrate AWS CloudFront with AWS Shield for content delivery during a large-scale attack?

Answer :

* CloudFront provides a global network to absorb attacks

Explanation :

AWS CloudFront, when integrated with AWS Shield, uses its global edge locations to absorb and mitigate attacks, ensuring reliable content delivery.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527279)

How would enabling multi-region replication improve the security of archived data stored in S3?

Answer :

* Enhances data availability and durability

Explanation :

Multi-region replication improves security by enhancing data availability and durability, ensuring data is accessible even if one region goes down.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527095)

Which of the following best describes the role of Multi-Factor Authentication (MFA) in securing AWS accounts?

Answer :

* MFA adds an extra security layer by using a second form of authentication.

Explanation :

MFA adds an extra layer of protection by requiring a second form of authentication, such as a physical device or app, in addition to the password.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527259)

Which of the following best describes the primary function of Amazon Macie in the context of AWS data security?

Answer :

* Monitoring data for sensitive information using machine learning

Explanation :

Amazon Macie uses machine learning to discover, classify, and protect sensitive data stored in AWS. It helps identify PII and other critical data.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527258)

What is the primary function of AWS Organizations in managing multiple AWS accounts?

Answer :

* To provide central governance across multiple AWS accounts

Explanation :

AWS Organizations helps in centrally managing policies, access, and compliance across multiple AWS accounts, thereby providing central governance.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527174)

Given an RPO (Recovery Point Objective) of 1 hour, which AWS service should be used to back up a relational database every 30 minutes and why?

Answer :

* AWS RDS Snapshots

Explanation :

AWS RDS Snapshots allow you to back up your relational database at regular intervals to meet specific RPO requirements, such as every 30 minutes.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527069)

Which AWS service integration is exclusive to AWS Shield Advanced for additional protection against DDoS attacks?

Answer :

* AWS Web Application Firewall (WAF)

Explanation :

AWS Shield Advanced integrates with AWS Web Application Firewall (WAF) to provide advanced protection and rate-based rules against DDoS attacks.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527223)

When setting up guardrails in AWS Control Tower, how would you enforce the use of encryption across all S3 buckets in your AWS accounts?

Answer :

* By configuring a guardrail in AWS Control Tower

Explanation :

AWS Control Tower guardrails help enforce compliance and security policies across your AWS accounts, including the use of encryption for S3 buckets.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527206)

To monitor and protect against suspicious activity in your VPC, which AWS service would you employ to analyze network traffic for potential threats?

Answer :

* AWS GuardDuty

Explanation :

AWS GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior within your AWS environment.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527145)

Which AWS service is most suitable for protecting API endpoints from malicious traffic and maintaining the integrity of API communications?

Answer :

* AWS WAF

Explanation :

AWS WAF is well-suited for protecting API endpoints by filtering and monitoring HTTP and HTTPS requests against known and custom threat signatures.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527224)

Why is it important to integrate AWS CloudFront with AWS Shield for content delivery during a large-scale attack?

Answer :

* CloudFront provides a global network to absorb attacks

Explanation :

AWS CloudFront, when integrated with AWS Shield, uses its global edge locations to absorb and mitigate attacks, ensuring reliable content delivery.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527279)

How would enabling multi-region replication improve the security of archived data stored in S3?

Answer :

* Enhances data availability and durability

Explanation :

Multi-region replication improves security by enhancing data availability and durability, ensuring data is accessible even if one region goes down.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527095)

Which of the following best describes the role of Multi-Factor Authentication (MFA) in securing AWS accounts?

Answer :

* MFA adds an extra security layer by using a second form of authentication.

Explanation :

MFA adds an extra layer of protection by requiring a second form of authentication, such as a physical device or app, in addition to the password.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527259)

Which of the following best describes the primary function of Amazon Macie in the context of AWS data security?

Answer :

* Monitoring data for sensitive information using machine learning

Explanation :

Amazon Macie uses machine learning to discover, classify, and protect sensitive data stored in AWS. It helps identify PII and other critical data.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527258)

What is the primary function of AWS Organizations in managing multiple AWS accounts?

Answer :

* To provide central governance across multiple AWS accounts

Explanation :

AWS Organizations helps in centrally managing policies, access, and compliance across multiple AWS accounts, thereby providing central governance.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527174)

Given an RPO (Recovery Point Objective) of 1 hour, which AWS service should be used to back up a relational database every 30 minutes and why?

Answer :

* AWS RDS Snapshots

Explanation :

AWS RDS Snapshots allow you to back up your relational database at regular intervals to meet specific RPO requirements, such as every 30 minutes.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527069)

Which AWS service integration is exclusive to AWS Shield Advanced for additional protection against DDoS attacks?

Answer :

* AWS Web Application Firewall (WAF)

Explanation :

AWS Shield Advanced integrates with AWS Web Application Firewall (WAF) to provide advanced protection and rate-based rules against DDoS attacks.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527223)

Which of the following best describes the analogy used in the course regarding responding to threats in AWS environments?

Answer :

* A castle's response to an attack

Explanation :

The analogy of responding to threats in AWS environments is likened to a castle's response to an attack, involving detection, containment, recovery, and preparation.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471457)

How could you test the effective implementation of MFA on an AWS IAM user account?

Answer :

* Attempt to login with just the password

Explanation :

Trying to login with just the password and without the MFA code will reveal whether MFA is successfully implemented. A failed login would confirm that MFA is active.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527078)

Which AWS service can be used to securely connect on-premises data centers to AWS cloud resources?

Answer :

* AWS Direct Connect

Explanation :

AWS Direct Connect is a service that provides a dedicated network connection between on-premises data centers and AWS cloud resources, ensuring secure connectivity.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471399)

How does the analogy of a vaccine relate to AWS Firewall Manager in the context of security?

Answer :

* It highlights the centralized protection provided by AWS Firewall Manager

Explanation :

The analogy of a vaccine relates to AWS Firewall Manager by highlighting its centralized approach to providing protection against known threats in AWS environments.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471464)

How do AWS Security Hub findings metrics help in understanding the security posture of an AWS environment over a period?

Answer :

* By quantifying security incidents and trends

Explanation :

AWS Security Hub findings metrics provide quantified insights into security incidents and trends, enabling better understanding and improvement of security posture.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527079)

Which AWS service is commonly used for centralized management of AWS accounts, including the creation and management of AWS Organizations?

Answer :

* AWS Organizations

Explanation :

AWS Organizations is the service commonly used for centralized management of AWS accounts, enabling the creation and management of account structures and policies.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471407)

What is the primary benefit of using server-side encryption with AWS S3-Managed Keys (SSE-S3) for archived data?

Answer :

* Simplified management of encryption keys

Explanation :

Server-side encryption with AWS S3-Managed Keys (SSE-S3) simplifies the management of encryption keys by having AWS handle encryption and decryption transparently.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527171)

What is the primary advantage of using AWS CloudHSM compared to AWS KMS for managing encryption keys?

Answer :

* Complete control over keys

Explanation :

AWS CloudHSM provides complete control over encryption keys as it runs on dedicated hardware managed by the customer, unlike AWS KMS which is fully managed by AWS.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527166)

Which AWS service acts as a Content Delivery Network (CDN) to cache content at edge locations globally?

Answer :

* AWS CloudFront

Explanation :

AWS CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527216)

In the context of data at rest, what is a primary benefit of using AWS CloudHSM?

Answer :

* Hardware-based key storage

Explanation :

AWS CloudHSM provides a hardware-based key storage solution that enhances security by isolating cryptographic operations within a tamper-evident, dedicated device.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527139)

Which AWS service is commonly used for managing access to secrets and enabling fine-grained permissions control?

Answer :

* AWS IAM

Explanation :

AWS Identity and Access Management (IAM) is commonly used for managing access to secrets and implementing fine-grained permissions control within AWS accounts.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471424)

Why is it important to enable MFA for root accounts on AWS?

