



# Amazon-Web-Services

## Exam Questions SCS-C01

AWS Certified Security- Specialty

#### NEW QUESTION 1

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

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

**Answer: C**

#### NEW QUESTION 2

Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks? Please select:

- A. Use CloudTrail Log File Integrity Validation.
- B. Use AWS Config SNS Subscriptions and process events in real time.
- C. Use CloudTrail backed up to AWS S3 and Glacier.
- D. Use AWS Config Timeline forensics.

**Answer: A**

#### Explanation:

The AWS Documentation mentions the following

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. You can use the AWS CLI to validate the files in the location where CloudTrail delivered them

Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.

Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs

For more information on Cloudtrail log file validation, please visit the below URL: <http://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html> The correct answer is: Use CloudTrail Log File Integrity Validation.

omit your Feedback/Queries to our Expert

#### NEW QUESTION 3

A Development team has asked for help configuring the IAM roles and policies in a new AWS account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).

Which of the following will allow the team to manage AWS KMS permissions in IAM without the complexity of editing individual key policies?

- A. The account's CMK key policy must allow the account's IAM roles to perform KMS EnableKey.
- B. Newly created CMKs must have a key policy that allows the root principal to perform all actions.
- C. Newly created CMKs must allow the root principal to perform the kms CreateGrant API operation.
- D. Newly created CMKs must mirror the IAM policy of the KMS key administrator.

**Answer: C**

#### NEW QUESTION 4

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 5

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 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 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 1AM 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 6**

Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.

Which of the following solutions will meet these requirements?

- A. Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.
- B. Route all traffic through a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.
- C. Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.
- D. Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer and the EC2 instances.

**Answer:** B

**NEW QUESTION 7**

The Accounting department at Example Corp. has made a decision to hire a third-party firm, AnyCompany, to monitor Example Corp.'s AWS account to help optimize costs.

The Security Engineer for Example Corp. has been tasked with providing AnyCompany with access to the required Example Corp. AWS resources. The Engineer has created an IAM role and granted permission to AnyCompany's AWS account to assume this role.

When customers contact AnyCompany, they provide their role ARN for validation. The Engineer is concerned that one of AnyCompany's other customers might deduce Example Corp.'s role ARN and potentially compromise the company's account.

What steps should the Engineer perform to prevent this outcome?

- A. Create an IAM user and generate a set of long-term credential
- B. Provide the credentials to AnyCompany.Monitor access in IAM access advisor and plan to rotate credentials on a recurring basis.
- C. Request an external ID from AnyCompany and add a condition with sts:ExternalId to the role's trust policy.
- D. Require two-factor authentication by adding a condition to the role's trust policy with aws:MultiFactorAuthPresent.
- E. Request an IP range from AnyCompany and add a condition with aws:SourceIp to the role's trust policy.

**Answer:** B

**NEW QUESTION 8**

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 1AM permissions by applying PutBucketPolicy permissions.
- B. Verify that the policy has the same name as the bucket nam
- 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 9**

A Security Architect is evaluating managed solutions for storage of encryption keys. The requirements are:

- Storage is accessible by using only VPCs.
- Service has tamper-evident controls.
- Access logging is enabled.
- Storage has high availability.

Which of the following services meets these requirements?

- A. Amazon S3 with default encryption
- B. AWS CloudHSM
- C. Amazon DynamoDB with server-side encryption
- D. AWS Systems Manager Parameter Store

**Answer:** B

#### NEW QUESTION 10

The Security Engineer has discovered that a new application that deals with highly sensitive data is storing Amazon S3 objects with the following key pattern, which itself contains highly sensitive data.

Pattern: "randomID\_datestamp\_PII.csv" Example:

"1234567\_12302017\_000-00-0000 csv"

The bucket where these objects are being stored is using server-side encryption (SSE). Which solution is the most secure and cost-effective option to protect the sensitive data?

- A. Remove the sensitive data from the object name, and store the sensitive data using S3 user-defined metadata.
- B. Add an S3 bucket policy that denies the action s3:GetObject
- C. Use a random and unique S3 object key, and create an S3 metadata index in Amazon DynamoDB using client-side encrypted attributes.
- D. Store all sensitive objects in Binary Large Objects (BLOBS) in an encrypted Amazon RDS instance.

**Answer:** C

#### NEW QUESTION 10

Your development team is using access keys to develop an application that has access to S3 and DynamoDB. A new security policy has outlined that the credentials should not be older than 2 months, and should be rotated. How can you achieve this?

