



# Amazon-Web-Services

## Exam Questions SCS-C01

AWS Certified Security- Specialty

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

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/awscloudtrail/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 2

Your developer is using the KMS service and an assigned key in their Java program. They get the below error when running the code `arn:aws:iam::113745388712:user/UserB` is not authorized to perform: `kms:DescribeKey` Which of the following could help resolve the issue?

Please select:

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

**Answer:** C

#### Explanation:

You need to ensure that UserB is given access via the Key policy for the Key `C:\Users\wk\Desktop\mudassar\Untitled.jpg`



Option is invalid because you don't assign roles to IAM users

For more information on Key policies please visit the below Link: <https://docs.aws.amazon.com/kms/latest/developerguide/key-poli>

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

### NEW QUESTION 3

A company has several Customer Master Keys (CMK), some of which have imported key material. Each CMK must be rotated annually. What two methods can the security team use to rotate each key? Select 2 answers from the options given below

Please select:

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

**Answer:** AD

#### Explanation:

The AWS Documentation mentions the following

Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material

(the value of the Origin field is External), but you can rotate these CMKs manually.

Rotating Keys Manually

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

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

Option B is invalid because you also need to point the key alias to the new key Option C is invalid because existing CMK keys cannot be rotated as they are Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key For more information on Key rotation please see the below Link: <https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

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

Point the key alias to the new CMK.

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 4

You currently have an S3 bucket hosted in an AWS Account. It holds information that needs to be accessed by a partner account. Which is the MOST secure way to allow the partner account to access the S3 bucket in your account? Select 3 options.

Please select:

- A. Ensure an IAM role is created which can be assumed by the partner account.
- B. Ensure an IAM user is created which can be assumed by the partner account.
- C. Ensure the partner uses an external id when making the request
- D. Provide the ARN for the role to the partner account
- E. Provide the Account Id to the partner account
- F. Provide access keys for your account to the partner account

**Answer:** ACD

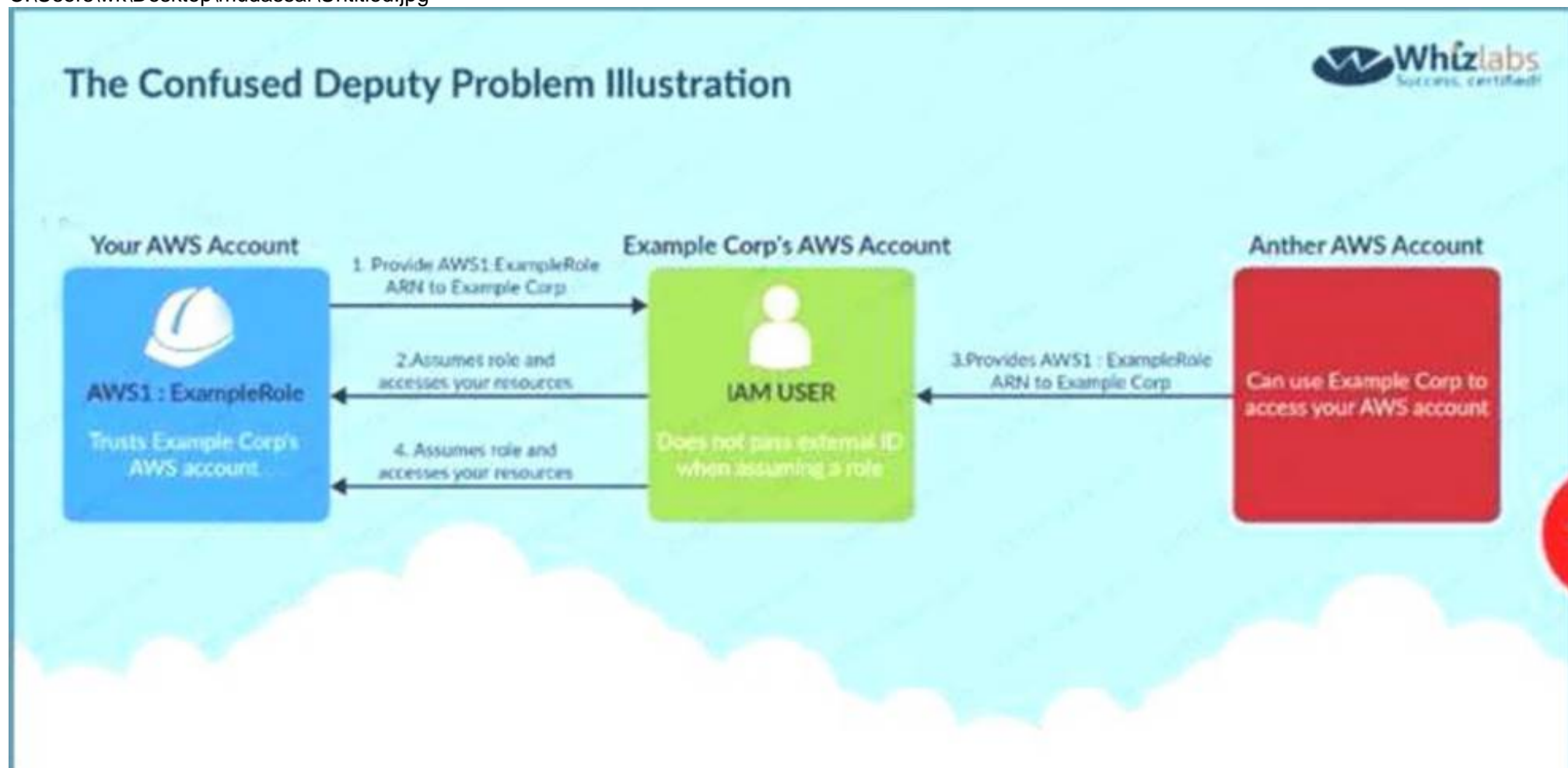
#### Explanation:

Option B is invalid because Roles are assumed and not IAM users

Option E is invalid because you should not give the account ID to the partner Option F is invalid because you should not give the access keys to the partner

The below diagram from the AWS documentation showcases an example on this wherein an IAM role and external ID is used to access an AWS account resource

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



For more information on creating roles for external ID'S please visit the following URL:

The correct answers are: Ensure an IAM role is created which can be assumed by the partner account. Ensure the partner uses an external id when making the request Provide the ARN for the role to the partner account

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 5

A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:

- Encryption at rest
- Logging of all object retrievals in AWS CloudTrail

Which of the following meet these security requirements? (Choose three.)

- A. Specify "aws:SecureTransport": "true" within a condition in the S3 bucket policy.
- B. Enable a security group for the S3 bucket that allows port 443, but not port 80.
- C. Set up default encryption for the S3 bucket.
- D. Enable Amazon CloudWatch Logs for the AWS account.
- E. Enable API logging of data events for all S3 objects.
- F. Enable S3 object versioning for the S3 bucket.

**Answer:** ACE

#### NEW QUESTION 6

You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?

Please select:

- A. AWS Cloudwatch
- B. AWS EC2
- C. AWS Trusted Advisor
- D. AWS SNS

**Answer:** C

#### Explanation:

Below is a snapshot of the service limits that the Trusted Advisor can monitor C:\Users\wk\Desktop\mudassar\Untitled.jpg

Service	Limits
Amazon Elastic Compute Cloud (Amazon EC2)	Elastic IP addresses (EIPs) Reserved Instances - purchase limit (monthly)
Amazon Elastic Block Store (Amazon EBS)	Active volumes Active snapshots General Purpose (SSD) volume storage (GiB) Provisioned IOPS Provisioned IOPS (SSD) volume storage (GiB) Magnetic volume storage (GiB)
Amazon Kinesis Streams	Shards

Option A is invalid because even though you can monitor resources, it cannot be checked against the service limit.

Option B is invalid because this is the Elastic Compute cloud service Option D is invalid because it can be send notification but not check on service limit For more information on the Trusted Advisor monitoring, please visit the below URL:

<https://aws.amazon.com/premiumsupport/ta-faqs>> The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

#### NEW QUESTION 7

The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used.

How can the InfoSec team ensure compliance with this mandate?

- A. Terminate all Amazon EC2 instances and relaunch them with approved AMIs.
- B. Patch all running instances by using AWS Systems Manager.
- C. Deploy AWS Config rules and check all running instances for compliance.
- D. Define a metric filter in Amazon CloudWatch Logs to verify compliance.

**Answer:** C

#### NEW QUESTION 8

Your company is planning on using AWS EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted.

Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.

Please select:

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

**Answer:** BC

#### Explanation:

The AWS Documentation mentions the following

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

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

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

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

Submit your Feedback/Queries to our Experts



#### NEW QUESTION 9

You are planning on using the AWS KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for encrypting? Choose 2 answers from the options given below

Please select:

- A. Image Objects
- B. Large files
- C. Password
- D. RSA Keys

**Answer:** CD

#### Explanation:

The CMK keys themselves can only be used for encrypting data that is maximum 4KB in size. Hence it can be used for encrypting information such as passwords and RSA keys.