Answer :

* To protect the account with the highest level of access

Explanation :

The root account has unrestricted access to all resources and settings in the account, making it critical to secure it with MFA to prevent unauthorized access.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527277)

If an AWS Organization has 5 accounts and each needs 4 different policies, how many total policies need to be managed without centralized deployment?

Answer :

* 20

Explanation :

Without centralized deployment, each of the 5 accounts would need 4 different policies, requiring a total of 5 \* 4 = 20 policies to be managed independently.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527110)

How does Amazon EventBridge handle the duplication of events when routing them to multiple targets?

Answer :

* Unique event IDs for each target invocation

Explanation :

Amazon EventBridge uses unique event identifiers for each target invocation to ensure that the same event is not processed multiple times by a single target.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527080)

For replicating data across AWS Regions to ensure disaster recovery, which service is the most suitable to configure in a multi-region setup?

Answer :

* Amazon S3 Cross-Region Replication (CRR)

Explanation :

Amazon S3 Cross-Region Replication (CRR) replicates objects between AWS Regions to meet higher redundancy, compliance needs, and disaster recovery scenarios.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527066)

A company is deploying a new web application on AWS. Based on their other web applications, they anticipate being the target of frequent DDoS attacks. Which steps can the company use to protect its application? Select 2 answers from the options given below.

Answer :

* Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic
* Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application

Explanation :

Option A is invalid because by default security groups don’t allow access Option C is invalid because AWS Inspector cannot be used to examine traffic

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20956)

To analyze API activity history via CloudTrail, which AWS service can be used to create visual reports and dashboards?

Answer :

* AWS QuickSight

Explanation :

AWS QuickSight can be used to create visual reports and dashboards for analyzing API activity history recorded by CloudTrail, helping in data visualization.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527141)

What is a baseline deviation and why is it important in monitoring AWS environments?

Answer :

* A deviation from normal operational performance, critical for understanding unusual activities.

Explanation :

A baseline deviation is a significant departure from normal operational performance, which helps in identifying unusual or potentially malicious activities.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527152)

How does the analogy of a ship navigating through stormy seas relate to responding to threats in AWS environments?

Answer :

* It emphasizes the need for continuous monitoring for threats

Explanation :

The analogy of a ship navigating through stormy seas highlights the importance of continuous monitoring for threats in AWS environments to ensure security.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471466)

Which AWS service provides temporary security credentials to applications to facilitate integration with an external identity provider?

Answer :

* AWS STS

Explanation :

AWS STS (Security Token Service) provides temporary security credentials to applications, facilitating secure integration with external identity providers.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527234)

Which AWS service is commonly used for managing access to secrets and enabling fine-grained permissions control?

Answer :

* AWS IAM

Explanation :

AWS Identity and Access Management (IAM) is commonly used for managing access to secrets and implementing fine-grained permissions control within AWS accounts.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471424)

Why is it important to enable MFA for root accounts on AWS?

Answer :

* To protect the account with the highest level of access

Explanation :

The root account has unrestricted access to all resources and settings in the account, making it critical to secure it with MFA to prevent unauthorized access.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527277)

If an AWS Organization has 5 accounts and each needs 4 different policies, how many total policies need to be managed without centralized deployment?

Answer :

* 20

Explanation :

Without centralized deployment, each of the 5 accounts would need 4 different policies, requiring a total of 5 \* 4 = 20 policies to be managed independently.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527110)

How does Amazon EventBridge handle the duplication of events when routing them to multiple targets?

Answer :

* Unique event IDs for each target invocation

Explanation :

Amazon EventBridge uses unique event identifiers for each target invocation to ensure that the same event is not processed multiple times by a single target.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527080)

For replicating data across AWS Regions to ensure disaster recovery, which service is the most suitable to configure in a multi-region setup?

Answer :

* Amazon S3 Cross-Region Replication (CRR)

Explanation :

Amazon S3 Cross-Region Replication (CRR) replicates objects between AWS Regions to meet higher redundancy, compliance needs, and disaster recovery scenarios.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527066)

A company is deploying a new web application on AWS. Based on their other web applications, they anticipate being the target of frequent DDoS attacks. Which steps can the company use to protect its application? Select 2 answers from the options given below.

Answer :

* Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic
* Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application

Explanation :

Option A is invalid because by default security groups don’t allow access Option C is invalid because AWS Inspector cannot be used to examine traffic

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20956)

To analyze API activity history via CloudTrail, which AWS service can be used to create visual reports and dashboards?

Answer :

* AWS QuickSight

Explanation :

AWS QuickSight can be used to create visual reports and dashboards for analyzing API activity history recorded by CloudTrail, helping in data visualization.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527141)

What is a baseline deviation and why is it important in monitoring AWS environments?

Answer :

* A deviation from normal operational performance, critical for understanding unusual activities.

Explanation :

A baseline deviation is a significant departure from normal operational performance, which helps in identifying unusual or potentially malicious activities.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527152)

How does the analogy of a ship navigating through stormy seas relate to responding to threats in AWS environments?

Answer :

* It emphasizes the need for continuous monitoring for threats

Explanation :

The analogy of a ship navigating through stormy seas highlights the importance of continuous monitoring for threats in AWS environments to ensure security.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471466)

Which AWS service provides temporary security credentials to applications to facilitate integration with an external identity provider?

Answer :

* AWS STS

Explanation :

AWS STS (Security Token Service) provides temporary security credentials to applications, facilitating secure integration with external identity providers.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527234)

What AWS service would you use for storing and managing access to encrypted database credentials for Amazon RDS?

Answer :

* AWS Secrets Manager

Explanation :

AWS Secrets Manager is the appropriate service for storing and managing access to encrypted database credentials in a secure manner.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527148)

Which AWS service provides a scalable and highly available Domain Name System (DNS) web service to route traffic to AWS resources?

Answer :

* AWS Route 53

Explanation :

AWS Route 53 is a scalable and highly available Domain Name System (DNS) web service that routes traffic to AWS resources securely.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471403)

What is the primary role of Amazon Route 53 in enhancing application resiliency during a DDoS attack?

Answer :

* Distributing traffic across multiple regions

Explanation :

Amazon Route 53 distributes traffic across multiple regions, helping to mitigate the impact of a DDoS attack by balancing the load.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527184)

Which AWS service does Control Tower utilize to automate account creation and governance in a multi-account environment?

Answer :

* AWS Organizations

Explanation :

AWS Control Tower leverages AWS Organizations to automate the account creation and governance process in a multi-account structure.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527222)

Under the AWS Shared Responsibility Model, why must customers manage the encryption of their data in transit?

Answer :

* Customers ensure regulatory compliance requirements

Explanation :

Customers must manage encryption in transit to meet regulatory compliance requirements, as AWS focuses on data encryption at rest.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527146)

When securing data in Amazon S3, what is the primary purpose of implementing bucket policies?

Answer :

* Controlling access to S3 buckets

Explanation :

Bucket policies in Amazon S3 are used to control access to S3 buckets, defining who can access the data stored within the buckets.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471427)

What is the primary benefit of encrypting a Secrets Manager secret using an AWS KMS key?

Answer :

* To add an extra layer of security

Explanation :

Encrypting a Secrets Manager secret with an AWS KMS key provides an additional layer of security for storing and managing secrets.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527167)

What is the primary purpose of having an Incident Response Plan (IRP) in AWS?

Answer :

* To ensure business continuity in case of security breaches.

Explanation :

An Incident Response Plan (IRP) ensures business continuity by providing a structured approach to responding to security breaches.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527179)

What is the primary purpose of using Amazon S3 access control lists (ACLs) in the context of data security?

Answer :

* To manage user permissions for specific buckets and objects.

Explanation :

Amazon S3 access control lists (ACLs) grant like-read and write permissions to objects and buckets for specific users and groups.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527182)

What is the primary purpose of using AWS KMS in conjunction with AWS Secrets Manager?

