

## AWS-Certified-Security-Specialty Dumps

### Amazon AWS Certified Security - Specialty

<https://www.certleader.com/AWS-Certified-Security-Specialty-dumps.html>



**NEW QUESTION 1**

You are hosting a web site via website hosting on an S3 bucket - <http://demo.s3-website-us-east-1.amazonaws.com>. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages, they are getting a blocked Javascript error. How can you rectify this? Please select:

- A. Enable CORS for the bucket
- B. Enable versioning for the bucket
- C. Enable MFA for the bucket
- D. Enable CRR for the bucket

**Answer:** A

**Explanation:**

Your answer is incorrect Answer-A

Such a scenario is also given in the AWS Documentation Cross-Origin Resource Sharing:

Use-case Scenarios

The following are example scenarios for using CORS:

- Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint <http://website.s3-website-us-east-1.amazonaws.com>. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket [website.s3.amazonaws.com](http://website.s3.amazonaws.com). A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from [website.s3-website-us-east-1.amazonaws.com](http://website.s3-website-us-east-1.amazonaws.com).
- Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.

Option B is invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objects

Option C is invalid because this is used as an extra measure of caution for deletion of objects Option D is invalid because this is used for Cross region replication of objects

For more information on Cross Origin Resource sharing, please visit the following URL

- <https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html>

The correct answer is: Enable CORS for the bucket

Submit your Feedback/Queries to our Experts

**NEW QUESTION 2**

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

Please select:

- A. Port 443 coming from 0.0.0.0/0
- B. Port 443 coming from 10.0.0.0/16
- C. Port 22 coming from 0.0.0.0/0
- D. Port 22 coming from 203.0.113.1/32

**Answer:** AD

**Explanation:**

Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.

Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet

Option C is invalid because allowing port 22 from the internet is a security risk For more information on AWS Security Groups, please visit the following UR

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>

The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

**NEW QUESTION 3**

You have an Ec2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective

Please select:

- A. Use a VPC endpoint
- B. Attach an Internet gateway to the subnet
- C. Attach a VPN connection to the VPC
- D. Use VPC Peering

**Answer:** A

**Explanation:**

The AWS Documentation mentions the following

You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and AWS KMS is conducted entirely within the AWS network.

Option B is invalid because this could open threats from the internet

Option C is invalid because this is normally used for communication between on-premise environments and AWS.

Option D is invalid because this is normally used for communication between VPCs

For more information on accessing KMS via an endpoint, please visit the following URL <https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html>

The correct answer is: Use a VPC endpoint Submit your Feedback/Queries to our Experts

**NEW QUESTION 4**

You are devising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy

But when you try to apply the policy you get the error "Action does not apply to any resource(s) in statement." What should be done to rectify the error Please select:

- A. Change the IAM permissions by applying PutBucketPolicy permissions.
- B. Verify that the policy has the same name as the bucket name
- C. If no
- D. make it the same.
- E. Change the Resource section to "arn:aws:s3:::appbucket/\*".
- F. Create the bucket "appbucket" and then apply the policy

**Answer: C**

**Explanation:**

When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the \* can be used to assign the permission to all objects in the bucket

Option A is invalid because the right permissions are already provided as per the question requirement

Option B is invalid because it is not necessary that the policy has the same name as the bucket Option D is invalid because this should be the default flow for applying the policy

For more information on bucket policies please visit the below URL: <https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: Change the Resource section to "arn:aws:s3:::appbucket/" Submit your Feedback/Queries to our Experts

**NEW QUESTION 5**

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 6

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

Please select:

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

**Answer: B**

#### Explanation:

In the test environment the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.

Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.

For more information on authorizing access to an instance, please visit the below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html> The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

#### NEW QUESTION 7

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 8

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 9**

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 10**

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 10**

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

Please select:

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

**Answer: BE**

**Explanation:**

The AWS Documentation mentions the following

To create an encrypted Amazon EBS volume, select the appropriate box in the Amazon EBS section of the Amazon EC2 console. You can use a custom customer master key (CMK) by choosing one from the list that appears below the encryption box. If you do not specify a custom CMK, Amazon EBS uses the AWS-managed CMK for Amazon EBS in your account. If there is no AWS-managed CMK for Amazon EBS in your account, Amazon EBS creates one.

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers).

You can protect data in transit by using

SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.

