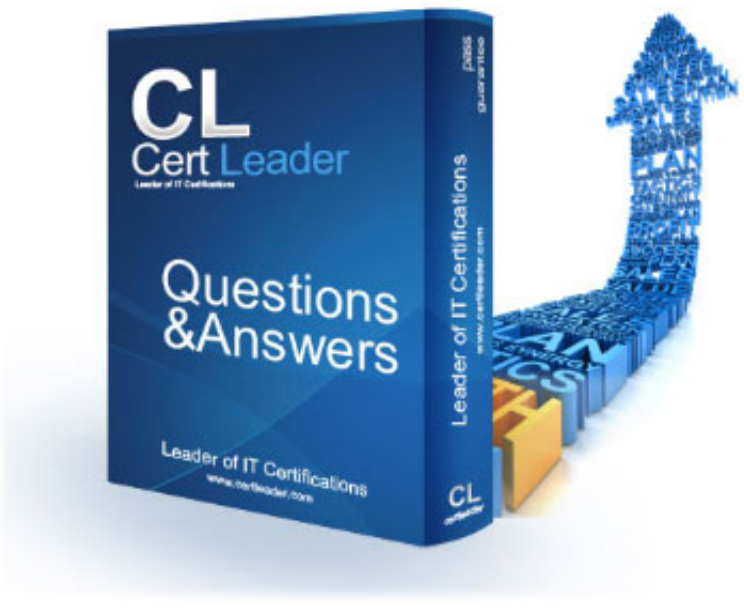
SCS-C01 Dumps

AWS Certified Security- Specialty

https://www.certleader.com/SCS-C01-dumps.html



NEW QUESTION 1
A Developer's laptop was stolen. The laptop was not encrypted, and it contained the SSH key used to access multiple Amazon EC2 instances. A Security Engineer has verified that the key has not been used, and has blocked port 22 to all EC2 instances while developing a response plan.
How can the Security Engineer further protect currently running instances?

A. Delete the key-pair key from the EC2 console, then create a new key pair.
B. Use the modify-instance-attribute API to change the key on any EC2 instance that is using the key.
C. Use the EC2 RunCommand to modify the authorized_keys file on any EC2 instance that is using the key.
D. Update the key pair in any AMI used to launch the EC2 instances, then restart the EC2 instances.

Answer: C

NEW QUESTION 2
An application uses Amazon Cognito to manage end users' permissions when directly accessing AWS resources, including Amazon DynamoDB. A new feature request reads as follows:
Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes.
The priorities are to reduce complexity and avoid potential for future security issues. Which approach will meet these requirements and priorities?

A. Create a new database field "suspended_status" and modify the application logic to validate that field when processing requests.
B. Add suspended customers to second Cognito user pool and update the application login flow to check both user pools.
C. Use Amazon Cognito Sync to push out a "suspension_status" parameter and split the IAM policy into normal users and suspended users.
D. Move suspended customers to a second Cognito group and define an appropriate IAM access policy for the group.

Answer: D

NEW QUESTION 3
A company has several Customer Master Keys (CMK), some of which have imported key material. Each CMK must be rotated annually.
What two methods can the security team use to rotate each key? Select 2 answers from the options given below
Please select:

A. Enable automatic key rotation for a CMK
B. Import new key material to an existing CMK
C. Use the CLI or console to explicitly rotate an existing CMK
D. Import new key material to a new CMK; Point the key alias to the new CMK.
E. Delete an existing CMK and a new default CMK will be created.

Answer: AD

Explanation:
The AWS Documentation mentions the following
Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (the value of the Origin field is External), but you can rotate these CMKs manually.
Rotating Keys Manually
You might want to create a newCMKand use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation.
When you begin using the new CMK, be sure to keep the original CMK enabled so that AWS KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the sam CMK to decrypt the data. As long as you keep both the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK.
Option B is invalid because you also need to point the key alias to the new key Option C is invalid because existing CMK keys cannot be rotated as they are Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key For more information on Key rotation please see the below Link: https://docs.aws.amazon.com/kms/latest/developereuide/rotate-keys.html
The correct answers are: Enable automatic key rotation for a CMK, Import new key material to a new CMK;
Point the key alias to the new CMK.
Submit your Feedback/Queries to our Experts

NEW QUESTION 4
You currently have an S3 bucket hosted in an AWS Account. It holds information that needs be accessed by a partner account. Which is the MOST secure way to allow the partner account to access the S3 bucket in your account? Select 3 options.
Please select:

A. Ensure an 1AM role is created which can be assumed by the partner account.
B. Ensure an 1AM user is created which can be assumed by the partner account.
C. Ensure the partner uses an external id when making the request
D. Provide the ARN for the role to the partner account
E. Provide the Account Id to the partner account
F. Provide access keys for your account to the partner account

Answer: ACD

Explanation:
Option B is invalid because Roles are assumed and not 1AM users
Option E is invalid because you should not give the account ID to the partner Option F is invalid because you should not give the access keys to the partner
The below diagram from the AWS documentation showcases an example on this wherein an 1AM role and external ID is us> access an AWS account resources
C:\Users\wk\Desktop\mudassar\Untitled.jpg

For more information on creating roles for external ID'S please visit the following URL:

The correct answers are: Ensure an 1AM role is created which can be assumed by the partner account. Ensure the partner uses an external id when making the request Provide the ARN for the role to the partner account
Submit your Feedback/Queries to our Experts

NEW QUESTION 5
You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?
Please select:

A. AWS Cloudwatch
B. AWS EC2
C. AWS Trusted Advisor
D. AWS SNS

Answer: C

Explanation:
Below is a snapshot of the service limits that the Trusted Advisor can monitor C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is invalid because even though you can monitor resources, it cannot be checked against the service limit.
Option B is invalid because this is the Elastic Compute cloud service Option D is invalid because it can be send notification but not check on service limit For more information on the Trusted Advisor monitoring, please visit the below URL:
https://aws.amazon.com/premiumsupport/ta-faqs> The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

NEW QUESTION 6
Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flaws. Which of the following can be done to ensure this? Choose 2 answers from the options given below.
Please select:

A. Use AWS Config to ensure that the servers have no critical flaws.
B. Use AWS inspector to ensure that the servers have no critical flaws.
C. Use AWS inspector to patch the servers
D. Use AWS SSM to patch the servers

Answer: BD

Explanation:
The AWS Documentation mentions the following on AWS Inspector
Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.
Option A is invalid because the AWS Config service is not used to check the vulnerabilities on servers Option C is invalid because the AWS Inspector service is not used to patch servers
For more information on AWS Inspector, please visit the following URL: https://aws.amazon.com/inspector>
Once you understand the list of servers which require critical updates, you can rectify them by installing the required patches via the SSM tool.
For more information on the Systems Manager, please visit the following URL: https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html
The correct answers are: Use AWS Inspector to ensure that the servers have no critical flaws.. Use AWS SSM to patch the servers

NEW QUESTION 7
A company has external vendors that must deliver files to the company. These vendors have cross-account that gives them permission to upload objects to one of

the company's S3 buckets.
What combination of steps must the vendor follow to successfully deliver a file to the company? Select 2 answers from the options given below
Please select:

A. Attach an 1AM role to the bucket that grants the bucket owner full permissions to the object
B. Add a grant to the objects ACL giving full permissions to bucket owner.
C. Encrypt the object with a KMS key controlled by the company.
D. Add a bucket policy to the bucket that grants the bucket owner full permissions to the object
E. Upload the file to the company's S3 bucket

Answer: BE

Explanation:
This scenario is given in the AWS Documentation
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.
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A and D are invalid because bucket ACL's are used to give grants to bucket Option C is not required since encryption is not part of the requirement For more information on this scenario please see the below Link:
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroushs-manaeing-access-example3.htmll The correct answers are: Add a grant to the objects ACL giving full permissions to bucket owner., Upload the
file to the company's S3 bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 8
A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of “Sensitive,” “Confidential,” and “Restricted.”
The security solution must meet all of the following requirements:
Each object must be encrypted using a unique key.
AWS KMS must automatically rotate encryption keys annually.
Which of the following meets these requirements?

A. Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annuall
B. For the “Restricted” CMK, define the MFA policy within the key polic
C. Use S3 SSE-KMS to encrypt the objects.
D. Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to tru
E. S3 can then use the grants to encrypt each object with a unique CMK.
F. Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA polic
G. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.
H. Create a CMK with unique imported key material for each data classification type, and rotate them annuall
I. For the “Restricted” key material, define the MFA policy in the key polic
J. Use S3 SSE-KMS to encrypt the objects.

Answer: A

NEW QUESTION 9
An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.
What actions should be taken to troubleshoot the issue while maintaining least privilege. (Select two.)

