AWS Certified Security – Specialty ( Security Engineering on AWS ) Quiz Questions and Answers part 1 of 3

A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is triggered whenever an object is stored within the S3 bucket. How should the Lambda function be given access to the DynamoDB table?

Answer :

* Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function

Explanation:

The ideal way is to create an IAM role which has the required permissions and then associate it with the Lambda function The AWS Documentation additionally mentions the following Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role: · If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role. · If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role. Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB

A company wants to have a secure way of generating, storing and managing cryptographic keys. But they want to have exclusive access for the keys. Which of the following can be used for this purpose?

Answer :

* Use Cloud HSM

Explanation :

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are designed and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

You are responsible for deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Which of the following services can be used to fulfill this requirement. Choose 2 answers from the options given below.

Answer :

* Amazon CloudWatch Logs
* Amazon Cloudtrail

Explanation :

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. Option B is incorrect because VPC flow logs can only check for flow to instances in a VPC Option C is incorrect because this can check for configuration changes only

Your company has confidential documents stored in the simple storage service. Due to compliance requirements, you have to ensure that the data in the S3 bucket is available in a different geographical location. As an architect, what change would you make to comply with this requirement?

Answer :

* Enable Cross region replication for the S3 bucket

Explanation :

You might configure cross-region replication on a bucket for various reasons, including the following: Compliance requirements – Although, by default, Amazon S3 stores your data across multiple geographically distant Availability Zones, compliance requirements might dictate that you store data at even further distances. Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these compliance requirements. Option A is invalid because Multi-AZ cannot be used to S3 buckets Option B is invalid because copying it to an EBS volume is not a recommended practice Option C is invalid because creating snapshots is not possible in S3

You are building a large-scale confidential documentation web server on AWS and all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use CloudFront to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below.

Answer :

* Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI

Explanation :

If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket, you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if user’s access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront access logs are less useful because they're incomplete.

Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company’s EC2 instances?

Answer :

* Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance

Explanation :

Option A is incorrect because Config rules cannot be set as target directly by using scheduled cloudWatch event rule. Managed config rule(restricted-common-ports) has to be specifically configured for all the required ports. Option B is incorrect because querying Trusted Advisor API’s are not possible Option C is incorrect because GuardDuty should be used to detect threats and not check the compliance of security protocols. Option D states that Run Amazon Inspector using runtime behaviour analysis rules which will analyze the behavior of your instances during an assessment run, and provide guidance about how to make your EC2 instances more secure.

When managing permissions for the API gateway, what can be used to ensure that the right level of permissions is given to developers, IT admins, and users? These permissions should be easily managed.

Answer :

* Use IAM Policies to create different policies for the different types of users

Explanation :

You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes: To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway. To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway. Option A , C and D are invalid because these cannot be used to control access to AWS services. This needs to be done via policies

A company is using CloudTrail to log all AWS API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files. What step will protect the log files from intentional or unintentional alteration?

Answer :

* Enable Cloud Trail to log file integrity validation

Explanation :

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose. Option E is invalid because Security Groups cannot be used to block calls from other services

Your company makes use of S3 buckets for storing data. There is a company policy that all services should have logging enabled. How can you ensure that logging is always enabled for created S3 buckets in the AWS Account?

Answer :

* Use AWS Config Rules to check whether logging is enabled for buckets

Explanation :

You add the AWS Config managed rule, S3\_BUCKET\_LOGGING\_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule. Option A is invalid because AWS Inspector cannot be used to scan all buckets Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets.

A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?

Answer :

* Use Bucket policies
* Use IAM user policies

Explanation :

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources. Option B and D are invalid because these cannot be used to control access to S3 bucket

A security team must present a daily briefing to the CISO that includes a report of which of the company’s thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day’s report. How can the security team fulfill these requirements?

Answer :

* Use Systems Manager Patch Manager to generate the report of out-of-compliance instances/ servers. Use Systems Manager Patch Manager to install the missing patches

Explanation :

AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement?

Answer :

* Access the S3 bucket through a VPC endpoint for S3

Explanation :

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. Option A is invalid because using a proxy server is not sufficient enough Option B and D are invalid because you need secure communication which should not traverse the internet

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?

Answer :

* Change the Inbound NACL to deny access from the suspecting IP

Explanation :

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL’s as an additional security layer for the subnet to deny traffic. Option D is invalid since just changing the Inbound Rules is sufficient. The AWS Documentation mentions the following A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC

Every application in a company’s portfolio has a separate AWS account for development and production. The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality?

Answer :

* Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit

Explanation :

As an administrator of the master account of an organization, you can restrict which AWS services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When AWS Organizations blocks access to a service or API action for a member account, a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an IAM policy. Organization permissions overrule account permissions.

Your company owns a large number of AWS accounts managed by AWS Organizations. To meet security compliance, the CloudTrail should always be enabled in all AWS accounts. However, during the last couple of weeks, it was noticed that IAM users in certain AWS accounts disabled the CloudTrail feature. You need to add a restriction rule to prevent such actions. What is the best way to achieve that?

Answer :

* Configure a Service Control Policy (SCP) to deny the CloudTrail StopLogging action and add the policy to the relevant OUs in the organization

Explanation :

Option A is incorrect: Because this is hard to manage as users have to maintain every IAM user and whenever there is a new user, the IAM policy needs to be configured as well. Option B is incorrect: Similar as Option A. It is better to use a central control to prevent such an action. Option C is CORRECT: Because a SCP can be configured in organizational units (OUs) as below: Option D is incorrect: Because it is time-consuming to maintain each IAM user and it is also possible for IAM user to modify the permission boundary unexpectedly. The best way is to use the SCP to deny the action.

The Security team wants to delegate user creation duties to the SysOps Administrator. However, the team must ensure that the SysOps Administrator creates users that adhere to the following company rules:

- Users cannot use IAM to create or manage users, groups, roles, or policies.  
- Users are denied access to the Amazon S3 logs bucket and cannot access production EC2 instances.

How can the team fulfil this task?

Answer :

* <p>Delegate the user creation duties using Permissions Boundaries.</p>

Explanation :

Since here the traffic needs to flow outbound from the Instance to a web service on Port 443 , the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port. Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

Answer :

* Enable MFA for these user accounts

Explanation :

The AWS Documentation mentions the following as a best practise for IAM users For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Which of the following is not a best practice for carrying out a security audit?

