

# Amazon

## Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty



#### NEW QUESTION 1

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

- A. Change the Inbound Security Groups to deny access from the suspecting IP
- B. Change the Outbound Security Groups to deny access from the suspecting IP
- C. Change the Inbound NACL to deny access from the suspecting IP
- D. Change the Outbound NACL to deny access from the suspecting IP

**Answer: C**

#### Explanation:

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.

Option D is invalid since just changing the Inbound Rules is sufficient The AWS Documentation mentions the following

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

#### NEW QUESTION 2

You have a vendor that needs access to an AWS resource. You create an AWS user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?

Please select:

- A. An AWS Managed Policy
- B. An Inline Policy
- C. A Bucket Policy
- D. A bucket ACL

**Answer: B**

#### Explanation:

The AWS Documentation gives an example on such a case

Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that it's applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the AWS Management Console to delete that principal entity the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity.

Option A is invalid because AWS Managed Policies are ok for a group of users, but for individual users, inline policies are better.

Option C and D are invalid because they are specifically meant for access to S3 buckets For more information on policies, please visit the following URL:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/access-managed-vs-inline>

The correct answer is: An Inline Policy Submit your Feedback/Queries to our Experts

#### NEW QUESTION 3

Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution

Please select:

- A. Create a Cloudwatch Events Rule
- B. Create a Cloudwatch Logs Rule
- C. Use a Lambda function
- D. Use Cloudtrail API call

**Answer: AC**

#### Explanation:

Below is a snippet from the AWS blogs on a solution

Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL:

<https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity>

The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function Submit your Feedback/Queries to our Experts

#### NEW QUESTION 4

Your company has an EC2 Instance that is hosted in an AWS VPC. There is a requirement to ensure that log files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution

Please select:

- A. Stream the log files to a separate Cloudtrail trail
- B. Stream the log files to a separate Cloudwatch Log group
- C. Create an IAM policy that gives the desired level of access to the Cloudtrail trail
- D. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group

**Answer: BD**

#### Explanation:

You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an IAM policy. Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement

For more information on Log Groups and Log Streams, please visit the following URL:

\* <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Working>

For more information on Access to Cloudwatch logs, please visit the following URL:

\* <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html> The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 5

When you enable automatic key rotation for an existing CMK key where the backing key is managed by AWS, after how long is the key rotated?

Please select:

- A. After 30 days
- B. After 128 days
- C. After 365 days
- D. After 3 years

**Answer: D**

#### Explanation:

The AWS Documentation states the following

- AWS managed CM Ks: You cannot manage key rotation for AWS managed CMKs. AWS KMS automatically rotates AWS managed keys every three years (1095 days).

Note: AWS-managed CMKs are rotated every 3yrs, Customer-Managed CMKs are rotated every 365- days from when rotation is enabled.

Option A, B, C are invalid because the settings for automatic key rotation is not changeable. For more information on key rotation please visit the below URL

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. This CMK is unique to your AWS account and region. Only the service that created the AWS managed CMK can use it

You can login to your IAM dashboard. Click on "Encryption Keys" You will find the list based on the services you are using as follows:

- aws/elasticfilesystem 1 aws/lightail
- aws/s3
- aws/rds and many more Detailed Guide: KMS

You can recognize AWS managed CMKs because their aliases have the format aws/service-name, such as aws/redshift. Typically, a service creates its AWS managed CMK in your account when you set up the service or the first time you use the CMK

The AWS services that integrate with AWS KMS can use it in many different ways. Some services create AWS managed CMKs in your account. Other services require that you specify a customer managed CMK that you have created. And, others support both types of CMKs to allow you the ease of an AWS managed CMK or the control of a customer-managed CMK

Rotation period for CMKs is as follows:

- AWS managed CMKs: 1095 days
- Customer managed CMKs: 365 days

Since question mentions about "CMK where backing keys is managed by AWS", its Amazon(AWS) managed and its rotation period turns out to be 1095 days(every 3 years)

For more details, please check below AWS Docs: <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html> The correct answer is: After 3 years

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 6

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.html>

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 7

Your company has mandated that all calls to the AWS KMS service be recorded. How can this be achieved?

Please select:

- A. Enable logging on the KMS service
- B. Enable a trail in Cloudtrail
- C. Enable Cloudwatch logs
- D. Use Cloudwatch metrics

**Answer: B**

**Explanation:**

The AWS Documentation states the following

AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP

address from which the request was made, who made the request when it was made, and so on. Option A is invalid because logging is not possible in the KMS service

Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL <https://docs.aws.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html> The correct answer is: Enable a trail in Cloudtrail

Submit your Feedback/Queries to our Experts

**NEW QUESTION 8**

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 here.

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](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 9**

Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?

Please select:

- A. Use AWS Inspector to inspect all the security Groups
- B. Use the AWS Trusted Advisor to see which security groups have compromised access.
- C. Use AWS Config to see which security groups have compromised access.
- D. Use the AWS CLI to query the security groups and then filter for the rules which have unrestricted accessd

**Answer: B**

**Explanation:**

The AWS Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

If you go to AWS Trusted Advisor, you can see the details

Option A is invalid because AWS Inspector is used to detect security vulnerabilities in instances and not for security groups.

Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.

Option D is partially valid but would just be a maintenance overhead

For more information on the AWS Trusted Advisor, please visit the below URL: <https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices>;

The correct answer is: Use the AWS Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

**NEW QUESTION 10**

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/awsccloudtrail/latest/userguide/cloudtrail-loe-file-validationintro.html>  
For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:  
<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-receive-logs-from-multipleaccounts.html>  
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 10

Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?  
Please select:

- A. Turn on Cloud trail and carry out the penetration test
- B. Turn on VPC Flow Logs and carry out the penetration test
- C. Submit a request to AWS Support
- D. Use a custom AWS Marketplace solution for conducting the penetration test

**Answer: C**

#### Explanation:

This concept is given in the AWS Documentation  
How do I submit a penetration testing request for my AWS resources? Issue  
I want to run a penetration test or other simulated event on my AWS architecture. How do I get permission from AWS to do that?  
Resolution  
Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.  
AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.  
If your request is approved, you'll receive an authorization number.  
Option A,B and D are all invalid because the first step is to get prior authorization from AWS for penetration tests  
For more information on penetration testing, please visit the below URL  
\* <https://aws.amazon.com/security/penetration-testing/>  
\* <https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/> (  
The correct answer is: Submit a request to AWS Support Submit your Feedback/Queries to our Experts

#### NEW QUESTION 14

Your company is planning on hosting an internal network in AWS. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.  
Please select:

- A. Consider using Windows Server 2016 Certificate Manager
- B. Consider using AWS Certificate Manager
- C. Consider using AWS Access keys to generate the certificates
- D. Consider using AWS Trusted Advisor for managing the certificates

**Answer: B**

#### Explanation:

The AWS Documentation mentions the following  
ACM is tightly linked with AWS Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally. Private certificates cannot be publicly trusted  
Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", AWS Certificate Manager should be used Option C and D are invalid because these cannot be used for managing certificates.  
For more information on ACM, please visit the below URL: <https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html>  
The correct answer is: Consider using AWS Certificate Manager Submit your Feedback/Queries to our Experts

#### NEW QUESTION 19

You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.  
Please select:

- A. Use the AWS Trusted Advisor to see what can be done.
- B. Use VPC Flow logs to diagnose the traffic
- C. Use AWS WAF to analyze the traffic
- D. Use AWS Guard Duty to analyze the traffic

**Answer: B**

#### Explanation:

Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application  
Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application  
Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application  
The AWS Documentation mentions the following  
VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security tool to monitor the traffic that reaches their instances, to profile network traffic, and to look for

abnormal traffic behaviors.

