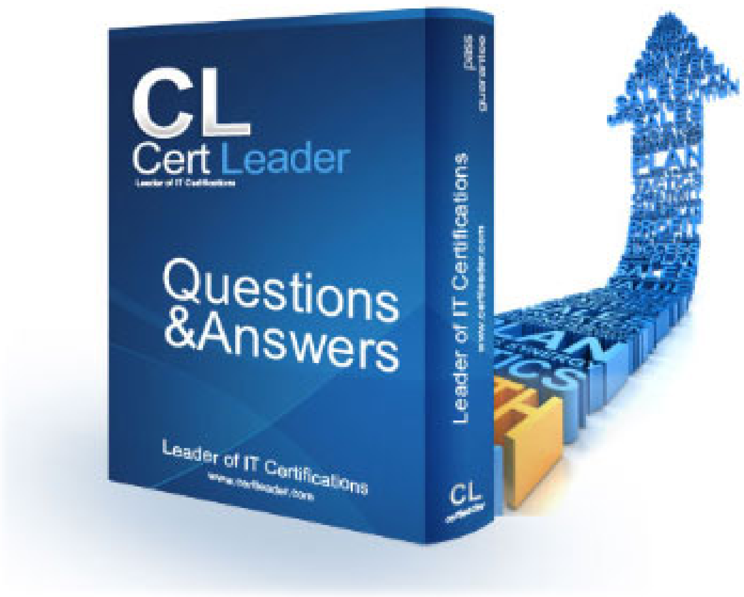
AWS-Certified-Security-Specialty Dumps

Amazon AWS Certified Security - Specialty

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



NEW QUESTION 1
A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?
Please select:

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

Answer: C

Explanation:
Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.
Option D is invalid since just changing the Inbound Rules is sufficient The AWS Documentation mentions the following
A network access control list (ACLJ is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.
The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

NEW QUESTION 2
You are designing a custom 1AM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?
A.

B.

C.

D.

A.

Answer: A

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

NEW QUESTION 3
Your company has an EC2 Instance that is hosted in an AWS VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

A. Stream the log files to a separate Cloudtrail trail
B. Stream the log files to a separate Cloudwatch Log group

C. Create an 1AM policy that gives the desired level of access to the Cloudtrail trail
D. Create an 1AM policy that gives the desired level of access to the Cloudwatch Log group

Answer: BD

Explanation:
You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an 1AM policy.
Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement
For more information on Log Groups and Log Streams, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Workinj
For more information on Access to Cloudwatch logs, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an 1AM policy that gives the desired level of access to the Cloudwatch Log group
Submit your Feedback/Queries to our Experts

NEW QUESTION 4
A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table.
The function is triggered whenever an object is stored within the S3 bucket.
How should the Lambda function be given access to the DynamoDB table? Please select:

A. Create a VPC endpoint for DynamoDB within a VP
B. Configure the Lambda function to access resources in the VPC.
C. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB tabl
D. Attach the poll to the DynamoDB table.
E. Create an 1AM user with permissions to write to the DynamoDB tabl
F. Store an access key for that user in the Lambda environment variables.
G. Create an 1AM service role with permissions to write to the DynamoDB tabl
H. Associate that role with the Lambda function.

Answer: D

Explanation:
The ideal way is to create an 1AM role which has the required permissions and then associate it with the Lambda function
The AWS Documentation additionally mentions the following
Each Lambda function has an 1AM role (execution role) associated with it. You specify the 1AM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the 1AM role:
If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.
If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.
Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB
Option B is invalid because resources policies are present for resources such as S3 and KMS, but not AWS Lambda
Option C is invalid because AWS Roles should be used and not 1AM Users
For more information on the Lambda permission model, please visit the below URL: https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html
The correct answer is: Create an 1AM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.
Submit your Feedback/Queries to our Exp

NEW QUESTION 5
You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?
Please select:

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

Answer: C

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

NEW QUESTION 6
You have an instance setup in a test environment in AWS. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?
Please select:

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

Answer: B

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

NEW QUESTION 7
Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?
Please select:

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

Answer: B

Explanation:
The AWS Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-ofservice 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 Dis 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 8
You have enabled Cloudtrail logs for your company's AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?
Please select:

A. Enable SSL certificates for the Cloudtrail logs
B. There is no need to do anything since the logs will already be encrypted
C. Enable Server side encryption for the trail
D. Enable Server side encryption for the destination S3 bucket