Answer :

* Conduct an audit on a yearly basis

Explanation :

You should audit your security configuration in the following situations: On a periodic basis. If there are changes in your organization, such as people leaving. If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need. If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWorks stacks, AWS CloudFormation templates, etc. If you ever suspect that an unauthorized person might have accessed your account.

Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances. Which of the following would be an effective way to achieve this?

Answer :

* Use the AWS Systems Manager Run Command

Explanation :

AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

A company has external vendors that must deliver files to the company. These vendors have cross-account permission to upload objects to one of the company’s S3 buckets. What combination of steps needs to be followed by the vendor to allow the company's user to access the uploaded files? Select 2 answers from the options given below.

Answer :

* Add a grant to the object’s ACL giving full permissions to bucket owner
* Upload the file to the company’s S3 bucket

Explanation :

A bucket owner can enable other AWS accounts to upload objects. These objects are owned by the accounts that created them. The bucket owner does not own objects that were not created by the bucket owner. Therefore, for the bucket owner to grant access to these objects, the object owner must first grant permission to the bucket owner using an object ACL. The bucket owner can then delegate those permissions via a bucket policy. In this example, the bucket owner delegates permission to users in its own account.

A security team must present a daily briefing to the CISO that includes a report of which of the company’s thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day’s report. How can the security team fulfill these requirements?

Answer :

* Use Systems Manager Patch Manager to generate the report of out-of-compliance instances/ servers. Use Systems Manager Patch Manager to install the missing patches

Explanation :

AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement?

Answer :

* Access the S3 bucket through a VPC endpoint for S3

Explanation :

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. Option A is invalid because using a proxy server is not sufficient enough Option B and D are invalid because you need secure communication which should not traverse the internet

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_20968)

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?

Answer :

* Change the Inbound NACL to deny access from the suspecting IP

Explanation :

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL’s as an additional security layer for the subnet to deny traffic. Option D is invalid since just changing the Inbound Rules is sufficient. The AWS Documentation mentions the following A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Every application in a company’s portfolio has a separate AWS account for development and production. The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality?

Answer :

* Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit

Explanation :

As an administrator of the master account of an organization, you can restrict which AWS services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When AWS Organizations blocks access to a service or API action for a member account, a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an IAM policy. Organization permissions overrule account permissions.

Your company owns a large number of AWS accounts managed by AWS Organizations. To meet security compliance, the CloudTrail should always be enabled in all AWS accounts. However, during the last couple of weeks, it was noticed that IAM users in certain AWS accounts disabled the CloudTrail feature. You need to add a restriction rule to prevent such actions. What is the best way to achieve that?

Answer :

* Configure a Service Control Policy (SCP) to deny the CloudTrail StopLogging action and add the policy to the relevant OUs in the organization

Explanation :

Option A is incorrect: Because this is hard to manage as users have to maintain every IAM user and whenever there is a new user, the IAM policy needs to be configured as well. Option B is incorrect: Similar as Option A. It is better to use a central control to prevent such an action. Option C is CORRECT: Because a SCP can be configured in organizational units (OUs) as below: Option D is incorrect: Because it is time-consuming to maintain each IAM user and it is also possible for IAM user to modify the permission boundary unexpectedly. The best way is to use the SCP to deny the action.

The Security team wants to delegate user creation duties to the SysOps Administrator. However, the team must ensure that the SysOps Administrator creates users that adhere to the following company rules:

- Users cannot use IAM to create or manage users, groups, roles, or policies.  
- Users are denied access to the Amazon S3 logs bucket and cannot access production EC2 instances.

How can the team fulfill this task?

Answer :

* <p>Delegate the user creation duties using Permissions Boundaries.</p>

Explanation :

Since here the traffic needs to flow outbound from the Instance to a web service on Port 443 , the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port. Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

Answer :

* Enable MFA for these user accounts

Explanation :

The AWS Documentation mentions the following as a best practise for IAM users For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Which of the following is not a best practice for carrying out a security audit?

Answer :

* Conduct an audit on a yearly basis

Explanation :

You should audit your security configuration in the following situations: On a periodic basis. If there are changes in your organization, such as people leaving. If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need. If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWorks stacks, AWS CloudFormation templates, etc. If you ever suspect that an unauthorized person might have accessed your account.

Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances. Which of the following would be an effective way to achieve this?

Answer :

* Use the AWS Systems Manager Run Command

Explanation :

AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

A company has external vendors that must deliver files to the company. These vendors have cross-account permission to upload objects to one of the company’s S3 buckets. What combination of steps needs to be followed by the vendor to allow the company's user to access the uploaded files? Select 2 answers from the options given below.

Answer :

* Add a grant to the object’s ACL giving full permissions to bucket owner
* Upload the file to the company’s S3 bucket

Explanation :

A bucket owner can enable other AWS accounts to upload objects. These objects are owned by the accounts that created them. The bucket owner does not own objects that were not created by the bucket owner. Therefore, for the bucket owner to grant access to these objects, the object owner must first grant permission to the bucket owner using an object ACL. The bucket owner can then delegate those permissions via a bucket policy. In this example, the bucket owner delegates permission to users in its own account.

A security team must present a daily briefing to the CISO that includes a report of which of the company’s thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day’s report. How can the security team fulfill these requirements?

Answer :

* Use Systems Manager Patch Manager to generate the report of out-of-compliance instances/ servers. Use Systems Manager Patch Manager to install the missing patches

Explanation :

AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement?

Answer :

* Access the S3 bucket through a VPC endpoint for S3

Explanation :

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. Option A is invalid because using a proxy server is not sufficient enough Option B and D are invalid because you need secure communication which should not traverse the internet

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?

Answer :

* Change the Inbound NACL to deny access from the suspecting IP

Explanation :

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL’s as an additional security layer for the subnet to deny traffic. Option D is invalid since just changing the Inbound Rules is sufficient. The AWS Documentation mentions the following A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Every application in a company’s portfolio has a separate AWS account for development and production. The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality?

Answer :

* Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit

Explanation :

As an administrator of the master account of an organization, you can restrict which AWS services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When AWS Organizations blocks access to a service or API action for a member account, a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an IAM policy. Organization permissions overrule account permissions.

Your company owns a large number of AWS accounts managed by AWS Organizations. To meet security compliance, the CloudTrail should always be enabled in all AWS accounts. However, during the last couple of weeks, it was noticed that IAM users in certain AWS accounts disabled the CloudTrail feature. You need to add a restriction rule to prevent such actions. What is the best way to achieve that?