Answer :

* To encrypt and protect secrets

Explanation :

AWS KMS (Key Management Service) is used to encrypt secrets stored in AWS Secrets Manager, ensuring data protection and security.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527183)

What AWS service would you use for storing and managing access to encrypted database credentials for Amazon RDS?

Answer :

* AWS Secrets Manager

Explanation :

AWS Secrets Manager is the appropriate service for storing and managing access to encrypted database credentials in a secure manner.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527148)

Which AWS service provides a scalable and highly available Domain Name System (DNS) web service to route traffic to AWS resources?

Answer :

* AWS Route 53

Explanation :

AWS Route 53 is a scalable and highly available Domain Name System (DNS) web service that routes traffic to AWS resources securely.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471403)

What is the primary role of Amazon Route 53 in enhancing application resiliency during a DDoS attack?

Answer :

* Distributing traffic across multiple regions

Explanation :

Amazon Route 53 distributes traffic across multiple regions, helping to mitigate the impact of a DDoS attack by balancing the load.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527184)

Which AWS service does Control Tower utilize to automate account creation and governance in a multi-account environment?

Answer :

* AWS Organizations

Explanation :

AWS Control Tower leverages AWS Organizations to automate the account creation and governance process in a multi-account structure.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527222)

Under the AWS Shared Responsibility Model, why must customers manage the encryption of their data in transit?

Answer :

* Customers ensure regulatory compliance requirements

Explanation :

Customers must manage encryption in transit to meet regulatory compliance requirements, as AWS focuses on data encryption at rest.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527146)

When securing data in Amazon S3, what is the primary purpose of implementing bucket policies?

Answer :

* Controlling access to S3 buckets

Explanation :

Bucket policies in Amazon S3 are used to control access to S3 buckets, defining who can access the data stored within the buckets.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471427)

What is the primary benefit of encrypting a Secrets Manager secret using an AWS KMS key?

Answer :

* To add an extra layer of security

Explanation :

Encrypting a Secrets Manager secret with an AWS KMS key provides an additional layer of security for storing and managing secrets.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527167)

What is the primary purpose of having an Incident Response Plan (IRP) in AWS?

Answer :

* To ensure business continuity in case of security breaches.

Explanation :

An Incident Response Plan (IRP) ensures business continuity by providing a structured approach to responding to security breaches.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527179)

What is the primary purpose of using Amazon S3 access control lists (ACLs) in the context of data security?

Answer :

* To manage user permissions for specific buckets and objects.

Explanation :

Amazon S3 access control lists (ACLs) grant like-read and write permissions to objects and buckets for specific users and groups.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527182)

What is the primary purpose of using AWS KMS in conjunction with AWS Secrets Manager?

Answer :

* To encrypt and protect secrets

Explanation :

AWS KMS (Key Management Service) is used to encrypt secrets stored in AWS Secrets Manager, ensuring data protection and security.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527183)

What AWS service would you use for storing and managing access to encrypted database credentials for Amazon RDS?

Answer :

* AWS Secrets Manager

Explanation :

AWS Secrets Manager is the appropriate service for storing and managing access to encrypted database credentials in a secure manner.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527148)

Which AWS service provides a scalable and highly available Domain Name System (DNS) web service to route traffic to AWS resources?

Answer :

* AWS Route 53

Explanation :

AWS Route 53 is a scalable and highly available Domain Name System (DNS) web service that routes traffic to AWS resources securely.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471403)

What is the primary role of Amazon Route 53 in enhancing application resiliency during a DDoS attack?

Answer :

* Distributing traffic across multiple regions

Explanation :

Amazon Route 53 distributes traffic across multiple regions, helping to mitigate the impact of a DDoS attack by balancing the load.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527184)

Which AWS service does Control Tower utilize to automate account creation and governance in a multi-account environment?

Answer :

* AWS Organizations

Explanation :

AWS Control Tower leverages AWS Organizations to automate the account creation and governance process in a multi-account structure.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527222)

Under the AWS Shared Responsibility Model, why must customers manage the encryption of their data in transit?

Answer :

* Customers ensure regulatory compliance requirements

Explanation :

Customers must manage encryption in transit to meet regulatory compliance requirements, as AWS focuses on data encryption at rest.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527146)

When securing data in Amazon S3, what is the primary purpose of implementing bucket policies?

Answer :

* Controlling access to S3 buckets

Explanation :

Bucket policies in Amazon S3 are used to control access to S3 buckets, defining who can access the data stored within the buckets.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471427)

What is the primary benefit of encrypting a Secrets Manager secret using an AWS KMS key?

Answer :

* To add an extra layer of security

Explanation :

Encrypting a Secrets Manager secret with an AWS KMS key provides an additional layer of security for storing and managing secrets.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527167)

What is the primary purpose of having an Incident Response Plan (IRP) in AWS?

Answer :

* To ensure business continuity in case of security breaches.

Explanation :

An Incident Response Plan (IRP) ensures business continuity by providing a structured approach to responding to security breaches.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527179)

What is the primary purpose of using Amazon S3 access control lists (ACLs) in the context of data security?

Answer :

* To manage user permissions for specific buckets and objects.

Explanation :

Amazon S3 access control lists (ACLs) grant like-read and write permissions to objects and buckets for specific users and groups.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527182)

What is the primary purpose of using AWS KMS in conjunction with AWS Secrets Manager?

Answer :

* To encrypt and protect secrets

Explanation :

AWS KMS (Key Management Service) is used to encrypt secrets stored in AWS Secrets Manager, ensuring data protection and security.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527183)

What AWS service would you use for storing and managing access to encrypted database credentials for Amazon RDS?

Answer :

* AWS Secrets Manager

Explanation :

AWS Secrets Manager is the appropriate service for storing and managing access to encrypted database credentials in a secure manner.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527148)

Which AWS service provides a scalable and highly available Domain Name System (DNS) web service to route traffic to AWS resources?

Answer :

* AWS Route 53

Explanation :

AWS Route 53 is a scalable and highly available Domain Name System (DNS) web service that routes traffic to AWS resources securely.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471403)

What is the primary role of Amazon Route 53 in enhancing application resiliency during a DDoS attack?

Answer :

* Distributing traffic across multiple regions

Explanation :

Amazon Route 53 distributes traffic across multiple regions, helping to mitigate the impact of a DDoS attack by balancing the load.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527184)

Which AWS service does Control Tower utilize to automate account creation and governance in a multi-account environment?

Answer :

* AWS Organizations

Explanation :

AWS Control Tower leverages AWS Organizations to automate the account creation and governance process in a multi-account structure.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527222)

Under the AWS Shared Responsibility Model, why must customers manage the encryption of their data in transit?

Answer :

* Customers ensure regulatory compliance requirements

Explanation :

Customers must manage encryption in transit to meet regulatory compliance requirements, as AWS focuses on data encryption at rest.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527146)

When securing data in Amazon S3, what is the primary purpose of implementing bucket policies?

Answer :

* Controlling access to S3 buckets

Explanation :

Bucket policies in Amazon S3 are used to control access to S3 buckets, defining who can access the data stored within the buckets.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471427)

What is the primary benefit of encrypting a Secrets Manager secret using an AWS KMS key?

Answer :

* To add an extra layer of security

Explanation :

Encrypting a Secrets Manager secret with an AWS KMS key provides an additional layer of security for storing and managing secrets.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527167)

What is the primary purpose of having an Incident Response Plan (IRP) in AWS?

Answer :

* To ensure business continuity in case of security breaches.

Explanation :

An Incident Response Plan (IRP) ensures business continuity by providing a structured approach to responding to security breaches.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527179)

What is the primary purpose of using Amazon S3 access control lists (ACLs) in the context of data security?

Answer :

* To manage user permissions for specific buckets and objects.

