

# Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

<https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/>



#### NEW QUESTION 1

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

A.

B.

C.

D.

A.

**Answer:** A

#### **Explanation:**

The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated.

Option B and C are wrong since the `aws:MultiFactorAuthPresent` clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is true, then allow access.

Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false."

Here in this scenario the boot attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.

For more information on an example on such a policy, please visit the following URL:

#### NEW QUESTION 2

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

Please select:

- A. Stream the log files to a separate Cloudtrail trail
- B. Stream the log files to a separate Cloudwatch Log group
- C. Create an 1AM policy that gives the desired level of access to the Cloudtrail trail
- D. Create an 1AM policy that gives the desired level of access to the Cloudwatch Log group

**Answer:** BD

#### **Explanation:**

You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an 1AM policy.

Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement

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

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

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

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

Submit your Feedback/Queries to our Experts

### NEW QUESTION 3

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security

authentication for these users. How can this be accomplished?

Please select:

- A. Enable MFA for these user accounts
- B. Enable versioning for these user accounts
- C. Enable accidental deletion for these user accounts
- D. Disable root access for the users

**Answer:** A

#### Explanation:

The AWS Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates 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).

Option B,C and D are invalid because no such security options are available in AWS For more information on IAM best practices, please visit the below URL <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The correct answer is: Enable MFA for these user accounts

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 IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted. Which of the following can help achieve this?

Please select:

- A. AWS KMS API
- B. AWS Certificate Manager
- C. API Gateway with STS
- D. IAM Access Key

**Answer:** A

#### Explanation:

The AWS Documentation mentions the following on AWS KMS

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data

A. AWS KMS is integrated with other AWS

services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage

Option B is incorrect - The AWS Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest

Option C is incorrect is again used for issuing tokens when using API gateway for traffic in transit. Option D is used for secure access to EC2 Instances  
For more information on AWS KMS, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/overview.html> The correct answer is:  
AWS KMS API  
Submit your Feedback/Queries to our Experts

#### NEW QUESTION 6

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 7

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 8

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

- A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/server
- B. Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- C. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
- D. Use Systems Manager Patch Manger to install the missing patches.
- E. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
- F. Redeploy all out of1 compliance instances/servers using an AMI with the latest patches.
- G. Use Trusted Advisor to generate the report of out of compliance instances/server
- H. Use Systems Manger Patch Manger to install the missing patches.

**Answer: B**

#### Explanation:

Use the Systems Manger Patch Manger to generate the report and also install the missing patches The AWS Documentation mentions the following

AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fileets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu

Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.



Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.  
Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers  
Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.  
For more information on the AWS Patch Manager, please visit the below URL: <https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html> (  
The correct answer is: Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manger to install the missing patches. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 9

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

- A. Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.
- B. Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic.
- C. Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
- D. Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
- E. Enable GuardDuty to block malicious traffic from reaching the application

**Answer:** BD

#### Explanation:

The below diagram from AWS shows the best case scenario for avoiding DDos attacks using services such as AWS Cloudfro WAF, ELB and Autoscaling  
Option A is invalid because by default security groups don't allow access Option C is invalid because AWS Inspector cannot be used to examine traffic  
Option E is invalid because this can be used for attacks on EC2 Instances but not against DDos attacks on the entire application For more information on DDos mitigation from AWS, please visit the below URL:  
<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitieationi>  
The correct answers are: Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic., Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application  
Submit your Feedback/Queries to our Experts

#### NEW QUESTION 10

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

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

**Answer:** B

#### Explanation:

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, whil protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance. especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.  
1AM roles are designed so that your applications can securely make API requests from your instances, without requiring yo manage the security credentials that the applications use.  
Option A.C and D are invalid because using AWS Credentials in an application in production is a direct no recommendation 1 secure access  
For more information on 1AM Roles, please visit the below URL: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>  
The correct answer is: Don't save your API credentials. Instead create a role in 1AM and assign this role to an EC2 instance when you first create it  
Submit your Feedback/Queries to our Experts

#### NEW QUESTION 14

A company has a set of resources defined in AWS. It is mandated that all API calls to the resources be monitored. Also all API calls must be stored for lookup purposes. Any log data greater than 6 months must be archived. Which of the following meets these requirements? Choose 2 answers from the options given below. Each answer forms part of the solution.