Answer :

* Configure a Service Control Policy (SCP) to deny the CloudTrail StopLogging action and add the policy to the relevant OUs in the organization

Explanation :

Option A is incorrect: Because this is hard to manage as users have to maintain every IAM user and whenever there is a new user, the IAM policy needs to be configured as well. Option B is incorrect: Similar as Option A. It is better to use a central control to prevent such an action. Option C is CORRECT: Because a SCP can be configured in organizational units (OUs) as below: Option D is incorrect: Because it is time-consuming to maintain each IAM user and it is also possible for IAM user to modify the permission boundary unexpectedly. The best way is to use the SCP to deny the action.

The Security team wants to delegate user creation duties to the SysOps Administrator. However, the team must ensure that the SysOps Administrator creates users that adhere to the following company rules:

- Users cannot use IAM to create or manage users, groups, roles, or policies.  
- Users are denied access to the Amazon S3 logs bucket and cannot access production EC2 instances.

How can the team fulfill this task?

Answer :

* <p>Delegate the user creation duties using Permissions Boundaries.</p>

Explanation :

Since here the traffic needs to flow outbound from the Instance to a web service on Port 443 , the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port. Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

Answer :

* Enable MFA for these user accounts

Explanation :

The AWS Documentation mentions the following as a best practise for IAM users For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Which of the following is not a best practice for carrying out a security audit?

Answer :

* Conduct an audit on a yearly basis

Explanation :

You should audit your security configuration in the following situations: On a periodic basis. If there are changes in your organization, such as people leaving. If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need. If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWorks stacks, AWS CloudFormation templates, etc. If you ever suspect that an unauthorized person might have accessed your account.

Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances. Which of the following would be an effective way to achieve this?

Answer :

* Use the AWS Systems Manager Run Command

Explanation :

AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

A company has external vendors that must deliver files to the company. These vendors have cross-account permission to upload objects to one of the company’s S3 buckets. What combination of steps needs to be followed by the vendor to allow the company's user to access the uploaded files? Select 2 answers from the options given below.

Answer :

* Add a grant to the object’s ACL giving full permissions to bucket owner
* Upload the file to the company’s S3 bucket

Explanation :

A bucket owner can enable other AWS accounts to upload objects. These objects are owned by the accounts that created them. The bucket owner does not own objects that were not created by the bucket owner. Therefore, for the bucket owner to grant access to these objects, the object owner must first grant permission to the bucket owner using an object ACL. The bucket owner can then delegate those permissions via a bucket policy. In this example, the bucket owner delegates permission to users in its own account.

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database – administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure- · sgLB – associated with the ELB · sgWeb – associated with the EC2 instances. · sgDB – associated with the database · sgBastion – associated with the bastion host Which security group configuration will allow the application to be secure and functional?

Answer :

* sgLB: Allow port 80 and 443traffic from 0.0.0.0/0 sgWeb: Allow port 80 and 443 traffic from sgLB sgDB: Allow port 3306traffic from sgWeb and sgBastion sgBastion: Allow port 22traffic from the corporate IP address range

Explanation :

The Load Balancer should accept traffic on ow port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer The database should allow traffic from the Web server And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer Option B and C are incorrect because the bastion host should only traffic from a corporate IP address

You have an Ec2 Instance in a private subnet that needs to access the KMS service privately within the AWS network. Which of the following methods can help fulfill this requirement, keeping security in perspective?

Answer :

* Use a VPC endpoint

Explanation :

You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint, communication between your VPC and AWS KMS is conducted entirely within the AWS network. Option B is invalid because this could open threats from the internet Option C is invalid because this is normally used for communication between on-premise environments and AWS. Option D is invalid because this is normally used for communication between VPC’s

A company has a legacy application that outputs all logs to a local text file. Logs from all applications running on AWS must be continually monitored for security-related messages. What can be done to allow the company to deploy the legacy application on Amazon EC2 and still meet the monitoring requirement?

Answer :

* Send the local text log files to CloudWatch Logs and configure a CloudWatch metric filter. Trigger CloudWatch alarms based on the metrics

Explanation :

One can send the log files to Cloudwatch Logs. Log files can also be sent from On-premise servers. You can then specify metrics to search the logs for any specific values. And then create alarms based on these metrics. Option A is invalid because this will be just a long over drawn process to achieve this requirement Option C is invalid because AWS Inspector cannot be used to monitor for security related messages. Option D is invalid because files cannot be exported to AWS Cloudtrail

A company continually generates sensitive records that it stores in an S3 bucket. All objects in the bucket are encrypted using SSE-KMS using one of the company’s CMKs. Company compliance policies require that no more than one month of data be encrypted using the same encryption key. What solution below will meet the company’s requirements?

Answer :

* Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK

Explanation :

You can use a Lambda function to create a new key and then update the S3 bucket to use the new key. Remember not to delete the old key , else you will not be able to decrypt the documents stored in the S3 bucket using the older key. Option B is incorrect because AWS KMS cannot rotate keys on a monthly basis Option C is incorrect because deleting the old key means that you cannot access the older objects Option D is incorrect because rotating key material is not possible.

As a DevOps engineer, you need to maintain Jenkins pipelines. Recently, you have created a new pipeline for a migration project. In one stage, you encrypted a file with below command: AWS KMS encrypt \ --key-id 1234abcd-fa85-46b5-56ef-1234567890ab \ --plaintext fileb://ExamplePlaintextFile \ --output text \ --query CiphertextBlob | base64 \ --decode > ExampleEncryptedFile A CMK key was used in the encryption operation. Then in another stage, the encrypted file needs to be decrypted with AWS KMS decrypt. In terms of this command, which statement is correct?

Answer :

* There is no need to add the CMK key information for this command

Explanation :

Option A~B are incorrect: The AWS CLI aws kms decrypt has the below format: aws kms decrypt \ --ciphertext-blob fileb://ExampleEncryptedFile \ --output text \ --query Plaintext | base64 --decode > ExamplePlaintextFile There is no need to add key information. This is different from aws kms encrypt. Option C is incorrect: Because the encryption does not use data key, so does the decryption. Option D is CORRECT: Refer to the above explanations.

You have enabled Cloudtrail logs for your company’s AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?