Answer: B

Explanation:
The AWS Documentation mentions the following.
By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encryption your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about lo file delivery and validation, you can set up Amazon SNS notifications.
Option A.C and D are not valid since logs will already be encrypted
For more information on how Cloudtrail works, please visit the following URL: https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/how-cloudtrail-works.htmll
The correct answer is: There is no need to do anything since the logs will already be encrypted Submit your Feedback/Queries to our Experts

NEW QUESTION 9
You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.
Please select:

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

Answer: B

Explanation:
Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application
Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application
Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application
The AWS Documentation mentions the following
VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security toi to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors.
For more information on AWS Security, please visit the following URL: https://aws.amazon.com/answers/networking/vpc-security-capabilities>
The correct answer is: Use VPC Flow logs to diagnose the traffic Submit your Feedback/Queries to our Experts

NEW QUESTION 10
Which of the following is not a best practice for carrying out a security audit? Please select:

A. Conduct an audit on a yearly basis
B. Conduct an audit if application instances have been added to your account
C. Conduct an audit if you ever suspect that an unauthorized person might have accessed your account
D. Whenever there are changes in your organization

Answer: A

Explanation:
A year's time is generally too long a gap for conducting security audits The AWS Documentation mentions the following
You should audit your security configuration in the following situations: On a periodic basis.
If there are changes in your organization, such as people leaving.
If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need.
If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWor stacks, AWS CloudFormation templates, etc.
If you ever suspect that an unauthorized person might have accessed your account.
Option B, C and D are all the right ways and recommended best practices when it comes to conducting audits For more information on Security Audit guideline, please visit the below URL: https://docs.aws.amazon.com/eeneral/latest/gr/aws-security-audit-euide.html
The correct answer is: Conduct an audit on a yearly basis Submit your Feedback/Queries to our Experts

NEW QUESTION 10
Which of the following is used as a secure way to log into an EC2 Linux Instance? Please select:

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

Answer: B

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

NEW QUESTION 12
A company has a set of resources defined in AWS. It is mandated that all API calls to the resources be monitored. Also all API calls must be stored for lookup purposes. Any log data greater than 6 months must be archived. Which of the following meets these requirements? Choose 2 answers from the options given below. Each answer forms part of the solution.
Please select:

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

Answer: AD

Explanation:
Cloudtrail publishes the trail of API logs to an S3 bucket
Option B is invalid because you cannot put the logs into Glacier from CloudTrail
Option C is invalid because lifecycle policies cannot be used to move data to EBS volumes For more information on Cloudtrail logging, please visit the below URL: https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/cloudtrail-find-log-files.htmll

You can then use Lifecycle policies to transfer data to Amazon Glacier after 6 months For more information on S3 lifecycle policies, please visit the below URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html
The correct answers are: Enable CloudTrail logging in all accounts into S3 buckets. Ensure a lifecycle policy is defined on the bucket to move the data to Amazon Glacier after 6 months.
Submit your Feedback/Queries to our Experts

NEW QUESTION 16
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 20
Your company makes use of S3 buckets for storing dat

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

Answer: B

Explanation:
This is given in the AWS Documentation as an example rule in AWS Config Example rules with triggers
Example rule with configuration change trigger
1. You add the AWS Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.
Option A is invalid because AWS Inspector cannot be used to scan all buckets
Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets.
For more information on Config Rules please see the below Link: https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html
The correct answer is: Use AWS Config Rules to check whether logging is enabled for buckets Submit your Feedback/Queries to our Experts

NEW QUESTION 23
A security engineer must ensure that all infrastructure launched in the company AWS account be monitored for deviation from compliance rules, specifically that all EC2 instances are launched from one of a specified list of AM Is and that all attached EBS volumes are encrypted. Infrastructure not in compliance should be terminated. What combination of steps should the Engineer implement? Select 2 answers from the options given below.
Please select:

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

Answer: BD

Explanation:
You can use AWS Config to monitor for such Event
Option A is invalid because you cannot set Cloudwatch events based on Trusted Advisor checks.
Option C is invalid Amazon inspector cannot be used to check whether instances are launched from a specific A
Option E is invalid because triggering a CLI command is not the preferred option, instead you should use Lambda functions for all automation purposes.
For more information on Config Rules please see the below Link: https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html
These events can then trigger a lambda function to terminate instances For more information on Cloudwatch events please see the below Link:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.
(
The correct answers are: Trigger a Lambda function from a scheduled Cloudwatch event that terminates non-compliant infrastructure., Monitor compliance with AWS Config Rules triggered by configuration changes
Submit your Feedback/Queries to our Experts