Please select:

- A. Use the application to rotate the keys in every 2 months via the SDK
- B. Use a script to query the creation date of the key
- C. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.
- D. Delete the user associated with the keys after every 2 month
- E. Then recreate the user again.
- F. Delete the 1AM Role associated with the keys after every 2 month
- G. Then recreate the 1AM Role again.

**Answer:** B

#### Explanation:

One can use the CLI command list-access-keys to get the access keys. This command also returns the "CreateDate" of the keys. If the CreateDate is older than 2 months, then the keys can be deleted.

The Returns list-access-keys CLI command returns information about the access key IDs associated with the specified 1AM user. If there are none, the action returns an empty list

Option A is incorrect because you might as use a script for such maintenance activities Option C is incorrect because you would not rotate the users themselves

Option D is incorrect because you don't use 1AM roles for such a purpose For more information on the CLI command, please refer to the below Link:

<http://docs.aws.amazon.com/cli/latest/reference/iam/list-access-keys.html>

The correct answer is: Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 14

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

Please select:

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

**Answer:** ACD

#### Explanation:

For ensuring that the instances are configured properly you need to ensure the followi .

1) You installed the latest version of the SSM Agent on your instance

2) Your instance is configured with an AWS Identity and Access Management (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-remote-commands.html>

The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure that agent is running on the Instances., Check the Instance status by using the Health API.

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 18



An organization is moving non-business-critical applications to AWS while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in AWS. The internet performance is unpredictable. Which configuration will ensure continued connectivity between sites MOST securely?

- A. VPN and a cached storage gateway
- B. AWS Snowball Edge
- C. VPN Gateway over AWS Direct Connect
- D. AWS Direct Connect

**Answer:** C

#### NEW QUESTION 19

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

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

**Answer:** B

#### Explanation:

The AWS Documentation mentions the following

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

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

Option D is invalid because this service is used to check for configuration changes For more information on executing remote commands, please visit the below U <https://docs.aws.amazon.com/systems-manageer/latest/userguide/execute-remote-commands.html> (

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

#### NEW QUESTION 23

A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an AWS Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.

Which approach will meet these requirements while protecting the external certificate during a breach?

- A. Use a Network Load Balancer (NLB) to pass through traffic on port 443 from the internet to port 443 on the instances.
- B. Purchase an external certificate, and upload it to the AWS Certificate Manager (for use with the ELB) and to the instance
- C. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.
- D. Generate an internal self-signed certificate and apply it to the instance
- E. Use AWS Certificate Manager to generate a new external certificate for the EL
- F. Have the ELB decrypt traffic, and route and re-encrypt with the internal certificate.
- G. Upload a new external certificate to the load balance
- H. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

**Answer:** C

#### NEW QUESTION 28

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 ODIC 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 30

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 33**

An IAM user with full EC2 permissions could not start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to “Pending”, but after a few seconds, it would switch back to “Stopped”.

An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.

The IAM user policy is as follows:

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

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

**Answer:** CE

**NEW QUESTION 37**

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

Which action should the Security Engineer take to allow communication over the public IP addresses?

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

**Answer:** D

**NEW QUESTION 38**

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-data-events-with-cloudtr> 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 43

A Security Analyst attempted to troubleshoot the monitoring of suspicious security group changes. The Analyst was told that there is an Amazon CloudWatch alarm in place for these AWS CloudTrail log events. The Analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.

Which of the following troubleshooting steps should the Analyst perform?

- A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst's AWS account
- B. Verify that a metric filter was created and then mapped to an alarm
- C. Check the alarm notification action.
- D. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.
- E. Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

**Answer: B**

#### NEW QUESTION 48

A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected.

What is the MOST efficient way to meet these requirements?

- A. Write an AWS Lambda function that logs into the EC2 instance to pull the application logs from the EC2 instance and persists them into an Amazon S3 bucket.
- B. Enable AWS CloudTrail logging for the AWS account, create a new Amazon S3 bucket, and then configure Amazon CloudWatch Logs to receive the application logs from CloudTrail.
- C. Create a simple cron job on the EC2 instances that synchronizes the application logs to an Amazon S3 bucket by using rsync.
- D. Install the Amazon CloudWatch Logs Agent on the EC2 instances, and configure it to send the application logs to CloudWatch Logs.