A. Configure and assign an MFA device to the role used by the instances.
B. Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.
C. Verify that the access key attached to the role used by the instances is active.
D. Attach the AmazonSQSFullAccess managed policy to the role used by the instances.
E. Verify that the role attached to the instances contains policies that allow access to the queue.

Answer: DE

NEW QUESTION 10
A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.
Which solution meets these requirements?

A. Use AWS KMS with AWS managed keys and the ScheduleKeyDeletion API with a PendingWindowInDays set to 0 to remove the keys if necessary.
B. Use KMS with AWS imported key material and then use the DeleteImportedKeyMaterial API to remove the key material if necessary.
C. Use AWS CloudHSM to store the keys and then use the CloudHSM API or the PKCS11 library to delete the keys if necessary.
D. Use the Systems Manager Parameter Store to store the keys and then use the service API operations to delete the key if necessary.

Answer: C

NEW QUESTION 10
Your application currently uses customer keys which are generated via AWS KMS in the US east region. You now want to use the same set of keys from the EU-Central region. How can this be accomplished?
Please select:

A. Export the key from the US east region and import them into the EU-Central region
B. Use key rotation and rotate the existing keys to the EU-Central region
C. Use the backing key from the US east region and use it in the EU-Central region
D. This is not possible since keys from KMS are region specific

Answer: D

Explanation:
Option A is invalid because keys cannot be exported and imported across regions. Option B is invalid because key rotation cannot be used to export keys
Option C is invalid because the backing key cannot be used to export keys This is mentioned in the AWS documentation
What geographic region are my keys stored in?
Keys are only stored and used in the region in which they are created. They cannot be transferred to another region. For example; keys created in the EU-Central (Frankfurt) region are only stored and used within the EU-Central (Frankfurt) region
For more information on KMS please visit the following URL: https://aws.amazon.com/kms/faqs/
The correct answer is: This is not possible since keys from KMS are region specific Submit your Feedback/Queries to our Experts

NEW QUESTION 15
You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process. Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.
Please select:

A. Check to see if the right role has been assigned to the EC2 instances
B. Check to see if the 1AM user has the right permissions for EC2
C. Ensure that agent is running on the instances.
D. Check the Instance status by using the Health API.

Answer: ACD

Explanation:
For ensuring that the instances are configured properly you need to ensure the followi .
1) You installed the latest version of the SSM Agent on your instance
2) Your instance is configured with an AWS Identity and Access Management (1AM) role that enables the instance to communicate with the Systems Manager API
3) You can use the Amazon EC2 Health API to quickly determine the following information about Amazon EC2 instances The status of one or more instances
The last time the instance sent a heartbeat value The version of the SSM Agent
The operating system
The version of the EC2Config service (Windows) The status of the EC2Config service (Windows)
Option B is invalid because 1AM users are not supposed to be directly granted permissions to EC2 Instances For more information on troubleshooting AWS SSM, please visit the following URL:
https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-remote-commands.html
The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure that agent is running on the Instances., Check the Instance status by using the Health API.
Submit your Feedback/Queries to our Experts

NEW QUESTION 20
An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions?
Please select:

A. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.
B. Create an 1AM user within the enterprise account assign a user policy to the 1AM user that allows only the actions required by the SaaS applicatio
C. Create a new access and secret key for the user and provide these credentials to the SaaS provider.
D. Create an 1AM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required

by the SaaS application.
E. Create an 1AM role for EC2 instances, assign it a policy that allows only the actions required tor the Saas application to work, provide the role ARN to the SaaS provider to use when launching their application instances.

Answer: C

Explanation:
The below diagram from an AWS blog shows how access is given to other accounts for the services in your own account
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Options A and B are invalid because you should not user 1AM users or 1AM Access keys Options D is invalid because you need to create a role for cross account access
For more information on Allowing access to external accounts, please visit the below URL:
|https://aws.amazon.com/blogs/apn/how-to-best-architect-your-aws-marketplace-saas-subscription-across-multip The correct answer is: Create an 1AM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
Submit your Feedback/Queries to our Experts

NEW QUESTION 25
An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.
Which of the following supports this requirement for AWS resources that are encrypted by AWS KMS?

A. Copy the application's AWS KMS CMK from the source region to the target region so that it can be used to decrypt the resource after it is copied to the target region.
B. Configure AWS KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.
C. Use AWS services that replicate data across regions, and re-wrap the data encryption key created in the source region by using the CMK in the target region so that the target region's CMK can decrypt the database encryption key.
D. Configure the target region's AWS service to communicate with the source region's AWS KMS so that it can decrypt the resource in the target region.

Answer: C

NEW QUESTION 29
A company has two AWS accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.

A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.
How can a Security Engineer securely set up the bastion host?

A. Move the bastion host to the VPC with VPN connectivit
B. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.

C. Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
D. Move the bastion host to the VPC with VPN connectivit
E. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
F. Create an AWS Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

Answer: C

NEW QUESTION 30
You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?
Please select:

A. Enable AWS Guard Duty for the Instance
B. Use AWS Trusted Advisor
C. Use AWS inspector
D. UseAWSMacie

Answer: C

Explanation:
The AWS Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security
Center for Internet security (CIS) Benchmarks
The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed nere.
Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities Options B and D are invalid because these services cannot give a list of vulnerabilities For more information
on the guidelines, please visit the below URL:
* https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cis.html The correct answer is: Use AWS Inspector
Submit your Feedback/Queries to our Experts

NEW QUESTION 31
An IAM user with fill EC2 permissions could bot start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".
An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.
The IAM user policy is as follows:

What additional items need to be added to the IAM user policy? (Choose two.)

A. kms:GenerateDataKey
B. kms:Decrypt
C. kms:CreateGrant
D. "Condition": {"Bool": {"kms:ViaService": "ec2.us-west-2.amazonaws.com"}}
E. "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}

Answer: CE

NEW QUESTION 35
Your company has created a set of keys using the AWS KMS service. They need to ensure that each key is only used for certain services. For example , they want one key to be used only for the S3 service. How can this be achieved?
Please select:

A. Create an 1AM policy that allows the key to be accessed by only the S3 service.
B. Create a bucket policy that allows the key to be accessed by only the S3 service.
C. Use the kms:ViaService condition in the Key policy
D. Define an 1AM user, allocate the key and then assign the permissions to the required service

Answer: C

Explanation:
Option A and B are invalid because mapping keys to services cannot be done via either the 1AM or bucket policy
Option D is invalid because keys for 1AM users cannot be assigned to services This is mentioned in the AWS Documentation
The kms:ViaService condition key limits use of a customer-managed CMK to requests from particular AWS services. (AWS managed CMKs in your account, such as aws/s3, are always restricted to the AWS service that created them.)
For example, you can use kms:V1aService to allow a user to use a customer managed CMK only for requests that Amazon S3 makes on their behalf. Or you can use it to deny the user permission to a CMK when a request on their behalf comes from AWS Lambda.
For more information on key policy's for KMS please visit the following URL: https://docs.aws.amazon.com/kms/latest/developereuide/policy-conditions.html
The correct answer is: Use the kms:ViaServtce condition in the Key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 40
An application makes calls to AWS services using the AWS SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.
Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

A. Confirm that the EC2 instance's security group authorizes S3 access.
B. Verify that the KMS key policy allows decrypt access for the KMS key for this IAM principle.
C. Check the S3 bucket policy for statements that deny access to objects.
D. Confirm that the EC2 instance is using the correct key pair.
E. Confirm that the IAM role associated with the EC2 instance has the proper privileges.
F. Confirm that the instance and the S3 bucket are in the same Region.

Answer: ABC

NEW QUESTION 42
Which of the following minimizes the potential attack surface for applications?

A. Use security groups to provide stateful firewalls for Amazon EC2 instances at the hypervisor level.
B. Use network ACLs to provide stateful firewalls at the VPC level to prevent access to any specific AWS resource.
C. Use AWS Direct Connect for secure trusted connections between EC2 instances within private subnets.
D. Design network security in a single layer within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet) to facilitate quicker responses to threats.

Answer: A

NEW QUESTION 43
A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.
Which action should the Security Engineer take to allow communication over the public IP addresses?

A. Associate the instances to the same security groups.
B. Add 0.0.0.0/0 to the egress rules of the instance security groups.
C. Add the instance IDs to the ingress rules of the instance security groups.
D. Add the public IP addresses to the ingress rules of the instance security groups.

Answer: D

NEW QUESTION 44
A company has enabled Amazon GuardDuty in all Regions as part of its security monitoring strategy. In one of the VPCs, the company hosts an Amazon EC2 instance working as an FTP server that is contacted by a high number of clients from multiple locations. This is identified by GuardDuty as a brute force attack due to the high number of connections that happen every hour.
The finding has been flagged as a false positive. However, GuardDuty keeps raising the issue. A Security Engineer has been asked to improve the signal-to-noise ratio. The Engineer needs to ensure that changes do not compromise the visibility of potential anomalous behavior.
How can the Security Engineer address the issue?