Explanation :

Amazon S3 access control lists (ACLs) grant like-read and write permissions to objects and buckets for specific users and groups.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527182)

What is the primary purpose of using AWS KMS in conjunction with AWS Secrets Manager?

Answer :

* To encrypt and protect secrets

Explanation :

AWS KMS (Key Management Service) is used to encrypt secrets stored in AWS Secrets Manager, ensuring data protection and security.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527183)

How does AWS WAF manage and filter incoming requests to protect web applications?

Answer :

* By defining custom rule sets

Explanation :

AWS WAF uses custom rule sets to filter and manage incoming requests, ensuring unauthorized and malicious traffic is blocked.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527085)

Given an S3 bucket with 100,000 files and Amazon Macie configured to process at 1,000 files per hour, how long will it take to complete the first full scan?

Answer :

* 100 hours

Explanation :

It will take Macie 100 hours to complete the scan of 100,000 files at a rate of 1,000 files per hour. (100,000 / 1,000 = 100)

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527070)

Which AWS CLI command retrieves the value of a secret stored in AWS Secrets Manager, assuming the secret's name is 'MySecret'?

Answer :

* aws secretsmanager get-secret-value --secret-id MySecret

Explanation :

The correct AWS CLI command is 'aws secretsmanager get-secret-value --secret-id MySecret' to retrieve the value of a secret.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527211)

Which AWS service provides real-time security recommendations for optimizing your AWS resources and improving your security posture?

Answer :

* AWS Trusted Advisor

Explanation :

AWS Trusted Advisor provides real-time recommendations to help you optimize your AWS resources following AWS best practices.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527233)

When combining both IAM policies and resource-based policies, what determines the final permissions a user has?

Answer :

* The intersection of IAM and resource-based policies

Explanation :

The final permissions are determined by the intersection of permissions granted by both the IAM and resource-based policies.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527191)

You are working in the cloud security team in a big company. In order to meet security compliance, you are in charge of applying AWS Config rules to AWS accounts in other organizational units (OUs). However, it has been found that the Config rules may be deleted by IAM users accidentally in these AWS accounts. You need to prevent such actions from happening again. How should you implement this?

Answer :

* Implement a SCP that contains a deny to DeleteConfigRule action and apply the SCP to organizational units in the AWS Organization

Explanation :

In this case, a central control using SCP is needed to prevent users in organizational units from deleting AWS Config rules

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20952)

To monitor and manage your AWS resources during an attack, which service would you use to gain better operational insights?

Answer :

* Amazon CloudWatch

Explanation :

Amazon CloudWatch provides monitoring and operational insights, helping you manage resources effectively during an attack.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527144)

When implementing AWS Web Application Firewall (WAF) for edge protection, how can you test the rules without blocking traffic?

Answer :

* Deploy rules in Count mode

Explanation :

Deploying WAF rules in Count mode allows you to test the rules and see their impact without actually blocking the traffic.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527201)

Which feature of AWS Shield Advanced allows for proactive engagement with AWSs DDoS response team?

Answer :

* 24x7 access to DDoS experts

Explanation :

AWS Shield Advanced provides 24x7 access to the AWS DDoS Response Team (DRT) for proactive engagement during DDoS attacks.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527248)

How can Amazon GuardDuty findings be used to initiate automated incident response?

Answer :

* By integrating with AWS Lambda to trigger functions.

Explanation :

Amazon GuardDuty findings can be integrated with AWS Lambda functions to automatically initiate incident response actions.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527072)

How does AWS WAF manage and filter incoming requests to protect web applications?

Answer :

* By defining custom rule sets

Explanation :

AWS WAF uses custom rule sets to filter and manage incoming requests, ensuring unauthorized and malicious traffic is blocked.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527085)

Given an S3 bucket with 100,000 files and Amazon Macie configured to process at 1,000 files per hour, how long will it take to complete the first full scan?

Answer :

* 100 hours

Explanation :

It will take Macie 100 hours to complete the scan of 100,000 files at a rate of 1,000 files per hour. (100,000 / 1,000 = 100)

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527070)

Which AWS CLI command retrieves the value of a secret stored in AWS Secrets Manager, assuming the secret's name is 'MySecret'?

Answer :

* aws secretsmanager get-secret-value --secret-id MySecret

Explanation :

The correct AWS CLI command is 'aws secretsmanager get-secret-value --secret-id MySecret' to retrieve the value of a secret.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527211)

Which AWS service provides real-time security recommendations for optimizing your AWS resources and improving your security posture?

Answer :

* AWS Trusted Advisor

Explanation :

AWS Trusted Advisor provides real-time recommendations to help you optimize your AWS resources following AWS best practices.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527233)

When combining both IAM policies and resource-based policies, what determines the final permissions a user has?

Answer :

* The intersection of IAM and resource-based policies

Explanation :

The final permissions are determined by the intersection of permissions granted by both the IAM and resource-based policies.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527191)

You are working in the cloud security team in a big company. In order to meet security compliance, you are in charge of applying AWS Config rules to AWS accounts in other organizational units (OUs). However, it has been found that the Config rules may be deleted by IAM users accidentally in these AWS accounts. You need to prevent such actions from happening again. How should you implement this?

Answer :

* Implement a SCP that contains a deny to DeleteConfigRule action and apply the SCP to organizational units in the AWS Organization

Explanation :

In this case, a central control using SCP is needed to prevent users in organizational units from deleting AWS Config rules

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20952)

To monitor and manage your AWS resources during an attack, which service would you use to gain better operational insights?

Answer :

* Amazon CloudWatch

Explanation :

Amazon CloudWatch provides monitoring and operational insights, helping you manage resources effectively during an attack.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527144)

When implementing AWS Web Application Firewall (WAF) for edge protection, how can you test the rules without blocking traffic?

Answer :

* Deploy rules in Count mode

Explanation :

Deploying WAF rules in Count mode allows you to test the rules and see their impact without actually blocking the traffic.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527201)

Which feature of AWS Shield Advanced allows for proactive engagement with AWSs DDoS response team?

Answer :

* 24x7 access to DDoS experts

Explanation :

AWS Shield Advanced provides 24x7 access to the AWS DDoS Response Team (DRT) for proactive engagement during DDoS attacks.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527248)

How can Amazon GuardDuty findings be used to initiate automated incident response?

Answer :

* By integrating with AWS Lambda to trigger functions.

Explanation :

Amazon GuardDuty findings can be integrated with AWS Lambda functions to automatically initiate incident response actions.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527072)

What is the primary benefit of using AWS Shield Advanced over AWS Shield Standard for protecting your infrastructure?

Answer :

* 24/7 access to the AWS DDoS Response Team (DRT)

Explanation :

AWS Shield Advanced includes 24/7 access to the AWS DDoS Response Team (DRT) for sophisticated and large-scale attacks.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527170)

If 'John' is assigned two IAM policies: one allowing 's3:PutObject' and another denying 's3:PutObject' on the same bucket, what is the effective permission?

Answer :

* Deny

Explanation :

In IAM policies, explicit deny always overrides allow. Therefore, 'John' will be denied the ability to 's3:PutObject'.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527118)

Why might a security engineer prefer to use AWS CLI for infrastructure management over SDKs?

Answer :

* CLI allows for easier script automation

Explanation :

AWS CLI facilitates easier script automation, which is valuable for consistent and repeatable security configurations.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527284)

When configuring a federated SSO in AWS, which AWS service allows you to manage user authentication with an external identity provider?

Answer :

* Amazon Cognito

Explanation :

Amazon Cognito provides features to manage user authentication, including federation with external identity providers.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527192)

Based on AWS best practices, how many IAM policies should an administrative role have compared to the root user account?

Answer :

* Irrelevant since root should have no policies

Explanation :

The root user account should have no policies attached directly to it; instead, create IAM roles with proper policies.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527059)

During a simulated DDoS attack, what metric would best measure the effectiveness of AWS Shield Advanced?