**Answer: D**

#### NEW QUESTION 50

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 53

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

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

Whether any ports to the database server other than ones from the web server security group are open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?

Please select:

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

**Answer: B**

#### Explanation:

Trusted Advisor checks for compliance with the following security recommendations:

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

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

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

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

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

instance on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and configuration data (telemetry), which it then passes to the Amazon Inspector service.

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

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

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

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

#### NEW QUESTION 58

The Security Engineer for a mobile game has to implement a method to authenticate users so that they can save their progress. Because most of the users are part of the same OpenID-Connect compatible social media website, the Security Engineer would like to use that as the identity provider.

Which solution is the SIMPLEST way to allow the authentication of users using their social media identities?

- A. Amazon Cognito
- B. AssumeRoleWithWebIdentity API
- C. Amazon Cloud Directory
- D. Active Directory (AD) Connector

**Answer: B**

#### NEW QUESTION 59

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

Please select:

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

**Answer: AE**

#### Explanation:

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

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

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

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

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

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

Configure permissions in AWS for your federated users

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

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

C:\Users\wk\Desktop\mudassar\Untitled.jpg

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

What directories can I use with AWS SSO?

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

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

Set up a VPC with the following:

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

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

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 60

Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.

Please select:

A.

B.

C.

D.



A.

**Answer:** A

**Explanation:**

The condition of "s3:x-amz-server-side-encryption":"aws:kms" ensures that objects uploaded need to be encrypted.

Options B,C and D are invalid because you have to ensure the condition of "s3:x-amz-server-side-encryption":"aws:kms" is present

For more information on AWS KMS best practices, just browse to the below URL: <https://dl.awsstatic.com/whitepapers/aws-kms-best-practices.pdf>

C:\Users\wk\Desktop\mudassar\Untitled.jpg

Submit your Feedback/Queries to our Expert

**NEW QUESTION 63**

There is a requirement for a company to transfer large amounts of data between AWS and an on-premise location. There is an additional requirement for low latency and high consistency traffic to AWS. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below

Please select:

- A. Provision a Direct Connect connection to an AWS region using a Direct Connect partner.
- B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.
- C. Create an IPSec tunnel for private connectivity, which increases network consistency and reduces latency.
- D. Create a VPC peering connection between AWS and the Customer gateway.

**Answer:** A

**Explanation:**

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect you can establish private connectivity between AWS and your datacenter, office, or colocation environment which in many cases can reduce your network costs, increase bandwidth throughput and provide a more consistent network experience than Internet-based connections.

Options B and C are invalid because these options will not reduce network latency Options D is invalid because this is only used to connect 2 VPC's

For more information on AWS direct connect, just browse to the below URL: <https://aws.amazon.com/directconnect>

The correct answer is: Provision a Direct Connect connection to an AWS region using a Direct Connect partner. omit your Feedback/Queries to our Experts

**NEW QUESTION 65**

You have been given a new brief from your supervisor for a client who needs a web application set up on AWS. The a 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. C:\Users\wk\Desktop\mudassar\Untitled.jpg

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 69**

An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

Please select:

- A. Create an IAM policy with the security group and use that security group for AWS console login
- B. Create an IAM policy with a condition which denies access when the IP address range is not from the organization
- C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
- D. Create an IAM policy with VPC and allow a secure gateway between the organization and AWS Console

**Answer:** B

**Explanation:**

You can actually use a Deny condition which will not allow the person to log in from outside. The below example shows the Deny condition to ensure that any address specified in the source address is not allowed to access the resources in aws.

Option A is invalid because you don't mention the security group in the 1AM policy Option C is invalid because security groups by default don't allow traffic

Option D is invalid because the 1AM policy does not have such an option For more information on 1AM policy conditions, please visit the URL:

<http://docs.aws.amazon.com/IAM/latest/UserGuide/access>

pol

examples.htm l#iam-policy-example-ec2-two-condition!

The correct answer is: Create an 1AM policy with a condition which denies access when the IP address range is not from the organization

Submit your Feedback/Queries to our Experts

**NEW QUESTION 72**

A company runs an application on AWS that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel.

How can the Security Engineer protect this workload so that only employees can access it?

- A. Add each employee's home IP address to the security group for the application so that only those users can access the workload.
- B. Create a virtual gateway for VPN connectivity for each employee, and restrict access to the workload from within the VPC.
- C. Use a VPN appliance from the AWS Marketplace for users to connect to, and restrict workload access to traffic from that appliance.
- D. Route all traffic to the workload through AWS WA
- E. Add each employee's home IP address into an AWS WAF rule, and block all other traffic.