A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed
B. Add the FTP server to a trusted IP list and deploy it to GuardDuty to stop receiving the notifications
C. Use GuardDuty filters with auto archiving enabled to close the findings
D. Create an AWS Lambda function that closes the finding whenever a new occurrence is reported

Answer: B

Explanation:
Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your AWS infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists. At any given time, you can have only one uploaded trusted IP list per AWS account per region.
References:

NEW QUESTION 49
Which option for the use of the AWS Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

A. Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.
B. Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.
C. Change the CMK alias every 90 days, and update key-calling applications with the new key alias.
D. Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

Answer: A

NEW QUESTION 52
You are responsible to 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. Also there is a need to monitor web application logs to identify any malicious activity. Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below
Please select:

A. Amazon Cloudwatch Logs
B. Amazon VPC Flow Logs

C. Amazon AWS Config
D. Amazon Cloudtrail

Answer: AD

Explanation:
The AWS Documentation mentions the following about these services
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
For more information on Cloudtrail, please refer to below URL: https://aws.amazon.com/cloudtrail;
You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Amazon Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs.
For more information on Cloudwatch logs, please refer to below URL: http://docs.aws.amazon.com/AmazonCloudWatch/latest/loes/WhatisCloudWatchLoES.htmll
The correct answers are: Amazon Cloudwatch Logs, Amazon Cloudtrail

NEW QUESTION 56
A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.
What combination of actions should the Engineer take? (Choose two.)

A. Create an AWS Lambda function that determines whether Flow Logs are enabled for a given VPC.
B. Create an AWS Config configuration item for each VPC in the company AWS account.
C. Create an AWS Config managed rule with a resource type of AWS:: Lambda:: Function.
D. Create an Amazon CloudWatch Event rule that triggers on events emitted by AWS Config.
E. Create an AWS Config custom rule, and associate it with an AWS Lambda function that contains the evaluating logic.

Answer: AE

NEW QUESTION 59
Your company has just started using AWS and created an AWS account. They are aware of the potential issues when root access is enabled. How can they best safeguard the account when it comes to root access? Choose 2 answers fro the options given below
Please select:

A. Delete the root access account
B. Create an Admin 1AM user with the necessary permissions
C. Change the password for the root account.
D. Delete the root access keys

Answer: BD

Explanation:
The AWS Documentation mentions the following
All AWS accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account. Because you cant restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create AWS Identity and Access Management (1AM) user credentials for everyday interaction with AWS.
Option A is incorrect since you cannot delete the root access account
Option C is partially correct but cannot be used as the ideal solution for safeguarding the account For more information on root access vs admin 1AM users, please refer to below URL: https://docs.aws.amazon.com/eeneral/latest/er/root-vs-iam.html
The correct answers are: Create an Admin 1AM user with the necessary permissions. Delete the root access keys Submit your Feedback/Queries to our Experts

NEW QUESTION 62
An application running on EC2 instances in a VPC must access sensitive data in the data center. The access must be encrypted in transit and have consistent low latency. Which hybrid architecture will meet these requirements?
Please select:

A. Expose the data with a public HTTPS endpoint.
B. A VPN between the VPC and the data center over a Direct Connect connection
C. A VPN between the VPC and the data center.
D. A Direct Connect connection between the VPC and data center

Answer: B

Explanation:
Since this is required over a consistency low latency connection, you should use Direct Connect. For encryption, you can make use of a VPN
Option A is invalid because exposing an HTTPS endpoint will not help all traffic to flow between a VPC and the data center.
Option C is invalid because low latency is a key requirement Option D is invalid because only Direct Connect will not suffice
For more information on the connection options please see the below Link: https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharint
The correct answer is: A VPN between the VPC and the data center over a Direct Connect connection Submit your Feedback/Queries to our Experts

NEW QUESTION 65
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 their application? Select 2 answers from the options given below.
Please select:

A. Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.

B. Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layertraffic.
C. Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
D. Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
E. Enable GuardDuty to block malicious traffic from reaching the application

Answer: BD

Explanation:
The below diagram from AWS shows the best case scenario for avoiding DDos attacks using services such as AWS Cloudfro WAF, ELB and Autoscaling
C:\Users\wk\Desktop\mudassar\Untitled.jpg

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
Option E is invalid because this can be used for attacks on EC2 Instances but not against DDos attacks on the entire application For more information on DDos mitigation from AWS, please visit the below URL:
https://aws.amazon.com/answers/networking/aws-ddos-attack-mitieationi
The correct answers are: 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
Submit your Feedback/Queries to our Experts

NEW QUESTION 67
A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The Security team has the following requirements for the architecture:
• Data must be encrypted in transit.
• Data must be encrypted at rest.
• The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Choose two.)

A. Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket.
B. Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.
C. Add a bucket policy that includes a deny if a PutObject request does not include aws:SecureTransport.
D. Add a bucket policy with aws:SourceIp to Allow uploads and downloads from the corporate intranet only.
E. Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-server-side-encryption: "aws:kms".
F. Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

Answer: BC

Explanation:
Bucket encryption using KMS will protect both in case disks are stolen as well as if the bucket is public. This is because the KMS key would need to have privileges granted to it for users outside of AWS.

NEW QUESTION 71
A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).

What mechanism will allow the company to implement all required network rules without incurring additional cost?

A. Configure AWS WAF rules to implement the required rules.
B. Use the operating system built-in, host-based firewall to implement the required rules.
C. Use a NAT gateway to control ingress and egress according to the requirements.
D. Launch an EC2-based firewall product from the AWS Marketplace, and implement the required rules in that product.

Answer: B

NEW QUESTION 75
Your company hosts a large section of EC2 instances in AWS. There are strict security rules governing the EC2 Instances. During a potential security breach , you need to ensure quick investigation of the underlying EC2 Instance. Which of the following service can help you quickly provision a test environment to look into the breached instance.
Please select:

A. AWS Cloudwatch
B. AWS Cloudformation
C. AWS Cloudtrail
D. AWS Config

Answer: B

Explanation:
The AWS Security best practises mentions the following
Unique to AWS, security practitioners can use CloudFormation to quickly create a new, trusted environment in which to conduct deeper investigation. The CloudFormation template can pre-configure instances in an isolated environment that contains all the necessary tools forensic teams need to determine the cause of the incident This cuts down on the time it takes to gather necessary tools, isolates systems under examination, and ensures that the team is operating in a clean room.
Option A is incorrect since this is a logging service and cannot be used to provision a test environment Option C is incorrect since this is an API logging service and cannot be used to provision a test environment Option D is incorrect since this is a configuration service and cannot be used to provision a test environment
For more information on AWS Security best practises, please refer to below URL: https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pd1
The correct answer is: AWS Cloudformation Submit your Feedback/Queries to our Experts

NEW QUESTION 80
A company stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket. In addition , it should be ensured that objects are available in a secondary region if the primary one goes down. Which of the following can help fulfil these requirements? Choose 2 answers from the options given below
Please select:

A. Enable bucket versioning and also enable CRR
B. Enable bucket versioning and enable Master Pays
C. For the Bucket policy add a condition for {"Null": {"aws:MultiFactorAuthAge": true}} i
D. Enable the Bucket ACL and add a condition for {"Null": {"aws:MultiFactorAuthAge": true}}

Answer: AC

Explanation:
The AWS Documentation mentions the following Adding a Bucket Policy to Require MFA
Amazon S3 supports MFA-protected API access, a feature that can enforce multi-factor authentication (MFA) for access to your Amazon S3 resources. Multi-factor authentication provides an extra level of security you can apply to your AWS environment. It is a security feature that requires users to prove physical possession of an MFA device by providing a valid MFA code. For more information, go to AWS Multi-Factor Authentication. You can require MFA authentication for any requests to access your Amazoi. S3 resources.
You can enforce the MFA authentication requirement using the aws:MultiFactorAuthAge key in a bucket policy. 1AM users car access Amazon S3 resources by using temporary credentials issued by the AWS Security Token Service (STS). You provide the MFA code at the time of the STS request.
When Amazon S3 receives a request with MFA authentication, the aws:MultiFactorAuthAge key provides a numeric value indicating how long ago (in seconds) the temporary credential was created. If the temporary credential provided in the request was not created using an MFA device, this key value is null (absent). In a bucket policy, you can add a condition to check this value, as shown in the following example bucket policy. The policy denies any Amazon S3 operation on the /taxdocuments folder in the examplebucket bucket if the request is not MFA authenticated. To learn more about MFA authentication, see Using Multi-Factor Authentication (MFA) in AWS in the 1AM User Guide.