- Use Server-Side Encryption - You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

- Use Client-Side Encryption - You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools. Option A is invalid because using EBS-optimized Amazon EC2 instances alone will not guarantee protection of instances at rest. Option C is invalid because this will not encrypt data at rest for S3 objects. Option D is invalid because you don't store data in Instance store. For more information on EBS encryption, please visit the below URL: <https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

For more information on S3 encryption, please visit the below URL: <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsinEEEncryption.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 13**

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 18**

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 [id=docs\\_orgs\\_console https://docs.aws.amazon.com/IAM/latest/UserGi manage attach-policy.html](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 19

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-contentrestrictions-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 20

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 22

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

Please select:

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

**Answer: B**

#### Explanation:

Since this is required over a consistency low latency connection, you should use Direct Connect. For encryption, you can make use of a VPN

Option A is invalid because exposing an HTTPS endpoint will not help all traffic to flow between a VPC and the data center.

Option C is invalid because low latency is a key requirement Option D is invalid because only Direct Connect will not suffice

For more information on the connection options please see the below Link: <https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharint>

The correct answer is: A VPN between the VPC and the data center over a Direct Connect connection Submit your Feedback/Queries to our Experts

#### NEW QUESTION 25

Your current setup in AWS consists of the following architecture. 2 public subnets, one subnet which has the web servers accessed by users across the internet and the other subnet for the database server. Which of the following changes to the architecture would add a better security boundary to the resources hosted in your setup

Please select:

- A. Consider moving the web server to a private subnet
- B. Consider moving the database server to a private subnet
- C. Consider moving both the web and database server to a private subnet
- D. Consider creating a private subnet and adding a NAT instance to that subnet

**Answer:** B

**Explanation:**

The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet. The below diagram from the AWS Documentation shows how this can be setup

Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users Option D is invalid because NAT instances should be present in the public subnet For more information on public and private subnets in AWS, please visit the following url [.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2).

The correct answer is: Consider moving the database server to a private subnet Submit your Feedback/Queries to our Experts

**NEW QUESTION 26**

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 27**

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/mspector/latest/userguide/inspector\\_runtime-behavioranalysis.html#insecure-protocols](https://docs.aws.amazon.com/mspector/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 30**

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 31**

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 fulfill 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 35**

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 IAM 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 39

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 account 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 use 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 42

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: A**Explanation:

#### 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 46

A company has an existing AWS account and a set of critical resources hosted in that account. The employee who was in-charge of the root account has left the company. What must be now done to secure the account. Choose 3 answers from the options given below.

Please select:

- A. Change the access keys for all IAM users.
- B. Delete all custom created IAM policies
- C. Delete the access keys for the root account
- D. Confirm MFA to a secure device
- E. Change the password for the root account
- F. Change the password for all IAM users

**Answer:** CDE

**Explanation:**

Now if the root account has a chance to be compromised, then you have to carry out the below steps

1. Delete the access keys for the root account
2. Confirm MFA to a secure device
3. Change the password for the root account

This will ensure the employee who has left has no change to compromise the resources in AWS. Option A is invalid because this would hamper the working of the current IAM users

Option B is invalid because this could hamper the current working of services in your AWS account Option F is invalid because this would hamper the working of the current IAM users

For more information on IAM root user, please visit the following URL: <https://docs.aws.amazon.com/IAM/latest/UserGuide/id-root-user.html>

The correct answers are: Delete the access keys for the root account Confirm MFA to a secure device. Change the password for the root account

Submit Your Feedback/Queries to our Experts

**NEW QUESTION 51**

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

Please select:

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

**Answer:** D

**Explanation:**

Option A is invalid because keys cannot be exported and imported across regions. Option B is invalid because key rotation cannot be used to export keys Option C is invalid because the backing key cannot be used to export keys This is mentioned in the AWS documentation

What geographic region are my keys stored in?