Answer :

* There is no need to do anything since the logs will already be encrypted

Explanation :

By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

In your organization, the security team requires that the key material of CMKs should be generated and maintained from your own infrastructure. Therefore you have created key material in local servers and get it imported. Then the CMKs are used for encryption/decryption with various AWS services. Which configurations or operations can you perform on these CMKs? (Select two)

Answer :

* Schedule key deletion and set a waiting period of 7 to 30 days
* Manually delete the imported key material

Explanation :

Option A is incorrect: Because automatic key rotation is not an option for CMKs with imported key material. Option B is CORRECT: Because Schedule key deletion can still be configured. Option C is CORRECT: Because users can manually delete the key material. After that, AWS KMS deletes the key material but does not delete the CMK or metadata. Option D is incorrect: Because AWS KMS NEVER provides CLI command or API to export key material outside of KMS.

A company is hosting a website that must be accessible to users for HTTPS traffic. Also, port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations is the most secure but still functional to support these requirements? Choose 2 answers from the options given below.

Answer :

* Port443 coming from 0.0.0.0/0
* Port 22 coming from 203.0.113.1/32

Explanation :

Since HTTPS traffic is required for all users on the Internet , Port 443 should be open on all IP addresses. For port 22 , the traffic should be restricted to an internal subnet. Option B is invalid , because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk For more information on AWS Security Groups, please visit the following URL:

You are working in the IT security team in a big company. In order to perform security checks in AWS services, you have written dozens of custom AWS Config rules. One of them is to check if the S3 bucket policy contains certain explicit denies. This particular Config rule is supposed to be applied for all S3 buckets. Your manager has asked you how to trigger the custom Config rule. Which answers are correct?

Answer :

* It can be triggered whenever there is a configuration change for a S3 bucket
* The custom Config rule can be triggered periodically such as every hour

Explanation :

There are two types of triggers: Configuration Changes and Periodic. There is no difference between AWS managed Config rule and custom Config rule in terms of triggers. Option B is incorrect: Because the rule can be triggered automatically. Manual triggering is not the only way. Option C is CORRECT: Because users can configure the trigger type as Configuration Changes: Option D is CORRECT: Because this is applicable according to the above link.

In your organization, a customer managed key named TestCMK has been created for a new project. This key is supposed to be used only by related AWS services in this project including EC2 and RDS in region us-west-2. For security concerns, you need to make sure that no other services can encrypt or decrypt using this particular CMK. In the meantime, EC2 and RDS should use the key without issues. How should you implement this?

Answer :

* Configure a key policy for this CMK. Use KMS:ViaService to check if the request comes from ec2.us-west-2.amazonAWS.com or rds.us-west-2.amazonAWS.com.

Explanation :

Option A is incorrect: Because this option cannot make sure that only EC2 or RDS can use this CMK. Option B is incorrect: Because other services may be able to use the CMK as well such as Lambda. The correct place to be configured should be in key policy. Option C is CORRECT: Because kms:ViaService is the correct key condition to filter that only EC2 and RDS can use the CMK. For example, the below condition can be added into the key policy:

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database – administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure- · sgLB – associated with the ELB · sgWeb – associated with the EC2 instances. · sgDB – associated with the database · sgBastion – associated with the bastion host Which security group configuration will allow the application to be secure and functional?

Answer :

* sgLB: Allow port 80 and 443traffic from 0.0.0.0/0 sgWeb: Allow port 80 and 443 traffic from sgLB sgDB: Allow port 3306traffic from sgWeb and sgBastion sgBastion: Allow port 22traffic from the corporate IP address range

Explanation :

The Load Balancer should accept traffic on ow port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer The database should allow traffic from the Web server And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer Option B and C are incorrect because the bastion host should only traffic from a corporate IP address

You have an Ec2 Instance in a private subnet that needs to access the KMS service privately within the AWS network. Which of the following methods can help fulfill this requirement, keeping security in perspective?

Answer :

* Use a VPC endpoint

Explanation :

You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint, communication between your VPC and AWS KMS is conducted entirely within the AWS network. Option B is invalid because this could open threats from the internet Option C is invalid because this is normally used for communication between on-premise environments and AWS. Option D is invalid because this is normally used for communication between VPC’s

A company has a legacy application that outputs all logs to a local text file. Logs from all applications running on AWS must be continually monitored for security-related messages. What can be done to allow the company to deploy the legacy application on Amazon EC2 and still meet the monitoring requirement?

Answer :

* Send the local text log files to CloudWatch Logs and configure a CloudWatch metric filter. Trigger CloudWatch alarms based on the metrics

Explanation :

One can send the log files to Cloudwatch Logs. Log files can also be sent from On-premise servers. You can then specify metrics to search the logs for any specific values. And then create alarms based on these metrics. Option A is invalid because this will be just a long over drawn process to achieve this requirement Option C is invalid because AWS Inspector cannot be used to monitor for security related messages. Option D is invalid because files cannot be exported to AWS Cloudtrail

A company continually generates sensitive records that it stores in an S3 bucket. All objects in the bucket are encrypted using SSE-KMS using one of the company’s CMKs. Company compliance policies require that no more than one month of data be encrypted using the same encryption key. What solution below will meet the company’s requirements?

Answer :

* Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK

Explanation :

You can use a Lambda function to create a new key and then update the S3 bucket to use the new key. Remember not to delete the old key , else you will not be able to decrypt the documents stored in the S3 bucket using the older key. Option B is incorrect because AWS KMS cannot rotate keys on a monthly basis Option C is incorrect because deleting the old key means that you cannot access the older objects Option D is incorrect because rotating key material is not possible.

As a DevOps engineer, you need to maintain Jenkins pipelines. Recently, you have created a new pipeline for a migration project. In one stage, you encrypted a file with below command: AWS KMS encrypt \ --key-id 1234abcd-fa85-46b5-56ef-1234567890ab \ --plaintext fileb://ExamplePlaintextFile \ --output text \ --query CiphertextBlob | base64 \ --decode > ExampleEncryptedFile A CMK key was used in the encryption operation. Then in another stage, the encrypted file needs to be decrypted with AWS KMS decrypt. In terms of this command, which statement is correct?

Answer :

* There is no need to add the CMK key information for this command

Explanation :

Option A~B are incorrect: The AWS CLI aws kms decrypt has the below format: aws kms decrypt \ --ciphertext-blob fileb://ExampleEncryptedFile \ --output text \ --query Plaintext | base64 --decode > ExamplePlaintextFile There is no need to add key information. This is different from aws kms encrypt. Option C is incorrect: Because the encryption does not use data key, so does the decryption. Option D is CORRECT: Refer to the above explanations.

You have enabled Cloudtrail logs for your company’s AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?