**Answer: C**

**NEW QUESTION 77**

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/servers.Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- B. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
- C. UseSystems Manager Patch Manger to install the missing patches.
- D. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers.Redeploy all out of1 compliance instances/servers using an AMI with the latest patches.
- E. Use Trusted Advisor to generate the report of out of compliance instances/server
- F. 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 fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

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 78**

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

What should the Security Engineer use to accomplish this?

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

**Answer: B**

**Explanation:**

Reference <https://aws.amazon.com/s3/faqs/>

**NEW QUESTION 83**

What are the MOST secure ways to protect the AWS account root user of a recently opened AWS account? (Choose two.)

- A. Use the AWS account root user access keys instead of the AWS Management Console
- B. Enable multi-factor authentication for the AWS IAM users with the AdministratorAccess managed policy attached to them
- C. Enable multi-factor authentication for the AWS account root user
- D. Use AWS KMS to encrypt all AWS account root user and AWS IAM access keys and set automatic rotation to 30 days
- E. Do not create access keys for the AWS account root user; instead, create AWS IAM users

**Answer:** BD

#### NEW QUESTION 88

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing. Which steps should be taken to troubleshoot the issue? (Choose two.)

- A. Use an EC2 run command to confirm that the “awslogs” service is running on all instances.
- B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.
- C. Check whether any application log entries were rejected because of invalid time stamps by reviewing/var/cwlogs/rejects.log.
- D. Check that the trust relationship grants the service “cwlogs.amazonaws.com” permission to write objects to the Amazon S3 staging bucket.
- E. Verify that the time zone on the application servers is in UTC.

**Answer:** AB

#### NEW QUESTION 90

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

C:\Users\wk\Desktop\mudassar\Untitled.jpg

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 practices 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 93

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

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

**Answer:** A

#### Explanation:

By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explicitly update the default key policy for these keys.

Option B,C and D are invalid because the key policy is the main entity used to provide access to the keys

For more information on upgrading key policies please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-upgrading.html>

The correct answer is: You have not explicitly given access via the key policy Submit your Feedback/Queries to our Experts

#### NEW QUESTION 96

Every application in a company's portfolio has a separate AWS account for development and production. The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality? 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 IAM policy that denies access to the service
- G. Associate the policy with an IAM group and enlist all users and the root users in this group.
- H. Create an IAM policy that denies access to the service
- I. Create a Config Rule that checks that all users have the policy assigned
- 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 IAM 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 IAM 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/UserGuide/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 100

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

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

**Answer: B**

#### Explanation:

Sometimes companies want to have custom solutions in place for monitoring intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.

C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A, C and D are all invalid because they cannot be used to conduct intrusion detection or prevention. For more information on using custom security solutions please visit the below URL [https://d1.awsstatic.com/Marketplace/security/AWSMP\\_Security\\_Solution%20Overview.pdf](https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%20Overview.pdf)

For more information on using custom security solutions please visit the below URL: [https://d1.awsstatic.com/Marketplace/security/AWSMP\\_Security\\_Solution%20Overview.pdf](https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%20Overview.pdf)

The correct answer is: Use a custom solution available in the AWS Marketplace. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 101

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

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

**Answer: C**

#### NEW QUESTION 105

Your company looks at the gaming domain and hosts several EC2 Instances as game servers. The servers each experience user loads in the thousands. There is a concern of DDoS attacks on the EC2 Instances which could cause a huge revenue loss to the company. Which of the following can help mitigate this security concern and also ensure minimum downtime for the servers. Please select:

- A. Use VPC Flow logs to monitor the VPC and then implement NACL's to mitigate attacks
- B. Use AWS Shield Advanced to protect the EC2 Instances
- C. Use AWS Inspector to protect the EC2 Instances
- D. Use AWS Trusted Advisor to protect the EC2 Instances

**Answer: B**

#### Explanation:

Below is an excerpt from the AWS Documentation on some of the use cases for AWS Shield: C:\Users\wk\Desktop\mudassar\Untitled.jpg



#### NEW QUESTION 110

You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks. Which of the following service can help in such a scenario  
Please select:

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

**Answer: B**

#### Explanation:

The AWS Documentation mentions the following

AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. AWS WAF allows you to create rules that can help protect against common web exploits like SQL injection and cross-site scripting. With AWS WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect.