Keys are only stored and used in the region in which they are created. They cannot be transferred to another region. For example; keys created in the EU-Central (Frankfurt) region are only stored and used within the EU-Central (Frankfurt) region

For more information on KMS please visit the following URL: <https://aws.amazon.com/kms/faqs/>

The correct answer is: This is not possible since keys from KMS are region specific Submit your Feedback/Queries to our Experts

**NEW QUESTION 54**

An EC2 Instance hosts a Java based application that access a DynamoDB table. This EC2 Instance is currently serving production based users. Which of the following is a secure way of ensuring that the EC2 Instance access the Dynamo table

Please select:

- A. Use 1AM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance
- B. Use KMS keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- C. Use 1AM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- D. Use 1AM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance

**Answer:** A

**Explanation:**

To always ensure secure access to AWS resources from EC2 Instances, always ensure to assign a Role to the EC2 Instance Option B is invalid because KMS keys are not used as a mechanism for providing EC2 Instances access to AWS services. Option C is invalid Access keys is not a safe mechanism for providing EC2 Instances access to AWS services. Option D is invalid because there is no way access groups can be assigned to EC2 Instances. For more information on 1AM Roles, please refer to the below URL:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id-roles.html>

The correct answer is: Use 1AM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

**NEW QUESTION 58**

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 62**

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 63**

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

Please select:

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

**Answer: B**

**Explanation:**

The AWS Documentation mentions the following

Data key caching stores data keys and related cryptographic material in a cache. When you encrypt or decrypt data, the AWS Encryption SDK looks for a matching data key in the cache. If it finds a match, it uses the cached data key rather than generating a new one. Data key caching can improve performance, reduce cost, and help you stay within service limits as your application scales. Option A,C and D are all incorrect since these options will not impact how the key is used.

For more information on data key caching, please refer to below URL: <https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-key-cache.html>

The correct answer is: Use Data key caching Submit your Feedback/Queries to our Experts

**NEW QUESTION 66**

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

Please select:

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

**Answer: B**

**Explanation:**

The AWS Security best practises mentions the following

Unique to AWS, security practitioners can use CloudFormation to quickly create a new, trusted environment in which to conduct deeper investigation. The CloudFormation template can preconfigure instances in an isolated environment that contains all the necessary tools forensic teams need to determine the cause of the incident This cuts down on the time it takes to gather necessary tools, isolates systems under examination, and ensures that the team is operating in a clean room. Option A is incorrect since this is a logging service and cannot be used to provision a test environment

Option C is incorrect since this is an API logging service and cannot be used to provision a test environment

Option D is incorrect since this is a configuration service and cannot be used to provision a test environment

For more information on AWS Security best practises, please refer to below URL: <https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf>

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

**NEW QUESTION 67**

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-la2b3c4d. 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 69**

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 72**

A DevOps team is currently looking at the security aspect of their CI/CD pipeline. They are making use of AWS resources 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 74**

You want to track access requests for a particular S3 bucket. How can you achieve this in the easiest possible way?  
Please select:

- A. Enable server access logging for the bucket
- B. Enable Cloudwatch metrics for the bucket
- C. Enable Cloudwatch logs for the bucket
- D. Enable AWS Config for the S3 bucket

**Answer:** A

**Explanation:**

The AWS Documentation mentions the foil  
To track requests for access to your bucket you can enable access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any.  
Options B and C are incorrect Cloudwatch is used for metrics and logging and cannot be used to track access requests.  
Option D is incorrect since this can be used for Configuration management but for not for tracking S3 bucket requests.  
For more information on S3 server logs, please refer to below UF <https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLoes.html>  
The correct answer is: Enable server access logging for the bucket Submit your Feedback/Queries to our Experts

**NEW QUESTION 79**

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

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

**Answer:** BD

**Explanation:**

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

**NEW QUESTION 82**

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 87**

A company has hired a third-party security auditor, and the auditor needs read-only access to all AWS resources and logs of all VPC records and events that have occurred on AWS. How can the company meet the auditor's requirements without comprising security in the AWS environment? Choose the correct answer from

the options below  
Please select:

- A. Create a role that has the required permissions for the auditor.
- B. Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
- C. The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to the third-party auditor.
- D. Enable CloudTrail logging and create an IAM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs.

**Answer: D**

**Explanation:**

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.