Answer :

* Network latency increase before and after mitigation

Explanation :

Network latency increase can show how quickly AWS Shield Advanced mitigates the attack and restores normal operations.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527062)

What is the main rationale behind AWSs recommendation to avoid using the root user for daily tasks?

Answer :

* Root user has unrestricted access

Explanation :

The root user has unrestricted access, and its credentials being compromised could lead to significant security risks.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527162)

You have created an AWS Managed Microsoft AD. How will you manage user permissions and roles?

Answer :

* Using IAM policies and IAM Identity Center

Explanation :

User permissions and roles in AWS Managed Microsoft AD can be managed using IAM policies and the IAM Identity Center.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527296)

An application role in your AWS account needs to access resources in another AWS account. Which IAM policy component is essential to set up this cross-account access?

Answer :

* Trust Policy

Explanation :

A trust policy is essential for cross-account access as it specifies the trusted entities allowed to assume the role.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527057)

How does the use of MFA affect the access permissions of an IAM user during a session?

Answer :

* MFA does not directly impact access permissions.

Explanation :

MFA itself does not alter access permissions. It simply acts as an additional security measure during authentication.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527090)

What is the primary benefit of using AWS Shield Advanced over AWS Shield Standard for protecting your infrastructure?

Answer :

* 24/7 access to the AWS DDoS Response Team (DRT)

Explanation :

AWS Shield Advanced includes 24/7 access to the AWS DDoS Response Team (DRT) for sophisticated and large-scale attacks.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527170)

If 'John' is assigned two IAM policies: one allowing 's3:PutObject' and another denying 's3:PutObject' on the same bucket, what is the effective permission?

Answer :

* Deny

Explanation :

In IAM policies, explicit deny always overrides allow. Therefore, 'John' will be denied the ability to 's3:PutObject'.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527118)

Why might a security engineer prefer to use AWS CLI for infrastructure management over SDKs?

Answer :

* CLI allows for easier script automation

Explanation :

AWS CLI facilitates easier script automation, which is valuable for consistent and repeatable security configurations.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527284)

When configuring a federated SSO in AWS, which AWS service allows you to manage user authentication with an external identity provider?

Answer :

* Amazon Cognito

Explanation :

Amazon Cognito provides features to manage user authentication, including federation with external identity providers.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527192)

Based on AWS best practices, how many IAM policies should an administrative role have compared to the root user account?

Answer :

* Irrelevant since root should have no policies

Explanation :

The root user account should have no policies attached directly to it; instead, create IAM roles with proper policies.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527059)

During a simulated DDoS attack, what metric would best measure the effectiveness of AWS Shield Advanced?

Answer :

* Network latency increase before and after mitigation

Explanation :

Network latency increase can show how quickly AWS Shield Advanced mitigates the attack and restores normal operations.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527062)

What is the main rationale behind AWSs recommendation to avoid using the root user for daily tasks?

Answer :

* Root user has unrestricted access

Explanation :

The root user has unrestricted access, and its credentials being compromised could lead to significant security risks.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527162)

You have created an AWS Managed Microsoft AD. How will you manage user permissions and roles?

Answer :

* Using IAM policies and IAM Identity Center

Explanation :

User permissions and roles in AWS Managed Microsoft AD can be managed using IAM policies and the IAM Identity Center.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527296)

An application role in your AWS account needs to access resources in another AWS account. Which IAM policy component is essential to set up this cross-account access?

Answer :

* Trust Policy

Explanation :

A trust policy is essential for cross-account access as it specifies the trusted entities allowed to assume the role.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527057)

How does the use of MFA affect the access permissions of an IAM user during a session?

Answer :

* MFA does not directly impact access permissions.

Explanation :

MFA itself does not alter access permissions. It simply acts as an additional security measure during authentication.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527090)

When archiving data, what configuration change can you make to an S3 bucket to ensure its contents are immutable?

Answer :

* Enforce S3 Object Lock

Explanation :

S3 Object Lock ensures that object versions cannot be deleted or overwritten, ensuring data immutability.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527190)

An Application team is designing a solution with two applications. The Security team wants the applications' logs to be captured in two different places, because one of the applications produces logs with sensitive data. Which solution meets the requirement with the least risk and effort?

Answer :

* Use Amazon CloudWatch Logs with two log groups, with one for each application, and use an AWS IAM policy to control access to the log groups, as required

Explanation :

Each application's log can be configured to send the log to a specific Amazon CloudWatch Logs log group.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_21079)

You need to review CloudTrail logs for API requests over the last 90 days. If each day generates approximately 100 MB of log data, approximately how much storage will you need to analyze all logs?

Answer :

* 9 GB

Explanation :

For 90 days with 100 MB of log data per day, the total storage required is 90 \* 100 MB = 9000 MB = 9 GB.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527299)

Which of the following ways to interact with AWS is most suited for creating and managing complex AWS Cloud infrastructure deployments across multiple regions?

Answer :

* AWS CloudFormation

Explanation :

AWS CloudFormation is designed to handle complex infrastructure deployments globally by using templates.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527263)

When experimenting with Amazon S3 bucket access, what command would you use to retrieve a list of existing buckets using the AWS CLI?

Answer :

* aws s3 ls

Explanation :

The command " "aws s3 ls " " lists all the S3 buckets owned by the authenticated sender of the request.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527198)

Which AWS service should you use to enable single sign-on (SSO) access to multiple AWS accounts and applications?

Answer :

* AWS IAM Identity Center (formerly AWS SSO)

Explanation :

AWS IAM Identity Center provides single sign-on (SSO) access to multiple AWS accounts and applications.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527239)

Which AWS services should you leverage to automatically classify and respond to a DDoS attack?

Answer :

* AWS Shield and AWS WAF

Explanation :

AWS Shield and AWS WAF are specifically designed to mitigate and respond to DDoS attacks automatically.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527244)

Which AWS service is primarily responsible for mitigating DDoS attacks at both the application and network layers?

Answer :

* AWS Shield

Explanation :

AWS Shield provides protection against DDoS attacks, covering both the application and network layers.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527226)

In an incident response scenario, if a team has a Response Time Objective (RTO) of 4 hours, and they start mitigation actions within 1 hour, how many hours do they have left to complete the mitigation?

Answer :

* 3 hours

Explanation :

With an RTO of 4 hours and 1 hour already spent, the team has 3 hours left to complete the mitigation.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527134)

If you have 5 AWS accounts managed under AWS Control Tower with each account having a monthly compliance check cost of $0.10, what is the total monthly cost for compliance checks?

Answer :

* $0.50

Explanation :

The total monthly cost for compliance checks is calculated as 5 accounts \* $0.10 per account = $0.50.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527122)

When archiving data, what configuration change can you make to an S3 bucket to ensure its contents are immutable?

Answer :

* Enforce S3 Object Lock

Explanation :

S3 Object Lock ensures that object versions cannot be deleted or overwritten, ensuring data immutability.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527190)

An Application team is designing a solution with two applications. The Security team wants the applications' logs to be captured in two different places, because one of the applications produces logs with sensitive data. Which solution meets the requirement with the least risk and effort?

Answer :

* Use Amazon CloudWatch Logs with two log groups, with one for each application, and use an AWS IAM policy to control access to the log groups, as required

Explanation :

Each application's log can be configured to send the log to a specific Amazon CloudWatch Logs log group.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_21079)

You need to review CloudTrail logs for API requests over the last 90 days. If each day generates approximately 100 MB of log data, approximately how much storage will you need to analyze all logs?

Answer :

* 9 GB

Explanation :

For 90 days with 100 MB of log data per day, the total storage required is 90 \* 100 MB = 9000 MB = 9 GB.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527299)

Which of the following ways to interact with AWS is most suited for creating and managing complex AWS Cloud infrastructure deployments across multiple regions?