For more information on AWS Security, please visit the following URL: <https://aws.amazon.com/answers/networking/vpc-security-capabilities>

The correct answer is: Use VPC Flow logs to diagnose the traffic Submit your Feedback/Queries to our Experts

#### NEW QUESTION 24

A security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure. They want to include steps to determine if the employee's 1AM permissions changed as part of the incident.

What steps should the team document in the plan? Please select:

- A. Use AWS Config to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.
- B. Use Made to examine the employee's 1AM permissions prior to the incident and compare them to the employee's A current 1AM permissions.
- C. Use CloudTrail to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.
- D. Use Trusted Advisor to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.

**Answer:** A

#### Explanation:

You can use the AWSConfig history to see the history of a particular item. The below snapshot shows an example configuration for a user in AWS Config

Option B,C and D are all invalid because these services cannot be used to see the history of a particular configuration item. This can only be accomplished by AWS Config.

For more information on tracking changes in AWS Config, please visit the below URL:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackineChanees.html> The correct answer is: Use AWS Config to examine the employee's 1AM permissions prior to the incident and compare them the employee's current 1AM permissions.

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 29

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 32

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 encryptio

**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 37

You need to ensure that objects in an S3 bucket are available in another region. This is because of the criticality of the data that is hosted in the S3 bucket. How can you achieve this in the easiest way possible?  
Please select:

- A. Enable cross region replication for the bucket
- B. Write a script to copy the objects to another bucket in the destination region
- C. Create an S3 snapshot in the destination region
- D. Enable versioning which will copy the objects to the destination region

**Answer:** A

#### Explanation:

Option B is partially correct but a big maintenance over head to create and maintain a script when the functionality is already available in S3  
Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The AWS Documentation mentions the following  
Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buck in different AWS Regions.  
For more information on Cross region replication in the Simple Storage Service, please visit the below URL:  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>  
The correct answer is: Enable cross region replication for the bucket Submit your Feedback/Queries to our Experts

#### NEW QUESTION 42

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

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 43

Every application in a company's portfolio has a separate AWS account for development and production. The security team wants to prevent the root user and all 1AM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality? Please select:

- A. Create a Service Control Policy that denies access to the service
- B. Assemble all production accounts in an organizational unit
- C. Apply the policy to that organizational unit.
- D. Create a Service Control Policy that denies access to the service
- E. Apply the policy to the root account.
- F. Create an 1AM policy that denies access to the service
- G. Associate the policy with an 1AM group and enlist all users and the root users in this group.
- H. Create an 1AM policy that denies access to the service
- I. Create a Config Rule that checks that all users have the policy m assigne
- J. Trigger a Lambda function that adds the policy when found missing.

**Answer:** A

#### Explanation:

As an administrator of the master account of an organization, you can restrict which AWS services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When AWS Organizations blocks access to a service or API action for a member account a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an 1AM policy. Organization permissions overrule account permissions. Option B is invalid because service policies cannot be assigned to the root account at the account level.  
Option C and D are invalid because 1AM policies alone at the account level would not be able to suffice the requirement  
For more information, please visit the below URL <https://docs.aws.amazon.com/IAM/latest/UserGuide/manage-attach-policy.html>  
The correct answer is: Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the



policy to that organizational unit  
Submit your Feedback/Queries to our Experts

**NEW QUESTION 44**

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 IAM 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, while 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.

IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you to 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 IAM 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 IAM and assign this role to an EC2 instance when you first create it

Submit your Feedback/Queries to our Experts

**NEW QUESTION 48**

Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances.

Which of the following would be an effective way to achieve this?

Please select:

- A. Use the AWS Systems Manager Parameter Store
- B. Use the AWS Systems Manager Run Command
- C. Use the AWS Inspector
- D. Use AWS Config

**Answer: B**

**Explanation:**

The AWS Documentation mentions the following

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

Option A is invalid because this service is used to store parameter Option C is invalid because this service is used to scan vulnerabilities in an EC2 Instance.

Option D is invalid because this service is used to check for configuration changes For more information on executing remote commands, please visit the below URL

<https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html> (

The correct answer is: Use the AWS Systems Manager Run Command Submit your Feedback/Queries to our Experts

**NEW QUESTION 49**

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

Please select:

- A. Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM 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 access 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 IAM 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-restricting-access-to-s3.html>

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 50**



Your company makes use of S3 buckets for storing data

- A. There is a company policy that all services should have logging enabled
- B. How can you ensure that logging is always enabled for created S3 buckets in the AWS Account? Please select:
- C. Use AWS Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
- D. Use AWS Config Rules to check whether logging is enabled for buckets
- E. Use AWS CloudWatch metrics to check whether logging is enabled for buckets
- F. Use AWS CloudWatch logs to check whether logging is enabled for buckets

**Answer: B**

**Explanation:**

This is given in the AWS Documentation as an example rule in AWS Config Example rules with triggers

Example rule with configuration change trigger

1. You add the AWS Config managed rule, S3\_BUCKET\_LOGGING\_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.

Option A is invalid because AWS Inspector cannot be used to scan all buckets

Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets.

For more information on Config Rules please see the below Link: <https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html>

The correct answer is: Use AWS Config Rules to check whether logging is enabled for buckets Submit your Feedback/Queries to our Experts

**NEW QUESTION 55**

A security engineer must ensure that all infrastructure launched in the company AWS account be monitored for deviation from compliance rules, specifically that all EC2 instances are launched from one of a specified list of AMIs and that all attached EBS volumes are encrypted. Infrastructure not in compliance should be terminated. What combination of steps should the Engineer implement? Select 2 answers from the options given below.

Please select:

- A. Set up a CloudWatch event based on Trusted Advisor metrics
- B. Trigger a Lambda function from a scheduled CloudWatch event that terminates non-compliant infrastructure.
- C. Set up a CloudWatch event based on Amazon Inspector findings
- D. Monitor compliance with AWS Config Rules triggered by configuration changes
- E. Trigger a CLI command from a CloudWatch event that terminates the infrastructure

**Answer: BD**

**Explanation:**

You can use AWS Config to monitor for such Event

Option A is invalid because you cannot set Cloudwatch events based on Trusted Advisor checks.

Option C is invalid Amazon Inspector cannot be used to check whether instances are launched from a specific AMI

Option E is invalid because triggering a CLI command is not the preferred option, instead you should use Lambda functions for all automation purposes.

For more information on Config Rules please see the below Link: <https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html>

These events can then trigger a lambda function to terminate instances For more information on Cloudwatch events please see the below Link:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents>.