C:\Users\wk\Desktop\mudassar\Untitled.jpg
Option B is invalid because just enabling bucket versioning will not guarantee replication of objects Option D is invalid because the condition for the bucket policy needs to be set accordingly For more information on example bucket policies, please visit the following URL: •
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html
Also versioning and Cross Region replication can ensure that objects will be available in the destination region in case the primary region fails.
For more information on CRR, please visit the following URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html
The correct answers are: Enable bucket versioning and also enable CRR, For the Bucket policy add a condition for {"Null": { "aws:MultiFactorAuthAge": true}}
Submit your Feedback/Queries to our Experts

NEW QUESTION 83
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 combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below
Please select:

A. Create an S3 bucket in a dedicated log account and grant the other accounts write only acces
B. Deliver all log files from every account to this S3 bucket.
C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check
D. Run the function every 10 minutes.
E. Enable CloudTrail log file integrity validation

F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
G. Create a Security Group that blocks all traffic except calls from the CloudTrail servic
H. Associate the security group with) all the Cloud Trail destination S3 buckets.

Answer: AC

Explanation:
The AWS Documentation mentions the following
To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log fill 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 For more information on Cloudtrail log file validation, please visit the below URL:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-loe-file-validation-intro.htmll For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.htm
The correct answers are: Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket, Enable Cloud Trail log file integrity validation
Submit your Feedback/Queries to our Experts

NEW QUESTION 86
A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.
Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

A. Have a Database Administrator encrypt the credentials and store the ciphertext in Amazon S3. Grant permission to the instance role associated with the EC2 instance to read the object and decrypt the ciphertext.
B. Configure a scheduled job that updates the credential in AWS Systems Manager Parameter Store and notifies the Engineer that the application needs to be restarted.
C. Configure automatic rotation of credentials in AWS Secrets Manager.
D. Store the credential in an encrypted string parameter in AWS Systems Manager Parameter Stor
E. Grant permission to the instance role associated with the EC2 instance to access the parameter and the AWS KMS key that is used to encrypt it.
F. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotate
G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

Answer: CE

NEW QUESTION 88
You company has mandated that all data in AWS be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below
Please select:

A. Use Windows bit locker for EBS volumes on Windows instances
B. Use TrueEncrypt for EBS volumes on Linux instances
C. Use AWS Systems Manager to encrypt the existing EBS volumes
D. Boot EBS volume can be encrypted during launch without using custom AMI

Answer: AB

Explanation:
EBS encryption can also be enabled when the volume is created and not for existing volumes. One can use existing tools for OS level encryption.
Option C is incorrect.
AWS Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.
Option D is incorrect
You cannot choose to encrypt a non-encrypted boot volume on instance launch. To have encrypted boot volumes during launch , your custom AMI must have it's boot volume encrypted before launch.
For more information on the Security Best practices, please visit the following URL: com/whit Security Practices.
The correct answers are: Use Windows bit locker for EBS volumes on Windows instances. Use TrueEncrypt for EBS volumes on Linux instances
Submit your Feedback/Queries to our Experts

NEW QUESTION 93
Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB. The company wants to retain full control of the encryption keys.
Which DynamoDB feature should the Engineer use to achieve compliance'?

A. Use AWS Certificate Manager to request a certificat
B. Use that certificate to encrypt data prior to uploading it to DynamoDB.
C. Enable S3 server-side encryption with the customer-provided key
D. Upload the data to Amazon S3, and then use S3Copy to move all data to DynamoDB
E. Create a KMS master ke
F. Generate per-record data keys and use them to encrypt data prior to uploading it to DynamoD
G. Dispose of the cleartext and encrypted data keys after encryption without storing.
H. Use the DynamoDB Java encryption client to encrypt data prior to uploading it to DynamoDB.

Answer: D

NEW QUESTION 94
A company plans to migrate a sensitive dataset to Amazon S3. A Security Engineer must ensure that the data is encrypted at rest. The encryption solution must enable the company to generate its own keys without needing to manage key storage or the encryption process.
What should the Security Engineer use to accomplish this?

A. Server-side encryption with Amazon S3-managed keys (SSE-S3)
B. Server-side encryption with AWS KMS-managed keys (SSE-KMS)
C. Server-side encryption with customer-provided keys (SSE-C)
D. Client-side encryption with an AWS KMS-managed CMK

Answer: B

Explanation:
Reference https://aws.amazon.com/s3/faqs/

NEW QUESTION 99
Development teams in your organization use S3 buckets to store the log files for various applications hosted ir development environments in AWS. The developers want to keep the logs for one month for troubleshooting purposes, and then purge the logs. What feature will enable this requirement?
Please select:

A. Adding a bucket policy on the S3 bucket.
B. Configuring lifecycle configuration rules on the S3 bucket.
C. Creating an 1AM policy for the S3 bucket.
D. Enabling CORS on the S3 bucket.

Answer: B

Explanation:
The AWS Documentation mentions the following on lifecycle policies
Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified a« follows:
Transition actions - In which you define when objects transition to another . For example, you may choose to transition objects to the STANDARDJA (IA, for infrequent access) storage class 30 days after creation, or
archive objects to the GLACIER storage class one year after creation.
Expiration actions - In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.
Option A and C are invalid because neither bucket policies neither 1AM policy's can control the purging of logs Option D is invalid CORS is used for accessing objects across domains and not for purging of logs For more information on AWS S3 Lifecycle policies, please visit the following URL:
com/AmazonS3/latest/d<
The correct answer is: Configuring lifecycle configuration rules on the S3 bucket. Submit your Feedback/Queries to our Experts

NEW QUESTION 103
An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the AWS Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.
How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

A. Use a filter in AWS CloudTrail to exclude the IP addresses of the Security team’s EC2 instances.
B. Add the Elastic IP addresses of the Security team’s EC2 instances to a trusted IP list in Amazon GuardDuty.
C. Install the Amazon Inspector agent on the EC2 instances that the Security team uses.
D. Grant the Security team’s EC2 instances a role with permissions to call Amazon GuardDuty API operations.

Answer: B

NEW QUESTION 105
You have a set of Customer keys created using the AWS KMS service. These keys have been used for around 6 months. You are now trying to use the new KMS features for the existing set of key's but are not able to do so. What could be the reason for this.
Please select:

A. You have not explicitly given access via the key policy
B. You have not explicitly given access via the 1AM policy
C. You have not given access via the 1AM roles
D. You have not explicitly given access via 1AM users

Answer: A

Explanation:
By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explii update the default key policy for these keys.
Option B,C and D are invalid because the key policy is the main entity used to provide access to the keys
For more information on upgrading key policies please visit the following URL: https://docs.aws.ama20n.com/kms/latest/developerguide/key-policy-upgrading.html
(
The correct answer is: You have not explicitly given access via the key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 109
A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target AWS account (123456789123) to perform their job functions.
A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

What should be done to enable the user to assume the appropriate role in the target account?

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 113
A Solutions Architect is designing a web application that uses Amazon CloudFront, an Elastic Load Balancing Application Load Balancer, and an Auto Scaling group of Amazon EC2 instances. The load balancer and EC2 instances are in the US West (Oregon) region. It has been decided that encryption in transit is necessary by using a customer-branded domain name from the client to CloudFront and from CloudFront to the load balancer.
Assuming that AWS Certificate Manager is used, how many certificates will need to be generated?

A. One in the US West (Oregon) region and one in the US East (Virginia) region.
B. Two in the US West (Oregon) region and none in the US East (Virginia) region.
C. One in the US West (Oregon) region and none in the US East (Virginia) region.
D. Two in the US East (Virginia) region and none in the US West (Oregon) region.

Answer: A

NEW QUESTION 118
A company has decided to migrate sensitive documents from on-premises data centers to Amazon S3. Currently, the hard drives are encrypted to meet a compliance requirement regarding data encryption. The CISO wants to improve security by encrypting each file using a different key instead of a single key. Using a different key would limit the security impact of a single exposed key.
Which of the following requires the LEAST amount of configuration when implementing this approach?

A. Place each file into a different S3 bucke
B. Set the default encryption of each bucket to use a different AWS KMS customer managed key.

C. Put all the files in the same S3 bucke
D. Using S3 events as a trigger, write an AWS Lambda function to encrypt each file as it is added using different AWS KMS data keys.
E. Use the S3 encryption client to encrypt each file individually using S3-generated data keys
F. Place all the files in the same S3 bucke
G. Use server-side encryption with AWS KMS-managed keys (SSE-KMS) to encrypt the data

Answer: D

NEW QUESTION 119
A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system. Which of the following would be ideal to implement?
Please select:

A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC
B. Use a custom solution available in the AWS Marketplace
C. Use VPC Flow logs to detect the issues and flag them accordingly.
D. Use AWS Cloudwatch to monitor all traffic

Answer: B

Explanation:
Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention. For more information on using custom security solutions please visit the below URL https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%200verview.pdf
For more information on using custom security solutions please visit the below URL: https://d1 .awsstatic.com/Marketplace/security/AWSMP Security Solution%20Overview.pd1
The correct answer is: Use a custom solution available in the AWS Marketplace Submit your Feedback/Queries to our Experts

NEW QUESTION 120
The Security Engineer created a new AWS Key Management Service (AWS KMS) key with the following key policy:

What are the effects of the key policy? (Choose two.)