Option A is invalid because this will only give advise on how you can better the security in your AWS account but not protect against threats mentioned in the question.

Option C is invalid because this can be used to scan EC2 Instances for vulnerabilities but not protect against threats mentioned in the question.

Option D is invalid because this can be used to check config changes but not protect against threats mentioned in the quest

For more information on AWS WAF, please visit the following URL: <https://aws.amazon.com/waf/details>;

The correct answer is: AWS WAF

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 114

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

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

**Answer: C**

#### NEW QUESTION 118

Your company has just set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server. Which of the below options is best suited to achieve this requirement.  
Please select:

- A. Set up VPC peering between the central server VPC and each of the teams VPCs.
- B. Set up AWS DirectConnect between the central server VPC and each of the teams VPCs.
- C. Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.
- D. None of the above options will work.

**Answer: A**

#### Explanation:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region.

Options B and C are invalid because you need to use VPC Peering Option D is invalid because VPC Peering is available

For more information on VPC Peering please see the below Link:

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>

The correct answer is: Set up VPC peering between the central server VPC and each of the teams VPCs. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 123

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 MFAto 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 128**

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

Please select:

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

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.

Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles

Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:

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

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

**NEW QUESTION 131**

A Developer who is following AWS best practices for secure code development requires an application to encrypt sensitive data to be stored at rest, locally in the application, using AWS KMS. What is the simplest and MOST secure way to decrypt this data when required?

- A. Request KMS to provide the stored unencrypted data key and then use the retrieved data key to decrypt the data.
- B. Keep the plaintext data key stored in Amazon DynamoDB protected with IAM policies
- C. Query DynamoDB to retrieve the data key to decrypt the data
- D. Use the Encrypt API to store an encrypted version of the data key with another customer managed key. Decrypt the data key and use it to decrypt the data when required.
- E. Store the encrypted data key alongside the encrypted data
- F. Use the Decrypt API to retrieve the data key to decrypt the data when required.

**Answer:** D

**NEW QUESTION 132**

A company requires that IP packet data be inspected for invalid or malicious content. Which of the following approaches achieve this requirement? (Choose two.)

- A. Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through it
- B. Perform inspection within proxy software on the EC2 instance.
- C. Configure the host-based agent on each EC2 instance within the VPC
- D. Perform inspection within the host-based agent.
- E. Enable VPC Flow Logs for all subnets in the VPC
- F. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.
- G. Configure Elastic Load Balancing (ELB) access log
- H. Perform inspection from the log data within the ELB access log files.
- I. Configure the CloudWatch Logs agent on each EC2 instance within the VPC
- J. Perform inspection from the log data within CloudWatch Logs.

**Answer:** AB

**NEW QUESTION 136**

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 139**

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](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 144**

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

Please select:

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

**Answer:** D

**Explanation:**

The AWS blogs mention the following to support the use of AWS GuardDuty

GuardDuty voraciously consumes multiple data streams, including several threat intelligence feeds, staying aware of malicious addresses, devious domains, and more importantly, learning to accurately identify malicious or unauthorized behavior in your AWS accounts. In combination with information gleaned from your VPC Flow Logs, AWS CloudTrail Event Logs, and DNS logs, th allows GuardDuty to detect many different types of dangerous and mischievous behavior including probes for known vulnerabilities, port scans and probes, and access from unusual locations. On the AWS side, it looks for suspicious AWS account activity such as unauthorized deployments, unusual CloudTrail activity, patterns of access to AWS API functions, and attempts to exceed multiple service limits. GuardDuty will also look for compromised EC2 instances talking to malicious entities or services, data exfiltration attempts, and instances that are mining cryptocurrency.

Options A, B and C are invalid because these services cannot be used to detect port scans For more information on AWS Guard Duty, please refer to the below Link:

[https://aws.amazon.com/blogs/aws/amazon-guardduty-continuous-security-monitoring-threat-detection;](https://aws.amazon.com/blogs/aws/amazon-guardduty-continuous-security-monitoring-threat-detection/) (

The correct answer is: Use AWS Guard Duty to monitor any malicious port scans Submit your Feedback/Queries to our Experts

**NEW QUESTION 148**

You want to launch an EC2 Instance with your own key pair in AWS. How can you achieve this? Choose 3 answers from the options given below.