(

The correct answers are: Trigger a Lambda function from a scheduled Cloudwatch event that terminates non-compliant infrastructure., Monitor compliance with AWS Config Rules triggered by configuration changes

Submit your Feedback/Queries to our Experts

**NEW QUESTION 58**

A company has external vendors that must deliver files to the company. These vendors have cross-account access 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 IAM role to the bucket that grants the bucket owner full permissions to the object
- B. Add a grant to the object's 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.

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-walkthroughs-managing-accessesexample3.html>

The correct answers are: Add a grant to the object's 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 60**

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

Please select:

- A. Use Bucket policies
- B. Use the Secure Token service
- C. Use IAM user policies
- D. Use AWS Access Keys

**Answer:** AC

**Explanation:**

The AWS Documentation mentions the following

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as

resource-based policies. For example, bucket policies and access control lists (ACLs) are resourcebased policies. You can also attach access policies to users in your account. These are called user

policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.

Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below

Link: <https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

The correct answers are: Use Bucket policies. Use IAM user policies Submit your Feedback/Queries to our Experts

**NEW QUESTION 63**

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.html>

The correct answers are: Amazon Cloudwatch Logs, Amazon Cloudtrail

**NEW QUESTION 68**

A company wishes to enable Single Sign On (SSO) so its employees can login to the management console using their corporate directory identity. Which steps below are required as part of the process? Select 2 answers from the options given below.

Please select:

- A. Create a Direct Connect connection between on-premise network and AW
- B. Use an AD connector for connecting AWS with on-premise active directory.
- C. Create IAM policies that can be mapped to group memberships in the corporate directory.
- D. Create a Lambda function to assign IAM roles to the temporary security tokens provided to the users.
- E. Create IAM users that can be mapped to the employees' corporate identities
- F. Create an IAM role that establishes a trust relationship between IAM and the corporate directory identity provider (IdP)

**Answer:** AE

**Explanation:**

Create a Direct Connect connection so that corporate users can access the AWS account

Option B is incorrect because IAM policies are not directly mapped to group memberships in the corporate directory. It is IAM roles which are mapped.

Option C is incorrect because Lambda functions is an incorrect option to assign roles.

Option D is incorrect because IAM users are not directly mapped to employees' corporate identities. For more information on Direct Connect, please refer to below URL:

' <https://aws.amazon.com/directconnect/>

From the AWS Documentation, for federated access, you also need to ensure the right policy permissions are in place

Configure permissions in AWS for your federated users

The next step is to create an IAM role that establishes a trust relationship between IAM and your organization's IdP that identifies your IdP as a principal (trusted entity) for purposes of federation. The role also defines what users authenticated your organization's IdP are allowed to do in AWS. You can use the IAM console to create this role. When you create the trust policy that indicates who can assume the role, you specify the SAML provider that you created earlier in IAM along with one or more SAML attributes that a user must match to be allowed to assume the role. For example, you can

specify that only users whose SAML eduPersonOrgDN value is ExampleOrg are allowed to sign in. The role wizard automatically adds a condition to test the saml:aud attribute to make sure that the role is assumed only for sign-in to the AWS Management Console. The trust policy for the role might look like this:

For more information on SAML federation, please refer to below URL: [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_enable](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable) Note:

What directories can I use with AWS SSO?

You can connect AWS SSO to Microsoft Active Directory, running either on-premises or in the AWS Cloud. AWS SSO supports AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, and AD Connector. AWS SSO does not support Simple AD. See AWS Directory Service Getting Started to learn more.

To connect to your on-premises directory with AD Connector, you need the following: VPC

Set up a VPC with the following:

- At least two subnets. Each of the subnets must be in a different Availability Zone.
- The VPC must be connected to your on-premises network through a virtual private network (VPN) connection or AWS Direct Connect.
- The VPC must have default hardware tenancy.
- <https://aws.amazon.com/single-sign-on/>
- <https://aws.amazon.com/single-sign-on/faqs/>
- <https://aws.amazon.com/bloj/using-corporate-credentials/>
- <https://docs.aws.amazon.com/directoryservice/latest/admin->

The correct answers are: Create a Direct Connect connection between on-premise network and AWS. Use an AD connector connecting AWS with on-premise active directory.. Create an 1AM role that establishes a trust relationship between 1AM and corporate directory identity provider (IdP)

Submit your Feedback/Queries to our Experts

### NEW QUESTION 73

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

Please select:

- A. Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.
- B. Configure the CMK to rotate the key material every month.
- C. Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK, updates the S3 bucket to use the new CMK, and deletes the old CMK.
- D. Trigger a Lambda function with a monthly CloudWatch event that rotates the key material in the CMK.

**Answer:** A

#### Explanation:

You can use a Lambda function to create a new key and then update the S3 bucket to use the new key. Remember not to delete the old key, else you will not be able to decrypt the documents stored in the S3 bucket using the older key.

Option B is incorrect because AWS KMS cannot rotate keys on a monthly basis

Option C is incorrect because deleting the old key means that you cannot access the older objects Option D is incorrect because rotating key material is not possible.

For more information on AWS KMS keys, please refer to below URL: <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html>

The correct answer is: Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.

Submit your Feedback/Queries to our Experts

### NEW QUESTION 78

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 recommended" 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.com/inspector/latest/userguide/inspector\\_runtime-behavioranalysis.html#insecure-protocols](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_runtime-behavioranalysis.html#insecure-protocols)

(

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 81

How can you ensure that instance in an VPC does not use AWS DNS for routing DNS requests. You want to use your own managed DNS instance. How can this be achieved?

Please select:

- A. Change the existing DHCP options set
- B. Create a new DHCP options set and replace the existing one.
- C. Change the route table for the VPC
- D. Change the subnet configuration to allow DNS requests from the new DNS Server

**Answer:** B

#### Explanation:

In order to use your own DNS server, you need to ensure that you create a new custom DHCP options set with the IP of the custom DNS server. You cannot modify the existing set, so you need to create a new one.

Option A is invalid because you cannot make changes to an existing DHCP options Set.

Option C is invalid because this can only be used to work with Routes and not with a custom DNS solution.

Option D is invalid because this needs to be done at the VPC level and not at the Subnet level For more information on DHCP options set, please visit the



following url <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC DHCP Options.html>

The correct answer is: Create a new DHCP options set and replace the existing one. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 85

A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working. What is the other step that needs to be followed to ensure that the AD domain join can work as intended

Please select:

- A. Change the VPC peering connection to a VPN connection
- B. Change the VPC peering connection to a Direct Connect connection
- C. Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets
- D. Ensure that the AD is placed in a public subnet

**Answer:** C

#### Explanation:

In addition to VPC peering and setting the right route tables, the security groups for the AD EC2 instance needs to ensure the right rules are put in place for allowing incoming traffic.

Option A and B is invalid because changing the connection type will not help. This is a problem with the Security Groups.

Option D is invalid since the AD should not be placed in a public subnet

For more information on allowing ingress traffic for AD, please visit the following url

[|https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html|](https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html)

The correct answer is: Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets Submit your Feedback/Queries to our Experts

#### NEW QUESTION 86

You need to have a cloud security device which would allow to generate encryption keys based on FIPS 140-2 Level 3. Which of the following can be used for this purpose.