Option A and B are invalid because the actual CMK key can only be used to encrypt small amounts of data and not large amounts of data. You have to generate the data key from the CMK key in order to encrypt high amounts of data

For more information on the concepts for KMS, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html>

The correct answers are: Password, RSA Keys Submit your Feedback/Queries to our Experts

#### NEW QUESTION 10

Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours.

What steps are necessary to identify the cause of this phenomenon? (Choose two.)

- A. Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.
- B. Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.
- C. Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.
- D. Create a CloudWatch Logs metric to isolate a value that changes at least once during the period before logging stops.
- E. Use AWS CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

**Answer:** AB

#### NEW QUESTION 10

Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flaws. Which of the following can be done to ensure this? Choose 2 answers from the options given below.

Please select:

- A. Use AWS Config to ensure that the servers have no critical flaws.
- B. Use AWS Inspector to ensure that the servers have no critical flaws.
- C. Use AWS Inspector to patch the servers
- D. Use AWS SSM to patch the servers

**Answer:** BD

#### Explanation:

The AWS Documentation mentions the following on AWS Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Option A is invalid because the AWS Config service is not used to check the vulnerabilities on servers Option C is invalid because the AWS Inspector service is not used to patch servers

For more information on AWS Inspector, please visit the following URL: <https://aws.amazon.com/inspector>

Once you understand the list of servers which require critical updates, you can rectify them by installing the required patches via the SSM tool.

For more information on the Systems Manager, please visit the following URL: <https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html>

The correct answers are: Use AWS Inspector to ensure that the servers have no critical flaws.. Use AWS SSM to patch the servers

#### NEW QUESTION 11

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 12

A security team is responsible for reviewing AWS API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future AWS regions.

What is the SIMPLEST way to meet these requirements?

- A. Enable AWS Trusted Advisor security checks in the AWS Console, and report all security incidents for all regions.
- B. Enable AWS CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
- C. Enable AWS CloudTrail by creating a new trail and applying the trail to all region

- D. Specify a single Amazon S3 bucket as the storage location.  
E. Enable Amazon CloudWatch logging for all AWS services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

**Answer:** C

#### NEW QUESTION 17

You have an EC2 instance with the following security configured:

- a: ICMP inbound allowed on Security Group
- b: ICMP outbound not configured on Security Group
- c: ICMP inbound allowed on Network ACL
- d: ICMP outbound denied on Network ACL

If Flow logs is enabled for the instance, which of the following flow records will be recorded? Choose 3 answers from the options give below  
Please select:

- A. An ACCEPT record for the request based on the Security Group
- B. An ACCEPT record for the request based on the NACL
- C. A REJECT record for the response based on the Security Group
- D. A REJECT record for the response based on the NACL

**Answer:** ABD

#### Explanation:

This example is given in the AWS documentation as well

For example, you use the ping command from your home computer (IP address is 203.0.113.12) to your instance (the network interface's private IP address is 172.31.16.139). Your security group's inbound rules allow ICMP traffic and the outbound rules do not allow ICMP traffic however, because security groups are stateful, the response ping from your instance is allowed. Your network ACL permits inbound ICMP traffic but does not permit outbound ICMP traffic. Because network ACLs are stateless, the response ping is dropped and will not reach your home computer. In a flow log, this is displayed as 2 flow log records:

An ACCEPT record for the originating ping that was allowed by both the network ACL and the security group, and therefore was allowed to reach your instance.

A REJECT record for the response ping that the network ACL denied.

Option C is invalid because the REJECT record would not be present For more information on Flow Logs, please refer to the below URL:

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>

The correct answers are: An ACCEPT record for the request based on the Security Group, An ACCEPT record for the request based on the NACL, A REJECT record for the response based on the NACL

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 20

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

Please select:

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

**Answer:** D

#### Explanation:

The AWS Documentation states the following

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

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

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

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

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

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

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

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

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

Rotation period for CMKs is as follows:

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

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

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

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 21

A company has external vendors that must deliver files to the company. These vendors have cross-account that gives them permission to upload objects to one of the company's S3 buckets.

What combination of steps must the vendor follow to successfully deliver a file to the company? Select 2 answers from the options given below

Please select:

- A. Attach an IAM role to the bucket that grants the bucket owner full permissions to the object
- B. Add a grant to the objects ACL giving full permissions to bucket owner.

- C. Encrypt the object with a KMS key controlled by the company.
- D. Add a bucket policy to the bucket that grants the bucket owner full permissions to the object
- E. Upload the file to the company's S3 bucket

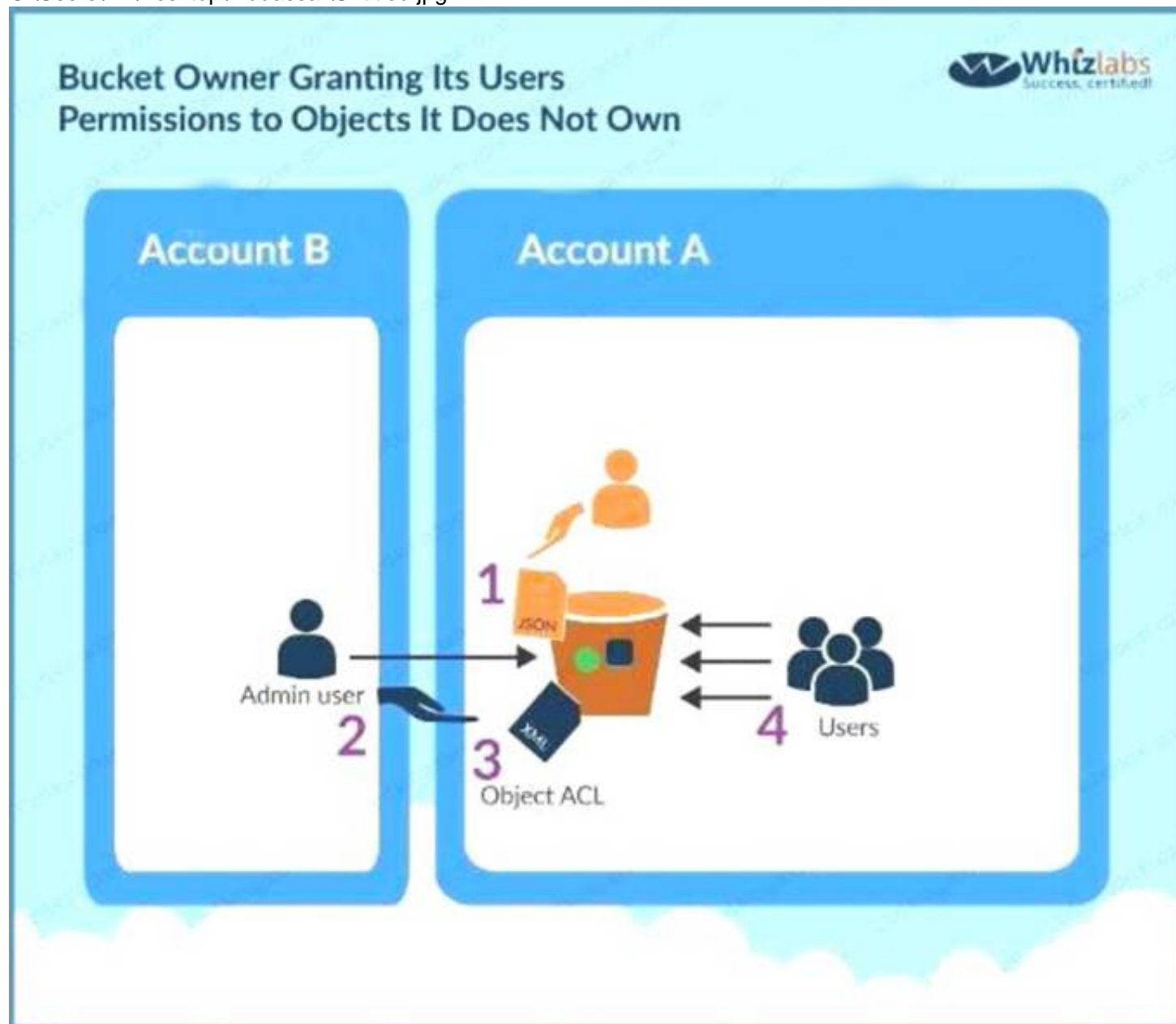
**Answer:** BE

**Explanation:**

This scenario is given in the AWS Documentation

A bucket owner can enable other AWS accounts to upload objects. These objects are owned by the accounts that created them. The bucket owner does not own objects that were not created by the bucket owner. Therefore, for the bucket owner to grant access to these objects, the object owner must first grant permission to the bucket owner using an object ACL. The bucket owner can then delegate those permissions via a bucket policy. In this example, the bucket owner delegates permission to users in its own account.