Answer :

* AWS CloudFormation

Explanation :

AWS CloudFormation is designed to handle complex infrastructure deployments globally by using templates.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527263)

When experimenting with Amazon S3 bucket access, what command would you use to retrieve a list of existing buckets using the AWS CLI?

Answer :

* aws s3 ls

Explanation :

The command " "aws s3 ls " " lists all the S3 buckets owned by the authenticated sender of the request.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527198)

Which AWS service should you use to enable single sign-on (SSO) access to multiple AWS accounts and applications?

Answer :

* AWS IAM Identity Center (formerly AWS SSO)

Explanation :

AWS IAM Identity Center provides single sign-on (SSO) access to multiple AWS accounts and applications.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527239)

Which AWS services should you leverage to automatically classify and respond to a DDoS attack?

Answer :

* AWS Shield and AWS WAF

Explanation :

AWS Shield and AWS WAF are specifically designed to mitigate and respond to DDoS attacks automatically.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527244)

Which AWS service is primarily responsible for mitigating DDoS attacks at both the application and network layers?

Answer :

* AWS Shield

Explanation :

AWS Shield provides protection against DDoS attacks, covering both the application and network layers.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527226)

In an incident response scenario, if a team has a Response Time Objective (RTO) of 4 hours, and they start mitigation actions within 1 hour, how many hours do they have left to complete the mitigation?

Answer :

* 3 hours

Explanation :

With an RTO of 4 hours and 1 hour already spent, the team has 3 hours left to complete the mitigation.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527134)

If you have 5 AWS accounts managed under AWS Control Tower with each account having a monthly compliance check cost of $0.10, what is the total monthly cost for compliance checks?

Answer :

* $0.50

Explanation :

The total monthly cost for compliance checks is calculated as 5 accounts \* $0.10 per account = $0.50.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527122)

When archiving data, what configuration change can you make to an S3 bucket to ensure its contents are immutable?

Answer :

* Enforce S3 Object Lock

Explanation :

S3 Object Lock ensures that object versions cannot be deleted or overwritten, ensuring data immutability.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527190)

An Application team is designing a solution with two applications. The Security team wants the applications' logs to be captured in two different places, because one of the applications produces logs with sensitive data. Which solution meets the requirement with the least risk and effort?

Answer :

* Use Amazon CloudWatch Logs with two log groups, with one for each application, and use an AWS IAM policy to control access to the log groups, as required

Explanation :

Each application's log can be configured to send the log to a specific Amazon CloudWatch Logs log group.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_21079)

You need to review CloudTrail logs for API requests over the last 90 days. If each day generates approximately 100 MB of log data, approximately how much storage will you need to analyze all logs?

Answer :

* 9 GB

Explanation :

For 90 days with 100 MB of log data per day, the total storage required is 90 \* 100 MB = 9000 MB = 9 GB.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527299)

Which of the following ways to interact with AWS is most suited for creating and managing complex AWS Cloud infrastructure deployments across multiple regions?

Answer :

* AWS CloudFormation

Explanation :

AWS CloudFormation is designed to handle complex infrastructure deployments globally by using templates.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527263)

When experimenting with Amazon S3 bucket access, what command would you use to retrieve a list of existing buckets using the AWS CLI?

Answer :

* aws s3 ls

Explanation :

The command " "aws s3 ls " " lists all the S3 buckets owned by the authenticated sender of the request.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527198)

Which AWS service should you use to enable single sign-on (SSO) access to multiple AWS accounts and applications?

Answer :

* AWS IAM Identity Center (formerly AWS SSO)

Explanation :

AWS IAM Identity Center provides single sign-on (SSO) access to multiple AWS accounts and applications.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527239)

Which AWS services should you leverage to automatically classify and respond to a DDoS attack?

Answer :

* AWS Shield and AWS WAF

Explanation :

AWS Shield and AWS WAF are specifically designed to mitigate and respond to DDoS attacks automatically.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527244)

Which AWS service is primarily responsible for mitigating DDoS attacks at both the application and network layers?

Answer :

* AWS Shield

Explanation :

AWS Shield provides protection against DDoS attacks, covering both the application and network layers.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527226)

In an incident response scenario, if a team has a Response Time Objective (RTO) of 4 hours, and they start mitigation actions within 1 hour, how many hours do they have left to complete the mitigation?

Answer :

* 3 hours

Explanation :

With an RTO of 4 hours and 1 hour already spent, the team has 3 hours left to complete the mitigation.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527134)

If you have 5 AWS accounts managed under AWS Control Tower with each account having a monthly compliance check cost of $0.10, what is the total monthly cost for compliance checks?

Answer :

* $0.50

Explanation :

The total monthly cost for compliance checks is calculated as 5 accounts \* $0.10 per account = $0.50.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527122)

When archiving data, what configuration change can you make to an S3 bucket to ensure its contents are immutable?

Answer :

* Enforce S3 Object Lock

Explanation :

S3 Object Lock ensures that object versions cannot be deleted or overwritten, ensuring data immutability.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527190)

An Application team is designing a solution with two applications. The Security team wants the applications' logs to be captured in two different places, because one of the applications produces logs with sensitive data. Which solution meets the requirement with the least risk and effort?

Answer :

* Use Amazon CloudWatch Logs with two log groups, with one for each application, and use an AWS IAM policy to control access to the log groups, as required

Explanation :

Each application's log can be configured to send the log to a specific Amazon CloudWatch Logs log group.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_21079)

You need to review CloudTrail logs for API requests over the last 90 days. If each day generates approximately 100 MB of log data, approximately how much storage will you need to analyze all logs?

Answer :

* 9 GB

Explanation :

For 90 days with 100 MB of log data per day, the total storage required is 90 \* 100 MB = 9000 MB = 9 GB.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527299)

Which of the following ways to interact with AWS is most suited for creating and managing complex AWS Cloud infrastructure deployments across multiple regions?

Answer :

* AWS CloudFormation

Explanation :

AWS CloudFormation is designed to handle complex infrastructure deployments globally by using templates.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527263)

When experimenting with Amazon S3 bucket access, what command would you use to retrieve a list of existing buckets using the AWS CLI?

Answer :

* aws s3 ls

Explanation :

The command " "aws s3 ls " " lists all the S3 buckets owned by the authenticated sender of the request.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527198)

Which AWS service should you use to enable single sign-on (SSO) access to multiple AWS accounts and applications?

Answer :

* AWS IAM Identity Center (formerly AWS SSO)

Explanation :

AWS IAM Identity Center provides single sign-on (SSO) access to multiple AWS accounts and applications.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527239)

Which AWS services should you leverage to automatically classify and respond to a DDoS attack?

Answer :

* AWS Shield and AWS WAF

Explanation :

AWS Shield and AWS WAF are specifically designed to mitigate and respond to DDoS attacks automatically.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527244)

Which AWS service is primarily responsible for mitigating DDoS attacks at both the application and network layers?

Answer :

* AWS Shield

Explanation :

AWS Shield provides protection against DDoS attacks, covering both the application and network layers.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527226)

In an incident response scenario, if a team has a Response Time Objective (RTO) of 4 hours, and they start mitigation actions within 1 hour, how many hours do they have left to complete the mitigation?

Answer :

* 3 hours

Explanation :

With an RTO of 4 hours and 1 hour already spent, the team has 3 hours left to complete the mitigation.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527134)

If you have 5 AWS accounts managed under AWS Control Tower with each account having a monthly compliance check cost of $0.10, what is the total monthly cost for compliance checks?

Answer :

* $0.50

Explanation :

The total monthly cost for compliance checks is calculated as 5 accounts \* $0.10 per account = $0.50.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527122)

Which AWS CLI command should be used to simulate the effect of an IAM policy attached to a role?

Answer :

* aws iam simulate-policy

Explanation :

The " "aws iam simulate-policy " " command is used to simulate the effects of a policy in AWS IAM.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527212)

In a lab, you create an IAM policy denying 's3:DeleteObject' on a specific bucket. What will be the outcome if you try to delete an object in that bucket using an IAM user with this policy attached?