Please select:

- A. AWS KMS
- B. AWS Customer Keys
- C. AWS managed keys
- D. AWS Cloud HSM

**Answer:** AD

#### Explanation:

AWS Key Management Service (KMS) now uses FIPS 140-2 validated hardware security modules (HSM) and supports FIPS 140-2 validated endpoints, which provide independent assurances about the confidentiality and integrity of your keys.

All master keys in AWS KMS regardless of their creation date or origin are automatically protected using FIPS 140-2 validated

HSMs. defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

- FIPS 140-2 Level 1 the lowest, imposes very limited requirements; loosely, all components must be "production-grade" and various egregious kinds of insecurity must be absent
- FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
- FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
- FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks.

AWS CloudHSM provides you with a FIPS 140-2 Level 3 validated single-tenant HSM cluster in your Amazon Virtual Private Cloud (VPC) to store and use your keys. You have exclusive control over how your keys are used via an authentication mechanism independent from AWS. You interact with keys in your AWS CloudHSM cluster similar to the way you interact with your applications running in Amazon EC2.

AWS KMS allows you to create and control the encryption keys used by your applications and supported AWS services in multiple regions around the world from a single console. The service uses a FIPS 140-2 validated HSM to protect the security of your keys. Centralized management of all your keys in AWS KMS lets you enforce who can use your keys under which conditions, when they get rotated, and who can manage them.

AWS KMS HSMs are validated at level 2 overall and at level 3 in the following areas:

- Cryptographic Module Specification
- Roles, Services, and Authentication
- Physical Security
- Design Assurance

So I think that we can have 2 answers for this question. Both A & D.

- <https://aws.amazon.com/blogs/security/aws-key-management-service-now-offers-fips-140-2-validated-cryptographic-modules-enabling-easier-adoption-of-the-service-for-regulated-workloads/>
- <https://aws.amazon.com/cloudhsm/faqs/>
- <https://aws.amazon.com/kms/faqs/>
- <https://en.wikipedia.org/wiki/RPS>

The AWS Documentation mentions the following

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java

Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries. CloudHSM is also standards-compliant and enables you to export all of your keys to most other commercially-available HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups. CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs.

All other options are invalid since AWS Cloud HSM is the prime service that offers FIPS 140-2 Level 3 compliance

For more information on CloudHSM, please visit the following url <https://aws.amazon.com/cloudhsm/>;

The correct answers are: AWS KMS, AWS Cloud HSM Submit your Feedback/Queries to our Experts

#### NEW QUESTION 91

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/UsingServerSideEncryption.html>

The correct answer is: AWS S3 Server side encryption Submit your Feedback/Queries to our Experts

**NEW QUESTION 92**

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}}
- 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 Amazon S3 resources.

You can enforce the MFA authentication requirement using the aws:MultiFactorAuthAge key in a bucket policy. IAM users can 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 IAM User Guide.

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 97**

You need to inspect the running processes on an EC2 Instance that may have a security issue. How can you achieve this in the easiest way possible. Also you need to ensure that the process does not interfere with the continuous running of the instance.

Please select:

- A. Use AWS Cloudtrail to record the processes running on the server to an S3 bucket.
- B. Use AWS Cloudwatch to record the processes running on the server
- C. Use the SSM Run command to send the list of running processes information to an S3 bucket.
- D. Use AWS Config to see the changed process information on the server

**Answer: C**

**Explanation:**

The SSM Run command can be used to send OS specific commands to an Instance. Here you can check and see the running processes on an instance and then send the output to an S3 bucket. Option A is invalid because this is used to record API activity and cannot be used to record running processes.

Option B is invalid because Cloudwatch is a logging and metric service and cannot be used to record running processes.

Option D is invalid because AWS Config is a configuration service and cannot be used to record running processes.

For more information on the Systems Manager Run command, please visit the following URL: [https://docs.aws.amazon.com/systems-](https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html)

[manaEer/latest/useruide/execute-remote-commands.html](https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html) The correct answer is: Use the SSM Run command to send the list of running processes information to an S3 bucket. Submit your Feedback/Queries to our Experts

**NEW QUESTION 98**

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 AP

**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 (IAM) 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 IAM 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-remotecommands.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 99**

You are trying to use the AWS Systems Manager run command on a set of Instances. The run command on a set of Instances. What can you do to diagnose the issue? Choose 2 answers from the options given

Please select:

- A. Ensure that the SSM agent is running on the target machine
- B. Check the /var/log/amazon/ssm/errors.log file
- C. Ensure the right AMI is used for the Instance
- D. Ensure the security groups allow outbound communication for the instance

**Answer:** AB

**Explanation:**

The AWS Documentation mentions the following

If you experience problems executing commands using Run Command, there might be a problem with the SSM Agent. Use the following information to help you troubleshoot the agent

View Agent Logs

The SSM Agent logs information in the following files. The information in these files can help you troubleshoot problems.

On Windows

%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log

%PROGRAMDATA%\Amazon\SSM\Logs\error.log

The default filename of the seelog is seelog-xml.template. If you modify a seelog, you must rename the file to seelog.xml.

On Linux

/var/log/amazon/ssm/amazon-ssm-agentlog /var/log/amazon/ssm/errors.log

Option C is invalid because the right AMI has nothing to do with the issues. The agent which is used to execute run commands can run on a variety of AMI'S

Option D is invalid because security groups does not come into the picture with the communication between the agent and the SSM service

For more information on troubleshooting AWS SSM, please visit the following URL: <https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-remotecommands.html>

The correct answers are: Ensure that the SSM agent is running on the target machine. Check the

/var/log/amazon/ssm/errors.log file

Submit your Feedback/Queries to our Experts

**NEW QUESTION 102**

You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between AWS and their On-premise Active Directory. Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below.

Please select:

- A. Ensure the right match is in place for On-premise AD Groups and IAM Roles.
- B. Ensure the right match is in place for On-premise AD Groups and IAM Groups.
- C. Configure AWS as the relying party in Active Directory
- D. Configure AWS as the relying party in Active Directory Federation services

**Answer:** AD

**Explanation:**

The AWS Documentation mentions some key aspects with regards to the configuration of Onpremise AD with AWS

One is the Groups configuration in AD Active Directory Configuration

Determining how you will create and delineate your AD groups and IAM roles in AWS is crucial to how you secure access to your account and manage resources.

SAML assertions to the AWS environment and the respective IAM role access will be managed through regular expression (regex) matching between your on-premises AD group name to an AWS IAM role.

One approach for creating the AD groups that uniquely identify the AWS IAM role mapping is by selecting a common group naming convention. For example, your AD groups would start with an identifier, for example, AWS-, as this will distinguish your AWS groups from others within the organization. Next include the 12-digit AWS account number. Finally, add the matching role name within the AWS account. Here is an example:

And next is the configuration of the relying party which is AWS

ADFS federation occurs with the participation of two parties; the identity or claims provider (in this case the owner of the identity repository - Active Directory) and the relying party, which is another application that wishes to outsource authentication to the identity provider; in this case Amazon Secure Token Service (STS).

The relying party is a federation partner that is represented by a claims provider trust in the federation service.