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



Option A and D are invalid because bucket ACL's are used to give grants to bucket Option C is not required since encryption is not part of the requirement For more information on this scenario please see the below Link:  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example3.html> The correct answers are: Add a grant to the objects ACL giving full permissions to bucket owner., Upload the file to the company's S3 bucket  
 Submit your Feedback/Queries to our Experts

**NEW QUESTION 25**

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?  
 Please select:

- A. Launch the test and production instances in separate regions and allow region wise access to the group
- B. Define the IAM policy which allows access based on the instance ID
- C. Create an IAM policy with a condition which allows access to only small instances
- D. Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specification tags

**Answer:** D

**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

Option A is invalid because this is not a recommended practices

Option B is invalid because this is an overhead to maintain this in policies Option C is invalid because the instance type will not resolve the requirement For information on resource tagging, please visit 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 answer is: Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags

Submit your Feedback/Queries to our Experts

**NEW QUESTION 26**

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 (1AM) 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 1AM 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 28**

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

Please select:

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

**Answer:** B

**NEW QUESTION 29**

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 32**

A company plans to move most of its IT infrastructure to AWS. The company wants to leverage its existing on-premises Active Directory as an identity provider for AWS.

Which steps should be taken to authenticate to AWS services using the company's on-premises Active Directory? (Choose three).

- A. Create IAM roles with permissions corresponding to each Active Directory group.
- B. Create IAM groups with permissions corresponding to each Active Directory group.
- C. Create a SAML provider with IAM.
- D. Create a SAML provider with Amazon Cloud Directory.
- E. Configure AWS as a trusted relying party for the Active Directory
- F. Configure IAM as a trusted relying party for Amazon Cloud Directory.

**Answer:** ACE

**NEW QUESTION 34**

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

Please select:

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

**Answer: C**

**Explanation:**

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

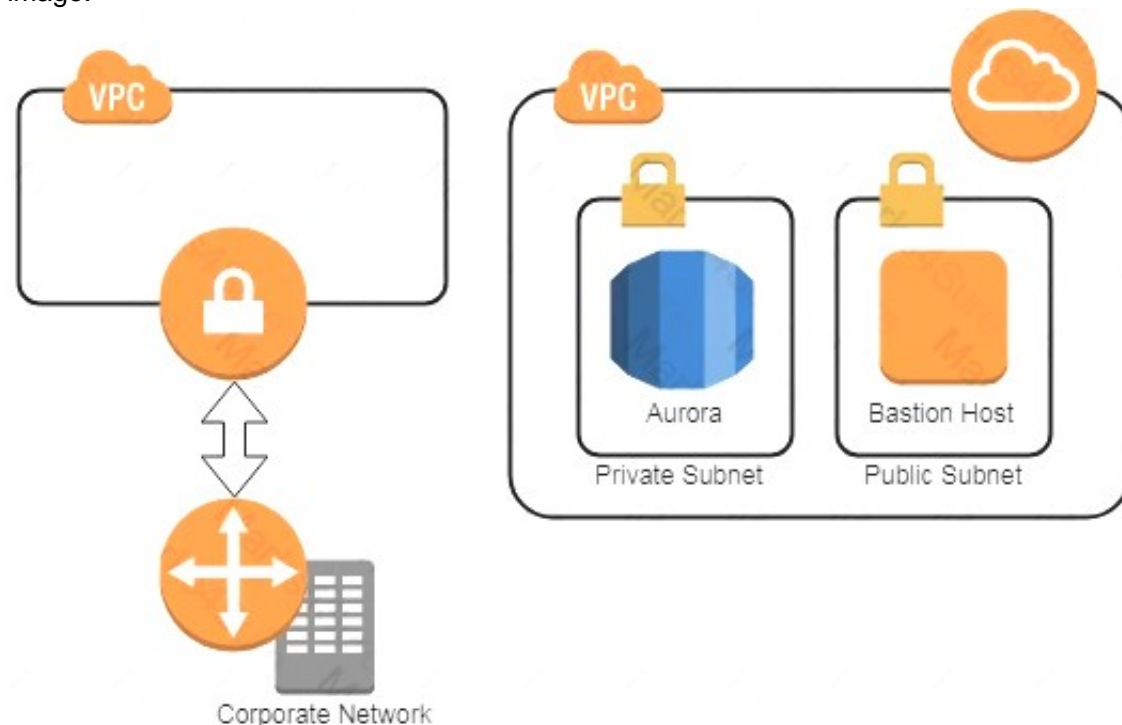
Option D is invalid since just changing the Inbound Rules is sufficient The AWS Documentation mentions the following

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

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

**NEW QUESTION 38**

A company has two AWS accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.

How can a Security Engineer securely set up the bastion host?

- A. Move the bastion host to the VPC with VPN connectivity
- B. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.
- C. Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
- D. Move the bastion host to the VPC with VPN connectivity
- E. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
- F. Create an AWS Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

**Answer: C**

**NEW QUESTION 40**

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

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

**Answer: D**

**Explanation:**

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

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

only be granted access in one location  
Option 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 bucket in the primary account and grant the auditor access to that single bucket in the primary account.  
Submit your Feedback/Queries to our Experts