A. The policy allows access for the AWS account 111122223333 to manage key access though IAM policies.
B. The policy allows all IAM users in account 111122223333 to have full access to the KMS key.
C. The policy allows the root user in account 111122223333 to have full access to the KMS key.
D. The policy allows the KMS service-linked role in account 111122223333 to have full access to the KMS key.
E. The policy allows all IAM roles in account 111122223333 to have full access to the KMS key.

Answer: BE

NEW QUESTION 123
A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption SSE-C, which of the below mentioned statements is true?
Please select:

A. The user should use the same encryption key for all versions of the same object
B. It is possible to have different encryption keys for different versions of the same object
C. AWS S3 does not allow the user to upload his own keys for server side encryption
D. The SSE-C does not work when versioning is enabled

Answer: B

Explanation:

anaging your own encryption keys, y
You can encrypt the object and send it across to S3
Option A is invalid because ideally you should use different encryption keys Option C is invalid because you can use you own encryption keys Option D is invalid because encryption works even if versioning is enabled For more information on client side encryption please visit the below Link:
""Keys.html https://docs.aws.ama2on.com/AmazonS3/latest/dev/UsingClientSideEncryption.html
The correct answer is: It is possible to have different encryption keys for different versions of the same object Submit your Feedback/Queries to our Experts

NEW QUESTION 125
Which of the following is the most efficient way to automate the encryption of AWS CloudTrail logs using a Customer Master Key (CMK) in AWS KMS?

A. Use the KMS direct encrypt function on the log data every time a CloudTrail log is generated.
B. Use the default Amazon S3 server-side encryption with S3-managed keys to encrypt and decrypt theCloudTrail logs.
C. Configure CloudTrail to use server-side encryption using KMS-managed keys to encrypt and decrypt CloudTrail logs.
D. Use encrypted API endpoints so that all AWS API calls generate encrypted CloudTrail log entries using the TLS certificate from the encrypted API call.

Answer: C

NEW QUESTION 128
You are planning to use AWS Configto check the configuration of the resources in your AWS account. You are planning on using an existing 1AM role and using it for the AWS Config resource. Which of the following is required to ensure the AWS config service can work as required?
Please select:

A. Ensure that there is a trust policy in place for the AWS Config service within the role
B. Ensure that there is a grant policy in place for the AWS Config service within the role
C. Ensure that there is a user policy in place for the AWS Config service within the role
D. Ensure that there is a group policy in place for the AWS Config service within the role

Answer: A

Explanation:

C:\Users\wk\Desktop\mudassar\Untitled.jpg
Options B,C and D are invalid because you need to ensure a trust policy is in place and not a grant, user or group policy or more information on the 1AM role permissions please visit the below Link:
https://docs.aws.amazon.com/config/latest/developerguide/iamrole-permissions.htmll
The correct answer is: Ensure that there is a trust policy in place for the AWS Config service within the role Submit your Feedback/Queries to our Experts

NEW QUESTION 133
What is the function of the following AWS Key Management Service (KMS) key policy attached to a customer master key (CMK)?

A. The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.
B. The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and AWS.
C. The CMK is to be used for encrypting and decrypting only when the principal is ExampleUser and therequest comes from WorkMail or SES in the specified region.
D. The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

Answer: C

NEW QUESTION 138
A large organization is planning on AWS to host their resources. They have a number of autonomous departments that wish to use AWS. What could be the strategy to adopt for managing the accounts.
Please select:

A. Use multiple VPCs in the account each VPC for each department
B. Use multiple 1AM groups, each group for each department
C. Use multiple 1AM roles, each group for each department
D. Use multiple AWS accounts, each account for each department

Answer: D

Explanation:
A recommendation for this is given in the AWS Security best practices C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is incorrect since this would be applicable for resources in a VPC Options B and C are incorrect since operationally it would be difficult to manage For more information on AWS Security best practices please refer to the below URL
https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdl
The correct answer is: Use multiple AWS accounts, each account for each department Submit your Feedback/Queries to our Experts

NEW QUESTION 140
A company requires that data stored in AWS be encrypted at rest. Which of the following approaches achieve this requirement? Select 2 answers from the options given below.
Please select:

A. When storing data in Amazon EBS, use only EBS-optimized Amazon EC2 instances.
B. When storing data in EBS, encrypt the volume by using AWS KMS.
C. When storing data in Amazon S3, use object versioning and MFA Delete.
D. When storing data in Amazon EC2 Instance Store, encrypt the volume by using KMS.
E. When storing data in S3, enable server-side encryption.

Answer: BE

Explanation:
The AWS Documentation mentions the following
To create an encrypted Amazon EBS volume, select the appropriate box in the Amazon EBS section of the Amazon EC2 console. You can use a custom customer master key (CMK) by choosing one from the list that appears below the encryption box. If you do not specify a custom CMK, Amazon EBS uses the AWS-managed CMK for Amazon EBS in your account. If there is no AWS-managed CMK for Amazon EBS in your account, Amazon EBS creates one.
Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.
• Use Server-Side Encryption - You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
• Use Client-Side Encryption - You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.
Option A is invalid because using EBS-optimized Amazon EC2 instances alone will not guarantee protection of instances at rest. Option C is invalid because this will not encrypt data at rest for S3 objects. Option D is invalid because you don't store data in Instance store. For more information on EBS encryption, please visit the below URL:
https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html For more information on S3 encryption, please visit the below URL:

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsinEEncryption.html
The correct answers are: When storing data in EBS, encrypt the volume by using AWS KMS. When storing data in S3, enable server-side encryption.
Submit your Feedback/Queries to our Experts

NEW QUESTION 141
You have an S3 bucket hosted in AWS. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?
Please select:

A. Use versioning and enable a timestamp for each version
B. Use Pre-signed URL's
C. Use 1AM Roles with a timestamp to limit the access
D. Use 1AM policies with a timestamp to limit the access

Answer: B

Explanation:
The AWS Documentation mentions the following
All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.
Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles
Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:
https://docs.aws.ama2on.com/AmazonS3/latest/dev/ShareObiectPreSisnedURL.html
The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 145
A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket.
What is a possible cause of the issue?

A. The S3 ACL for the S3 bucket fails to explicitly grant access to the Application Developer
B. The AWS KMS key for the S3 bucket fails to list the Application Developer as an administrator
C. The S3 bucket policy fails to explicitly grant access to the Application Developer
D. The S3 bucket policy explicitly denies access to the Application Developer

Answer: C

NEW QUESTION 146
A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational AWS resource purposes.
How can the Administrator restrict usage of member root user accounts across the organization?

A. Disable the use of the root user account at the organizational roo
B. Enable multi-factor authentication of the root user account for each organizational member account.
C. Configure IAM user policies to restrict root account capabilities for each Organizations member account.
D. Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root use
E. Add all operational accounts to the new OU.
F. Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

Answer: C

NEW QUESTION 150
Your company is hosting a set of EC2 Instances in AWS. They want to have the ability to detect if any port scans occur on their AWS EC2 Instances. Which of the following can help in this regard?
Please select:

A. Use AWS inspector to consciously inspect the instances for port scans
B. Use AWS Trusted Advisor to notify of any malicious port scans
C. Use AWS Config to notify of any malicious port scans
D. Use AWS Guard Duty to monitor any malicious port scans

Answer: D

Explanation:
The AWS blogs mention the following to support the use of AWS GuardDuty
GuardDuty voraciously consumes multiple data streams, including several threat intelligence feeds, staying aware of malicious addresses, devious domains, and more importantly, learning to accurately identify malicious or unauthorized behavior in your AWS accounts. In combination with information gleaned from your VPC Flow Logs, AWS CloudTrail Event Logs, and DNS logs, th allows GuardDuty to detect many different types of dangerous and mischievous behavior including probes for known vulnerabilities, port scans and probes, and access from unusual locations. On the AWS side, it looks for suspicious AWS account activity such as unauthorized deployments, unusual CloudTrail activity, patterns of access to AWS API functions, and attempts to exceed multiple service limits. GuardDuty will also look for compromised EC2 instances talking to malicious entities or services, data exfiltration attempts, and instances that are mining cryptocurrency.
Options A, B and C are invalid because these services cannot be used to detect port scans For more information on AWS Guard Duty, please refer to the below Link:
https://aws.amazon.com/blogs/aws/amazon-guardduty-continuous-security-monitoring-threat-detection; (
The correct answer is: Use AWS Guard Duty to monitor any malicious port scans Submit your Feedback/Queries to our Experts