Option B is invalid because AD groups should not be matched to 1AM Groups

Option C is invalid because the relying party should be configured in Active Directory Federation services

For more information on the federated access, please visit the following URL:

1 <https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directoryfederation-services-ad-fs/>

The correct answers are: Ensure the right match is in place for On-premise AD Groups and 1AM Roles., Configure AWS as the relying party in Active Directory Federation services

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 106

Which technique can be used to integrate AWS 1AM (Identity and Access Management) with an on Questions & Answers PDF P-63 premise LDAP (Lightweight Directory Access Protocol) directory service? Please select:

- A. Use an 1AM policy that references the LDAP account identifiers and the AWS credentials.
- B. Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.
- C. Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.
- D. Use 1AM roles to automatically rotate the 1AM credentials when LDAP credentials are update

**Answer: B**

#### Explanation:

On the AWS Blog site the following information is present to help on this context

The newly released whitepaper. Single Sign-On: Integrating AWS, OpenLDAP, and Shibboleth, will help you integrate your existing LDAP-based user directory with AWS. When you integrate your existing directory with AWS, your users can access AWS by using their existing credentials. This means that your users don't need to maintain yet another user name and password just to access AWS resources.

Option A.C and D are all invalid because in this sort of configuration, you have to use SAML to enable single sign on.

For more information on integrating AWS with LDAP for Single Sign-On, please visit the following URL:

<https://aws.amazon.eom/blogs/security/new-whitepaper-sinEle-sign-on-inteErating-aws-openldapand-shibboleth/>

The correct answer is: Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 108

You have an EBS volume attached to an EC2 Instance which uses KMS for Encryption. Someone has now gone ahead and deleted the Customer Key which was used for the EBS encryption. What should be done to ensure the data can be decrypted.

Please select:

- A. Create a new Customer Key using KMS and attach it to the existing volume
- B. You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable.
- C. Request AWS Support to recover the key
- D. Use AWS Config to recover the key

**Answer: B**

#### Explanation:

Deleting a customer master key (CMK) in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.

<https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html>

A is incorrect because Creating a new CMK and attaching it to the exiting volume will not allow the data to be decrypted, you cannot attach customer master keys after the volume is encrypted

Option C and D are invalid because once the key has been deleted, you cannot recover it For more information on EBS Encryption with KMS, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

The correct answer is: You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 109

You have a requirement to serve up private content using the keys available with Cloudfront. How can this be achieved?

Please select:

- A. Add the keys to the backend distribution.
- B. Add the keys to the S3 bucket
- C. Create pre-signed URL's
- D. Use AWS Access keys

**Answer: C**

#### Explanation:

Option A and B are invalid because you will not add keys to either the backend distribution or the S3 bucket.

Option D is invalid because this is used for programmatic access to AWS resources

You can use Cloudfront key pairs to create a trusted pre-signed URL which can be distributed to users Specifying the AWS Accounts That Can Create Signed URLs and Signed Cookies (Trusted Signers) Topics

- Creating CloudFront Key Pairs for Your Trusted Signers
- Reformatting the CloudFront Private Key (.NET and Java Only)
- Adding Trusted Signers to Your Distribution
- Verifying that Trusted Signers Are Active (Optional) 1 Rotating CloudFront Key Pairs

To create signed URLs or signed cookies, you need at least one AWS account that has an active CloudFront key pair. This accou is known as a trusted signer.

The trusted signer has two purposes:

- As soon as you add the AWS account ID for your trusted signer to your distribution, CloudFront starts to require that users us signed URLs or signed cookies to access your objects.



' When you create signed URLs or signed cookies, you use the private key from the trusted signer's key pair to sign a portion of the URL or the cookie. When someone requests a restricted object CloudFront compares the signed portion of the URL or cookie with the unsigned portion to verify that the URL or cookie hasn't been tampered with. CloudFront also verifies that the URL or cookie is valid, meaning, for example, that the expiration date and time hasn't passed.

For more information on Cloudfront private trusted content please visit the following URL:

• <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contenttrusted-s>

The correct answer is: Create pre-signed URL's Submit your Feedback/Queries to our Experts

#### NEW QUESTION 114

You are building a system to distribute confidential training videos to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publicly accessible from S3 directly?

Please select:

- A. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- B. Add the CloudFront account security group "amazon-cf/amazon-cf-sg" to the appropriate S3 bucket policy.
- C. Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- D. Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

**Answer:** AExplanation:

#### Explanation:

You can optionally secure the content in your Amazon S3 bucket so users can access it through

CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it

To require that users access your content through CloudFront URLs, you perform the following tasks: Create a special CloudFront user called an origin access identity.

Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects.

Option B,C and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.

For more information on serving private content via Cloudfront, please visit the following URL:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket t that OAI.

You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it

To require that users access your content through CloudFront URLs, you perform the following tasks: Create a special CloudFront user called an origin access identity.

Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects.

Option B,C and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.

For more information on serving private content via Cloudfront, please visit the following URL:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket t that OAI.

Submit your Feedback/Queries to our Experts Submit your Feedback/Queries to our Experts

#### NEW QUESTION 117

A company had developed an incident response plan 18 months ago. Regular implementations of the response plan are carried out. No changes have been made to the response plan have been made since its creation. Which of the following is a right statement with regards to the plan?

Please select:

- A. It places too much emphasis on already implemented security controls.
- B. The response plan is not implemented on a regular basis
- C. The response plan does not cater to new services
- D. The response plan is complete in its entirety

**Answer:** C

#### Explanation:

So definitely the case here is that the incident response plan is not catering to newly created services. AWS keeps on changing and adding new services and hence the response plan must cater to these new services.

Option A and B are invalid because we don't know this for a fact.

Option D is invalid because we know that the response plan is not complete, because it does not cater to new features of AWS

For more information on incident response plan please visit the following URL: <https://aws.amazon.com/blogs/publicsector/buildins-a-cloud-specific-incident-response-plan>; The correct answer is: The response plan does not cater to new services Submit your Feedback/Queries to our Experts

#### NEW QUESTION 119

You have a requirement to conduct penetration testing on the AWS Cloud for a couple of EC2 Instances. How could you go about doing this? Choose 2 right answers from the options given below. Please select:

- A. Get prior approval from AWS for conducting the test
- B. Use a pre-approved penetration testing tool.
- C. Work with an AWS partner and no need for prior approval request from AWS
- D. Choose any of the AWS instance type

**Answer:** AB

#### Explanation:

You can use a pre-approved solution from the AWS Marketplace. But till date the AWS Documentation still mentions that you have to get prior approval before conducting a test on the AWS Cloud for EC2 Instances.

Option C and D are invalid because you have to get prior approval first. AWS Docs Provides following details:

"For performing a penetration test on AWS resources first of all we need to take permission from AWS and complete a requisition form and submit it for approval.



The form should contain information about the instances you wish to test identify the expected start and end dates/times of your test and requires you to read and agree to Terms and Conditions specific to penetration testing and to the use of appropriate tools for testing. Note that the end date may not be more than 90 days from the start date."

(

At this time, our policy does not permit testing small or micro RDS instance types. Testing of ml

.small, t1 .micro or t2.nano EC2 instance types is not permitted.