#### NEW QUESTION 43

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:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        <Action>
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
      ]
      <CONDITION>
    }
  ]
}
```

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 48

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

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

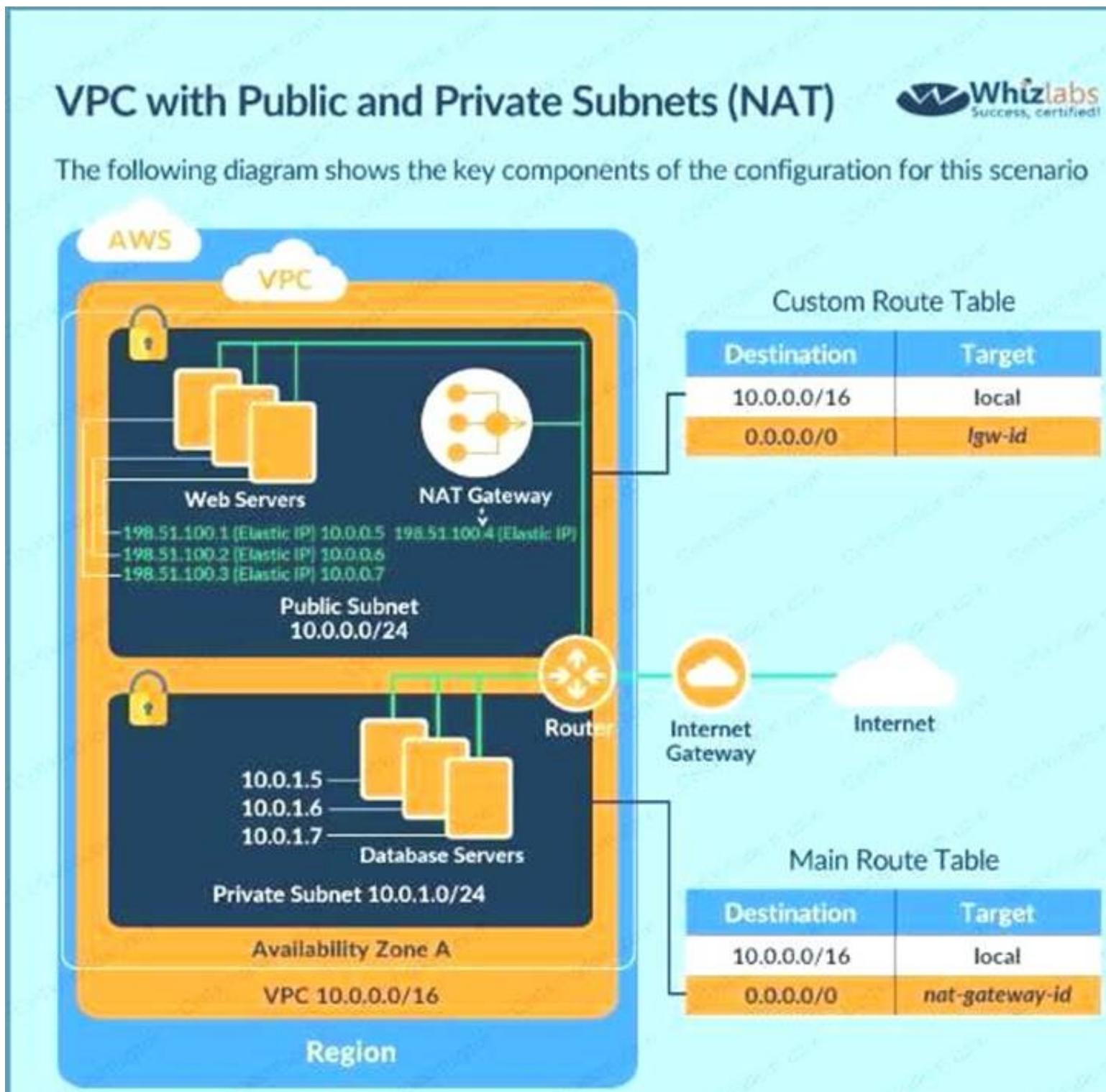
**Answer:** B

#### Explanation:

The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet.

The below diagram from the AWS Documentation shows how this can be setup C:\Users\wk\Desktop\mudassar\Untitled.jpg





Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users Option D is invalid because NAT instances should be present in the public subnet

For more information on public and private subnets in AWS, please visit the following url [com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2).

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

#### NEW QUESTION 50

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

Please select:

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

**Answer:** A

#### Explanation:

Option B is partially correct but a big maintenance over head to create and maintain a script when the functionality is already available in S3

Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The AWS Documentation mentions the following

Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buck in different AWS Regions.

For more information on Cross region replication in the Simple Storage Service, please visit the below URL:

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

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

#### NEW QUESTION 55

An application has been written that publishes custom metrics to Amazon CloudWatch. Recently, IAM changes have been made on the account and the metrics are no longer being reported.

Which of the following is the LEAST permissive solution that will allow the metrics to be delivered?

- A. Add a statement to the IAM policy used by the application to allow logs:putLogEvents and logs:createLogStream
- B. Modify the IAM role used by the application by adding the CloudWatchFullAccess managed policy.
- C. Add a statement to the IAM policy used by the application to allow cloudwatch:putMetricData.
- D. Add a trust relationship to the IAM role used by the application for cloudwatch.amazonaws.com.

**Answer:** C



#### NEW QUESTION 59

Some highly sensitive analytics workloads are to be moved to Amazon EC2 hosts. Threat modeling has found that a risk exists where a subnet could be maliciously or accidentally exposed to the internet.

Which of the following mitigations should be recommended?

- A. Use AWS Config to detect whether an Internet Gateway is added and use an AWS Lambda function to provide auto-remediation.
- B. Within the Amazon VPC configuration, mark the VPC as private and disable Elastic IP addresses.
- C. Use IPv6 addressing exclusively on the EC2 hosts, as this prevents the hosts from being accessed from the internet.
- D. Move the workload to a Dedicated Host, as this provides additional network security controls and monitoring.

**Answer:** A

#### NEW QUESTION 60

A company has enabled Amazon GuardDuty in all Regions as part of its security monitoring strategy. In one of the VPCs, the company hosts an Amazon EC2 instance working as an FTP server that is contacted by a high number of clients from multiple locations. This is identified by GuardDuty as a brute force attack due to the high number of connections that happen every hour.

The finding has been flagged as a false positive. However, GuardDuty keeps raising the issue. A Security Engineer has been asked to improve the signal-to-noise ratio. The Engineer needs to ensure that changes do not compromise the visibility of potential anomalous behavior.

How can the Security Engineer address the issue?

- A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed
- B. Add the FTP server to a trusted IP list and deploy it to GuardDuty to stop receiving the notifications
- C. Use GuardDuty filters with auto archiving enabled to close the findings
- D. Create an AWS Lambda function that closes the finding whenever a new occurrence is reported

**Answer:** B

#### Explanation:

Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your AWS infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists. At any given time, you can have only one uploaded trusted IP list per AWS account per region.

References:

#### NEW QUESTION 65

A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.

What combination of actions should the Engineer take? (Choose two.)

- A. Create an AWS Lambda function that determines whether Flow Logs are enabled for a given VPC.
- B. Create an AWS Config configuration item for each VPC in the company AWS account.
- C. Create an AWS Config managed rule with a resource type of AWS::Lambda::Function.
- D. Create an Amazon CloudWatch Event rule that triggers on events emitted by AWS Config.
- E. Create an AWS Config custom rule, and associate it with an AWS Lambda function that contains the evaluating logic.

**Answer:** AE

#### NEW QUESTION 68

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

- A. The external ID used by the Auditor is missing or incorrect.
- B. The Auditor is using the incorrect password.
- C. The Auditor has not been granted sts:AssumeRole for the role in the destination account.
- D. The Amazon EC2 role used by the Auditor must be set to the destination account role.
- E. The secret key used by the Auditor is missing or incorrect.
- F. The role ARN used by the Auditor is missing or incorrect.

**Answer:** ACF

#### NEW QUESTION 70

A Security Engineer must implement mutually authenticated TLS connections between containers that communicate inside a VPC.

Which solution would be MOST secure and easy to maintain?

- A. Use AWS Certificate Manager to generate certificates from a public certificate authority and deploy them to all the containers.
- B. Create a self-signed certificate in one container and use AWS Secrets Manager to distribute the certificate to the other containers to establish trust.
- C. Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then create the private keys in the containers and sign them using the ACM PCA API.
- D. Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then use AWS Certificate Manager to generate the private certificates and deploy them to all the containers.

**Answer:** C

#### NEW QUESTION 73

A company uses AWS Organization to manage 50 AWS accounts. The finance staff members log in as AWS IAM users in the FinanceDept AWS account. The staff members need to read the consolidated billing information in the MasterPayer AWS account. They should not be able to view any other resources in the MasterPayer AWS account. IAM access to billing has been enabled in the MasterPayer account.

Which of the following approaches grants the finance staff the permissions they require without granting any unnecessary permissions?

- A. Create an IAM group for the finance users in the FinanceDept account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.
- B. Create an IAM group for the finance users in the MasterPayer account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.
- C. Create an AWS IAM role in the FinanceDept account with the ViewBilling permission, then grant the finance users in the MasterPayer account the permission to assume that role.
- D. Create an AWS IAM role in the MasterPayer account with the ViewBilling permission, then grant the finance users in the FinanceDept account the permission to assume that role.

**Answer:** D

#### NEW QUESTION 75

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

Please select:

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

**Answer:** AD

#### Explanation:

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

All master keys in AWS KMS regardless of their creation date or origin are automatically protected using FIPS 140-2 validated HSMs. defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

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

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

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

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

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

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

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

The AWS Documentation mentions the following

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

With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries. CloudHSM is also standards-compliant and enables you to export all of your keys to most other commercially-available HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching,

high-availability, and backups. CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs.

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

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

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

#### NEW QUESTION 80

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 81

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 1AM policies that can be mapped to group memberships in the corporate directory.
- D. Create a Lambda function to assign 1AM roles to the temporary security tokens provided to the users.
- E. Create 1AM users that can be mapped to the employees' corporate identities
- F. Create an 1AM role that establishes a trust relationship between 1AM 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 1AM policies are not directly mapped to group memberships in the corporate directory. It is 1AM roles which are mapped.

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

Option D is incorrect because 1AM 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 1AM role that establishes a trust relationship between 1AM 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 1AM 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 1AM 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

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": { "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/ExampleOrgSSOProvider" },
    "Action": "sts:AssumeRoleWithSAML",
    "Condition": { "StringEquals": {
      "saml:edupersonorgdn": "ExampleOrg",
      "saml:aud": "https://signin.aws.amazon.com/saml"
    }
    }
  ]
}
```

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

What directories can I use with AWS SSO?

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

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

Set up a VPC with the following:

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

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

Submit your Feedback/Queries to our Experts

**NEW QUESTION 85**

A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The Security team has the following requirements for the architecture:

- Data must be encrypted in transit.
- Data must be encrypted at rest.
- The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Choose two.)

- A. Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket.
- B. Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.
- C. Add a bucket policy that includes a deny if a PutObject request does not include aws:SecureTransport.
- D. Add a bucket policy with aws:SourceIp to Allow uploads and downloads from the corporate intranet only.
- E. Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-server-side-encryption: "aws:kms".



F. Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

**Answer:** BC

**Explanation:**

Bucket encryption using KMS will protect both in case disks are stolen as well as if the bucket is public. This is because the KMS key would need to have privileges granted to it for users outside of AWS.

**NEW QUESTION 87**

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

A.

```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
  "Sid":"DenyUploads",
  "Effect":"Deny",
  "Principal":"*",
  "Action":"s3:PutObject",
  "Resource":"arn:aws:s3:::demo/*",
  "Condition":{"
    "StringNotEquals":{"
      "s3:x-amz-server-side-encryption":"aws:kms"
    }
  }
}]
}
```

B.

```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
  "Sid":"DenyUploads",
  "Effect":"Deny",
  "Principal":"*",
  "Action":"s3:PutObject",
  "Resource":"arn:aws:s3:::demo/*",
  "Condition":{"
    "StringEquals":{"
      "s3:x-amz-server-side-encryption":"aws:kms"
    }
  }
}]
}
```

C.

```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
  "Sid":"DenyUploads",
  "Effect":"Deny",
  "Principal":"*",
  "Action":"s3:PutObject",
  "Resource":"arn:aws:s3:::demo/*"
}]
}
```

D.



```
"Version": "2012-10-17",
"Id": "PutObj",
"Statement": [{
  "Sid": "DenyUploads",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObjectEncrypted",
  "Resource": "arn:aws:s3:::demo/*"
}]
}
```

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>

The correct answer is: {

```
"Version": "2012-10-17",
"Id": "PutObj",
"Statement": [{
  "Sid": "DenyUploads",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::demo/*",
  "Condition": {
    "StringNotEquals": {
      "s3:x-amz-server-side-encryption": "aws:kms"
    }
  }
}]
}
```

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

Submit your Feedback/Queries to our Expert

**NEW QUESTION 91**

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

Please select:

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

**Answer:** B

**Explanation:**

The AWS Security best practices mentions the following

Unique to AWS, security practitioners can use CloudFormation to quickly create a new, trusted environment in which to conduct deeper investigation. The CloudFormation template can pre-configure instances in an isolated environment that contains all the necessary tools forensic teams need to determine the cause of the incident. This cuts down on the time it takes to gather necessary tools, isolates systems under examination, and ensures that the team is operating in a clean

room.