Answer :

* There is no need to do anything since the logs will already be encrypted

Explanation :

By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

In your organization, the security team requires that the key material of CMKs should be generated and maintained from your own infrastructure. Therefore you have created key material in local servers and get it imported. Then the CMKs are used for encryption/decryption with various AWS services. Which configurations or operations can you perform on these CMKs? (Select two)

Answer :

* Schedule key deletion and set a waiting period of 7 to 30 days
* Manually delete the imported key material

Explanation :

Option A is incorrect: Because automatic key rotation is not an option for CMKs with imported key material. Option B is CORRECT: Because Schedule key deletion can still be configured. Option C is CORRECT: Because users can manually delete the key material. After that, AWS KMS deletes the key material but does not delete the CMK or metadata. Option D is incorrect: Because AWS KMS NEVER provides CLI command or API to export key material outside of KMS.

A company is hosting a website that must be accessible to users for HTTPS traffic. Also, port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations is the most secure but still functional to support these requirements? Choose 2 answers from the options given below.

Answer :

* Port443 coming from 0.0.0.0/0
* Port 22 coming from 203.0.113.1/32

Explanation :

Since HTTPS traffic is required for all users on the Internet , Port 443 should be open on all IP addresses. For port 22 , the traffic should be restricted to an internal subnet. Option B is invalid , because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk For more information on AWS Security Groups, please visit the following URL:

You are working in the IT security team in a big company. In order to perform security checks in AWS services, you have written dozens of custom AWS Config rules. One of them is to check if the S3 bucket policy contains certain explicit denies. This particular Config rule is supposed to be applied for all S3 buckets. Your manager has asked you how to trigger the custom Config rule. Which answers are correct?

Answer :

* It can be triggered whenever there is a configuration change for a S3 bucket
* The custom Config rule can be triggered periodically such as every hour

Explanation :

There are two types of triggers: Configuration Changes and Periodic. There is no difference between AWS managed Config rule and custom Config rule in terms of triggers. Option B is incorrect: Because the rule can be triggered automatically. Manual triggering is not the only way. Option C is CORRECT: Because users can configure the trigger type as Configuration Changes: Option D is CORRECT: Because this is applicable according to the above link.

In your organization, a customer managed key named TestCMK has been created for a new project. This key is supposed to be used only by related AWS services in this project including EC2 and RDS in region us-west-2. For security concerns, you need to make sure that no other services can encrypt or decrypt using this particular CMK. In the meantime, EC2 and RDS should use the key without issues. How should you implement this?

Answer :

* Configure a key policy for this CMK. Use KMS:ViaService to check if the request comes from ec2.us-west-2.amazonAWS.com or rds.us-west-2.amazonAWS.com.

Explanation :

Option A is incorrect: Because this option cannot make sure that only EC2 or RDS can use this CMK. Option B is incorrect: Because other services may be able to use the CMK as well such as Lambda. The correct place to be configured should be in key policy. Option C is CORRECT: Because kms:ViaService is the correct key condition to filter that only EC2 and RDS can use the CMK. For example, the below condition can be added into the key policy:

A security team must present a daily briefing to the CISO that includes a report of which of the company’s thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day’s report. How can the security team fulfill these requirements?

Answer :

* Use Systems Manager Patch Manager to generate the report of out-of-compliance instances/ servers. Use Systems Manager Patch Manager to install the missing patches

Explanation :

AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement?

Answer :

* Access the S3 bucket through a VPC endpoint for S3

Explanation :

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. Option A is invalid because using a proxy server is not sufficient enough Option B and D are invalid because you need secure communication which should not traverse the internet

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?

Answer :

* Change the Inbound NACL to deny access from the suspecting IP

Explanation :

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL’s as an additional security layer for the subnet to deny traffic. Option D is invalid since just changing the Inbound Rules is sufficient. The AWS Documentation mentions the following A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Every application in a company’s portfolio has a separate AWS account for development and production. The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality?

Answer :

* Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit

Explanation :

As an administrator of the master account of an organization, you can restrict which AWS services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When AWS Organizations blocks access to a service or API action for a member account, a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an IAM policy. Organization permissions overrule account permissions.

Your company owns a large number of AWS accounts managed by AWS Organizations. To meet security compliance, the CloudTrail should always be enabled in all AWS accounts. However, during the last couple of weeks, it was noticed that IAM users in certain AWS accounts disabled the CloudTrail feature. You need to add a restriction rule to prevent such actions. What is the best way to achieve that?

Answer :

* Configure a Service Control Policy (SCP) to deny the CloudTrail StopLogging action and add the policy to the relevant OUs in the organization

Explanation :

Option A is incorrect: Because this is hard to manage as users have to maintain every IAM user and whenever there is a new user, the IAM policy needs to be configured as well. Option B is incorrect: Similar as Option A. It is better to use a central control to prevent such an action. Option C is CORRECT: Because a SCP can be configured in organizational units (OUs) as below: Option D is incorrect: Because it is time-consuming to maintain each IAM user and it is also possible for IAM user to modify the permission boundary unexpectedly. The best way is to use the SCP to deny the action.

The Security team wants to delegate user creation duties to the SysOps Administrator. However, the team must ensure that the SysOps Administrator creates users that adhere to the following company rules:

- Users cannot use IAM to create or manage users, groups, roles, or policies.  
- Users are denied access to the Amazon S3 logs bucket and cannot access production EC2 instances.

How can the team fulfill this task?

Answer :

* <p>Delegate the user creation duties using Permissions Boundaries.</p>

Explanation :

Since here the traffic needs to flow outbound from the Instance to a web service on Port 443 , the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port. Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

Answer :

* Enable MFA for these user accounts

Explanation :

The AWS Documentation mentions the following as a best practise for IAM users For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Which of the following is not a best practice for carrying out a security audit?

Answer :

* Conduct an audit on a yearly basis

Explanation :

You should audit your security configuration in the following situations: On a periodic basis. If there are changes in your organization, such as people leaving. If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need. If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWorks stacks, AWS CloudFormation templates, etc. If you ever suspect that an unauthorized person might have accessed your account.

Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances. Which of the following would be an effective way to achieve this?

Answer :

* Use the AWS Systems Manager Run Command

Explanation :

AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

A company has external vendors that must deliver files to the company. These vendors have cross-account permission to upload objects to one of the company’s S3 buckets. What combination of steps needs to be followed by the vendor to allow the company's user to access the uploaded files? Select 2 answers from the options given below.