Please select:

- A. Enable CloudTrail logging in all accounts into S3 buckets
- B. Enable CloudTrail logging in all accounts into Amazon Glacier
- C. Ensure a lifecycle policy is defined on the S3 bucket to move the data to EBS volumes after 6 months.
- D. Ensure a lifecycle policy is defined on the S3 bucket to move the data to Amazon Glacier after 6 months.

**Answer:** AD

**Explanation:**

Cloudtrail publishes the trail of API logs to an S3 bucket

Option B is invalid because you cannot put the logs into Glacier from CloudTrail

Option C is invalid because lifecycle policies cannot be used to move data to EBS volumes For more information on Cloudtrail logging, please visit the below URL:

<https://docs.aws.amazon.com/awscloudtrail/latest/useruide/cloudtrail-find-log-files.html>

You can then use Lifecycle policies to transfer data to Amazon Glacier after 6 months For more information on S3 lifecycle policies, please visit the below URL:

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

The correct answers are: Enable CloudTrail logging in all accounts into S3 buckets. Ensure a lifecycle policy is defined on the bucket to move the data to Amazon Glacier after 6 months.

Submit your Feedback/Queries to our Experts

**NEW QUESTION 17**

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 Cloud Front to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below

Please select:

- A. Create an Identity and Access Management (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 19**

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-sharing/>

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 20**

A company has several Customer Master Keys (CMK), some of which have imported key material.

Each CMK must be rotated annually.

What two methods can the security team use to rotate each key? Select 2 answers from the options given below

Please select:

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

**Answer:** AD

**Explanation:**

The AWS Documentation mentions the following

Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (the value of the Origin field is External), but you can rotate these CMKs manually.

Rotating Keys Manually

You might want to create a new CMK and use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation.

When you begin using the new CMK, be sure to keep the original CMK enabled so that AWS KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the same CMK to decrypt the data.

A. As long as you keep both

the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK.

Option B is invalid because you also need to point the key alias to the new key. Option C is invalid because existing CMK keys cannot be rotated as they are

Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key.

For more information on Key rotation please see the below Link: <https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

The correct answers are: Enable automatic key rotation for a CMK, Import new key material to a new CMK; Point the key alias to the new CMK.

Submit your Feedback/Queries to our Experts

**NEW QUESTION 22**

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

Please select:

A. Access the S3 bucket through a proxy server

B. Access the S3 bucket through a NAT gateway.

C. Access the S3 bucket through a VPC endpoint for S3

D. Access the S3 bucket through the SSL protected S3 endpoint

**Answer:** C

**Explanation:**

The AWS Documentation mentions the following

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

Option A is invalid because using a proxy server is not sufficient enough

Option B and D are invalid because you need secure communication which should not traverse the internet

For more information on VPC endpoints please see the below link <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html>

The correct answer is: Access the S3 bucket through a VPC endpoint for S3. Submit your Feedback/Queries to our Experts

**NEW QUESTION 23**

When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users?

These permissions should be easily managed.

Please select:

A. Use the secure token service to manage the permissions for the different users

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

C. Use the AWS Config tool to manage the permissions for the different users

D. Use IAM Access Keys to create sets of keys for the different types of user

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following

You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes:

\* To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.

\* To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway.

Option A, C and D are invalid because these cannot be used to control access to AWS services. This needs to be done via policies. For more information on permissions with the API gateway, please visit the following URL: <https://docs.aws.amazon.com/apigateway/latest/developerguide/permissions.html>

The correct answer is: Use IAM Policies to create different policies for the different types of users. Submit your Feedback/Queries to our Experts

**NEW QUESTION 27**

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database - administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure-

\* sgLB - associated with the ELB

\* sgWeb - associated with the EC2 instances.

\* sgDB - associated with the database

\* sgBastion - associated with the bastion host Which security group configuration will allow the application to be secure and functional?

Please select: A.

sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from 0.0.0.0/0 sgDB :allow port 3306 traffic from sgWeb and sgBastion

sgBastion: allow port 22 traffic from the corporate IP address range

B.

sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgLB

sgBastion: allow port 22 traffic from the VPC IP address range C.

sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB



sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the VPC IP address range D.  
sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB  
sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

A.