Option A and C are incorrect since CloudTrail needs to be used as part of the solution Option B is incorrect since the auditor needs to have access to CloudTrail For more information on CloudTrail, please visit the below URL: <https://aws.amazon.com/cloudtrail>

The correct answer is: Enable CloudTrail logging and create an IAM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs. Submit your Feedback/Queries to our Experts

**NEW QUESTION 88**

An auditor needs access to logs that record all API events on AWS. The auditor only needs read-only access to the log files and does not need access to each AWS account. The company has multiple AWS accounts, and the auditor needs access to all the logs for all the accounts. What is the best way to configure access for the auditor to view event logs from all accounts? Choose the correct answer from the options below

Please select:

- A. Configure the CloudTrail service in each AWS account, and have the logs delivered to an AWS bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary IAM account that can assume a read-only role in the secondary AWS accounts.
- B. Configure the CloudTrail service in the primary AWS account and configure consolidated billing for all the secondary account
- C. Then grant the auditor access to the S3 bucket that receives the CloudTrail log files.
- D. Configure the CloudTrail service in each AWS account and enable consolidated logging inside of CloudTrail.
- E. Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bucket in the primary account and grant the auditor access to that single bucket in the primary account

**Answer: D**

**Explanation:**

Given the current requirements, assume the method of "least privilege" security design and only allow the auditor access to the minimum amount of AWS resources as possible

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 events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting

only be granted access in one location

Option A is incorrect since the auditor should have access to all accounts B is incorrect since consolidated billing is not a key requirement as part of the question

Option C is incorrect since there is not consolidated logging

For more information on CloudTrail please refer to the below URL: <https://aws.amazon.com/cloudtrail>

The correct answer is: Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bucket in the primary account and grant the auditor access to that single bucket in the primary account.

Submit your Feedback/Queries to our Experts

**NEW QUESTION 92**

You have been given a new brief from your supervisor for a client who needs a web application set up on AWS. The most important requirement is that MySQL must be used as the database, and this database must not be hosted in the public cloud, but rather at the client's data center due to security risks. Which of the following solutions would be the best to assure that the client's requirements are met? Choose the correct answer from the options below

Please select:

- A. Build the application server on a public subnet and the database at the client's data center
- B. Connect them with a VPN connection which uses IPsec.
- C. Use the public subnet for the application server and use RDS with a storage gateway to access and synchronize the data securely from the local data center.
- D. Build the application server on a public subnet and the database on a private subnet with a NAT instance between them.
- E. Build the application server on a public subnet and build the database in a private subnet with a secure ssh connection to the private subnet from the client's data center.

**Answer: A**

**Explanation:**

Since the database should not be hosted on the cloud all other options are invalid. The best option is to create a VPN connection for securing traffic as shown below.

Option B is invalid because this is the incorrect use of the Storage gateway Option C is invalid since this is the incorrect use of the NAT instance Option D is invalid since this is an incorrect configuration For more information on VPN connections, please visit the below URL

[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_VPN.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

The correct answer is: Build the application server on a public subnet and the database at the client's data center. Connect them with a VPN connection which uses IPsec

Submit your Feedback/Queries to our Experts

**NEW QUESTION 94**

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 99**

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 101**

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 102**

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 107**

Your company has an EC2 Instance hosted in AWS. This EC2 Instance hosts an application. Currently this application is experiencing a number of issues. You need to inspect the network packets to see what the type of error that is occurring? Which one of the below steps can help address this issue? Please select:

- A. Use the VPC Flow Logs.
- B. Use a network monitoring tool provided by an AWS partner.
- C. Use another instance
- D. Setup a port to "promiscuous mode" and sniff the traffic to analyze the packet
- E. -
- F. Use Cloudwatch metric

**Answer: B**

**NEW QUESTION 108**

A company hosts critical data in an S3 bucket. Even though they have assigned the appropriate permissions to the bucket, they are still worried about data deletion. What measures can be taken to restrict the risk of data deletion on the bucket. Choose 2 answers from the options given below Please select:

- A. Enable versioning on the S3 bucket
- B. Enable data at rest for the objects in the bucket
- C. Enable MFA Delete in the bucket policy
- D. Enable data in transit for the objects in the bucket

**Answer: AC**

**Explanation:**

One of the AWS Security blogs mentions the following

Versioning keeps multiple versions of an object in the same bucket. When you enable it on a bucket Amazon S3 automatically adds a unique version ID to every

object stored in the bucket. At that point, a simple DELETE action does not permanently delete an object version; it merely associates a delete marker with the object. If you want to permanently delete an object version, you must specify its version ID in your DELETE request. You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your AWS accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket. Option B is invalid because enabling encryption does not guarantee risk of data deletion. Option D is invalid because this option does not guarantee risk of data deletion. For more information on AWS S3 versioning and MFA please refer to the below URL: <https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/>

**NEW QUESTION 111**

The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy Submit your Feedback/Queries to our Experts  
Your company has mandated that all data in AWS be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below  
Please select:

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

**Answer:** AB

**Explanation:**

EBS encryption can also be enabled when the volume is created and not for existing volumes. One can use existing tools for OS level encryption.