NEW QUESTION 26
A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement?
Please select:

A. Access the S3 bucket through a proxy server
B. Access the S3 bucket through a NAT gateway.
C. Access the S3 bucket through a VPC endpoint for S3
D. Access the S3 bucket through the SSL protected S3 endpoint

Answer: C

Explanation:
The AWS Documentation mentions the following
A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.
Option A is invalid because using a proxy server is not sufficient enough
Option B and D are invalid because you need secure communication which should not traverse the internet
For more information on VPC endpoints please see the below link https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.htmll
The correct answer is: Access the S3 bucket through a VPC endpoint for S3 Submit your Feedback/Queries to our Experts

NEW QUESTION 31
Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company's EC2 instances?
Please select:

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

Answer: D

Explanation:
Option B is incorrect because querying Trusted Advisor API's are not possible
Option C is incorrect because GuardDuty should be used to detect threats and not check the compliance of security protocols.
Option D states that Run Amazon Inspector using runtime behavior analysis rules which will analyze the behavior of your instances during an assessment run, and provide guidance about how to make your EC2 instances more secure.
Insecure Server Protocols
This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.
For more information, please refer to below URL: https://docs.aws.amazon.eom/mspector/latest/userguide/inspector_runtime-behavioranalysis. html#insecure-protocols
(
The correct answer is: Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.
Submit your Feedback/Queries to our Experts

NEW QUESTION 34
A company is planning on extending their on-premise AWS Infrastructure to the AWS Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum. Which of the following would help fulfil this requirement? Choose 2 answers from the options given below
Please select:

A. AWS VPN
B. AWS VPC Peering
C. AWS NAT gateways
D. AWS Direct Connect

Answer: AD

Explanation:
The AWS Document mention the following which supports the requirement

Option B is invalid because VPC peering is only used for connection between VPCs and cannot be used to connect On-premise infrastructure to the AWS Cloud.
Option C is invalid because NAT gateways is used to connect instances in a private subnet to the internet For more information on VPN Connections, please visit the following url https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/pn-connections.html
The correct answers are: AWS VPN, AWS Direct Connect Submit your Feedback/Queries to our Experts

NEW QUESTION 39
Which technique can be used to integrate AWS 1AM (Identity and Access Management) with an on Questions & Answers PDF P-63
premise LDAP (Lightweight Directory Access Protocol) directory service? Please select:

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

Answer: B

Explanation:
On the AWS Blog site the following information is present to help on this context
The newly released whitepaper. Single Sign-On: Integrating AWS, OpenLDAP, and Shibboleth, will help you integrate your existing LDAP-based user directory with AWS. When you integrate your existing directory with AWS, your users can access AWS by using their existing credentials. This means that your users don't need to maintain yet another user name and password just to access AWS resources.
Option A.C and D are all invalid because in this sort of configuration, you have to use SAML to enable single sign on.
For more information on integrating AWS with LDAP for Single Sign-On, please visit the following URL:
https://aws.amazon.eom/blogs/security/new-whitepaper-sinEle-sign-on-inteErating-aws-openldapand- shibboleth/l
The correct answer is: Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP. Submit your Feedback/Queries to our Experts

NEW QUESTION 44
A company has resources hosted in their AWS Account. There is a requirement to monitor all API activity for all regions. The audit needs to be applied for future regions as well. Which of the following can be used to fulfil this requirement.
Please select:

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

Answer: B

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

NEW QUESTION 46
One of your company's EC2 Instances have been compromised. The company has strict po thorough investigation on finding the culprit for the security breach. What would you do in from the options given below.
Please select:

A. Take a snapshot of the EBS volume
B. Isolate the machine from the network
C. Make sure that logs are stored securely for auditing and troubleshooting purpose
D. Ensure all passwords for all 1AM users are changed
E. Ensure that all access kevs are rotate