**Answer: D**

**Explanation:**

The Load Balancer should accept traffic on port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer  
The database should allow traffic from the Web server

And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on AWS Security Groups, please refer to below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>

The correct answer is: sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB

sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range Submit your Feedback/Queries to our Experts

**NEW QUESTION 28**

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 33**

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

Please select:

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



**Answer:** AB

**Explanation:**

The AWS Documentation mentions the following

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

View Agent Logs

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

On Windows

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

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

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

On Linux

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

**NEW QUESTION 37**

Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service? Please select:

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

**Answer:** B

**Explanation:**

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

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

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

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

<https://aws.amazon.com/blogs/security/new-whitepaper-single-sign-on-integrating-aws-openldap-and-shibboleth/>

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

**NEW QUESTION 42**

You need to ensure that the CloudTrail logs which are being delivered in your AWS account are encrypted. How can this be achieved in the easiest way possible? Please select:

- A. Don't do anything since CloudTrail logs are automatically encrypted.
- B. Enable S3-SSE for the underlying bucket which receives the log files
- C. Enable S3-KMS for the underlying bucket which receives the log files
- D. Enable KMS encryption for the logs which are sent to Cloudwatch

**Answer:** A

**Explanation:**

The AWS Documentation mentions the following

By default the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3)

Option B, C and D are all invalid because by default all logs are encrypted when they are sent by CloudTrail to S3 buckets

For more information on AWS CloudTrail log encryption, please visit the following URL: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html>

The correct answer is: Don't do anything since CloudTrail logs are automatically encrypted. Submit your Feedback/Queries to our Experts

**NEW QUESTION 43**

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 URLs
- 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-signers.html>

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

#### NEW QUESTION 47

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 to 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 to that OAI.

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

#### NEW QUESTION 48

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 50

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

- A. Adding a bucket policy on the S3 bucket.
- B. Configuring lifecycle configuration rules on the S3 bucket.
- C. Creating an IAM policy for the S3 bucket.

D. Enabling CORS on the S3 bucket

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following on lifecycle policies

Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified as follows:

Transition actions - In which you define when objects transition to another. 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.

Expiration actions - In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

Option A and C are invalid because neither bucket policies nor IAM policy's can control the purging of logs. Option D is invalid. CORS is used for accessing objects across domains and not for purging of logs. For more information on AWS S3 Lifecycle policies, please visit the following URL:

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

The correct answer is: Configuring lifecycle configuration rules on the S3 bucket. Submit your Feedback/Queries to our Experts

**NEW QUESTION 55**

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

Please select:

A. Use CloudWatch metrics and logs to watch for errors

B. Use CloudTrail to monitor for errors

C. Use the AWS Config service to monitor for errors

D. Use the AWS Inspector service to monitor for errors

**Answer:** A

**Explanation:**

The AWS Documentation mentions the following

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

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

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

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

**NEW QUESTION 56**

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

Please select:

A. Use AWS Access keys to encrypt the data

B. Use SSL certificates to encrypt the data

C. Enable server side encryption on the S3 bucket

D. Enable MFA on the S3 bucket

**Answer:** C

**Explanation:**

The AWS Documentation mentions the following

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

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

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

Submit your Feedback/Queries to our Experts

**NEW QUESTION 60**

Your company hosts critical data in an S3 bucket. There is a requirement to ensure that all data is encrypted. There is also metadata about the information stored in the bucket that needs to be encrypted as well. Which of the below measures would you take to ensure that the metadata is encrypted?

Please select:

A. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server side encryption.

B. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server KMS encryption.

C. Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time.

D. Put the metadata in the S3 bucket itself

**Answer:** C

**Explanation:**

Option A, B and D are all invalid because the metadata will not be encrypted in any case and this is a key requirement from the question.

One key thing to note is that when the S3 bucket objects are encrypted, the meta data is not encrypted. So the best option is to use an encrypted DynamoDB table. Important

All GET and PUT requests for an object protected by AWS KMS will fail if they are not made via SSL or by using SigV4. SSE-KMS encrypts only the object data.