For more information on penetration testing please visit the following URL: <https://aws.amazon.com/security/penetration-testing/>

The correct answers are: Get prior approval from AWS for conducting the test Use a pre-approved penetration testing tool. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 120

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 IAM 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 IAM 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 IAM or bucket policy

Option D is invalid because keys for IAM 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/developerguide/policy-conditions.html>

The correct answer is: Use the kms:ViaService condition in the Key policy Submit your Feedback/Queries to our Experts

#### NEW QUESTION 124

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 IAM policy
- C. You have not given access via the IAM roles
- D. You have not explicitly given access via IAM 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 explicitly 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.amazon.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 126

You are planning on hosting a web application on AWS. You create an EC2 Instance in a public subnet. This instance needs to connect to an EC2 Instance that will host an Oracle database. Which of the following steps should be followed to ensure a secure setup is in place? Select 2 answers.

Please select:

- A. Place the EC2 Instance with the Oracle database in the same public subnet as the Web server for faster communication
- B. Place the EC2 Instance with the Oracle database in a separate private subnet
- C. Create a database security group and ensure the web security group to allowed incoming access
- D. Ensure the database security group allows incoming traffic from 0.0.0.0/0

**Answer: BC**

#### Explanation:

The best secure option is to place the database in a private subnet. The below diagram from the AWS Documentation shows this setup. Also ensure that access is not allowed from all sources but just from the web servers.

Option A is invalid because databases should not be placed in the public subnet

Option D is invalid because the database security group should not allow traffic from the internet For more information on this type of setup, please refer to the below URL: [https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/PC\\_Scenario2.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/PC_Scenario2.html)

The correct answers are: Place the EC2 Instance with the Oracle database in a separate private subnet Create a database security group and ensure the web security group to allowed incoming access

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 127

An application running on EC2 instances processes sensitive information stored on Amazon S3. The information is accessed over the Internet. The security team is concerned that the Internet connectivity to Amazon S3 is a security risk. Which solution will resolve the security concern? Please select:

- A. Access the data through an Internet Gateway.
- B. Access the data through a VPN connection.
- C. Access the data through a NAT Gateway.
- D. Access the data through a VPC endpoint for Amazon S3

**Answer:** D

**Explanation:**

The AWS Documentation mentions the followii

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Option A,B and C are all invalid because the question specifically mentions that access should not be provided via the Internet

For more information on VPC endpoints, please refer to the below URL:

The correct answer is: Access the data through a VPC endpoint for Amazon S3

**NEW QUESTION 130**

A company is using a Redshift cluster to store their data warehouse. There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database. How can this be achieved?

Please select:

- A. Encrypt the EBS volumes of the underlying EC2 Instances
- B. Use AWS KMS Customer Default master key
- C. Use SSL/TLS for encrypting the data
- D. Use S3 Encryption

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following

Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either AWS Key Management Servic (AWS KMS) or a hardware security module (HSM) to manage the toplevel encryption keys in this hierarchy. The process that Amazon Redshift uses for encryption differs depending on how you manage keys.

Option A is invalid because its the cluster that needs to be encrypted

Option C is invalid because this encrypts objects in transit and not objects at rest Option D is invalid because this is used only for objects in S3 buckets

For more information on Redshift encryption, please visit the following URL: <https://docs.aws.amazon.com/redshift/latest/memt/workine-with-db-encryption.html>

The correct answer is: Use AWS KMS Customer Default master key Submit your Feedback/Queries to our Experts

**NEW QUESTION 135**

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 region

**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/2015/12/turn-on-cloudtrail-across-all-reeions-andsupport- for-multiple-trails>

The correct answer is: Ensure one Cloudtrail trail is enabled for all regions. Submit your Feedback/Queries to our Experts

**NEW QUESTION 137**

A company is planning to run a number of Admin related scripts using the AWS Lambda service. There is a need to understand if there are any errors encountered when the script run. How can this be accomplished in the most effective manner.

Please select:

- A. Use Cloudwatch metrics and logs to watch for errors
- B. Use Cloudtrail to monitor for errors
- C. Use the AWS Config service to monitor for errors
- D. Use the AWS inspector service to monitor for errors

**Answer:** A

**Explanation:**

The AWS Documentation mentions the following

AWS Lambda automatically monitors Lambda functions on your behalf, reporting metrics through Amazon CloudWatch. To help you troubleshoot failures in a function. Lambda logs all requests handled by your function and also automatically stores logs generated by your code through Amazon CloudWatch Logs.

Option B,C and D are all invalid because these services cannot be used to monitor for errors. I

For more information on Monitoring Lambda functions, please visit the following URL: <https://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-logs.html>

The correct answer is: Use Cloudwatch metrics and logs to watch for errors Submit your Feedback/Queries to our Experts

**NEW QUESTION 139**

A company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to encrypt at rest. How can this be achieved? Please select:

- A. Use AWS Access keys to encrypt the data
- B. Use SSL certificates to encrypt the data
- C. Enable server side encryption on the S3 bucket
- D. Enable MFA on the S3 bucket

**Answer:** C

**Explanation:**

The AWS Documentation mentions the following

Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects.

Options A and B are invalid because neither Access Keys nor SSL certificates can be used to encrypt data.

Option D is invalid because MFA is just used as an extra level of security for S3 buckets For more information on S3 server side encryption, please refer to the below Link: <https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

Submit your Feedback/Queries to our Experts

**NEW QUESTION 142**

Your company has a requirement to work with a DynamoDB table. There is a security mandate that all data should be encrypted at rest. What is the easiest way to accomplish this for DynamoDB. Please select:

- A. Use the AWS SDK to encrypt the data before sending it to the DynamoDB table
- B. Encrypt the DynamoDB table using KMS during its creation
- C. Encrypt the table using AWS KMS after it is created
- D. Use S3 buckets to encrypt the data before sending it to DynamoDB

**Answer:** B

**Explanation:**

The most easiest option is to enable encryption when the DynamoDB table is created. The AWS Documentation mentions the following

Amazon DynamoDB offers fully managed encryption at rest. DynamoDB encryption at rest provides enhanced security by encrypting your data at rest using an AWS Key Management Service (AWS KMS) managed encryption key for DynamoDB. This functionality eliminates the operational burden and complexity involved in protecting sensitive data.

Option A is partially correct, you can use the AWS SDK to encrypt the data, but the easier option would be to encrypt the table before hand.

Option C is invalid because you cannot encrypt the table after it is created

Option D is invalid because encryption for S3 buckets is for the objects in S3 only.

For more information on securing data at rest for DynamoDB please refer to below URL:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.html> The correct answer is: Encrypt the DynamoDB table using KMS during its creation Submit your Feedback/Queries to our Experts

**NEW QUESTION 144**

One of your company's EC2 Instances have been compromised. The company has strict thorough investigation on finding the culprit for the security breach. What would you do in from the options given below.

Please select:

- A. Take a snapshot of the EBS volume
- B. Isolate the machine from the network
- C. Make sure that logs are stored securely for auditing and troubleshooting purpose
- D. Ensure all passwords for all IAM users are changed
- E. Ensure that all access keys are rotate

**Answer:** ABC

**Explanation:**

Some of the important aspects in such a situation are

1) First isolate the instance so that no further security harm can occur on other AWS resources

2) Take a snapshot of the EBS volume for further investigation. This is incase if you need to shutdown the initial instance and do a separate investigation on the data

3) Next is Option C. This indicates that we have already got logs and we need to make sure that it is stored securely so that n unauthorised person can access it and manipulate it.