Option C is incorrect.

AWS Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.

Option D is incorrect

You cannot choose to encrypt a non-encrypted boot volume on instance launch. To have encrypted boot volumes during launch, your custom AMI must have its boot volume encrypted before launch. For more information on the Security Best practices, please visit the following URL:

[.com/whit](https://aws.amazon.com/whit) Security Practices.

The correct answers are: Use Windows bit locker for EBS volumes on Windows instances. Use TrueEncrypt for EBS volumes on Linux instances  
Submit your Feedback/Queries to our Experts

**NEW QUESTION 115**

A company has a set of EC2 instances hosted in AWS. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are not required.  
Please select:

- A. Use lifecycle policies for the EBS volumes
- B. Use EBS Snapshots
- C. Use EBS volume replication
- D. Use EBS volume encryption

**Answer:** CD

**Explanation:**

Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability.

You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes.

With lifecycle management, you can be sure that snapshots are cleaned up regularly and keep costs under control.

EBS Lifecycle Policies

A lifecycle policy consists of these core settings:

- Resource type—The AWS resource managed by the policy, in this case, EBS volumes.
- Target tag—The tag that must be associated with an EBS volume for it to be managed by the policy.
- Schedule—Defines how often to create snapshots and the maximum number of snapshots to keep. Snapshot creation starts within an hour of the specified start time. If creating a new snapshot exceeds the maximum number of snapshots to keep for the volume, the oldest snapshot is deleted.

Option C is correct. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. But it does not have an explicit feature like that.

Option D is correct Encryption does not ensure data durability

For information on security for Compute Resources, please visit the below URL [https://d1.awsstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdf](https://d1.awsstatic.com/whitepapers/Security/Security%20Compute%20Services%20Whitepaper.pdf)

The correct answers are: Use EBS volume replication. Use EBS volume encryption Submit your Feedback/Queries to our Experts

**NEW QUESTION 119**

Your company has the following setup in AWS

- A. A set of EC2 Instances hosting a web application
- B. An application load balancer placed in front of the EC2 Instances
- C. There seems to be a set of malicious requests coming from a set of IP addresses. Which of the following can be used to protect against these requests? Please select:
- D. Use Security Groups to block the IP addresses
- E. Use VPC Flow Logs to block the IP addresses
- F. Use AWS inspector to block the IP addresses
- G. Use AWS WAF to block the IP addresses

**Answer:** D

**Explanation:**

Your answer is incorrect Answer -D

The AWS Documentation mentions the following on AWS WAF which can be used to protect Application Load Balancers and Cloud front

A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to. You can allow or block the following types of requests:

Originate from an IP address or a range of IP addresses Originate from a specific country or countries

Contain a specified string or match a regular expression (regex) pattern in a particular part of requests

Exceed a specified length

Appear to contain malicious SQL code (known as SQL injection)

Appear to contain malicious scripts (known as cross-site scripting)

Option A is invalid because by default Security Groups have the Deny policy

Options B and C are invalid because these services cannot be used to block IP addresses For information on AWS WAF, please visit the below URL:

<https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html>

The correct answer is: Use AWS WAF to block the IP addresses Submit your Feedback/Queries to our Experts

### NEW QUESTION 123

You need to establish a secure backup and archiving solution for your company, using AWS. Documents should be immediately accessible for three months and available for five years for compliance reasons. Which AWS service fulfills these requirements in the most cost-effective way?

Choose the correct answer

Please select:

- A. Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
- B. Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.
- C. Use Direct Connect to upload data to S3 and use 1AM policies to move the data into Glacier for long-term archiving.
- D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

**Answer:** A

#### Explanation:

amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as

\$0,004 per gigabyte per month, a significant savings compared to on-premises solutions.

With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARD\_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because 1AM policies cannot be used to move data to Glacier

Option D is invalid because lifecycle policies is not used to move data to Redshift For more information on S3 lifecycle policies, please visit the URL:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

The correct answer is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.