Answer :

* Add a grant to the object’s ACL giving full permissions to bucket owner
* Upload the file to the company’s S3 bucket

Explanation :

A bucket owner can enable other AWS accounts to upload objects. These objects are owned by the accounts that created them. The bucket owner does not own objects that were not created by the bucket owner. Therefore, for the bucket owner to grant access to these objects, the object owner must first grant permission to the bucket owner using an object ACL. The bucket owner can then delegate those permissions via a bucket policy. In this example, the bucket owner delegates permission to users in its own account.

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database – administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure- · sgLB – associated with the ELB · sgWeb – associated with the EC2 instances. · sgDB – associated with the database · sgBastion – associated with the bastion host Which security group configuration will allow the application to be secure and functional?

Answer :

* sgLB: Allow port 80 and 443traffic from 0.0.0.0/0 sgWeb: Allow port 80 and 443 traffic from sgLB sgDB: Allow port 3306traffic from sgWeb and sgBastion sgBastion: Allow port 22traffic from the corporate IP address range

Explanation :

The Load Balancer should accept traffic on ow port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer The database should allow traffic from the Web server And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer Option B and C are incorrect because the bastion host should only traffic from a corporate IP address

You have an Ec2 Instance in a private subnet that needs to access the KMS service privately within the AWS network. Which of the following methods can help fulfill this requirement, keeping security in perspective?

Answer :

* Use a VPC endpoint

Explanation :

You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint, communication between your VPC and AWS KMS is conducted entirely within the AWS network. Option B is invalid because this could open threats from the internet Option C is invalid because this is normally used for communication between on-premise environments and AWS. Option D is invalid because this is normally used for communication between VPC’s

A company has a legacy application that outputs all logs to a local text file. Logs from all applications running on AWS must be continually monitored for security-related messages. What can be done to allow the company to deploy the legacy application on Amazon EC2 and still meet the monitoring requirement?

Answer :

* Send the local text log files to CloudWatch Logs and configure a CloudWatch metric filter. Trigger CloudWatch alarms based on the metrics

Explanation :

One can send the log files to Cloudwatch Logs. Log files can also be sent from On-premise servers. You can then specify metrics to search the logs for any specific values. And then create alarms based on these metrics. A company continually generates sensitive records that it stores in an S3 bucket. All objects in the bucket are encrypted using SSE-KMS using one of the company’s CMKs. Company compliance policies require that no more than one month of data be encrypted using the same encryption key. What solution below will meet the company’s requirements?

Answer :

* Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK

Explanation :

You can use a Lambda function to create a new key and then update the S3 bucket to use the new key. Remember not to delete the old key , else you will not be able to decrypt the documents stored in the S3 bucket using the older key. Option B is incorrect because AWS KMS cannot rotate keys on a monthly basis Option C is incorrect because deleting the old key means that you cannot access the older objects Option D is incorrect because rotating key material is not possible.

Option D is invalid because files cannot be exported to AWS Cloudtrail

As a DevOps engineer, you need to maintain Jenkins pipelines. Recently, you have created a new pipeline for a migration project. In one stage, you encrypted a file with below command: AWS KMS encrypt \ --key-id 1234abcd-fa85-46b5-56ef-1234567890ab \ --plaintext fileb://ExamplePlaintextFile \ --output text \ --query CiphertextBlob | base64 \ --decode > ExampleEncryptedFile A CMK key was used in the encryption operation. Then in another stage, the encrypted file needs to be decrypted with AWS KMS decrypt. In terms of this command, which statement is correct?

Answer :

* There is no need to add the CMK key information for this command

Explanation :

Option A~B are incorrect: The AWS CLI aws kms decrypt has the below format: aws kms decrypt \ --ciphertext-blob fileb://ExampleEncryptedFile \ --output text \ --query Plaintext | base64 --decode > ExamplePlaintextFile There is no need to add key information. This is different from aws kms encrypt. Option C is incorrect: Because the encryption does not use data key, so does the decryption. Option D is CORRECT: Refer to the above explanations.

You have enabled Cloudtrail logs for your company’s AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?

Answer :

* There is no need to do anything since the logs will already be encrypted

Explanation :

By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

In your organization, the security team requires that the key material of CMKs should be generated and maintained from your own infrastructure. Therefore you have created key material in local servers and get it imported. Then the CMKs are used for encryption/decryption with various AWS services. Which configurations or operations can you perform on these CMKs? (Select two)

Answer :

* Schedule key deletion and set a waiting period of 7 to 30 days
* Manually delete the imported key material

Explanation :

Option A is incorrect: Because automatic key rotation is not an option for CMKs with imported key material. Option B is CORRECT: Because Schedule key deletion can still be configured. Option C is CORRECT: Because users can manually delete the key material. After that, AWS KMS deletes the key material but does not delete the CMK or metadata. Option D is incorrect: Because AWS KMS NEVER provides CLI command or API to export key material outside of KMS.

A company is hosting a website that must be accessible to users for HTTPS traffic. Also, port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations is the most secure but still functional to support these requirements? Choose 2 answers from the options given below.

Answer :

* Port443 coming from 0.0.0.0/0
* Port 22 coming from 203.0.113.1/32

Explanation :

Since HTTPS traffic is required for all users on the Internet , Port 443 should be open on all IP addresses. For port 22 , the traffic should be restricted to an internal subnet. Option B is invalid , because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk For more information on AWS Security Groups, please visit the following URL:

You are working in the IT security team in a big company. In order to perform security checks in AWS services, you have written dozens of custom AWS Config rules. One of them is to check if the S3 bucket policy contains certain explicit denies. This particular Config rule is supposed to be applied for all S3 buckets. Your manager has asked you how to trigger the custom Config rule. Which answers are correct?

Answer :

* It can be triggered whenever there is a configuration change for a S3 bucket
* The custom Config rule can be triggered periodically such as every hour

Explanation :

There are two types of triggers: Configuration Changes and Periodic. There is no difference between AWS managed Config rule and custom Config rule in terms of triggers. Option B is incorrect: Because the rule can be triggered automatically. Manual triggering is not the only way. Option C is CORRECT: Because users can configure the trigger type as Configuration Changes: Option D is CORRECT: Because this is applicable according to the above link.

In your organization, a customer managed key named TestCMK has been created for a new project. This key is supposed to be used only by related AWS services in this project including EC2 and RDS in region us-west-2. For security concerns, you need to make sure that no other services can encrypt or decrypt using this particular CMK. In the meantime, EC2 and RDS should use the key without issues. How should you implement this?