Option D and E are invalid because they could have adverse effects for the other IAM users. For more information on adopting a security framework, please refer to below URL [https://d1.awsstatic.com/whitepapers/compliance/NIST Cybersecurity Framework](https://d1.awsstatic.com/whitepapers/compliance/NIST%20Cybersecurity%20Framework.pdf)

Note:

In the question we have been asked to take actions to find the culprit and to help the investigation or to further reduce the damage that has happened due to the security breach. So by keeping logs secure is one way of helping the investigation.

The correct answers are: Take a snapshot of the EBS volume. Isolate the machine from the network. Make sure that logs are stored securely for auditing and troubleshooting purpose

Submit your Feedback/Queries to our Experts

**NEW QUESTION 145**

Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol.



There is a security mandate that all traffic between the client and the EC2 Instances need to be secure. How would you accomplish this? Please select:

- A. Use an Application Load balancer and terminate the SSL connection at the ELB
- B. Use a Classic Load balancer and terminate the SSL connection at the ELB
- C. Use an Application Load balancer and terminate the SSL connection at the EC2 Instances
- D. Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

**Answer:** D

**Explanation:**

Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic needs to be secure till the EC2 Instances, the SSL termination should occur on the EC2 Instances. Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application.

Option B is incorrect since encryption is required until the EC2 Instance

For more information on HTTPS listeners for classic load balancers, please refer to below URL

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.html> The correct answer is: Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

Submit your Feedback/Queries to our Experts

**NEW QUESTION 148**

Your company use AWS KMS for management of its customer keys. From time to time, there is a requirement to delete existing keys as part of housekeeping activities. What can be done during the deletion process to verify that the key is no longer being used.

Please select:

- A. Use CloudTrail to see if any KMS API request has been issued against existing keys
- B. Use Key policies to see the access level for the keys
- C. Rotate the keys once before deletion to see if other services are using the keys
- D. Change the IAM policy for the keys to see if other services are using the keys

**Answer:** A

**Explanation:**

The AWS documentation mentions the following

You can use a combination of AWS CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an alarm that notifies you of AWS KMS API requests that attempt to use a customer master key (CMK) that is pending deletion. If you receive a notification from such an alarm, you might want to cancel deletion of the CMK to give yourself more time to determine whether you want to delete it

Options B and D are incorrect because Key policies nor IAM policies can be used to check if the keys are being used.

Option C is incorrect since rotation will not help you check if the keys are being used. For more information on deleting keys, please refer to below URL:

<https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-creating-cloudwatchalarm.html>

The correct answer is: Use CloudTrail to see if any KMS API request has been issued against existing keys Submit your Feedback/Queries to our Experts

**NEW QUESTION 153**

You have a bucket and a VPC defined in AWS. You need to ensure that the bucket can only be accessed by the VPC endpoint. How can you accomplish this? Please select:

- A. Modify the security groups for the VPC to allow access to the S3 bucket
- B. Modify the route tables to allow access for the VPC endpoint
- C. Modify the IAM Policy for the bucket to allow access for the VPC endpoint
- D. Modify the bucket Policy for the bucket to allow access for the VPC endpoint

**Answer:** D

**Explanation:**

This is mentioned in the AWS Documentation Restricting Access to a Specific VPC Endpoint

The following is an example of an S3 bucket policy that restricts access to a specific bucket, examplebucket only from the VPC endpoint with the ID vpce-1a2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The aws:sourceVpce condition is used to specify the endpoint. The aws:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

Options A and B are incorrect because using Security Groups nor route tables will help to allow access specifically for that bucket via the VPC endpoint. Here you specifically need to ensure the bucket policy is changed.

Option C is incorrect because it is the bucket policy that needs to be changed and not the IAM policy. For more information on example bucket policies for VPC endpoints, please refer to below URL: <https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html>

The correct answer is: Modify the bucket Policy for the bucket to allow access for the VPC endpoint Submit your Feedback/Queries to our Experts

**NEW QUESTION 156**

In order to encrypt data in transit for a connection to an AWS RDS instance, which of the following would you implement? Please select:

- A. Transparent data encryption
- B. SSL from your application
- C. Data keys from AWS KMS
- D. Data Keys from CloudHSM

**Answer:** B

**Explanation:**

This is mentioned in the AWS Documentation

You can use SSL from your application to encrypt a connection to a DB instance running MySQL MariaDB, Amazon Aurora, SQL Server, Oracle, or PostgreSQL.



Option A is incorrect since Transparent data encryption is used for data at rest and not in transit Options C and D are incorrect since keys can be used for encryption of data at rest

For more information on working with RDS and SSL, please refer to below URL:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html>

The correct answer is: SSL from your application Submit your Feedback/Queries to our Experts

#### NEW QUESTION 157

A Devops team is currently looking at the security aspect of their CI/CD pipeline. They are making use of AWS resource? for their infrastructure. They want to ensure that the EC2 Instances don't have any high security vulnerabilities. They want to ensure a complete DevSecOps process. How can this be achieved? Please select:

- A. Use AWS Config to check the state of the EC2 instance for any sort of security issues.
- B. Use AWS Inspector API's in the pipeline for the EC2 Instances
- C. Use AWS Trusted Advisor API's in the pipeline for the EC2 Instances
- D. Use AWS Security Groups to ensure no vulnerabilities are present

**Answer:** B

#### Explanation:

Amazon Inspector offers a programmatic way to find security defects or misconfigurations in your operating systems and applications. Because you can use API calls to access both the processing of assessments and the results of your assessments, integration of the findings into workflow and notification systems is simple. DevOps teams can integrate Amazon Inspector into their CI/CD pipelines and use it to identify any pre-existing issues or when new issues are introduced. Option A.C and D are all incorrect since these services cannot check for Security Vulnerabilities. These can only be checked by the AWS Inspector service.

For more information on AWS Security best practices, please refer to below URL: [https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdf](https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf)

The correct answer is: Use AWS Inspector API's in the pipeline for the EC2 Instances Submit your Feedback/Queries to our Experts

#### NEW QUESTION 160

You need to create a Linux EC2 instance in AWS. Which of the following steps is used to ensure secure authentication the EC2 instance from a windows machine. Choose 2 answers from the options given below.

Please select:

- A. Ensure to create a strong password for logging into the EC2 Instance
- B. Create a key pair using putty
- C. Use the private key to log into the instance
- D. Ensure the password is passed securely using SSL

**Answer:** BC

#### Explanation:

The AWS Documentation mentions the following

You can use Amazon EC2 to create your key pair. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt login information, so it's important that you store your private keys in a secure place.