Submit your Feedback/Queries to our Experts

### NEW QUESTION 128

Your company is planning on using AWS EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted. Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.

Please select:

- A. Ensure the load balancer listens on port 80
- B. Ensure the load balancer listens on port 443
- C. Ensure the HTTPS listener sends requests to the instances on port 443
- D. Ensure the HTTPS listener sends requests to the instances on port 80

**Answer:** BC

#### Explanation:

The AWS Documentation mentions the following

You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted, if the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.

Option A is invalid because there is a need for secure traffic, so port 80 should not be used Option D is invalid because for the HTTPS listener you need to use port 443

For more information on HTTPS with ELB, please refer to the below Link: <https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-loadbalancer.html>

The correct answers are: Ensure the load balancer listens on port 443, Ensure the HTTPS listener sends requests to the instances on port 443

Submit your Feedback/Queries to our Experts

### NEW QUESTION 131

Your company is planning on developing an application in AWS. This is a web based application. The application user will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this.

Please select:

- A. Create an OIDC identity provider in AWS
- B. Create a SAML provider in AWS
- C. Use AWS Cognito to manage the user profiles
- D. Use IAM users to manage the user profiles

**Answer:** C

#### Explanation:

The AWS Documentation mentions the following

A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers. Whether your users sign in directly or through a third

party, all members of the user pool have a directory profile that you can access through an SDK.

User pools provide:

Sign-up and sign-in services.

A built-in, customizable web UI to sign in users.

Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user pool.

User directory management and user profiles.

Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.

Customized workflows and user migration through AWS Lambda triggers. Options A and B are invalid because these are not used to manage users Option D is invalid because this would be a maintenance overhead

For more information on Cognito User Identity pools, please refer to the below Link: <https://docs.aws.amazon.com/coenito/latest/developerguide/cognito-user-identity-pools.html>

The correct answer is: Use AWS Cognito to manage the user profiles Submit your Feedback/Queries to our Experts

#### NEW QUESTION 134

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

Please select:

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

**Answer: B**

#### Explanation:

The AWS Documentation mentions the following

Amazon S3 is integrated with AWS CloudTrail. CloudTrail is a service that captures specific API calls made to Amazon S3 from your AWS account and delivers the log files to an Amazon S3 bucket that you specify. It captures API calls made from the Amazon S3 console or from the Amazon S3 API. Using the information collected by CloudTrail, you can determine what request was made to Amazon S3, the source IP address from which the request was made, who made the request when it was made, and so on

Options A,C and D are invalid because these services cannot be used to get the source IP address of the calls to S3 buckets

For more information on Cloudtrail logging, please refer to the below Link:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logeins.html>

The correct answer is: Monitor the S3 API calls by using Cloudtrail logging Submit your Feedback/Queries to our Experts

#### NEW QUESTION 136

A company has set up EC2 instances on the AWS Cloud. There is a need to see all the IP addresses which are accessing the EC2 Instances. Which service can help achieve this?

Please select:

- A. Use the AWS Inspector service
- B. Use AWS VPC Flow Logs
- C. Use Network ACL's
- D. Use Security Groups

**Answer: B**

#### Explanation:

The AWS Documentation mentions the following

A flow log record represents a network flow in your flow log. Each record captures the network flow for a specific 5-tuple, for a specific capture window. A 5-tuple is a set of five different values that specify the source, destination, and protocol for an internet protocol (IP) flow.

Options A,C and D are all invalid because these services/tools cannot be used to get the IP addresses which are accessing the EC2 Instances

For more information on VPC Flow Logs please visit the URL <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>

The correct answer is: Use AWS VPC Flow Logs Submit your Feedback/Queries to our Experts

#### NEW QUESTION 138

You have private video content in S3 that you want to serve to subscribed users on the Internet. User IDs, credentials, and subscriptions are stored in an Amazon RDS database. Which configuration will allow you to securely serve private content to your users?

Please select:

- A. Generate pre-signed URLs for each user as they request access to protected S3 content
- B. Create an IAM user for each subscribed user and assign the GetObject permission to each IAM user
- C. Create an S3 bucket policy that limits access to your private content to only your subscribed users'credentials
- D. Create a Cloud Front Origin Identity user for your subscribers and assign the GetObject permission to this user

**Answer: A**

#### Explanation:

All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able upload a specific object to your bucket but you don't require them to have AWS security credentials or permissions. When you create a pre-signed URL, you must provide your security credentials, specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The pre-signed URLs are valid only for the specified duration.