NEW QUESTION 154
An application is designed to run on an EC2 Instance. The applications needs to work with an S3 bucket. From a security perspective , what is the ideal way for the

EC2 instance/ application to be configured?
Please select:

A. Use the AWS access keys ensuring that they are frequently rotated.
B. Assign an 1AM user to the application that has specific access to only that S3 bucket
C. Assign an 1AM Role and assign it to the EC2 Instance
D. Assign an 1AM group and assign it to the EC2 Instance

Answer: C

Explanation:
The below diagram from the AWS whitepaper shows the best security practicse of allocating a role that has access to the S3 bucket
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Options A,B and D are invalid because using users, groups or access keys is an invalid security practise when giving access to resources from other AWS resources.
For more information on the Security Best practices, please visit the following URL: https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdl
The correct answer is: Assign an 1AM Role and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 159
Your application currently use AWS Cognito for authenticating users. Your application consists of different types of users. Some users are only allowed read access to the application and others are given contributor access. How wou you manage the access effectively?
Please select:

A. Create different cognito endpoints, one for the readers and the other for the contributors.
B. Create different cognito groups, one for the readers and the other for the contributors.
C. You need to manage this within the application itself
D. This needs to be managed via Web security tokens

Answer: B

Explanation:
The AWS Documentation mentions the following
You can use groups to create a collection of users in a user pool, which is often done to set the permissions for those users. For example, you can create separate groups for users who are readers, contributors, and editors of your website and app.
Option A is incorrect since you need to create cognito groups and not endpoints
Options C and D are incorrect since these would be overheads when you can use AWS Cognito For more information on AWS Cognito user groups please refer to the below Link: https://docs.aws.amazon.com/coenito/latest/developersuide/cognito-user-pools-user-groups.htmll
The correct answer is: Create different cognito groups, one for the readers and the other for the contributors. Submit your Feedback/Queries to our Experts

NEW QUESTION 162
The AWS Systems Manager Parameter Store is being used to store database passwords used by an AWS Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an AWS KMS key that allows access through IAM. When the function executes, this parameter cannot be retrieved as the result of an access denied error.
Which of the following actions will resolve the access denied error?

A. Update the ssm.amazonaws.com principal in the KMS key policy to allow kms: Decrypt.
B. Update the Lambda configuration to launch the function in a VPC.
C. Add a policy to the role that the Lambda function uses, allowing kms: Decrypt for the KMS key.
D. Add lambda.amazonaws.com as a trusted entity on the IAM role that the Lambda function uses.

Answer: A

NEW QUESTION 167
You have several S3 buckets defined in your AWS account. You need to give access to external AWS accounts to these S3 buckets. Which of the following can allow you to define the permissions for the external accounts? Choose 2 answers from the options given below
Please select:

A. 1AM policies
B. Buckets ACL's
C. 1AM users
D. Bucket policies

Answer: BD

Explanation:
The AWS Security whitepaper gives the type of access control and to what level the control can be given C:\Users\wk\Desktop\mudassar\Untitled.jpg

Options A and C are incorrect since for external access to buckets, you need to use either Bucket policies or Bucket ACL's or more information on Security for storage services role please refer to the below URL:
https://d1.awsstatic.com/whitepapers/Security/Security Storage Services Whitepaper.pdf The correct answers are: Buckets ACL's, Bucket policies
Submit your Feedback/Queries to our Experts

NEW QUESTION 172
A company has a large set of keys defined in AWS KMS. Their developers frequently use the keys for the applications being developed. What is one of the ways that can be used to reduce the cost of accessing the keys in the AWS KMS service.
Please select:

A. Enable rotation of the keys
B. Use Data key caching
C. Create an alias of the key
D. Use the right key policy

Answer: B

Explanation:
The AWS Documentation mentions the following
Data key caching stores data keys and related cryptographic material in a cache. When you encrypt or decrypt data, the AWS Encryption SDK looks for a matching data key in the cache. If it finds a match, it uses the cached data key rather than generatir a new one. Data key caching can improve performance, reduce cost, and help you stay within service limits as your application scales.
Option A.C and D are all incorrect since these options will not impact how the key is used. For more information on data key caching, please refer to below URL:
https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-key-cachine.htmll The correct answer is: Use Data key caching Submit your Feedback/Queries to our Experts

NEW QUESTION 173
A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet with port 80 and a Database server in the private subnet with port 3306. The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). which of the below mentioned entries is required in the private subnet database security group DBSecGrp?
Please select:

A. Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp.
B. Allow Inbound on port 3306 from source 20.0.0.0/16
C. Allow Outbound on port 3306 for Destination Web Server Security Group WebSecGrp.
D. Allow Outbound on port 80 for Destination NAT Instance IP

Answer: A

Explanation:
Since the Web server needs to talk to the database server on port 3306 that means that the database server should allow incoming traffic on port 3306. The below table from the aws documentation shows how the security groups should be set up.
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option B is invalid because you need to allow incoming access for the database server from the WebSecGrp security group.
Options C and D are invalid because you need to allow Outbound traffic and not inbound traffic For more information on security groups please visit the below Link:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC
Scenario2.html
The correct answer is: Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp. Submit your Feedback/Queries to our Experts

NEW QUESTION 176
A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other AWS account resources by using the EC2 instance metadata service.
What can the Administrator do to protect against this potential attack?

A. Disable the EC2 instance metadata service.
B. Log all student SSH interactive session activity.
C. Implement ip tables-based restrictions on the instances.
D. Install the Amazon Inspector agent on the instances.

Answer: C

NEW QUESTION 177
An organization policy states that all encryption keys must be automatically rotated every 12 months. Which AWS Key Management Service (KMS) key type should be used to meet this requirement?

A. AWS managed Customer Master Key (CMK)
B. Customer managed CMK with AWS generated key material
C. Customer managed CMK with imported key material
D. AWS managed data key

Answer: B

NEW QUESTION 179

In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly.
What must be done to prevent users from accessing the S3 objects directly by using URLs?

A. Change the S3 bucket/object permission so that only the bucket owner has access.
B. Set up a CloudFront origin access identity (OAI), and change the S3 bucket/object permission so that only the OAI has access.
C. Create IAM roles for CloudFront, and change the S3 bucket/object permission so that only the IAM role has access.
D. Redirect S3 bucket access to the corresponding CloudFront distribution.

Answer: B

NEW QUESTION 184
Which of the following is used as a secure way to log into an EC2 Linux Instance? Please select:

A. 1AM User name and password
B. Key pairs
C. AWS Access keys
D. AWS SDK keys

Answer: B

Explanation:
The AWS Documentation mentions the following
Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.
Option A.C and D are all wrong because these are not used to log into EC2 Linux Instances For more information on AWS Security credentials, please visit the below URL: https://docs.aws.amazon.com/eeneral/latest/er/aws-sec-cred-types.html
The correct answer is: Key pairs
Submit your Feedback/Queries to our Experts

NEW QUESTION 185
The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using AWS CloudFormation templates with EC2 Auto Scaling groups:
-Have the EC2 instances bootstrapped to connect to a backend database.
-Ensure that the database credentials are handled securely.
-Ensure that retrievals of database credentials are logged.
Which of the following is the MOST efficient way to meet these requirements?

A. Pass databases credentials to EC2 by using CloudFormation stack parameters with the property set to tru
B. Ensure that the instance is configured to log to Amazon CloudWatch Logs.
C. Store database passwords in AWS Systems Manager Parameter Store by using SecureString parameters.Set the IAM role for the EC2 instance profile to allow access to the parameters.
D. Create an AWS Lambda that ingests the database password and persists it to Amazon S3 with server-side encryptio
E. Have the EC2 instances retrieve the S3 object on startup, and log all script invocations to syslog.
F. Write a script that is passed in as UserData so that it is executed upon launch of the EC2 instance.Ensure that the instance is configured to log to Amazon CloudWatch Logs.

Answer: C

NEW QUESTION 189
A Security Engineer is working with a Product team building a web application on AWS. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.
Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

A. Create a custom authorization service using AWS Lambda.
B. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.
C. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.
D. Configure an Amazon Cognito identity pool to integrate with social login providers.
E. Update DynamoDB to store the user email addresses and passwords.
F. Update API Gateway to use a COGNITO_USER_POOLS authorizer.