Answer :

* Delete operation will be denied

Explanation :

The policy explicitly denies 's3:DeleteObject', so any attempt to delete an object will be denied.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527129)

If an AWS KMS key is used to encrypt 100,000 objects per day, calculate the annual cost assuming the first 20,000 requests are free and each additional request costs $0.03 per 10,000 requests.

Answer :

* $219

Explanation :

Annual cost = (100,000 - 20,000) requests/day \* 365 days/year \* $0.03 per 10,000 requests = $219.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527108)

If an AWS STS token is valid for an hour and a user acquires it via federation at 2:00 PM, when will the token expire?

Answer :

* 3:00 PM

Explanation :

If the STS token is acquired at 2:00 PM and is valid for one hour, it will expire at 3:00 PM.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527111)

If AWS Shield Advanced charges an additional fee of $3,000 per month plus $0.05 per GB of data processed during a DDoS attack, calculate the additional cost for processing 1000 GB in one month.

Answer :

* $3,500

Explanation :

The cost is calculated as follows: $3,000 (monthly fee) + (1000 GB \* $0.05 per GB) = $3,500.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527117)

Which of the following AWS services can be used to query VPC flow logs using SQL-like syntax?

Answer :

* Amazon Athena

Explanation :

Amazon Athena can be used to run SQL queries on data stored in S3, including VPC flow logs.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527256)

If a company has 3 AWS Managed Microsoft AD directories, each handling 500 users, how many user accounts in total can these directories manage?

Answer :

* 1500

Explanation :

Each directory manages 500 users, so 3 directories handle a total of 3 \* 500 = 1500 users.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527102)

Your department is in charge of developing an ecommerce website where customers can browse and purchase products online. The application is developed in AWS platform and a wide range of AWS services are used including EC2, Lambda, CloudFormation, etc. Recently, internal security auditors asked you to provide a document to state that the related AWS services met the Payment Card Industry (PCI) compliance. How should you provide the document?

Answer :

* Download Payment Card Industry (PCI) compliance document from AWS Artifact and provide it to auditors

Explanation :

When compliance document is mentioned for AWS services, AWS Artifact should be considered

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20949)

Given an incident response scenario, calculate the expected time to resolve an incident if the mean time to detect (MTTD) is 2 hours and the mean time to respond (MTTR) is 3 hours.

Answer :

* 5 hours

Explanation :

Time to resolve an incident is typically the sum of MTTD and MTTR, thus 2 + 3 = 5 hours.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527068)

Which AWS tool allows you to manage your AWS resources using programming languages like Python, Go, Ruby, and others?

Answer :

* AWS SDKs

Explanation :

AWS SDKs allow you to interact with AWS services using various programming languages.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527245)

Which AWS CLI command should be used to simulate the effect of an IAM policy attached to a role?

Answer :

* aws iam simulate-policy

Explanation :

The " "aws iam simulate-policy " " command is used to simulate the effects of a policy in AWS IAM.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527212)

In a lab, you create an IAM policy denying 's3:DeleteObject' on a specific bucket. What will be the outcome if you try to delete an object in that bucket using an IAM user with this policy attached?

Answer :

* Delete operation will be denied

Explanation :

The policy explicitly denies 's3:DeleteObject', so any attempt to delete an object will be denied.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527129)

If an AWS KMS key is used to encrypt 100,000 objects per day, calculate the annual cost assuming the first 20,000 requests are free and each additional request costs $0.03 per 10,000 requests.

Answer :

* $219

Explanation :

Annual cost = (100,000 - 20,000) requests/day \* 365 days/year \* $0.03 per 10,000 requests = $219.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527108)

If an AWS STS token is valid for an hour and a user acquires it via federation at 2:00 PM, when will the token expire?

Answer :

* 3:00 PM

Explanation :

If the STS token is acquired at 2:00 PM and is valid for one hour, it will expire at 3:00 PM.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527111)

If AWS Shield Advanced charges an additional fee of $3,000 per month plus $0.05 per GB of data processed during a DDoS attack, calculate the additional cost for processing 1000 GB in one month.

Answer :

* $3,500

Explanation :

The cost is calculated as follows: $3,000 (monthly fee) + (1000 GB \* $0.05 per GB) = $3,500.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527117)

Which of the following AWS services can be used to query VPC flow logs using SQL-like syntax?

Answer :

* Amazon Athena

Explanation :

Amazon Athena can be used to run SQL queries on data stored in S3, including VPC flow logs.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527256)

If a company has 3 AWS Managed Microsoft AD directories, each handling 500 users, how many user accounts in total can these directories manage?

Answer :

* 1500

Explanation :

Each directory manages 500 users, so 3 directories handle a total of 3 \* 500 = 1500 users.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527102)

Your department is in charge of developing an ecommerce website where customers can browse and purchase products online. The application is developed in AWS platform and a wide range of AWS services are used including EC2, Lambda, CloudFormation, etc. Recently, internal security auditors asked you to provide a document to state that the related AWS services met the Payment Card Industry (PCI) compliance. How should you provide the document?

Answer :

* Download Payment Card Industry (PCI) compliance document from AWS Artifact and provide it to auditors

Explanation :

When compliance document is mentioned for AWS services, AWS Artifact should be considered

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20949)

Given an incident response scenario, calculate the expected time to resolve an incident if the mean time to detect (MTTD) is 2 hours and the mean time to respond (MTTR) is 3 hours.

Answer :

* 5 hours

Explanation :

Time to resolve an incident is typically the sum of MTTD and MTTR, thus 2 + 3 = 5 hours.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527068)

Which AWS tool allows you to manage your AWS resources using programming languages like Python, Go, Ruby, and others?

Answer :

* AWS SDKs

Explanation :

AWS SDKs allow you to interact with AWS services using various programming languages.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527245)

Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following · Whether any ports are left open other than admin ones like SSH and RDP · Whether any ports to the database server other than ones from the web server security group are open Which of the following can help achieve this in the easiest way possible so that you don’t have to carry out an extra configuration change?

Answer :

* AWS Trusted Advisor

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?

Answer :

* Define the tags on the test and production servers and add a condition to the IAMpolicy which allows access to specific tags

Your company is planning on AWS hosting its AWS resources. There is a company policy that mandates that all key pairs are completely managed within the company itself. Which of the following is the correct measure of following this policy?

Answer :

* Generating the key pairs for the EC2 Instances using puttygen

A Security Engineer is tasked to automate the encryption of AWS CloudTrail logs using a Customer Master Key (CMK) in AWS KMS. The CMK will also be used to encrypt and decrypt log files for multiple accounts across all regions.

Answer :

* <p>Use server-side encryption with AWS KMS&ndash;managed keys (SSE-KMS) for the CloudTrail log files.</p>

An organization has set up multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

Answer :

* Create an IAM policy with a condition which denies access when the IP address range is not from the organization

Your company is hosting a set of EC2 Instances in AWS. They want to have the ability to detect if any port scans occur on their AWS EC2 Instances. Which of the following can help in this regard?

Answer :

* Use AWS Guard Duty to monitor any malicious port scans

Your company is planning on developing an application in AWS. This is a web-based application. The application users will use their Facebook or Google identities for authentication. Which of the following is a step you include in your implementation for the web application?

Answer :

* Create an OIDC identity provider in AWS

Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?

Answer :

* Monitor the S3 API calls by using Cloudtrail logging

A company has been using the AWS KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys that are no longer in use. What are the ways that can be incorporated to see which keys are in use?

Answer :

* <p>Use CloudTrail to see if any KMS API request has been issued against existing keys</p>

Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following · Whether any ports are left open other than admin ones like SSH and RDP · Whether any ports to the database server other than ones from the web server security group are open Which of the following can help achieve this in the easiest way possible so that you don’t have to carry out an extra configuration change?