Answer :

* Configure a key policy for this CMK. Use KMS:ViaService to check if the request comes from ec2.us-west-2.amazonAWS.com or rds.us-west-2.amazonAWS.com.

Explanation :

Option A is incorrect: Because this option cannot make sure that only EC2 or RDS can use this CMK. Option B is incorrect: Because other services may be able to use the CMK as well such as Lambda. The correct place to be configured should be in key policy. Option C is CORRECT: Because kms:ViaService is the correct key condition to filter that only EC2 and RDS can use the CMK. For example, the below condition can be added into the key policy:

What steps are involved in setting up multi-Region keys using AWS Management Console for KMS?

Answer :

* Create key in primary Region, select replicate to second Region, activate key

Explanation :

To set up multi-Region keys in KMS, you first create the key in the primary region, then select the option to replicate it to a second region, and finally activate the replicated key.

What is the primary function of Amazon GuardDuty in the context of monitoring and security on AWS?

Answer :

* Analyzing security findings and threats

Explanation :

Amazon GuardDuty is a threat detection service that continuously analyzes security findings and potential threats in AWS environments, helping to protect against malicious activities.

How does enabling AWS CloudTrail contribute to enhancing security and compliance in AWS environments?

Answer :

* Monitoring and logging API calls

Explanation :

AWS CloudTrail monitors and logs API calls made on AWS resources, providing visibility into user activity, resource changes, and aiding in security analysis and compliance auditing.

Why might an organization prefer AWS Firewall Manager over manual security policy management?

Answer :

* AWS Firewall Manager ensures consistent and scalable policy enforcement

Explanation :

Organizations prefer AWS Firewall Manager because it ensures consistent and scalable policy enforcement, which is less error-prone and more efficient compared to manual management.

Explain the rationale behind choosing AWS Shield Advanced instead of standard AWS Shield for a business with a high risk of DDoS attacks.

Answer :

* Advanced threat detection and comprehensive protection

Explanation :

AWS Shield Advanced offers more robust protection, including advanced threat detection, cost protection, and expert support, which are crucial for businesses with higher DDoS risk.

What is the primary function of AWS Shield in the context of infrastructure protection on AWS?

Answer :

* Protecting against DDoS attacks

Explanation :

AWS Shield is a service designed to protect against Distributed Denial of Service (DDoS) attacks, safeguarding AWS infrastructure from malicious traffic and ensuring availability.

When implementing access controls for data stored in AWS RDS, which method helps you to ensure least privilege?

Answer :

* Using IAM database authentication

Explanation :

Using IAM database authentication allows for fine-grained access control and helps enforce the least privilege principle by assigning specific permissions to IAM roles and users.

How does IAM Identity Center simplify the management of user identities and access within AWS environments?

Answer :

* By offering a centralized approach for role-based access management

Explanation :

IAM Identity Center simplifies identity and access management by providing a centralized, role-based approach to managing user permissions and access across various AWS accounts.

Describe the step needed to rotate an encrypted secret in AWS Secrets Manager that is used by an RDS instance?

Answer :

* Configure automated rotation in Secrets Manager and update the RDS configuration to use it

Explanation :

Configuring automated rotation in Secrets Manager allows the secret to be rotated without manual intervention, and the RDS instance remains updated with the rotated credentials.

What is the primary benefit of using Amazon S3 Versioning for data replication and protection?

Answer :

* It enhances data durability

Explanation :

Amazon S3 Versioning helps you easily recover from unintended user actions and applications failures, thus enhancing data durability by maintaining multiple versions of objects.

What is the primary benefit of using Amazon S3 Versioning for data replication and protection?

Answer :

* It enhances data durability

Explanation :

Amazon S3 Versioning helps you easily recover from unintended user actions and applications failures, thus enhancing data durability by maintaining multiple versions of objects.

What steps are involved in setting up multi-Region keys using AWS Management Console for KMS?

Answer :

* Create key in primary Region, select replicate to second Region, activate key

Explanation :

To set up multi-Region keys in KMS, you first create the key in the primary region, then select the option to replicate it to a second region, and finally activate the replicated key.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527189)

What is the primary function of Amazon GuardDuty in the context of monitoring and security on AWS?

Answer :

* Analyzing security findings and threats

Explanation :

Amazon GuardDuty is a threat detection service that continuously analyzes security findings and potential threats in AWS environments, helping to protect against malicious activities.

How does enabling AWS CloudTrail contribute to enhancing security and compliance in AWS environments?

Answer :

* Monitoring and logging API calls

Explanation :

AWS CloudTrail monitors and logs API calls made on AWS resources, providing visibility into user activity, resource changes, and aiding in security analysis and compliance auditing.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471450)

Why might an organization prefer AWS Firewall Manager over manual security policy management?

Answer :

* AWS Firewall Manager ensures consistent and scalable policy enforcement

Explanation :

Organizations prefer AWS Firewall Manager because it ensures consistent and scalable policy enforcement, which is less error-prone and more efficient compared to manual management.

Explain the rationale behind choosing AWS Shield Advanced instead of standard AWS Shield for a business with a high risk of DDoS attacks.

Answer :

* Advanced threat detection and comprehensive protection

Explanation :

AWS Shield Advanced offers more robust protection, including advanced threat detection, cost protection, and expert support, which are crucial for businesses with higher DDoS risk.

What is the primary function of AWS Shield in the context of infrastructure protection on AWS?

Answer :

* Protecting against DDoS attacks

Explanation :

AWS Shield is a service designed to protect against Distributed Denial of Service (DDoS) attacks, safeguarding AWS infrastructure from malicious traffic and ensuring availability.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_471437)

When implementing access controls for data stored in AWS RDS, which method helps you to ensure least privilege?

Answer :

* Using IAM database authentication

Explanation :

Using IAM database authentication allows for fine-grained access control and helps enforce the least privilege principle by assigning specific permissions to IAM roles and users.

How does IAM Identity Center simplify the management of user identities and access within AWS environments?

Answer :

* By offering a centralized approach for role-based access management

Explanation :

IAM Identity Center simplifies identity and access management by providing a centralized, role-based approach to managing user permissions and access across various AWS accounts.

Describe the step needed to rotate an encrypted secret in AWS Secrets Manager that is used by an RDS instance?

Answer :

* Configure automated rotation in Secrets Manager and update the RDS configuration to use it

Explanation :

Configuring automated rotation in Secrets Manager allows the secret to be rotated without manual intervention, and the RDS instance remains updated with the rotated credentials.