Answer: ABE

NEW QUESTION 191
Your team is experimenting with the API gateway service for an application. There is a need to implement a custom module which can be used for authentication/authorization for calls made to the API gateway. How can this be achieved?
Please select:

A. Use the request parameters for authorization
B. Use a Lambda authorizer
C. Use the gateway authorizer
D. Use CORS on the API gateway

Answer: B

Explanation:
The AWS Documentation mentions the following
An Amazon API Gateway Lambda authorizer (formerly known as a custom authorize?) is a Lambda function that you provide to control access to your API

methods. A Lambda authorizer uses bearer token authentication strategies, such as OAuth or SAML. It can also use information described by headers, paths, query strings, stage variables, or context variables request parameters.
Options A,C and D are invalid because these cannot be used if you need a custom authentication/authorization for calls made to the API gateway
For more information on using the API gateway Lambda authorizer please visit the URL:
https://docs.aws.amazon.com/apisateway/latest/developerguide/apieateway-use-lambda-authorizer.htmll The correct answer is: Use a Lambda authorizer
Submit your Feedback/Queries to our Experts

NEW QUESTION 196
You are building a large-scale confidential documentation web server on AWSand 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 Cloud Front to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below
Please select:

A. Create an Identity and Access Management (1AM) user for CloudFront and grant access to the objects in your S3 bucket to that 1AM User.
B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
C. Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.
D. Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: B

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 ace logs are less useful because they're incomplete.
Option A is invalid because you need to create a Origin Access Identity for Cloudfront and not an 1AM user Option C and D are invalid because using policies will not help fulfil the requirement
For more information on Origin Access Identity please see the below Link:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restrictine-access-to-s3.
The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
(
Submit your Feedback/Queries to our Experts

NEW QUESTION 199
You are creating a Lambda function which will be triggered by a Cloudwatch Event. The data from these events needs to be stored in a DynamoDB table. How should the Lambda function be given access to the DynamoDB table?
Please select:

A. Put the AWS Access keys in the Lambda function since the Lambda function by default is secure
B. Use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function.
C. Use the AWS Access keys which has access to DynamoDB and then place it in an S3 bucket.
D. Create a VPC endpoint for the DynamoDB tabl
E. Access the VPC endpoint from the Lambda function.

Answer: B

Explanation:
AWS Lambda functions uses roles to interact with other AWS services. So use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function.
Options A and C are all invalid because you should never use AWS keys for access. Option D is invalid because the VPC endpoint is used for VPCs
For more information on Lambda function Permission model, please visit the URL https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html
The correct answer is: Use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function. Submit your Feedback/Queries to our Experts

NEW QUESTION 203
You have an instance setup in a test environment in AWS. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?
Please select:

A. Shutdown the instance
B. Remove the rule for incoming traffic on port 22 for the Security Group
C. Change the AMI for the instance
D. Change the Instance type for the instance

Answer: B

Explanation:
In the test environment the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.
Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.
For more information on authorizing access to an instance, please visit the below URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.htmll
The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

NEW QUESTION 208
You have a 2 tier application hosted in AWS. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2

answers from the options given below.
Please select:

A. wg-123 -Allow ports 80 and 443 from 0.0.0.0/0
B. db-345 - Allow port 1433 from wg-123
C. wg-123 - Allow port 1433 from wg-123
D. db-345 -Allow ports 1433 from 0.0.0.0/0

Answer: AB

Explanation:
The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.
The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration
Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.htmll
The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123
Submit your Feedback/Queries to our Experts

NEW QUESTION 209
A Security Engineer is trying to determine whether the encryption keys used in an AWS service are in compliance with certain regulatory standards.
Which of the following actions should the Engineer perform to get further guidance?

A. Read the AWS Customer Agreement.
B. Use AWS Artifact to access AWS compliance reports.
C. Post the question on the AWS Discussion Forums.
D. Run AWS Config and evaluate the configuration outputs.

Answer: B

NEW QUESTION 214
You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your server's on-premises will be communicating with your VPC instances. You will be establishing IPSec tunnels over the internet. Yo will be using VPN gateways and terminating the IPsec tunnels on AWS-supported customer gateways. Which of the following objectives would you achieve by implementing an IPSec tunnel as outlined above? Choose 4 answers form the options below
Please select:

A. End-to-end protection of data in transit
B. End-to-end Identity authentication
C. Data encryption across the internet
D. Protection of data in transit over the Internet
E. Peer identity authentication between VPN gateway and customer gateway
F. Data integrity protection across the Internet

Answer: CDEF

Explanation:
IPSec is a widely adopted protocol that can be used to provide end to end protection for data

NEW QUESTION 215
A company has resources hosted in their AWS Account. There is a requirement to monitor all API activity for all regions. The audit needs to be applied for future regions as well. Which of the following can be used to fulfil this requirement.
Please select:

A. Ensure Cloudtrail for each regio
B. Then enable for each future region.
C. Ensure one Cloudtrail trail is enabled for all regions.
D. Create a Cloudtrail for each regio
E. Use Cloudformation to enable the trail for all future regions.
F. Create a Cloudtrail for each regio
G. Use AWS Config to enable the trail for all future regions.

Answer: B

Explanation:
The AWS Documentation mentions the following
You can now turn on a trail across all regions for your AWS account. CloudTrail will deliver log files from all regions to the Amazon S3 bucket and an optional CloudWatch Logs log group you specified. Additionally, when AWS launches a new region, CloudTrail will create the same trail in the new region. As a result you will receive log files containing API activity for the new region without taking any action.
Option A and C is invalid because this would be a maintenance overhead to enable cloudtrail for every region Option D is invalid because this AWS Config cannot be used to enable trails
For more information on this feature, please visit the following URL:
https://aws.ama2on.com/about-aws/whats-new/20l5/l2/turn-on-cloudtrail-across-all-reeions-and-support-for-mul The correct answer is: Ensure one Cloudtrail trail is enabled for all regions. Submit your Feedback/Queries to our Experts

NEW QUESTION 217
A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized AWS IAM user from the IP address range 10.10.10.0/24:

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message.
What does the Administrator need to change to grant access to the user?

A. Change the “Resource” from “arn: aws:s3:::Bucket” to “arn:aws:s3:::Bucket/*”.
B. Change the “Principal” from “*” to {AWS:”arn:aws:iam: : account-number: user/username”}
C. Change the “Version” from “2012-10-17” to the last revised date of the policy
D. Change the “Action” from [“s3:*”] to [“s3:GetObject”, “s3:ListBucket”]

Answer: A

NEW QUESTION 221
A financial institution has the following security requirements:

Cloud-based users cannot access on-premises systems.
As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.
How would the organization manage its resources in the MOST secure manner? (Choose two.)

A. Configure an AWS Managed Microsoft AD to manage the cloud resources.
B. Configure an additional on-premises Active Directory service to manage the cloud resources.
C. Establish a one-way trust relationship from the existing Active Directory to the new Active Directory service.
D. Establish a one-way trust relationship from the new Active Directory to the existing Active Directory service.
E. Establish a two-way trust between the new and existing Active Directory services.

Answer: AD

NEW QUESTION 226
Your company has been using AWS for the past 2 years. They have separate S3 buckets for logging the various AWS services that have been used. They have hired an external vendor for analyzing their log files. They have their own AWS account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below
Please select:

A. Create an 1AM user in the company account
B. Create an 1AM Role in the company account
C. Ensure the 1AM user has access for read-only to the S3 buckets
D. Ensure the 1AM Role has access for read-only to the S3 buckets

Answer: BD

Explanation:
The AWS Documentation mentions the following
To share log files between multiple AWS accounts, you must perform the following general steps. These steps are explained in detail later in this section.
Create an 1AM role for each account that you want to share log files with.
For each of these 1AM roles, create an access policy that grants read-only access to the account you want to share the log files with.
Have an 1AM user in each account programmatically assume the appropriate role and retrieve the log files. Options A and C are invalid because creating an 1AM user and then sharing the 1AM user credentials with the
vendor is a direct 'NO' practise from a security perspective.