Answer: ABC

Explanation:
Some of the important aspects in such a situation are
1) First isolate the instance so that no further security harm can occur on other AWS resources
2) Take a snapshot of the EBS volume for further investigation. This is incase if you need to shutdown the initial instance and do a separate investigation on the data
3) Next is Option C. This indicates that we have already got logs and we need to make sure that it is stored securely so that n unauthorised person can access it and manipulate it.
Option D and E are invalid because they could have adverse effects for the other 1AM users. For more information on adopting a security framework, please refer to below URL https://d1 .awsstatic.com/whitepapers/compliance/NIST Cybersecurity Framework
Note:
In the question we have been asked to take actions to find the culprit and to help the investigation or to further reduce the damage that has happened due to the security breach. So by keeping logs secure is one way of helping the investigation.
The correct answers are: Take a snapshot of the EBS volume. Isolate the machine from the network. Make sure that logs are stored securely for auditing and troubleshooting purpose
Submit your Feedback/Queries to our Experts

NEW QUESTION 50
A company has set up the following structure to ensure that their S3 buckets always have logging enabled

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

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

Answer: B

Explanation:
The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes.
Option A is invalid because this is more of a permission instead of a configuration rule issue. Option C is invalid because changing the language will not be the core solution.
Option D is invalid because you don't necessarily need to use the API gateway service
For more information on accessing resources from a Lambda function, please refer to below URL https://docs.aws.amazon.com/lambda/latest/ds/accessing-resources.htmll
The correct answer is: The AWS Lambda function does not have appropriate permissions for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 51
Your company has a set of EBS volumes defined in AWS. The security mandate is that all EBS volumes are encrypted. What can be done to notify the IT admin staff if there are any unencrypted volumes in the account.
Please select:

A. Use AWS Inspector to inspect all the EBS volumes
B. Use AWS Config to check for unencrypted EBS volumes
C. Use AWS Guard duty to check for the unencrypted EBS volumes
D. Use AWS Lambda to check for the unencrypted EBS volumes

Answer: B

Explanation:
The enc config rule for AWS Config can be used to check for unencrypted volumes. encrypted-volurrn
5 volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryptio using the kmsld parameter, the rule checks if the EBS volumes in an attached state are encrypted
with that KMS key*1.
Options A and C are incorrect since these services cannot be used to check for unencrypted EBS volumes
Option D is incorrect because even though this is possible, trying to implement the solution alone with just the Lambda servk
would be too difficult
For more information on AWS Config and encrypted volumes, please refer to below URL:
https://docs.aws.amazon.com/config/latest/developerguide/encrypted-volumes.html Submit your Feedback/Queries to our Experts

NEW QUESTION 56
You have a bucket and a VPC defined in AWS. You need to ensure that the bucket can only be accessed by the VPC endpoint. How can you accomplish this?
Please select:

A. Modify the security groups for the VPC to allow access to the 53 bucket
B. Modify the route tables to allow access for the VPC endpoint
C. Modify the 1AM Policy for the bucket to allow access for the VPC endpoint
D. Modify the bucket Policy for the bucket to allow access for the VPC endpoint

Answer: D

Explanation:
This is mentioned in the AWS Documentation Restricting Access to a Specific VPC Endpoint
The following is an example of an S3 bucket policy that restricts access to a specific bucket,
examplebucket only from the VPC endpoint with the ID vpce-la2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The aws:sourceVpce condition is used to the specify the endpoint. The aws:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

Options A and B are incorrect because using Security Groups nor route tables will help to allow access specifically for that bucke via the VPC endpoint Here you specifically need to ensure the bucket policy is changed.
Option C is incorrect because it is the bucket policy that needs to be changed and not the 1AM policy. For more information on example bucket policies for VPC endpoints, please refer to below URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html
The correct answer is: Modify the bucket Policy for the bucket to allow access for the VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 61
In order to encrypt data in transit for a connection to an AWS RDS instance, which of the following would you implement
Please select:

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

Answer: B

Explanation:
This is mentioned in the AWS Documentation
You can use SSL from your application to encrypt a connection to a DB instance running MySQL MariaDB, Amazon Aurora, SQL Server, Oracle, or PostgreSQL.
Option A is incorrect since Transparent data encryption is used for data at rest and not in transit Options C and D are incorrect since keys can be used for encryption of data at rest
For more information on working with RDS and SSL, please refer to below URL:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html
The correct answer is: SSL from your application Submit your Feedback/Queries to our Experts

NEW QUESTION 62
A Devops team is currently looking at the security aspect of their CI/CD pipeline. They are making use of AWS resource? for their infrastructure. They want to ensure that the EC2 Instances don't have any high security vulnerabilities. They want to ensure a complete DevSecOps process. How can this be achieved?