A. Any object metadata is not encrypted. For

more information on using KMS encryption for S3, please refer to below URL: 1 <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html>

The correct answer is: Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 65

A company has set up the following structure to ensure that their S3 buckets always have logging enabled

If there are any changes to the configuration to an S3 bucket, a config rule gets checked. If logging is disabled, then Lambda function is invoked. This Lambda function will again enable logging on the S3 bucket. Now there is an issue being encountered with the entire flow. You have verified that the Lambda function is being invoked. But when logging is disabled for the bucket, the lambda function does not enable it again. Which of the following could be an issue Please select:

- A. The AWS Config rule is not configured properly
- B. The AWS Lambda function does not have appropriate permissions for the bucket
- C. The AWS Lambda function should use Node.js instead of python.
- D. You need to also use the API gateway to invoke the lambda function

**Answer:** B

#### Explanation:

The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes. Option A is invalid because this is more of a permission instead of a configuration rule issue. Option C is invalid because changing the language will not be the core solution.

Option D is invalid because you don't necessarily need to use the API gateway service

For more information on accessing resources from a Lambda function, please refer to below URL <https://docs.aws.amazon.com/lambda/latest/ds/accessing-resources.html>

The correct answer is: The AWS Lambda function does not have appropriate permissions for the bucket Submit your Feedback/Queries to our Experts

#### NEW QUESTION 67

Which of the following is the responsibility of the customer? Choose 2 answers from the options given below.

Please select:

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

**Answer:** BC

#### Explanation:

Below is the snapshot of the Shared Responsibility Model

For more information on AWS Security best practises, please refer to below URL

[.awsstatic.com/whitepapers/Security/AWS Practices](https://awsstatic.com/whitepapers/Security/AWS%20Practices).

The correct answers are: Encryption of data at rest Protection of data in transit Submit your Feedback/Queries to our Experts



#### NEW QUESTION 69

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

- A. IAM policies
- B. Buckets ACL's
- C. IAM users
- D. Bucket policies

**Answer:** BD

#### Explanation:

The AWS Security whitepaper gives the type of access control and to what level the control can be given

Options A and C are incorrect since for external access to buckets, you need to use either Bucket policies or Bucket ACL's or more information on Security for storage services role please refer to the below URL:

[https://d1.awsstatic.com/whitepapers/Security/Security Storage Services Whitepaper.pdf](https://d1.awsstatic.com/whitepapers/Security/Security%20Storage%20Services%20Whitepaper.pdf) The correct answers are: Buckets ACL's, Bucket policies

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 71

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 74

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 79**

Which of the below services can be integrated with the AWS Web application firewall service. Choose 2 answers from the options given below

Please select:

- A. AWS CloudFront
- B. AWS Lambda
- C. AWS Application Load Balancer
- D. AWS Classic Load Balancer

**Answer:** AC

**Explanation:**

The AWS documentation mentions the following on the Application Load Balancer

AWS WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of Amazon CloudFront it can be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations and as part of the Application Load Balancer it can protect your origin web servers running behind the ALBs.

Options B and D are invalid because only CloudFront and the Application Load Balancer services are supported by AWS WAF.

For more information on the web application firewall please refer to the below URL: <https://aws.amazon.com/waf/faq>;

The correct answers are: AWS CloudFront AWS Application Load Balancer Submit your Feedback/Queries to our Experts

**NEW QUESTION 80**

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 BitLocker 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 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 83

Your company has an external web site. This web site needs to access the objects in an S3 bucket. Which of the following would allow the web site to access the objects in the most secure manner? Please select:

- A. Grant public access for the bucket via the bucket policy
- B. Use the aws:Referer key in the condition clause for the bucket policy
- C. Use the aws:sites key in the condition clause for the bucket policy
- D. Grant a role that can be assumed by the web site

**Answer: B**

#### Explanation:

An example of this is given in the AWS Document titled Restricting Access to a Specific HTTP Referrer

Suppose you have a website with domain name (www.example.com or example.com) with links to photos and videos stored in your S3 bucket examplebucket. By default, all the S3 resources are private, so only the AWS account that created the resources can access them. To allow read access to these objects from your website, you can add a bucket policy that allows s3:GetObject permission with a condition, using the aws:referer key, that the get request must originate from specific webpages. The following policy specifies the StringLike condition with the aws:Referer condition key.