For more information on sharing cloudtrail logs files, please visit the following URL https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-sharine-loes.htmll
The correct answers are: Create an 1AM Role in the company account Ensure the 1AM Role has access for read-only to the S3 buckets
Submit your Feedback/Queries to our Experts

NEW QUESTION 230
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?
Please select:

A. Trigger an AWS Config Rules evaluation of the restricted-common-ports rule against every EC2 instance.
B. Query the Trusted Advisor API for all best practice security checks and check for "action recommened" status.
C. Enable a GuardDuty threat detection analysis targeting the port configuration on every EC2 instance.
D. Run an Amazon inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

Answer: D

Explanation:
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 behavior 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.
Insecure Server Protocols
This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.
For more information, please refer to below URL: https://docs.aws.amazon.eom/mspector/latest/userguide/inspector_runtime-behavior-analysis.html#insecure-prot (
The correct answer is: Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.
Submit your Feedback/Queries to our Experts

NEW QUESTION 231
A company's AWS account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?
Please select:

A. Create a new role and add each user to the IAM role
B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
C. Create a policy and apply it to multiple users using a JSON script
D. Create an S3 bucket policy with unlimited access which includes each user's AWS account ID

Answer: B

Explanation:
Option A is incorrect since you don't add a user to the 1AM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach
An 1AM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group
For more information on 1AM Groups, just browse to the below URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the 1AM groups and add users, based upon their role, to different groups and apply the policy to group
Submit your Feedback/Queries to our Experts

NEW QUESTION 232
Which of the following is the responsibility of the customer? Choose 2 answers from the options given below. Please select:

A. Management of the Edge locations
B. Encryption of data at rest
C. Protection of data in transit
D. Decommissioning of old storage devices

Answer: BC

Explanation:
Below is the snapshot of the Shared Responsibility Model

C:\Users\wk\Desktop\mudassar\Untitled.jpg
For more information on AWS Security best practises, please refer to below URL awsstatic corn/whitepapers/Security/AWS Practices.
The correct answers are: Encryption of data at rest Protection of data in transit Submit your Feedback/Queries to our Experts

NEW QUESTION 234
A Security Engineer must design a solution that enables the Incident Response team to audit for changes to a user’s IAM permissions in the case of a security incident.
How can this be accomplished?

A. Use AWS Config to review the IAM policy assigned to users before and after the incident.
B. Run the GenerateCredentialReport via the AWS CLI, and copy the output to Amazon S3 daily for auditing purposes.
C. Copy AWS CloudFormation templates to S3, and audit for changes from the template.
D. Use Amazon EC2 Systems Manager to deploy images, and review AWS CloudTrail logs for changes.

Answer: A

NEW QUESTION 236
Which of the below services can be integrated with the AWS Web application firewall service. Choose 2 answers from the options given below
Please select:

A. AWS Cloudfront
B. AWS Lambda
C. AWS Application Load Balancer
D. AWS Classic Load Balancer

Answer: AC

Explanation:
The AWS documentation mentions the following on the Application Load Balancer
AWS WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of Amazon CloudFront it car be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations and as part of the Application Load Balancer it can protect your origin web servers running behind the ALBs.
Options B and D are invalid because only Cloudfront and the Application Load Balancer services are supported by AWS WAF.
For more information on the web application firewall please refer to the below URL: https://aws.amazon.com/waf/faq;
The correct answers are: AWS Cloudfront AWS Application Load Balancer Submit your Feedback/Queries to our Experts

NEW QUESTION 241
What is the result of the following bucket policy?

Choose the correct answer
Please select:

A. It will allow all access to the bucket mybucket
B. It will allow the user mark from AWS account number 111111111 all access to the bucket but deny everyone else all access to the bucket
C. It will deny all access to the bucket mybucket
D. None of these

Answer: C

Explanation:
The policy consists of 2 statements, one is the allow for the user mark to the bucket and the next is the deny
policy for all other users. The deny permission will override the allow and hence all users will not have access to the bucket.
Options A,B and D are all invalid because this policy is used to deny all access to the bucket mybucket For examples on S3 bucket policies, please refer to the below Link: http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.htmll
The correct answer is: It will deny all access to the bucket mybucket Submit your FeedbacK/Quenes to our Experts

NEW QUESTION 243
You are designing a custom 1AM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?
A.

B.

C.

D.

A.

Answer: A

Explanation:
The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated. Option B and C are wrong since the aws:MultiFactorAuthPresent clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is true, then allow access.
Option D is invalid because the "boor clause is missing in the evaluation for the condition clause.
Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false."
Here in this scenario the boot attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.
For more information on an example on such a policy, please visit the following URL:

NEW QUESTION 245
In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an AWS Auto Scaling group, your instances are constantly being re-created. What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below
Please select:

A. Give only the necessary access to the Apache servers so that the developers can gain access to the log files.
B. Give root access to your Apache servers to the developers.
C. Give read-only access to your developers to the Apache servers.
D. Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

Answer: D

Explanation:
One important security aspect is to never give access to actual servers, hence Option A.B and C are just totally wrong from a security perspective.
The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3.
Options A,B and C are all invalid because you should not give access to the developers on the Apache se For more information on S3, please refer to the below link
https://aws.amazon.com/documentation/s3j
The correct answer is: Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.
Submit vour Feedback/Queries to our Experts

NEW QUESTION 247
You need to have a requirement to store objects in an S3 bucket with a key that is automatically managed and rotated. Which of the following can be used for this purpose?
Please select:

A. AWS KMS
B. AWS S3 Server side encryption
C. AWS Customer Keys
D. AWS Cloud HSM

Answer: B

Explanation:
The AWS Documentation mentions the following
Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
All other options are invalid since here you need to ensure the keys are manually rotated since you manage the entire key set Using AWS S3 Server side encryption, AWS will manage the rotation of keys automatically.
For more information on Server side encryption, please visit the following URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsineServerSideEncryption.htmll
The correct answer is: AWS S3 Server side encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 251
You are working in the media industry and you have created a web application where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security?
Please select:

A. Save the API credentials to your PHP files.
B. Don't save your API credentials, instead create a role in 1AM and assign this role to an EC2 instance when you first create it.
C. Save your API credentials in a public Github repository.
D. Pass API credentials to the instance using instance userdata.

Answer: B

Explanation:
Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, whil protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance. especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.
1AM roles are designed so that your applications can securely make API requests from your instances, without requiring yo manage the security credentials that the applications use.
Option A.C and D are invalid because using AWS Credentials in an application in production is a direct no recommendation 1 secure access

For more information on 1AM Roles, please visit the below URL:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html
The correct answer is: Don't save your API credentials. Instead create a role in 1AM and assign this role to an EC2 instance when you first create it
Submit your Feedback/Queries to our Experts

NEW QUESTION 252
The Development team receives an error message each time the team members attempt to encrypt or decrypt a Secure String parameter from the SSM Parameter Store by using an AWS KMS customer managed key (CMK).
Which CMK-related issues could be responsible? (Choose two.)

A. The CMK specified in the application does not exist.
B. The CMK specified in the application is currently in use.
C. The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.
D. The CMK specified in the application is not enabled.
E. The CMK specified in the application is using an alias.

Answer: AD

NEW QUESTION 254
Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?
Please select:

A. Enable VPC flow logs to know the source IP addresses
B. Monitor the S3 API calls by using Cloudtrail logging
C. Monitor the S3 API calls by using Cloudwatch logging
D. Enable AWS Inspector for the S3 bucket

Answer: B

Explanation:
The AWS Documentation mentions the following
Amazon S3 is integrated with AWS CloudTrail. CloudTrail is a service that captures specific API calls made to Amazon S3 from your AWS account and delivers the log files to an Amazon S3 bucket that you specify. It captures API calls made from the Amazon S3 console or from the Amazon S3 API.
Using the information collected by CloudTrail, you can determine what request was made to Amazon S3, the source IP address from which the request was made, who made the request when it was made, and so on Options A,C and D are invalid because these services cannot be used to get the source IP address of the calls to S3 buckets
For more information on Cloudtrail logging, please refer to the below Link: https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logeins.htmll
The correct answer is: Monitor the S3 API calls by using Cloudtrail logging Submit your Feedback/Queries to our Experts

NEW QUESTION 255
The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.
What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

A. Use AWS Certificate Manager to encrypt all traffic between the client and application servers.
B. Review the application security groups to ensure that only the necessary ports are open.
C. Use Elastic Load Balancing to offload Secure Sockets Layer encryption.
D. Use Amazon Inspector to periodically scan the backend instances.
E. Use AWS Key Management Services to encrypt all the traffic between the client and application servers.

Answer: BC

NEW QUESTION 257
A Security Engineer is setting up an AWS CloudTrail trail for all regions in an AWS account. For added security, the logs are stored using server-side encryption with AWS KMS-managed keys (SSE-KMS) and have log integrity validation enabled.
While testing the solution, the Security Engineer discovers that the digest files are readable, but the log files are not. What is the MOST likely cause?

A. The log files fail integrity validation and automatically are marked as unavailable.
B. The KMS key policy does not grant the Security Engineer's IAM user or role permissions to decrypt with it.
C. The bucket is set up to use server-side encryption with Amazon S3-managed keys (SSE-S3) as the default and does not allow SSE-KMS-encrypted files.
D. An IAM policy applicable to the Security Engineer’s IAM user or role denies access to the "CloudTrail/" prefix in the Amazon S3 bucket

Answer: B

NEW QUESTION 262
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SCS-C01 Exam with Our Prep Materials Via below:

https://www.certleader.com/SCS-C01-dumps.html