Option A is incorrect since this is a logging service and cannot be used to provision a test environment Option C is incorrect since this is an API logging service and cannot be used to provision a test environment Option D is incorrect since this is a configuration service and cannot be used to provision a test environment For more information on AWS Security best practises, please refer to below URL: <https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf>  
The correct answer is: AWS Cloudformation Submit your Feedback/Queries to our Experts

#### NEW QUESTION 94

A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.

Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

- A. Have a Database Administrator encrypt the credentials and store the ciphertext in Amazon S3. Grant permission to the instance role associated with the EC2 instance to read the object and decrypt the ciphertext.
- B. Configure a scheduled job that updates the credential in AWS Systems Manager Parameter Store and notifies the Engineer that the application needs to be restarted.
- C. Configure automatic rotation of credentials in AWS Secrets Manager.
- D. Store the credential in an encrypted string parameter in AWS Systems Manager Parameter Store
- E. Grant permission to the instance role associated with the EC2 instance to access the parameter and the AWS KMS key that is used to encrypt it.
- F. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotate
- G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

**Answer:** CE

#### NEW QUESTION 99

An organization has setup multiple 1AM users. The organization wants that each 1AM user accesses the 1AM console only within the organization and not from outside. How can it achieve this?

Please select:

- A. Create an 1AM policy with the security group and use that security group for AWS console login
- B. Create an 1AM 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 1AM 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 102

You have setup a set of applications across 2 VPC's. You have also setup VPC Peering. The applications are still not able to communicate across the Peering connection. Which network troubleshooting steps should be taken to resolve the issue?

Please select:

- A. Ensure the applications are hosted in a public subnet
- B. Check to see if the VPC has an Internet gateway attached.
- C. Check to see if the VPC has a NAT gateway attached.
- D. Check the Route tables for the VPC's

**Answer:** D

#### Explanation:

After the VPC peering connection is established, you need to ensure that the route tables are modified to ensure traffic can between the VPCs

Option A ,B and C are invalid because allowing access the Internet gateway and usage of public subnets can help for Inter, access, but not for VPC Peering.

For more information on VPC peering routing, please visit the below URL: [com/AmazonVPC/latest/Peeri](http://com/AmazonVPC/latest/Peeri)

The correct answer is: Check the Route tables for the VPCs Submit your Feedback/Queries to our Experts

#### NEW QUESTION 104

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 109

Your company has many AWS accounts defined and all are managed via AWS Organizations. One AWS account has a S3 bucket that has critical data. How can we ensure that all the users in the AWS organisation have access to this bucket?  
Please select:

- A. Ensure the bucket policy has a condition which involves aws:PrincipalOrgID
- B. Ensure the bucket policy has a condition which involves aws:AccountNumber
- C. Ensure the bucket policy has a condition which involves aws:PrincipalID
- D. Ensure the bucket policy has a condition which involves aws:OrgID

**Answer:** A

**Explanation:**

The AWS Documentation mentions the following

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

Option B.C and D are invalid because the condition in the bucket policy has to mention aws:PrincipalOrgID For more information on controlling access via Organizations, please refer to the below Link:

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-p/> (

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

**NEW QUESTION 110**

The Information Technology department has stopped using Classic Load Balancers and switched to Application Load Balancers to save costs. After the switch, some users on older devices are no longer able to connect to the website.  
What is causing this situation?

- A. Application Load Balancers do not support older web browsers.
- B. The Perfect Forward Secrecy settings are not configured correctly.
- C. The intermediate certificate is installed within the Application Load Balancer.
- D. The cipher suites on the Application Load Balancers are blocking connections.

**Answer:** D

**NEW QUESTION 111**

An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.  
What techniques will limit lateral movement and allow evidence gathering?

- A. Remove the instance from the load balancer and terminate it.
- B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.
- C. Reboot the instance and check for any Amazon CloudWatch alarms.
- D. Stop the instance and make a snapshot of the root EBS volume.

**Answer:** B

**NEW QUESTION 116**

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 117**

Which of the following are valid event sources that are associated with web access control lists that trigger AWS WAF rules? (Choose two.)

- A. Amazon S3 static web hosting
- B. Amazon CloudFront distribution
- C. Application Load Balancer
- D. Amazon Route 53
- E. VPC Flow Logs

**Answer:** BC

**Explanation:**

A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon API Gateway API, Amazon CloudFront distribution or Application Load Balancer responds to.

**NEW QUESTION 121**

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:



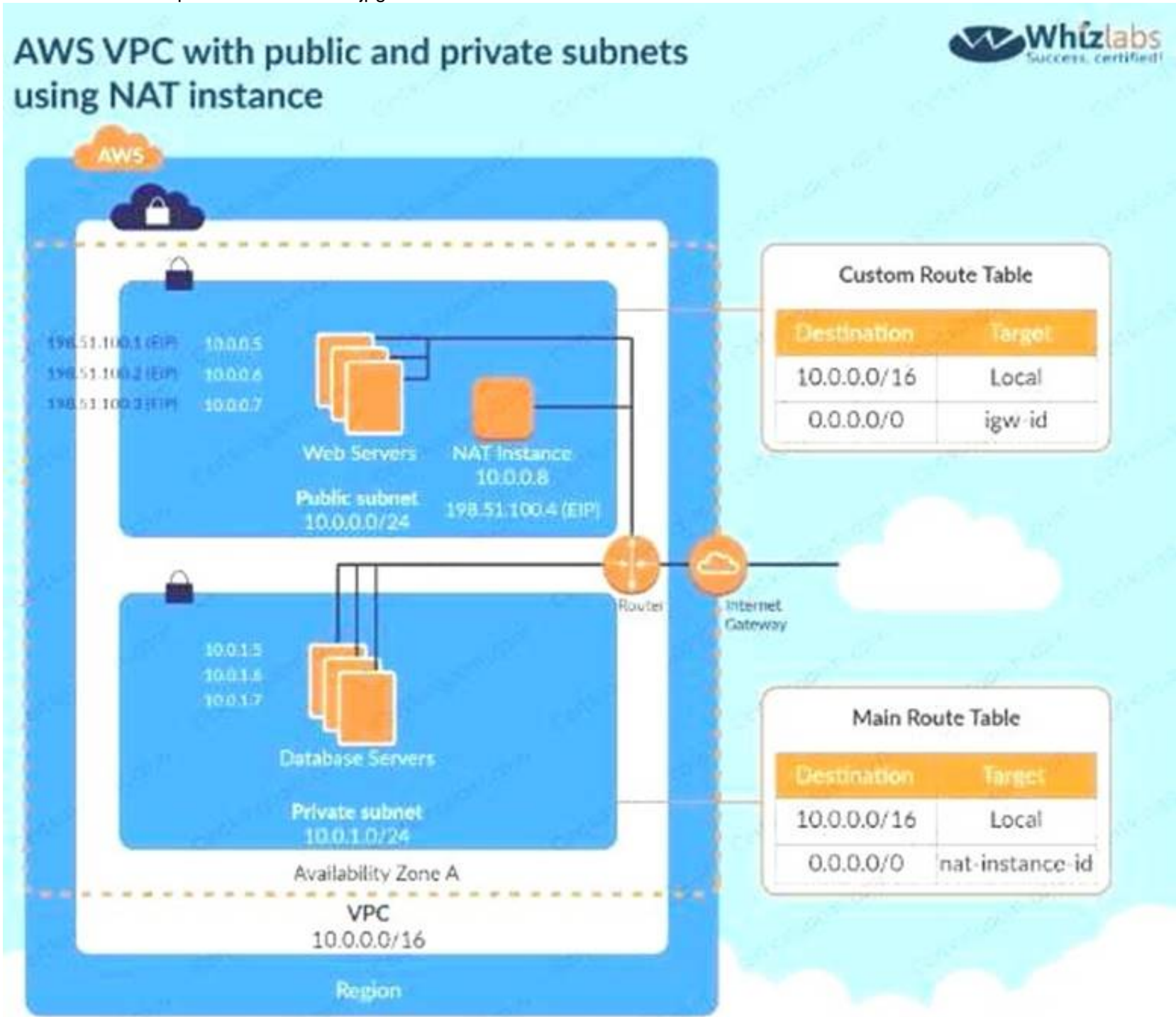
- A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
- B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
- C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
- D. EC2 instances in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

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



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 Instance.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 126**

A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target AWS account (123456789123) to perform their job functions. A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/JobFunctionRole"
      ],
      "Effect": "Allow"
    }
  ]
}
```

What should be done to enable the user to assume the appropriate role in the target account?

**A** Update the IAM policy attached to the role in the identity account to be:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::123456789123:role/JobFunctionRole"
      ],
      "Effect": "Allow"
    }
  ]
}
```

B Update the trust policy on the role in the target account to be:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::987654321987:role/IdentityRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

C Update the trust policy on the role in the identity account to be:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::987654321987:root" },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

D Update the IAM policy attached to the role in the target account to be:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1502946463000",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::123456789123:role/JobFunctionRole"
    }
  ]
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** A

#### NEW QUESTION 131

During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.