Option A is invalid because giving public access is not a secure way to provide access. Option C is invalid because aws:sites is not a valid condition key. Option D is invalid because IAM roles will not be assigned to web sites.

For more information on example bucket policies, please visit the below Link:

1 <https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: Use the aws:Referer key in the condition clause for the bucket policy. Submit your Feedback/Queries to our Experts

### NEW QUESTION 87

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>

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

### NEW QUESTION 92

A company is planning on using AWS EC2 and AWS Cloudfront for their web application. For which one of the below attacks is usage of Cloudfront most suited for?

Please select:

- A. Cross side scripting
- B. SQL injection
- C. DDoS attacks
- D. Malware attacks

**Answer:** C

**Explanation:**

The below table from AWS shows the security capabilities of AWS Cloudfront AWS Cloudfront is more prominent for DDoS attacks.

Options A,B and D are invalid because Cloudfront is specifically used to protect sites against DDoS attacks For more information on security with Cloudfront, please refer to the below Link: <https://d1.awsstatic.com/whitepapers/Security/Secure content delivery with CloudFront whitepaper.pdf>

The correct answer is: DDoS attacks

Submit your Feedback/Queries to our Experts

**NEW QUESTION 93**

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 98**

Your company is planning on developing an application in AWS. This is a web based application. The application users will use their facebook or google identities for authentication. 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:** B

**Explanation:**

The AWS Documentation mentions the following The AWS Documentation mentions the following

OIDC identity providers are entities in IAM that describe an identity provider (IdP) service that supports the OpenID Connect (OIDC) standard. You use an OIDC identity provider when you want to establish trust between an OIDC-compatible IdP—such as Google, Salesforce, and many others—and your AWS account This is useful if you are creating a mobile app or web application that requires access to AWS resources, but you don't want to create custom sign-in code or manage your own user identities

Option A is invalid because in the security groups you would not mention this information/ Option C is invalid because SAML is used for federated authentication

Option D is invalid because you need to use the OIDC identity provider in AWS For more information on OIDC identity providers, please refer to the below Link:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_create\\_oidc.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_create_oidc.html) The correct answer is: Create an OIDC identity provider in AWS

**NEW QUESTION 99**

Your company has many AWS accounts defined and all are managed via AWS Organizations. One AWS account has a S3 bucket that has critical data

A. How can we ensure that all the users in the AWS organisation have access to this bucket? Please select:

B. Ensure the bucket policy has a condition which involves aws:PrincipalOrgID

C. Ensure the bucket policy has a condition which involves aws:AccountNumber

D. Ensure the bucket policy has a condition which involves aws:PrincipalID

E. Ensure the bucket policy has a condition which involves aws:OrgID

**Answer:** A

**Explanation:**

The AWS Documentation mentions the following

AWS Identity and Access Management (IAM) now makes it easier for you to control access to your AWS resources by using the AWS organization of IAM principals (users and roles). For some services, you grant permissions using resource-based policies to specify the accounts and principals that can access the resource and what actions they can perform on it. Now, you can use a new condition key, aws:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account in the organization

Option B,C and D are invalid because the condition in the bucket policy has to mention aws:PrincipalOrgID

For more information on controlling access via Organizations, please refer to the below Link: <https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-awsorganization-of-iam-principal/>

(  
The correct answer is: Ensure the bucket policy has a condition which involves aws:PrincipalOrgID Submit your Feedback/Queries to our Experts

**NEW QUESTION 104**

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

Please select:

A. Use the request parameters for authorization

B. Use a Lambda authorizer

C. Use the gateway authorizer

D. Use CORS on the API gateway

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following

An Amazon API Gateway Lambda authorizer (formerly known as a custom authorize?) is a Lambda function that you provide to control access to your API methods. A Lambda authorizer uses bearer token authentication strategies, such as OAuth or SAML. It can also use information described by headers, paths, query strings, stage variables, or context variables request parameters.