Please select:

- A. Use a third party tool to create the Key pair
- B. Create a new key pair using the AWS CLI
- C. Import the public key into EC2
- D. Import the private key into EC2

**Answer:** ABC

**Explanation:**

This is given in the AWS Documentation Creating a Key Pair

You can use Amazon EC2 to create your key pair. For more information, see Creating a Key Pair Using Amazon EC2.

Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see Importing Your Own Public Key to Amazon EC2.

Option B is Correct, because you can use the AWS CLI to create a new key pair 1 <https://docs.aws.amazon.com/cli/latest/userguide/cli-ec2-keypairs.html>

Option D is invalid because the public key needs to be stored in the EC2 Instance For more information on EC2 Key pairs, please visit the below URL:

\* <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs>

The correct answers are: Use a third party tool to create the Key pair. Create a new key pair using the AWS CLI, Import the public key into EC2

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 151

An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, AWS Lambda functions must issue queries to the RDS database by using the same database credentials.

The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.

What should the Security Engineer do to meet these requirements?

- A. Store the database credentials in AWS Key Management Service (AWS KMS). Create an IAM role with access to AWS KMS by using the EC2 and Lambda service principals in the role's trust policy
- B. Add the role to an EC2 instance profile
- C. Attach the instance profile to the EC2 instance
- D. Set up Lambda to use the new role for execution.
- E. Store the database credentials in AWS KM
- F. Create an IAM role with access to KMS by using the EC2 and Lambda service principals in the role's trust policy
- G. Add the role to an EC2 instance profile
- H. Attach the instance profile to the EC2 instances and the Lambda function.
- I. Store the database credentials in AWS Secrets Manager
- J. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy
- K. Add the role to an EC2 instance profile
- L. Attach the instance profile to the EC2 instances and the Lambda function.
- M. Store the database credentials in AWS Secrets Manager
- N. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy
- O. Add the role to an EC2 instance profile
- P. Attach the instance profile to the EC2 instance
- Q. Set up Lambda to use the new role for execution.

**Answer:** D

#### NEW QUESTION 155

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

Which of the following actions will resolve the access denied error?

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

**Answer:** A

#### NEW QUESTION 158

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

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

**Answer:** C

#### Explanation:

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

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

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

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

|<https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html>|

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

#### NEW QUESTION 163

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

Please select:

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

**Answer:** A

#### Explanation:

Since the Web server needs to talk to the database server on port 3306 that means that the database server should allow incoming traffic on port 3306. The below table from the aws documentation shows how the security groups should be set up.



C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option B is invalid because you need to allow incoming access for the database server from the WebSecGrp security group. Options C and D are invalid because you need to allow Outbound traffic and not inbound traffic For more information on security groups please visit the below Link:

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPCScenario2.html>

The correct answer is: Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 164

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://docsaws.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 165

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

Please select:

- A. Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag
- B. <
- C. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance call.
- D. Modify the 1AM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
- E. Modify the 1AM policy on the user to require MFA before deleting EC2 instances

**Answer: AB**

#### Explanation:

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

Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance. For more information on tagging answer resources please refer to the below URL: [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_Tags.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html)

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

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 168

In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly.

What must be done to prevent users from accessing the S3 objects directly by using URLs?

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

**Answer:** B

#### NEW QUESTION 172

While analyzing a company's security solution, a Security Engineer wants to secure the AWS account root user. What should the Security Engineer do to provide the highest level of security for the account?

- A. Create a new IAM user that has administrator permissions in the AWS account
- B. Delete the password for the AWS account root user.
- C. Create a new IAM user that has administrator permissions in the AWS account
- D. Modify the permissions for the existing IAM users.
- E. Replace the access key for the AWS account root user
- F. Delete the password for the AWS account root user.
- G. Create a new IAM user that has administrator permissions in the AWS account
- H. Enable multi-factor authentication for the AWS account root user.

**Answer:** D

#### Explanation:

If you continue to use the root user credentials, we recommend that you follow the security best practice to enable multi-factor authentication (MFA) for your account. Because your root user can perform sensitive operations in your account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available.

#### NEW QUESTION 176

AWS CloudTrail is being used to monitor API calls in an organization. An audit revealed that CloudTrail is failing to deliver events to Amazon S3 as expected. What initial actions should be taken to allow delivery of CloudTrail events to S3? (Select two.)