Options A and D are incorrect since you should use key pairs for secure access to Ec2 Instances For more information on EC2 key pairs, please refer to below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

The correct answers are: Create a key pair using putty. Use the private key to log into the instance Submit your Feedback/Queries to our Experts

#### NEW QUESTION 162

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.html> 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 164

Your company has a hybrid environment, with on-premise servers and servers hosted in the AWS cloud. They are planning to use the Systems Manager for patching servers. Which of the following is a pre-requisite for this to work;

Please select:

- A. Ensure that the on-premise servers are running on Hyper-V.
- B. Ensure that an IAM service role is created
- C. Ensure that an IAM User is created
- D. Ensure that an IAM Group is created for the on-premise servers

**Answer:** B

**Explanation:**

You need to ensure that an IAM service role is created for allowing the on-premise servers to communicate with the AWS Systems Manager.

Option A is incorrect since it is not necessary that servers should only be running Hyper-V Options C and D are incorrect since it is not necessary that IAM users and groups are created For more information on the Systems Manager role please refer to the below URL:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-iam.html>

The correct answer is: Ensure that an IAM service role is created Submit your Feedback/Queries to our Experts

**NEW QUESTION 167**

An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below

Please select:

- A. Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag.
- B. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance call.
- C. Modify the IAM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
- D. Modify the IAM policy on the user to require MFA before deleting EC2 instances

**Answer:** AB

**Explanation:**

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define

Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance.

For more information on tagging answer resources please refer to the below URL: [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_Tags.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html)

The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance

Submit your Feedback/Queries to our Experts

**NEW QUESTION 171**

A company has been using the AWS KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below

Please select:

- A. Determine the age of the master key
- B. See who is assigned permissions to the master key
- C. See CloudTrail for usage of the key
- D. Use AWS CloudWatch events for events generated for the key

**Answer:** BC

**Explanation:**

The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs

Option A is invalid because seeing how long ago the key was created would not determine the usage of the key

Option D is invalid because CloudTrail Event is better for seeing for events generated by the key This is also mentioned in the AWS Documentation

Examining CMK Permissions to Determine the Scope of Potential Usage

Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an AWS KMS Customer Master Key.

Examining AWS CloudTrail Logs to Determine Actual Usage

AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is

located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it

For more information on determining the usage of CMK keys, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html>

The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key Submit your Feedback/Queries to our Experts

**NEW QUESTION 175**

A company wants to use Cloudtrail for logging all API activity. They want to segregate the logging of data events and management events. How can this be achieved? Choose 2 answers from the options given below

Please select:

- A. Create one Cloudtrail log group for data events
- B. Create one trail that logs data events to an S3 bucket
- C. Create another trail that logs management events to another S3 bucket
- D. Create another Cloudtrail log group for management events

**Answer:** BC

**Explanation:**

The AWS Documentation mentions the following

You can configure multiple trails differently so that the trails process and log only the events that you specify. For example, one trail can log read-only data and management events, so that all read-only events are delivered to one S3 bucket. Another trail can log only write-only data and management events, so that all write-only events are delivered to a separate S3 bucket

Options A and D are invalid because you have to create a trail and not a log group

For more information on managing events with cloudtrail, please visit the following URL:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/loHEing-manasement-and-dataevents- with-cloudtrai>

The correct answers are: Create one trail that logs data events to an S3 bucket. Create another trail that logs management events to another S3 bucket

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 176

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 IAM user in the company account
- B. Create an IAM Role in the company account
- C. Ensure the IAM user has access for read-only to the S3 buckets
- D. Ensure the IAM 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 IAM role for each account that you want to share log files with.

For each of these IAM roles, create an access policy that grants read-only access to the account you want to share the log files with.

Have an IAM user in each account programmatically assume the appropriate role and retrieve the log files.

Options A and C are invalid because creating an IAM user and then sharing the IAM 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-share-logs.html>

The correct answers are: Create an IAM Role in the company account Ensure the IAM Role has access for read-only to the S3 buckets

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 177

Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following

Whether any ports are left open other than admin ones like SSH and RDP

Whether any ports to the database server other than ones from the web server security group are

open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?

Please select:

- A. AWS Config
- B. AWS Trusted Advisor
- C. AWS Inspector D. AWS GuardDuty

**Answer: B**

#### Explanation:

Trusted Advisor checks for compliance with the following security recommendations:

Limited access to common administrative ports to only a small subset of addresses. This includes ports 22 (SSH), 23 (Telnet) 3389 (RDP), and 5500 (VNC).

Limited access to common database ports. This includes ports 1433 (Microsoft SQL Server), 1434 (Microsoft SQL Monitor), 3306 (MySQL), Oracle (1521) and 5432 (PostgreSQL).

Option A is partially correct but then you would need to write custom rules for this. The AWS trusted advisor can give you all of these checks on its dashboard

Option C is incorrect. Amazon Inspector needs a software agent to be installed on all EC2 instances that are included in the

assessment target, the security of which you want to evaluate with Amazon Inspector. It monitors the behavior of the EC2

instance on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and

configuration data (telemetry), which it then passes to the Amazon Inspector service.

Our question's requirement is to choose a choice that is easy to implement. Hence Trusted Advisor is more appropriate for this question.

Options D is invalid because this service doesn't provide these details.

For more information on the Trusted Advisor, please visit the following URL <https://aws.amazon.com/premiumsupport/trustedadvisor>

The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

#### NEW QUESTION 182

An application is designed to run on an EC2 Instance. The application 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 IAM user to the application that has specific access to only that S3 bucket
- C. Assign an IAM Role and assign it to the EC2 Instance
- D. Assign an IAM group and assign it to the EC2 Instance

**Answer: C**

#### Explanation:

The below diagram from the AWS whitepaper shows the best security practice of allocating a role that has access to the S3 bucket

Options A, B and D are invalid because using users, groups or access keys is an invalid security practice 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.pdf](https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf)

The correct answer is: Assign an IAM Role and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

#### NEW QUESTION 185

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 can 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 189

You are planning to use AWS Config to check the configuration of the resources in your AWS account. You are planning on using an existing IAM 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:

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 IAM role permissions please visit the below Link: <https://docs.aws.amazon.com/config/latest/developerguide/iamrole-permissions.html>

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 194

Your developer is using the KMS service and an assigned key in their Java program. They get the below error when running the code

arn:aws:iam::113745388712:user/UserB is not authorized to perform: kms:DescribeKey Which of the following could help resolve the issue?

Please select:

- A. Ensure that UserB is given the right IAM role to access the key
- B. Ensure that UserB is given the right permissions in the IAM policy
- C. Ensure that UserB is given the right permissions in the Key policy
- D. Ensure that UserB is given the right permissions in the Bucket policy

**Answer:** C

#### Explanation:

You need to ensure that UserB is given access via the Key policy for the Key

Option is invalid because you don't assign roles to IAM users For more information on Key policies please visit the below Link:

<https://docs.aws.amazon.com/kms/latest/developerguide/key-poli>

The correct answer is: Ensure that UserB is given the right permissions in the Key policy

#### NEW QUESTION 197

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### AWS-Certified-Security-Specialty Practice Exam Features:

- \* AWS-Certified-Security-Specialty Questions and Answers Updated Frequently
- \* AWS-Certified-Security-Specialty Practice Questions Verified by Expert Senior Certified Staff
- \* AWS-Certified-Security-Specialty Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* AWS-Certified-Security-Specialty Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The AWS-Certified-Security-Specialty Practice Test Here](#)**