What could have been done to detect and automatically remediate the incident?

- A. Using Amazon Inspector, review all of the API calls and configure the inspector agent to leverage SNS topics to notify security of the change to AWS CloudTrail, and revoke the new API keys for the root user.
- B. Using AWS Config, create a config rule that detects when AWS CloudTrail is disabled, as well as any calls to the root user create-api-key.
- C. Then use a Lambda function to re-enable CloudTrail logs and deactivate the root API keys.
- D. Using Amazon CloudWatch, create a CloudWatch event that detects AWS CloudTrail deactivation and a separate Amazon Trusted Advisor check to automatically detect the creation of root API key.

- E. Then use a Lambda function to enable AWS CloudTrail and deactivate the root API keys.
- F. Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API key
- G. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.

**Answer:** B

#### NEW QUESTION 136

An AWS account includes two S3 buckets: bucket1 and bucket2. The bucket2 does not have a policy defined, but bucket1 has the following bucket policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam: : 123456789012: user/alice" },
      "Action": "s3:*",
      "Resource": [ "arn:aws:s3: : :bucket1", "arn:aws:s3: : :bucket1/*" ]
    }
  ]
}
```

In addition, the same account has an IAM User named "alice", with the following IAM policy.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": [ "arn:aws:s3: : :bucket2", "arn:aws:s3: : :bucket2/*" ]
  }]
}
```

Which buckets can user "alice" access?

- A. Bucket1 only
- B. Bucket2 only
- C. Both bucket1 and bucket2
- D. Neither bucket1 nor bucket2

**Answer:** C

#### NEW QUESTION 138

An organization has tens of applications deployed on thousands of Amazon EC2 instances. During testing, the Application team needs information to let them know whether the network access control lists (network ACLs) and security groups are working as expected. How can the Application team's requirements be met?

- A. Turn on VPC Flow Logs, send the logs to Amazon S3, and use Amazon Athena to query the logs.
- B. Install an Amazon Inspector agent on each EC2 instance, send the logs to Amazon S3, and use Amazon EMR to query the logs.
- C. Create an AWS Config rule for each network ACL and security group configuration, send the logs to Amazon S3, and use Amazon Athena to query the logs.
- D. Turn on AWS CloudTrail, send the trails to Amazon S3, and use AWS Lambda to query the trails.

**Answer:** A

#### NEW QUESTION 139

The Security Engineer created a new AWS Key Management Service (AWS KMS) key with the following key policy:

```
{
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
  "Action": "kms:*";
  "Resource": "*"
}
```

What are the effects of the key policy? (Choose two.)

- A. The policy allows access for the AWS account 111122223333 to manage key access through IAM policies.
- B. The policy allows all IAM users in account 111122223333 to have full access to the KMS key.
- C. The policy allows the root user in account 111122223333 to have full access to the KMS key.
- D. The policy allows the KMS service-linked role in account 111122223333 to have full access to the KMS key.
- E. The policy allows all IAM roles in account 111122223333 to have full access to the KMS key.

**Answer:** BE

#### NEW QUESTION 142

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption SSE-C, which of the below mentioned statements is true?

Please select:

- A. The user should use the same encryption key for all versions of the same object
- B. It is possible to have different encryption keys for different versions of the same object
- C. AWS S3 does not allow the user to upload his own keys for server side encryption
- D. The SSE-C does not work when versioning is enabled

**Answer:** B

#### Explanation:

Managing your own encryption keys, you

You can encrypt the object and send it across to S3

Option A is invalid because ideally you should use different encryption keys Option C is invalid because you can use your own encryption keys Option D is invalid because encryption works even if versioning is enabled For more information on client side encryption please visit the below Link:

""Keys.html <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

The correct answer is: It is possible to have different encryption keys for different versions of the same object Submit your Feedback/Queries to our Experts

#### NEW QUESTION 144

You are planning to use AWS Config to check the configuration of the resources in your AWS account. You are planning on using an existing IAM role and using it for the AWS Config resource. Which of the following is required to ensure the AWS Config service can work as required?

Please select:

- A. Ensure that there is a trust policy in place for the AWS Config service within the role
- B. Ensure that there is a grant policy in place for the AWS Config service within the role
- C. Ensure that there is a user policy in place for the AWS Config service within the role
- D. Ensure that there is a group policy in place for the AWS Config service within the role

**Answer:** A

#### Explanation:



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

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

Options B,C and D are invalid because you need to ensure a trust policy is in place and not a grant, user or group policy or more information on the 1AM role permissions please visit the below Link:

<https://docs.aws.amazon.com/config/latest/developerguide/iamrole-permissions.html>

The correct answer is: Ensure that there is a trust policy in place for the AWS Config service within the role Submit your Feedback/Queries to our Experts

#### NEW QUESTION 145

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 149

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 154

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

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

**Answer:** BC

#### Explanation:

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

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

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

Examining CMK Permissions to Determine the Scope of Potential Usage

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

Examining AWS CloudTrail Logs to Determine Actual Usage

AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it

For more information on determining the usage of CMK keys, please visit the following URL:



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

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

#### NEW QUESTION 159

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

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

**Answer:** BE

#### Explanation:

The AWS Documentation mentions the following

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

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

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

- Use Server-Side Encryption - You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
- Use Client-Side Encryption - You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Option A is invalid because using EBS-optimized Amazon EC2 instances alone will not guarantee protection of instances at rest. Option C is invalid because this will not encrypt data at rest for S3 objects. Option D is invalid because you don't store data in Instance store. For more information on EBS encryption, please visit the below URL:

<https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html> For more information on S3 encryption, please visit the below URL:

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

The correct answers are: When storing data in EBS, encrypt the volume by using AWS KMS. When storing data in S3, enable server-side encryption.

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 164

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 IAM 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 IAM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- D. Use IAM 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 IAM 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 IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

#### NEW QUESTION 165

A company has five AWS accounts and wants to use AWS CloudTrail to log API calls. The log files must be stored in an Amazon S3 bucket that resides in a new account specifically built for centralized services with a unique top-level prefix for each trail. The configuration must also enable detection of any modification to the logs.

Which of the following steps will implement these requirements? (Choose three.)

- A. Create a new S3 bucket in a separate AWS account for centralized storage of CloudTrail logs, and enable "Log File Validation" on all trails.
- B. Use an existing S3 bucket in one of the accounts, apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3:PutObject" action and the "s3:GetBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.
- C. Apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3:PutObject" action and the "s3:GetBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.
- D. Use unique log file prefixes for trails in each AWS account.
- E. Configure CloudTrail in the centralized account to log all accounts to the new centralized S3 bucket.
- F. Enable encryption of the log files by using AWS Key Management Service

**Answer:** ACE

#### NEW QUESTION 170

The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.

Which architecture should the Security Engineer use to meet these requirements?

- A. Use AWS Shield to scan inbound traffic for web exploit
- B. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.
- C. Use AWS Shield to scan inbound traffic for web exploit
- D. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.
- E. Use AWS WAF to scan inbound traffic for web exploit
- F. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.
- G. Use AWS WAF to scan inbound traffic for web exploit
- H. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.

**Answer:** D

#### NEW QUESTION 171

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

Please select:

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

**Answer:** B

#### Explanation:

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

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

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

For more information on integrating AWS with LDAP for Single Sign-On, please visit the following URL: <https://aws.amazon.com/blogs/security/new-whitepaper-single-sign-on-integrating-aws-openldap-and-shibboleth> The correct answer is: Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 176

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 need to ensure the right rules are put in place for allowing incoming traffic.

Option A and B are 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 177

During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.

What solution will allow the Security team to complete this request?

- A. Using Amazon Athena, query the impacted S3 buckets by using the PII query identifier functio
- B. Then, create a new Amazon CloudWatch metric for Amazon S3 object access to alert when the objects are accessed.
- C. Enable Amazon Macie on the S3 buckets that were impacted, then perform data classificatio
- D. For identified objects that contain PII, use the research function for auditing AWS CloudTrail logs and S3 bucket logs for GET operations.
- E. Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classificatio
- F. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.
- G. Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classificatio
- H. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

**Answer:** B

#### NEW QUESTION 182

An organization policy states that all encryption keys must be automatically rotated every 12 months. Which AWS Key Management Service (KMS) key type should be used to meet this requirement?