- A. Verify that the S3 bucket policy allow CloudTrail to write objects.
- B. Verify that the IAM role used by CloudTrail has access to write to Amazon CloudWatch Logs.
- C. Remove any lifecycle policies on the S3 bucket that are archiving objects to Amazon Glacier.
- D. Verify that the S3 bucket defined in CloudTrail exists.
- E. Verify that the log file prefix defined in CloudTrail exists in the S3 bucket.

**Answer:** AD

#### NEW QUESTION 181

A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation. What should the Security Engineer use to isolate and research this event? (Choose three.)

- A. AWS CloudTrail
- B. Amazon Athena
- C. AWS Key Management Service (AWS KMS)
- D. VPC Flow Logs
- E. AWS Firewall Manager
- F. Security groups

**Answer:** ADF

#### NEW QUESTION 183

You have an instance setup in a test environment in AWS. You installed the required application and then 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 185

The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock 12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault. What is the MOST cost-effective way to correct this?

- A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.
- B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.
- C. Update the policy, keeping the vault lock in place.
- D. Update the policy and call initiate-vault-lock again to apply the new policy.

**Answer:** A

#### NEW QUESTION 187

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/>

The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy Submit your Feedback/Queries to our Experts

#### NEW QUESTION 191


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

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

**Answer:** B

#### Explanation:

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

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

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

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

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

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

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

#### NEW QUESTION 196

A Security Engineer who was reviewing AWS Key Management Service (AWS KMS) key policies found this statement in each key policy in the company AWS account.

What does the statement allow?

- A. All principals from all AWS accounts to use the key.
- B. Only the root user from account 111122223333 to use the key.
- C. All principals from account 111122223333 to use the key but only on Amazon S3.
- D. Only principals from account 111122223333 that have an IAM policy applied that grants access to this key to use the key.

**Answer:** D

#### NEW QUESTION 198

An organization is using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon CloudWatch to send alerts when new access keys are created. However, the alerts are no longer appearing in the Security Operations mail box.

Which of the following actions would resolve this issue?

- A. In CloudTrail, verify that the trail logging bucket has a log prefix configured.
- B. In Amazon SNS, determine whether the "Account spend limit" has been reached for this alert.
- C. In SNS, ensure that the subscription used by these alerts has not been deleted.
- D. In CloudWatch, verify that the alarm threshold "consecutive periods" value is equal to, or greater than 1.

**Answer:** B

#### NEW QUESTION 200

A financial institution has the following security requirements:

Cloud-based users cannot access on-premises systems.

As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.

How would the organization manage its resources in the MOST secure manner? (Choose two.)

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

**Answer:** AD

#### NEW QUESTION 202

A company has a requirement to create a DynamoDB table. The company's software architect has provided the following CLI command for the DynamoDB table

Which of the following has been taken of from a security perspective from the above command? Please select:

- A. Since the ID is hashed, it ensures security of the underlying table.
- B. The above command ensures data encryption at rest for the Customer table
- C. The above command ensures data encryption in transit for the Customer table
- D. The right throughput has been specified from a security perspective

**Answer:** B

#### Explanation:

The above command with the "-sse-specification Enabled=true" parameter ensures that the data for the DynamoDB table is encrypted at rest.

Options A,C and D are all invalid because this command is specifically used to ensure data encryption at rest For more information on DynamoDB encryption, please visit the URL: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/encryption.tutorial.html>

The correct answer is: The above command ensures data encryption at rest for the Customer table

#### NEW QUESTION 204

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

Please select:

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

**Answer:** A

#### Explanation:

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

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

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

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

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

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 206

An Amazon EC2 instance is part of an EC2 Auto Scaling group that is behind an Application Load Balancer (ALB). It is suspected that the EC2 instance has been compromised.

Which steps should be taken to investigate the suspected compromise? (Choose three.)

- A. Detach the elastic network interface from the EC2 instance.
- B. Initiate an Amazon Elastic Block Store volume snapshot of all volumes on the EC2 instance.
- C. Disable any Amazon Route 53 health checks associated with the EC2 instance.



- D. De-register the EC2 instance from the ALB and detach it from the Auto Scaling group.
- E. Attach a security group that has restrictive ingress and egress rules to the EC2 instance.
- F. Add a rule to an AWS WAF to block access to the EC2 instance.