Please select:

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

Answer: B

Explanation:
Amazon Inspector offers a programmatic way to find security defects or misconfigurations in your operating systems and applications. Because you can use API calls to access both the processing of assessments and the results of your assessments, integration of the findings into workflow and notification systems is simple. DevOps teams can integrate Amazon Inspector into their CI/CD pipelines and use it to identify any pre-existing issues or when new issues are introduced.
Option A.C and D are all incorrect since these services cannot check for Security Vulnerabilities. These can only be checked by the AWS Inspector service.
For more information on AWS Security best practices, please refer to below URL: https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdl
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 67
You want to track access requests for a particular S3 bucket. How can you achieve this in the easiest possible way?
Please select:

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

Answer: A

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

NEW QUESTION 70
Your application currently use AWS Cognito for authenticating users. Your application consists of different types of users. Some users are only allowed read access to the application and others are given contributor access. How wou you manage the access effectively?
Please select:

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

Answer: B

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

NEW QUESTION 74
An auditor needs access to logs that record all API events on AWS. The auditor only needs read-only access to the log files and does not need access to each AWS account. The company has multiple AWS accounts, and the auditor needs access to all the logs for all the accounts. What is the best way to configure access for the auditor to view event logs from all accounts? Choose the correct answer from the options below
Please select:

A. Configure the CloudTrail service in each AWS account, and have the logs delivered to an AWS bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary 1AM account that can assume a read-only role in the secondary AWS accounts.
B. Configure the CloudTrail service in the primary AWS account and configure consolidated billing for all the secondary account
C. Then grant the auditor access to the S3 bucket that receives theCloudTrail log files.
D. Configure the CloudTrail service in each AWS account and enable consolidated logging inside of CloudTrail.
E. Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bucket in the primary account and erant the auditor access to that single bucket in the orimarvaccoun

Answer: D

Explanation:
Given the current requirements, assume the method of "least privilege" security design and only allow the auditor access to the minimum amount of AWS resources as possibli
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events
related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS

Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting
only be granted access in one location
Option Option A is incorrect since the auditor should B is incorrect since consolidated billing is not a key requirement as part of the question
Option C is incorrect since there is not consolidated logging
For more information on Cloudtrail please refer to the below URL: https://aws.amazon.com/cloudtraiL
(
The correct answer is: Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bud in the primary account and grant the auditor access to that single bucket in the primary account.
Submit your Feedback/Queries to our Experts

NEW QUESTION 79
A large organization is planning on AWS to host their resources. They have a number of autonomous departments that wish to use AWS. What could be the strategy to adopt for managing the accounts. Please select:

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

Answer: D

Explanation:
A recommendation for this is given in the AWS Security best practices

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

NEW QUESTION 83
A company has been using the AW5 KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below
Please select:

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

Answer: BC

Explanation:
The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs
Option A is invalid because seeing how long ago the key was created would not determine the usage of the key
Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the AWS Documentation
Examining CMK Permissions to Determine the Scope of Potential Usage
Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an AWS KMS Customer Master Key.
Examining AWS CloudTrail Logs to Determine Actual Usage
AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is
located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it
For more information on determining the usage of CMK keys, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html
The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key Submit your Feedback/Queries to our Experts

NEW QUESTION 87
Which of the following is the correct sequence of how KMS manages the keys when used along with the Redshift cluster service
Please select:

A. The master keys encrypts the cluster ke
B. The cluster key encrypts the database ke
C. The database key encrypts the data encryption keys.
D. The master keys encrypts the database ke
E. The database key encrypts the data encryption keys.
F. The master keys encrypts the data encryption key
G. The data encryption keys encrypts the database key
H. The master keys encrypts the cluster key, database key and data encryption keys

Answer: A

Explanation:
This is mentioned in the AWS Documentation
Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a master key.
Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomlygenerated AES-256 key. These keys are encrypted by using the database key for the cluster.
The database key encrypts data encryption keys in the cluster. The database key is a randomlygenerated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster
and passed to the cluster across a secure channel.
The cluster key encrypts the database key for the Amazon Redshift cluster.
Option B is incorrect because the master key encrypts the cluster key and not the database key Option C is incorrect because the master key encrypts the cluster key and not the data encryption keys
Option D is incorrect because the master key encrypts the cluster key only
For more information on how keys are used in Redshift, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developereuide/services-redshift.html
The correct answer is: The master keys encrypts the cluster key. The cluster key encrypts the database key. The database key encrypts the data encryption keys.
Submit your Feedback/Queries to our Experts