Options A,C and D are invalid because these cannot be used if you need a custom authentication/authorization for calls made to the API gateway

For more information on using the API gateway Lambda authorizer please visit the URL:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambdaauthorizer.html>

The correct answer is: Use a Lambda authorizer Submit your Feedback/Queries to our Experts

**NEW QUESTION 108**

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 112**

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 CloudFront 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 to 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 114**

You currently operate a web application in the AWS US-East region. The application runs on an autoscaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your EC2, IAM and RDS resources. The solution must ensure the integrity and confidentiality of your log data

- A. Which of these solutions would you recommend? Please select:
- B. Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected
- C. Use IAM roles, S3 bucket policies and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
- D. Create a new CloudTrail with one new S3 bucket to store the log
- E. Configure SNS to send log file delivery notifications to your management system
- F. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs.
- G. Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected
- H. Use S3 ACLs and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
- I. Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tool
- J. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs.

**Answer:** A

**Explanation:**

AWS Identity and Access Management (IAM) is integrated with AWS CloudTrail, a service that logs AWS events made by or on behalf of your AWS account.

CloudTrail logs authenticated AWS API calls and also AWS sign-in events, and collects this event information in files that are delivered to Amazon S3 buckets.

You need to ensure that all services are included. Hence option B is partially correct. Option B is invalid because you need to ensure that global services is selected

Option C is invalid because you should use bucket policies

Option D is invalid because you should ideally just create one S3 bucket For more information on CloudTrail, please visit the below URL:

<http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html>

The correct answer is: Create a new CloudTrail trail with one new S3 bucket to store the logs and with

the global services option selected. Use IAM roles, S3 bucket policies and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs

Submit your Feedback/Queries to our Experts

**NEW QUESTION 119**

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 121**

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 123**

Your company is planning on using bastion hosts for administering the servers in AWS. Which of the following is the best description of a bastion host from a security perspective? Please select:

- A. A Bastion host should be on a private subnet and never a public subnet due to security concerns
- B. A Bastion host sits on the outside of an internal network and is used as a gateway into the private network and is considered the critical strong point of the network
- C. Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources.
- D. A Bastion host should maintain extremely tight security and monitoring as it is available to the public

**Answer: C**

**Explanation:**

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. In AWS, A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets. Options A and B are invalid because the bastion host needs to sit on the public network. Option D is invalid because bastion hosts are not used for monitoring For more information on bastion hosts, just browse to the below URL: <https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html>  
The correct answer is: Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources. Submit your Feedback/Queries to our Experts

**NEW QUESTION 127**

Your CTO is very worried about the security of your AWS account. How best can you prevent hackers from completely hijacking your account? Please select:

- A. Use short but complex password on the root account and any administrators.
- B. Use AWS IAM Geo-Lock and disallow anyone from logging in except for in your city.
- C. Use MFA on all users and accounts, especially on the root account.
- D. Don't write down or remember the root account password after creating the AWS account

**Answer: C**

**Explanation:**

Multi-factor authentication can add one more layer of security to your AWS account Even when you go to your Security Credentials dashboard one of the items is to enable MFA on your root account

Option A is invalid because you need to have a good password policy Option B is invalid because there is no IAM Geo-Lock Option D is invalid because this is not a recommended practice For more information on MFA, please visit the below URL: [http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_mfa.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html)  
The correct answer is: Use MFA on all users and accounts, especially on the root account. Submit your Feedback/Queries to our Experts

**NEW QUESTION 129**

You work at a company that makes use of AWS resources. One of the key security policies is to ensure that all data is encrypted both at rest and in transit. Which of the following is one of the right ways to implement this. Please select:

- A. Use S3 SSE and use SSL for data in transit
- B. SSL termination on the ELB
- C. Enabling Proxy Protocol
- D. Enabling sticky sessions on your load balancer

**Answer: A**

**Explanation:**

By disabling SSL termination, you are leaving an unsecured connection from the ELB to the back end instances. Hence this means that part of the data transit is not being encrypted. Option B is incorrect because this would not guarantee complete encryption of data in transit Option C and D are incorrect because these would not guarantee encryption For more information on SSL Listeners for your load balancer, please visit the below URL: <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.html> The correct answer is: Use S3 SSE and use SSL for data in transit Submit your Feedback/Queries to our Experts

#### NEW QUESTION 132

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 136

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-Certified-Security-Specialty Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AWS-Certified-Security-Specialty Product From:

<https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/>

## Money Back Guarantee

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

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