What is the primary benefit of using Amazon S3 Versioning for data replication and protection?

Answer :

* It enhances data durability

Explanation :

Amazon S3 Versioning helps you easily recover from unintended user actions and applications failures, thus enhancing data durability by maintaining multiple versions of objects.

What steps are involved in setting up multi-Region keys using AWS Management Console for KMS?

Answer :

* Create key in primary Region, select replicate to second Region, activate key

Explanation :

To set up multi-Region keys in KMS, you first create the key in the primary region, then select the option to replicate it to a second region, and finally activate the replicated key.

What is the primary function of Amazon GuardDuty in the context of monitoring and security on AWS?

Answer :

* Analyzing security findings and threats

Explanation :

Amazon GuardDuty is a threat detection service that continuously analyzes security findings and potential threats in AWS environments, helping to protect against malicious activities.

How does enabling AWS CloudTrail contribute to enhancing security and compliance in AWS environments?

Answer :

* Monitoring and logging API calls

Explanation :

AWS CloudTrail monitors and logs API calls made on AWS resources, providing visibility into user activity, resource changes, and aiding in security analysis and compliance auditing.

Why might an organization prefer AWS Firewall Manager over manual security policy management?

Answer :

* AWS Firewall Manager ensures consistent and scalable policy enforcement

Explanation :

Organizations prefer AWS Firewall Manager because it ensures consistent and scalable policy enforcement, which is less error-prone and more efficient compared to manual management.

Explain the rationale behind choosing AWS Shield Advanced instead of standard AWS Shield for a business with a high risk of DDoS attacks.

Answer :

* Advanced threat detection and comprehensive protection

Explanation :

AWS Shield Advanced offers more robust protection, including advanced threat detection, cost protection, and expert support, which are crucial for businesses with higher DDoS risk.

What is the primary function of AWS Shield in the context of infrastructure protection on AWS?

Answer :

* Protecting against DDoS attacks

Explanation :

AWS Shield is a service designed to protect against Distributed Denial of Service (DDoS) attacks, safeguarding AWS infrastructure from malicious traffic and ensuring availability.

When implementing access controls for data stored in AWS RDS, which method helps you to ensure least privilege?

Answer :

* Using IAM database authentication

Explanation :

Using IAM database authentication allows for fine-grained access control and helps enforce the least privilege principle by assigning specific permissions to IAM roles and users.

How does IAM Identity Center simplify the management of user identities and access within AWS environments?

Answer :

* By offering a centralized approach for role-based access management

Explanation :

IAM Identity Center simplifies identity and access management by providing a centralized, role-based approach to managing user permissions and access across various AWS accounts.

Describe the step needed to rotate an encrypted secret in AWS Secrets Manager that is used by an RDS instance?

Answer :

* Configure automated rotation in Secrets Manager and update the RDS configuration to use it

Explanation :

Configuring automated rotation in Secrets Manager allows the secret to be rotated without manual intervention, and the RDS instance remains updated with the rotated credentials.

What is the primary benefit of using Amazon S3 Versioning for data replication and protection?

Answer :

* It enhances data durability

Explanation :

Amazon S3 Versioning helps you easily recover from unintended user actions and applications failures, thus enhancing data durability by maintaining multiple versions of objects.

What steps are involved in setting up multi-Region keys using AWS Management Console for KMS?

Answer :

* Create key in primary Region, select replicate to second Region, activate key

Explanation :

To set up multi-Region keys in KMS, you first create the key in the primary region, then select the option to replicate it to a second region, and finally activate the replicated key.

What is the primary function of Amazon GuardDuty in the context of monitoring and security on AWS?

Answer :

* Analyzing security findings and threats

Explanation :

Amazon GuardDuty is a threat detection service that continuously analyzes security findings and potential threats in AWS environments, helping to protect against malicious activities.

How does enabling AWS CloudTrail contribute to enhancing security and compliance in AWS environments?

Answer :

* Monitoring and logging API calls

Explanation :

AWS CloudTrail monitors and logs API calls made on AWS resources, providing visibility into user activity, resource changes, and aiding in security analysis and compliance auditing.

Why might an organization prefer AWS Firewall Manager over manual security policy management?

Answer :

* AWS Firewall Manager ensures consistent and scalable policy enforcement

Explanation :

Organizations prefer AWS Firewall Manager because it ensures consistent and scalable policy enforcement, which is less error-prone and more efficient compared to manual management.

Explain the rationale behind choosing AWS Shield Advanced instead of standard AWS Shield for a business with a high risk of DDoS attacks.

Answer :

* Advanced threat detection and comprehensive protection

Explanation :

AWS Shield Advanced offers more robust protection, including advanced threat detection, cost protection, and expert support, which are crucial for businesses with higher DDoS risk.

What is the primary function of AWS Shield in the context of infrastructure protection on AWS?

Answer :

* Protecting against DDoS attacks

Explanation :

AWS Shield is a service designed to protect against Distributed Denial of Service (DDoS) attacks, safeguarding AWS infrastructure from malicious traffic and ensuring availability.

When implementing access controls for data stored in AWS RDS, which method helps you to ensure least privilege?

Answer :

* Using IAM database authentication

Explanation :

Using IAM database authentication allows for fine-grained access control and helps enforce the least privilege principle by assigning specific permissions to IAM roles and users.

How does IAM Identity Center simplify the management of user identities and access within AWS environments?

Answer :

* By offering a centralized approach for role-based access management

Explanation :

IAM Identity Center simplifies identity and access management by providing a centralized, role-based approach to managing user permissions and access across various AWS accounts.

Describe the step needed to rotate an encrypted secret in AWS Secrets Manager that is used by an RDS instance?

Answer :

* Configure automated rotation in Secrets Manager and update the RDS configuration to use it

Explanation :

Configuring automated rotation in Secrets Manager allows the secret to be rotated without manual intervention, and the RDS instance remains updated with the rotated credentials.

   Like   Dislike [Comment](https://www.koenig-solutions.com/aws-certified-security-specialty-security-engineering-on-aws-quiz-questions-answers#collapse_5000_527061)

What is the primary benefit of using Amazon S3 Versioning for data replication and protection?

Answer :

* It enhances data durability

Explanation :

Amazon S3 Versioning helps you easily recover from unintended user actions and applications failures, thus enhancing data durability by maintaining multiple versions of objects.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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

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.

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)