NEW QUESTION 90
A company wants to use Cloudtrail for logging all API activity. They want to segregate the logging of data events and management events. How can this be achieved? Choose 2 answers from the options given below
Please select:

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

Answer: BC

Explanation:
The AWS Documentation mentions the following
You can configure multiple trails differently so that the trails process and log only the events that you specify. For example, one trail can log read-only data and management events, so that all read-only events are delivered to one S3 bucket. Another trail can log only write-only data and management events, so that all write-only events are delivered to a separate S3 bucket
Options A and D are invalid because you have to create a trail and not a log group
For more information on managing events with cloudtrail, please visit the following URL:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/loHEing-manasement-and-dataevents- with-cloudtrai
The correct answers are: Create one trail that logs data events to an S3 bucket. Create another trail that logs management events to another S3 bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 91
An application is designed to run on an EC2 Instance. The applications needs to work with an S3 bucket. From a security perspective , what is the ideal way for the EC2 instance/ application to be configured?
Please select:

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

Answer: C

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

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

NEW QUESTION 92
You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your server's on-premises will be communicating with your VPC instances. You will be establishing IPSec
tunnels over the internet. Yo will be using VPN gateways and terminating the IPsec tunnels on AWSsupported customer gateways. Which of the following

objectives would you achieve by
implementing an IPSec tunnel as outlined above? Choose 4 answers form the options below Please select:

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

Answer: CDEF

Explanation:
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.

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

NEW QUESTION 96
Your IT Security team has identified a number of vulnerabilities across critical EC2 Instances in the company's AWS Account. Which would be the easiest way to ensure these vulnerabilities are remediated?
Please select:

A. Create AWS Lambda functions to download the updates and patch the servers.
B. Use AWS CLI commands to download the updates and patch the servers.
C. Use AWS inspector to patch the servers
D. Use AWS Systems Manager to patch the servers

Answer: D

Explanation:
The AWS Documentation mentions the following
You can quickly remediate patch and association compliance issues by using Systems Manager Run Command. You can tat either instance IDs or Amazon EC2 tags and execute the AWSRefreshAssociation document or the AWS-RunPatchBaseline document. If refreshing the association
or re-running the patch baseline fails to resolve the compliance issue, then you need to investigate your associations, patch baselines, or instance configurations to understand why the Run Command executions did not resolve the problem
Options A and B are invalid because even though this is possible, still from a maintenance perspective it would be difficult to maintain the Lambda functions
Option C is invalid because this service cannot be used to patch servers
For more information on using Systems Manager for compliance remediation please visit the below Link:
https://docs.aws.amazon.com/systems-manaeer/latest/usereuide/sysman-compliance-fixing.html The correct answer is: Use AWS Systems Manager to patch the servers Submit your Feedback/Queries to our Experts

NEW QUESTION 97
You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script

from S3 that deploys an application via GIT.
Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.
Please select:

A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
D. EC2 instances in our private subnet, no EIPs, route outgoing traffic via the NAT

Answer: D

Explanation:
The below diagram shows how the NAT instance works. To make EC2 instances very secure, they need to be in a private sub such as the database server shown below with no EIP and all traffic routed via the NAT.

Options A and B are invalid because the instances need to be in the private subnet
Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance
For more information on NAT instance, please refer to the below Link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC lnstance.html!
The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

NEW QUESTION 100
Your team is experimenting with the API gateway service for an application. There is a need to implement a custom module which can be used for authentication/authorization for calls made to the API gateway. How can this be achieved?
Please select:

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

Answer: B

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

NEW QUESTION 104
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

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 PutObjectAcI call to S3 to make the object private.
|https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintendedpermissions- in-amazon-s3-bbiect-acls-with-cloudwatch-events/
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 al public access, the Lambda function overwrites it to be private. If a bucket policy is found, the Lambda function creatt 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-toamazon- s3-buckets-allowinj
Based on these facts Option D seems to be more appropriate then 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-toamazon- s3-buckets-allowinj
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 109
There is a requirement for a company to transfer large amounts of data between AWS and an onpremise 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 gatewa

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 InternetQuestions
& Answers PDF P-140 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 113
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 S5H 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.htl
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 118
You work at a company that makes use of AWS resources. One of the key security policies is to ensure that all data i encrypted both at rest and in transit. Which of the following is one of the right ways to implement this.
Please select:

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

Answer: A

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

NEW QUESTION 120
......