- A. AWS managed Customer Master Key (CMK)
- B. Customer managed CMK with AWS generated key material
- C. Customer managed CMK with imported key material
- D. AWS managed data key

**Answer:** B

#### NEW QUESTION 184

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

Please select:

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

**Answer:** B

#### Explanation:

The AWS Documentation gives an example on such a case

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

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

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

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

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

#### NEW QUESTION 186

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

Please select:

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

**Answer:** B

#### Explanation:

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

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

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

Option C and D are invalid because once the key has been deleted, you cannot recover it For more information on EBS Encryption with KMS, please visit the following URL:

<https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

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

Experts

#### NEW QUESTION 191

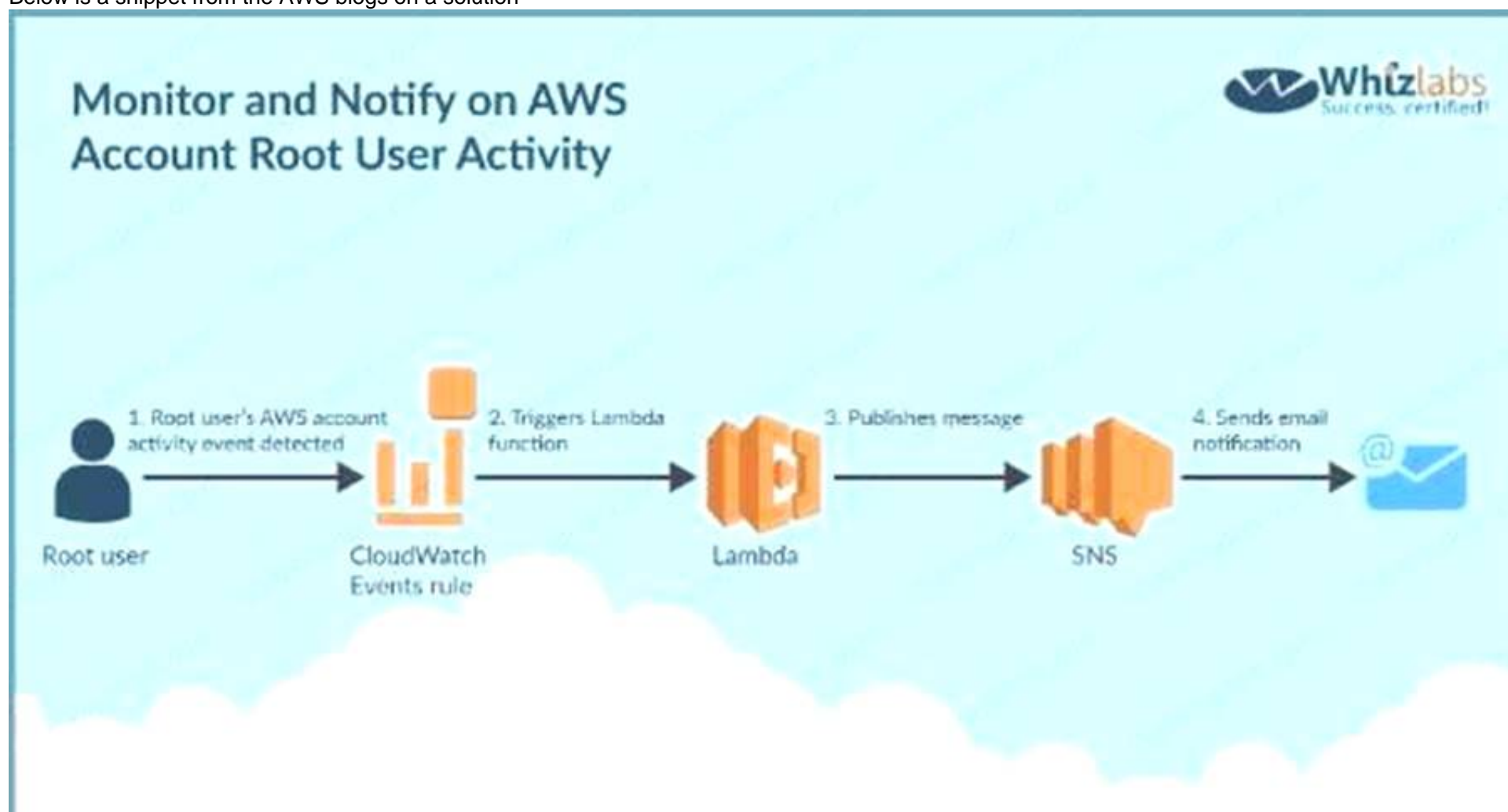
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution  
Please select:

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

**Answer:** AC

#### Explanation:

Below is a snippet from the AWS blogs on a solution



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

Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL:  
<https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity> The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function Submit your Feedback/Queries to our Experts

#### NEW QUESTION 195

Your company has a set of resources defined in the AWS Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner?  
Please select:

- A. Create a powershell script using the AWS CL
- B. Query for all resources with the tag of production.
- C. Create a bash shell script with the AWS CL
- D. Query for all resources in all region
- E. Store the results in an S3 bucket.
- F. Use Cloud Trail to get the list of all resources
- G. Use AWS Config to get the list of all resources

**Answer:** D

#### Explanation:

The most feasible option is to use AWS Config. When you turn on AWS Config, you will get a list of resources defined in your AWS Account. A sample snapshot of the resources dashboard in AWS Config is shown below C:\Users\wk\Desktop\mudassar\Untitled.jpg

Resources	
Total resource count	131
Top 10 resource types	Total
 IAM Policy	45
 IAM Role	40
 EC2 Subnet	7
 EC2 SecurityGroup	6
 EC2 RouteTable	6
 EC2 VPC	4
 EC2 NetworkAcl	4

Option A is incorrect because this would give the list of production based resources and now all resources Option B is partially correct But this will just add more maintenance overhead.

Option C is incorrect because this can be used to log API activities but not give an account of all resou For more information on AWS Config, please visit the below URL: <https://docs.aws.amazon.com/config/latest/developereuide/how-does-confie-work.html>

The correct answer is: Use AWS Config to get the list of all resources

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 199

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

Please select:

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

**Answer:** AB

#### Explanation:

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

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

"For performing a penetration test on AWS resources first of all we need to take permission from AWS and complete a requisition form and submit it for approval. The form should contain information about the instances you wish to test identify the expected start and end dates/times of your test and requires you to read and agree to Terms and Conditions specific to penetration testing and to the use of appropriate tools for testing. Note that the end date may not be more than 90 days from the start date."

(

At this time, our policy does not permit testing small or micro RDS instance types. Testing of ml .small, t1

.m icro or t2.nano EC2 instance types is not permitted.

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

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

#### NEW QUESTION 203

Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.

Which of the following methods will ensure that the data is unreadable by anyone else?

- A. Change the volume encryption on the EBS volume to use a different encryption mechanis
- B. Then, release the EBS volumes back to AWS.
- C. Release the volumes back to AW



- D. AWS immediately wipes the disk after it is deprovisioned.
- E. Delete the encryption key used to encrypt the EBS volume
- F. Then, release the EBS volumes back to AWS.
- G. Delete the data by using the operating system delete command
- H. Run Quick Format on the drive and then release the EBS volumes back to AWS.

**Answer:** B

#### NEW QUESTION 204

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

Please select:

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

**Answer:** C

#### Explanation:

This concept is given in the AWS Documentation

How do I submit a penetration testing request for my AWS resources? Issue

I want to run a penetration test or other simulated event on my AWS architecture. How do I get permission from AWS to do that?

Resolution

Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.

AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.

If your request is approved, you'll receive an authorization number.

Option A,B and D are all invalid because the first step is to get prior authorization from AWS for penetration tests

For more information on penetration testing, please visit the below URL

\* <https://aws.amazon.com/security/penetration-testing/>

\* <https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/>

(

The correct answer is: Submit a request to AWS Support Submit your Feedback/Queries to our Experts

#### NEW QUESTION 205

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

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

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

**Answer:** A

#### Explanation:

You can use the AWSConfig history to see the history of a particular item.

The below snapshot shows an example configuration for a user in AWS Config



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

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

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

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

The correct answer is: Use AWS Config to examine the employee's 1AM permissions prior to the incident and compare them the employee's current 1AM permissions.