Option B is invalid because this would be too difficult to implement at a user level. Option C is invalid because this is not possible

Option D is invalid because this is used to serve private content via Cloudfront For more information on pre-signed urls, please refer to the Link:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html>

The correct answer is: Generate pre-signed URLs for each user as they request access to protected S3 content Submit your Feedback/Queries to our Experts

**NEW QUESTION 141**

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

Please select:

- A. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.
- B. Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS application
- C. Create a new access and secret key for the user and provide these credentials to the SaaS provider.
- D. Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
- E. Create an IAM role for EC2 instances, assign it a policy that allows only the actions required for the SaaS application to work, provide the role ARN to the SaaS provider to use when launching their application instances.

**Answer: C**

**Explanation:**

The below diagram from an AWS blog shows how access is given to other accounts for the services in your own account

Options A and B are invalid because you should not use IAM users or IAM Access keys Option D is invalid because you need to create a role for cross account access

For more information on Allowing access to external accounts, please visit the below URL:

<https://aws.amazon.com/blogs/apn/how-to-best-architect-your-aws-marketplace-saas-subscription-across-multiple-aws-accounts>;

The correct answer is: Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.

Submit your Feedback/Queries to our Experts

**NEW QUESTION 142**

You have an S3 bucket defined in AWS. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this.

Please select:

- A. Enable server side encryption for the S3 bucket
- B. This request will ensure that the data is encrypted first.
- C. Use the AWS Encryption CLI to encrypt the data first
- D. Use a Lambda function to encrypt the data before sending it to the S3 bucket.
- E. Enable client encryption for the bucket

**Answer: B**

**Explanation:**

One can use the AWS Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL: <https://aws.amazon.com/blogs/security/how-to-encrypt-and-decrypt-your-data-with-the-aws-encryption-cli>

The correct answer is: Use the AWS Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

**NEW QUESTION 147**

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

Please select:

- A. Create a new role and add each user to the IAM role

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

**Answer:** B

**Explanation:**

Option A is incorrect since you don't add a user to the 1AM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach

An 1AM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group

For more information on 1AM Groups, just browse to the below URL:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_eroups.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_eroups.html)

The correct answer is: Use the 1AM groups and add users, based upon their role, to different groups and apply the policy to group

Submit your Feedback/Queries to our Experts

**NEW QUESTION 148**

You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?

Please select:

- A. Add an AWS managed policy for the user
- B. Add a service policy for the user
- C. Add an 1AM role for the user
- D. Add an inline policy for the user

**Answer:** D

**Explanation:**

Options A and B are incorrect since you need to add an inline policy just for the user Option C is invalid because you don't assign an 1AM role to a user

The AWS Documentation mentions the following

An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.

For more information on 1AM Access and Inline policies, just browse to the below URL: <https://docs.aws.amazon.com/IAM/latest/UserGuide/access>

The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

**NEW QUESTION 150**

There are currently multiple applications hosted in a VPC. During monitoring it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP Address's.

Please select:

- A. Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.
- B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.
- C. Add a rule to all of the VPC Security Groups to deny access from the IP Address block.
- D. Modify the Windows Firewall settings on all AMI'S that your organization uses in that VPC to deny access from the IP address block.

**Answer:** B

**Explanation:**

NACL acts as a firewall at the subnet level of the VPC and we can deny the offending IP address block

at the subnet level using NACL rules to block the incoming traffic to the VPC instances. Since NACL rules are applied as per the Rule numbers make sure that this rule number should take precedence over other rule numbers if there are any such rules that will allow traffic from these IP ranges. The lowest rule number has more precedence over a rule that has a higher number.

The AWS Documentation mentions the following as a best practices for 1AM users

For extra security, enable multi-factor authentication (MFA) for privileged 1AM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone). Options C is invalid because these options are not available

Option D is invalid because there is not root access for users

For more information on 1AM best practices, please visit the below URL: <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

The correct answer is: Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.

omit your Feedback/Queries to our Experts

**NEW QUESTION 154**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

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

\* One year free update

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

\* Trusted by Millions

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

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your AWS-Certified-Security-Specialty Exam with Our Prep Materials Via below:**

<https://www.certleader.com/AWS-Certified-Security-Specialty-dumps.html>