Answer :

* AWS Trusted Advisor

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?

Answer :

* Define the tags on the test and production servers and add a condition to the IAMpolicy which allows access to specific tags

Your company is planning on AWS hosting its AWS resources. There is a company policy that mandates that all key pairs are completely managed within the company itself. Which of the following is the correct measure of following this policy?

Answer :

* Generating the key pairs for the EC2 Instances using puttygen

A Security Engineer is tasked to automate the encryption of AWS CloudTrail logs using a Customer Master Key (CMK) in AWS KMS. The CMK will also be used to encrypt and decrypt log files for multiple accounts across all regions.

Answer :

* <p>Use server-side encryption with AWS KMS&ndash;managed keys (SSE-KMS) for the CloudTrail log files.</p>

An organization has set up multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

Answer :

* Create an IAM policy with a condition which denies access when the IP address range is not from the organization

Your company is hosting a set of EC2 Instances in AWS. They want to have the ability to detect if any port scans occur on their AWS EC2 Instances. Which of the following can help in this regard?

Answer :

* Use AWS Guard Duty to monitor any malicious port scans

Your company is planning on developing an application in AWS. This is a web-based application. The application users will use their Facebook or Google identities for authentication. Which of the following is a step you include in your implementation for the web application?

Answer :

* Create an OIDC identity provider in AWS

Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?

Answer :

* Monitor the S3 API calls by using Cloudtrail logging

A company has been using the AWS KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys that are no longer in use. What are the ways that can be incorporated to see which keys are in use?

Answer :

* <p>Use CloudTrail to see if any KMS API request has been issued against existing keys</p>

Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following · Whether any ports are left open other than admin ones like SSH and RDP · Whether any ports to the database server other than ones from the web server security group are open Which of the following can help achieve this in the easiest way possible so that you don’t have to carry out an extra configuration change?

Answer :

* AWS Trusted Advisor

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?

Answer :

* Define the tags on the test and production servers and add a condition to the IAMpolicy which allows access to specific tags

Your company is planning on AWS hosting its AWS resources. There is a company policy that mandates that all key pairs are completely managed within the company itself. Which of the following is the correct measure of following this policy?

Answer :

* Generating the key pairs for the EC2 Instances using puttygen

A Security Engineer is tasked to automate the encryption of AWS CloudTrail logs using a Customer Master Key (CMK) in AWS KMS. The CMK will also be used to encrypt and decrypt log files for multiple accounts across all regions.

Answer :

* <p>Use server-side encryption with AWS KMS&ndash;managed keys (SSE-KMS) for the CloudTrail log files.</p>

An organization has set up multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

Answer :

* Create an IAM policy with a condition which denies access when the IP address range is not from the organization

Your company is hosting a set of EC2 Instances in AWS. They want to have the ability to detect if any port scans occur on their AWS EC2 Instances. Which of the following can help in this regard?

Answer :

* Use AWS Guard Duty to monitor any malicious port scans

Your company is planning on developing an application in AWS. This is a web-based application. The application users will use their Facebook or Google identities for authentication. Which of the following is a step you include in your implementation for the web application?

Answer :

* Create an OIDC identity provider in AWS

Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?

Answer :

* Monitor the S3 API calls by using Cloudtrail logging

A company has been using the AWS KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys that are no longer in use. What are the ways that can be incorporated to see which keys are in use?

Answer :

* <p>Use CloudTrail to see if any KMS API request has been issued against existing keys</p>

Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following · Whether any ports are left open other than admin ones like SSH and RDP · Whether any ports to the database server other than ones from the web server security group are open Which of the following can help achieve this in the easiest way possible so that you don’t have to carry out an extra configuration change?

Answer :

* AWS Trusted Advisor

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?

Answer :

* Define the tags on the test and production servers and add a condition to the IAMpolicy which allows access to specific tags

Your company is planning on AWS hosting its AWS resources. There is a company policy that mandates that all key pairs are completely managed within the company itself. Which of the following is the correct measure of following this policy?

Answer :

* Generating the key pairs for the EC2 Instances using puttygen

A Security Engineer is tasked to automate the encryption of AWS CloudTrail logs using a Customer Master Key (CMK) in AWS KMS. The CMK will also be used to encrypt and decrypt log files for multiple accounts across all regions.

Answer :

* <p>Use server-side encryption with AWS KMS&ndash;managed keys (SSE-KMS) for the CloudTrail log files.</p>

An organization has set up multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

Answer :

* Create an IAM policy with a condition which denies access when the IP address range is not from the organization

Your company is hosting a set of EC2 Instances in AWS. They want to have the ability to detect if any port scans occur on their AWS EC2 Instances. Which of the following can help in this regard?

Answer :

* Use AWS Guard Duty to monitor any malicious port scans

Your company is planning on developing an application in AWS. This is a web-based application. The application users will use their Facebook or Google identities for authentication. Which of the following is a step you include in your implementation for the web application?

Answer :

* Create an OIDC identity provider in AWS

Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?

Answer :

* Monitor the S3 API calls by using Cloudtrail logging

A company has been using the AWS KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys that are no longer in use. What are the ways that can be incorporated to see which keys are in use?

Answer :

* <p>Use CloudTrail to see if any KMS API request has been issued against existing keys</p>

A company is planning on using AWS for hosting its applications. They want complete separation and isolation of their production, testing, and development environments. Which of the following is an ideal way to design such a set up?

Answer :

* Use separate AWS accounts for each of the environments

A company has a set of EC2 instances hosted in AWS. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are required? Choose 2 Options.

Answer :

* Use lifecycle policies for the EBS snapshots.
* Use EBS volume replication

Your company is performing a security audit of the AWS environment and the security specialist asked you to provide a document that contained the status of all IAM users in the AWS account. In this document, it should include information such as when users were created, when passwords were used or changed last time, whether or not MFA was enabled, etc. What is the best way to provide this documentation?

Answer :

* Generate and download an IAM credential report through AWS Management Console or AWS SDKs

Explanation :

Option B is CORRECT: Because users can download a new credential report every 4 hour

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20939)

GuardDuty requires manual updates from CrowdStrike.

Answer :

* False

Explanation :

GuradDuty automatically collectes Threst Intel information from CrowdStrike

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20969)

A security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure. They want to include steps to determine if the employee’s IAM permissions changed as part of the incident. What steps should the team document in the plan?

Answer :

* Use AWS Config to examine the employee’s IAM permissions prior to the incident and compare them to the employee’s current IAM permissions

Explanation :

You can use the AWS Config history to see the history of a particular item.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20942)

GuardDuty requires manual updates from ProofPoint.

Answer :

* False

Explanation :

GuradDuty automatically collectes Threst Intel information from Proofpoint

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20930)

How many IAM roles can you attach to an EC2 instance at a time?

Answer :

* One

Explanation :

Only one IAM role can be attached to an EC2 instance at any given time.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527092)

Which field in VPC Flow Logs indicates the originating source IP address?

Answer :

* srcAddr

Explanation :

'srcAddr' refers to the source IP address in a VPC Flow Log record.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527249)

Which service is useful to check Common Vulnerabilities and Exposures in the OS?

Answer :

* AWS Inspector

Explanation :

Inpector checks your servers for CVEs from MITRE organization

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20934)

If a company uses AWS Directory Service with 50 users, each incurring a monthly cost of $5, what is the total cost for directory service access in a month?

Answer :

* $250

Explanation :

The total cost is calculated as 50 users \* $5/user = $250.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527103)

With the help of which service can I detect credit card numbers in my excel files stored in S3?

Answer :

* AWS Macie

Explanation :

Macie helps detecting PII data in S3 buckets

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20945)

Which service is useful to do Center of Internet Security Benchmarks assessments?

Answer :

* AWS Inspector

Explanation :

Inspector provides CIS Benchmark Asssesments