**Answer:** BDE

#### NEW QUESTION 210

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

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

**Answer:** BC

#### Explanation:

Below is the snapshot of the Shared Responsibility Model

C:\Users\wk\Desktop\mudassar\Untitled.jpg

For more information on AWS Security best practises, please refer to below URL [awsstatic.com/whitepapers/Security/AWS Practices](https://awsstatic.com/whitepapers/Security/AWS%20Practices.pdf).

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

#### NEW QUESTION 215

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

Please select:

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

**Answer:** C

#### Explanation:

The SSM Run command can be used to send OS specific commands to an Instance. Here you can check and see the running processes on an instance and then send the output to an S3 bucket.

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

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

For more information on the Systems Manager Run command, please visit the following URL:

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

The correct answer is: Use the SSM Run command to send the list of running processes information to an S3 bucket. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 220

A company is hosting sensitive data in an AWS S3 bucket. It needs to be ensured that the bucket always remains private. How can this be ensured continually?

Choose 2 answers from the options given below

Please select:

- A. Use AWS Config to monitor changes to the AWS Bucket
- B. Use AWS Lambda function to change the bucket policy
- C. Use AWS Trusted Advisor API to monitor the changes to the AWS Bucket
- D. Use AWS Lambda function to change the bucket ACL

**Answer:** AD

#### Explanation:

One of the AWS Blogs mentions the usage of AWS Config and Lambda to achieve this. Below is the diagram representation of this

C:\Users\wk\Desktop\mudassar\Untitled.jpg

ption C is invalid because the Trusted Advisor API cannot be used to monitor changes to the AWS Bucket Option B doesn't seems to be the most appropriate.

1. If the object is in a bucket in which all the objects need to be private and the object is not private anymore, the Lambda function makes a PutObjectAcl call to S3 to make the object private.

[https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintended-permissions-in-a](https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintended-permissions-in-a-bucket/) The following link also specifies that

Create a new Lambda function to examine an Amazon S3 buckets ACL and bucket policy. If the bucket ACL is found to be public access, the Lambda function overwrites it to be private. If a bucket policy is found, the Lambda function creates an SNS message, puts the policy in the message body, and publishes it to the Amazon SNS topic we created. Bucket policies can be complex, and overwriting your policy may cause unexpected loss of access, so this Lambda function doesn't attempt to alter your policy in any way.

[https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-bucke](https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-bucket-permissions-changes/) Based on these facts Option D seems to be more appropriate than Option B.

For more information on implementation of this use case, please refer to the Link:

[https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-bucke](https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-bucket-permissions-changes/)

The correct answers are: Use AWS Config to monitor changes to the AWS Bucket Use AWS Lambda function to change the bucket ACL

#### NEW QUESTION 224

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

Please select:

- A. Apply Multi-AZ for the underlying S3 bucket
- B. Copy the data to an EBS Volume in another Region
- C. Create a snapshot of the S3 bucket and copy it to another region
- D. Enable Cross region replication for the S3 bucket

**Answer:** D

**Explanation:**

This is mentioned clearly as a use case for S3 cross-region replication

You might configure cross-region replication on a bucket for various reasons, including the following:

- Compliance requirements - Although, by default Amazon S3 stores your data across multiple geographically distant Availability Zones, compliance requirements might dictate that you store data at even further distances. Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these compliance requirements.

Option A is invalid because Multi-AZ cannot be used to S3 buckets

Option B is invalid because copying it to an EBS volume is not a recommended practice

Option C is invalid because creating snapshots is not possible in S3

For more information on S3 cross-region replication, please visit the following URL: <https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>

The correct answer is: Enable Cross region replication for the S3 bucket Submit your Feedback/Queries to our Experts

**NEW QUESTION 227**

The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.

What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

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

**Answer:** BC

**NEW QUESTION 232**

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

Please select:

- A. Use KMS and the normal KMS encryption keys
- B. Use KMS and use an external key material
- C. Use S3 Server Side encryption
- D. Use Cloud HSM

**Answer:** D

**Explanation:**

The AWS Documentation mentions the following

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

Option A,B and C are invalid because in all of these cases, the management of the key will be with AWS. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM

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

The correct answer is: Use Cloud HSM Submit your Feedback/Queries to our Experts

**NEW QUESTION 235**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questons and Answers in PDF Format

### SCS-C01 Practice Exam Features:

- \* SCS-C01 Questions and Answers Updated Frequently
- \* SCS-C01 Practice Questions Verified by Expert Senior Certified Staff
- \* SCS-C01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SCS-C01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SCS-C01 Practice Test Here](#)**