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 207

Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a

resource. What is the best option to accomplish this requirement?  
Please select:

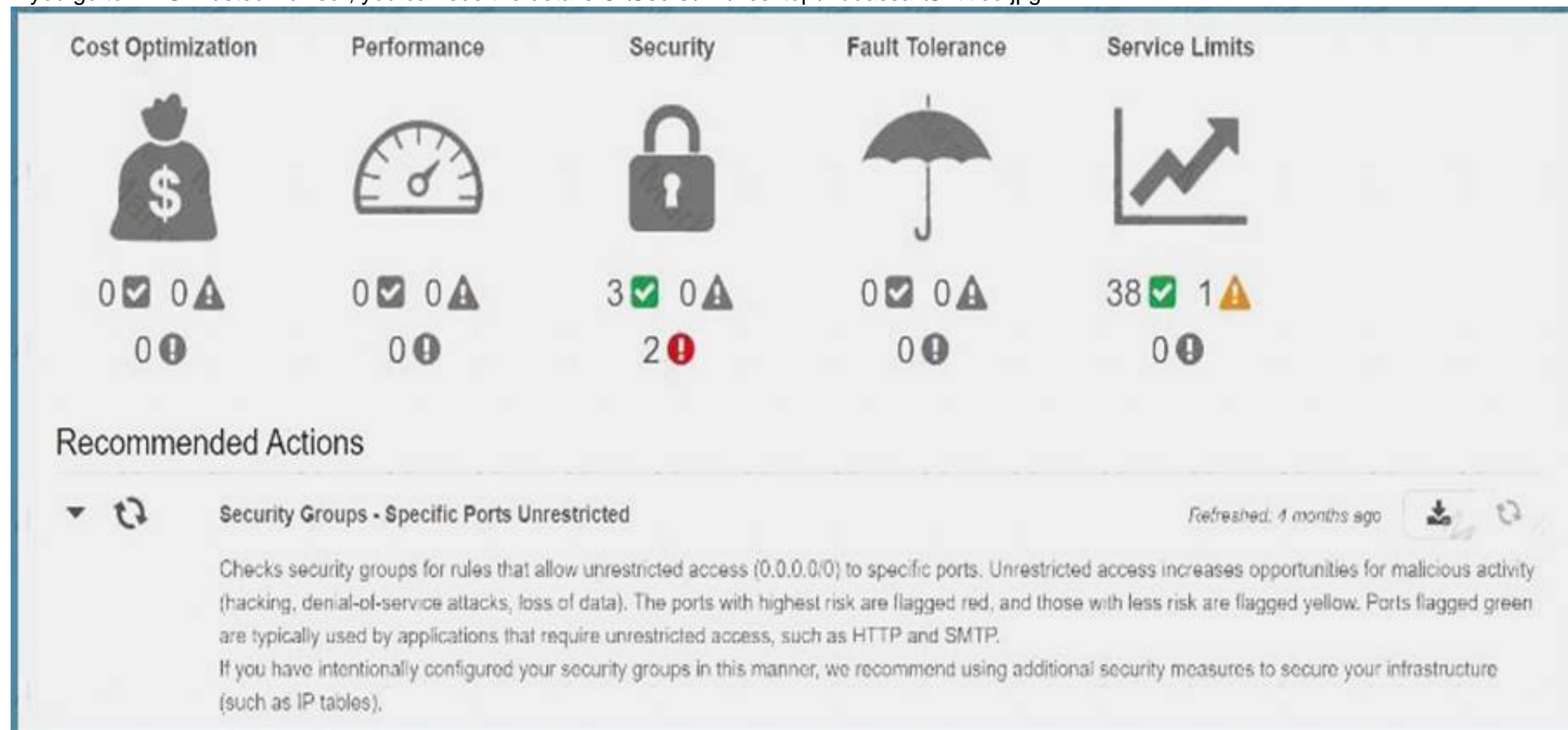
- A. Use AWS Inspector to inspect all the security Groups
- B. Use the AWS Trusted Advisor to see which security groups have compromised access.
- C. Use AWS Config to see which security groups have compromised access.
- D. Use the AWS CLI to query the security groups and then filter for the rules which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

**Answer: B**

**Explanation:**

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

If you go to AWS Trusted Advisor, you can see the details C:\Users\wk\Desktop\mudassar\Untitled.jpg



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 209**

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 213**

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. You will be using VPN gateways and terminating the IPsec tunnels on AWS-supported customer gateways. Which of the following objectives would you achieve by implementing an IPsec tunnel as outlined above? Choose 4 answers from 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:**

IPSec is a widely adopted protocol that can be used to provide end to end protection for data

**NEW QUESTION 214**

You have just developed a new mobile application that handles analytics workloads on large scale datasets that are stored on Amazon Redshift. Consequently, the application needs to access Amazon Redshift tables. Which of the below methods would be the best both practically and security-wise, to access the tables?  
Choose the correct answer from the options below

Please select:

- A. Create an IAM user and generate encryption keys for that use
- B. Create a policy for Redshift read-only access
- C. Embed the keys in the application.
- D. Create an HSM client certificate in Redshift and authenticate using this certificate.
- E. Create a Redshift read-only access policy in IAM and embed those credentials in the application.
- F. Use roles that allow a web identity federated user to assume a role that allows access to the Redshift table by providing temporary credentials.

**Answer: D**

**Explanation:**

The AWS Documentation mentions the following

"When you write such an app, you'll make requests to AWS services that must be signed with an AWS access key. However, we strongly recommend that you do not embed or distribute long-term AWS credentials with apps that a user downloads to a device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamically when needed using web identity federation. The supplied temporary credentials map to an AWS role that has only the permissions needed to perform the tasks required by the mobile app".

Option A, B and C are all automatically incorrect because you need to use IAM Roles for Secure access to services. For more information on web identity federation, please refer to the below link:

➤ [http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_oidc.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)

The correct answer is: Use roles that allow a web identity federated user to assume a role that allows access to the Redshift table by providing temporary credentials.

Submit your Feedback/Queries to our Experts

**NEW QUESTION 219**

A Security Administrator is performing a log analysis as a result of a suspected AWS account compromise. The Administrator wants to analyze suspicious AWS CloudTrail log files but is overwhelmed by the volume of audit logs being generated.

What approach enables the Administrator to search through the logs MOST efficiently?

- A. Implement a "write-only" CloudTrail event filter to detect any modifications to the AWS account resources.
- B. Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.
- C. Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.
- D. Enable Amazon S3 event notifications to trigger an AWS Lambda function that sends an email alarm when there are new CloudTrail API entries.

**Answer: C**

**NEW QUESTION 224**

A company has multiple production AWS accounts. Each account has AWS CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.

Which steps should be taken to troubleshoot the issue? (Choose three.)

- A. Verify that the log file prefix is set to the name of the S3 bucket where the logs should go.
- B. Verify that the S3 bucket policy allows access for CloudTrail from the production AWS account IDs.
- C. Create a new CloudTrail configuration in the account, and configure it to log to the account's S3 bucket.
- D. Confirm in the CloudTrail Console that each trail is active and healthy.
- E. Open the global CloudTrail configuration in the master account, and verify that the storage location is set to the correct S3 bucket.
- F. Confirm in the CloudTrail Console that the S3 bucket name is set correctly.

**Answer: BDF**

**NEW QUESTION 227**

A company has a forensic logging use case whereby several hundred applications running on Docker on EC2 need to send logs to a central location. The Security Engineer must create a logging solution that is able to perform real-time analytics on the log files, grants the ability to replay events, and persists data.

Which AWS Services, together, can satisfy this use case? (Select two.)

- A. Amazon Elasticsearch
- B. Amazon Kinesis
- C. Amazon SQS
- D. Amazon CloudWatch
- E. Amazon Athena

**Answer: AB**

**NEW QUESTION 230**

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 fulfill this requirement.

Please select:

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

**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.amazon.com/about-aws/whats-new/2015/12/turn-on-cloudtrail-across-all-regions-and-support-for-multiple-regions/> The correct answer is: Ensure one Cloudtrail trail is enabled for all regions. Submit your Feedback/Queries to our Experts

**NEW QUESTION 235**

A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized AWS IAM user from the IP address range 10.10.10.0/24:

```
{
  "Version": "2012-10-17",
  "Id": "S3Policy1",
  "Statement": [
    {
      "Sid": ["OfficeAllowIP"],
      "Effect": ["Allow"],
      "Principal": ["*"],
      "Action": ["s3:*"],
      "Resource": ["arn:aws:s3:::Bucket"],
      "Condition": {
        "IpAddress": [
          {
            "aws:SourceIp": "10.10.10.0/24"
          }
        ]
      }
    }
  ]
}
```

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message. What does the Administrator need to change to grant access to the user?

- A. Change the "Resource" from "arn:aws:s3:::Bucket" to "arn:aws:s3:::Bucket/\*".
- B. Change the "Principal" from "\*" to {"AWS":"arn:aws:iam::account-number:user/username"}
- C. Change the "Version" from "2012-10-17" to the last revised date of the policy
- D. Change the "Action" from ["s3:\*"] to ["s3:GetObject", "s3:ListBucket"]

**Answer: A**

**NEW QUESTION 237**

Your company has been using AWS for the past 2 years. They have separate S3 buckets for logging the various AWS services that have been used. They have hired an external vendor for analyzing their log files. They have their own AWS account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below

Please select:

- A. Create an IAM user in the company account
- B. Create an IAM Role in the company account
- C. Ensure the IAM user has access for read-only to the S3 buckets
- D. Ensure the IAM Role has access for read-only to the S3 buckets

**Answer: BD**

**Explanation:**

The AWS Documentation mentions the following

To share log files between multiple AWS accounts, you must perform the following general steps. These steps are explained in detail later in this section.

Create an IAM role for each account that you want to share log files with.  
For each of these IAM roles, create an access policy that grants read-only access to the account you want to share the log files with.  
Have an IAM user in each account programmatically assume the appropriate role and retrieve the log files. Options A and C are invalid because creating an IAM user and then sharing the IAM user credentials with the vendor is a direct 'NO' practise from a security perspective.  
For more information on sharing cloudtrail logs files, please visit the following URL <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-share-logs.html>  
The correct answers are: Create an IAM Role in the company account Ensure the IAM Role has access for read-only to the S3 buckets  
Submit your Feedback/Queries to our Experts

**NEW QUESTION 242**

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 244**

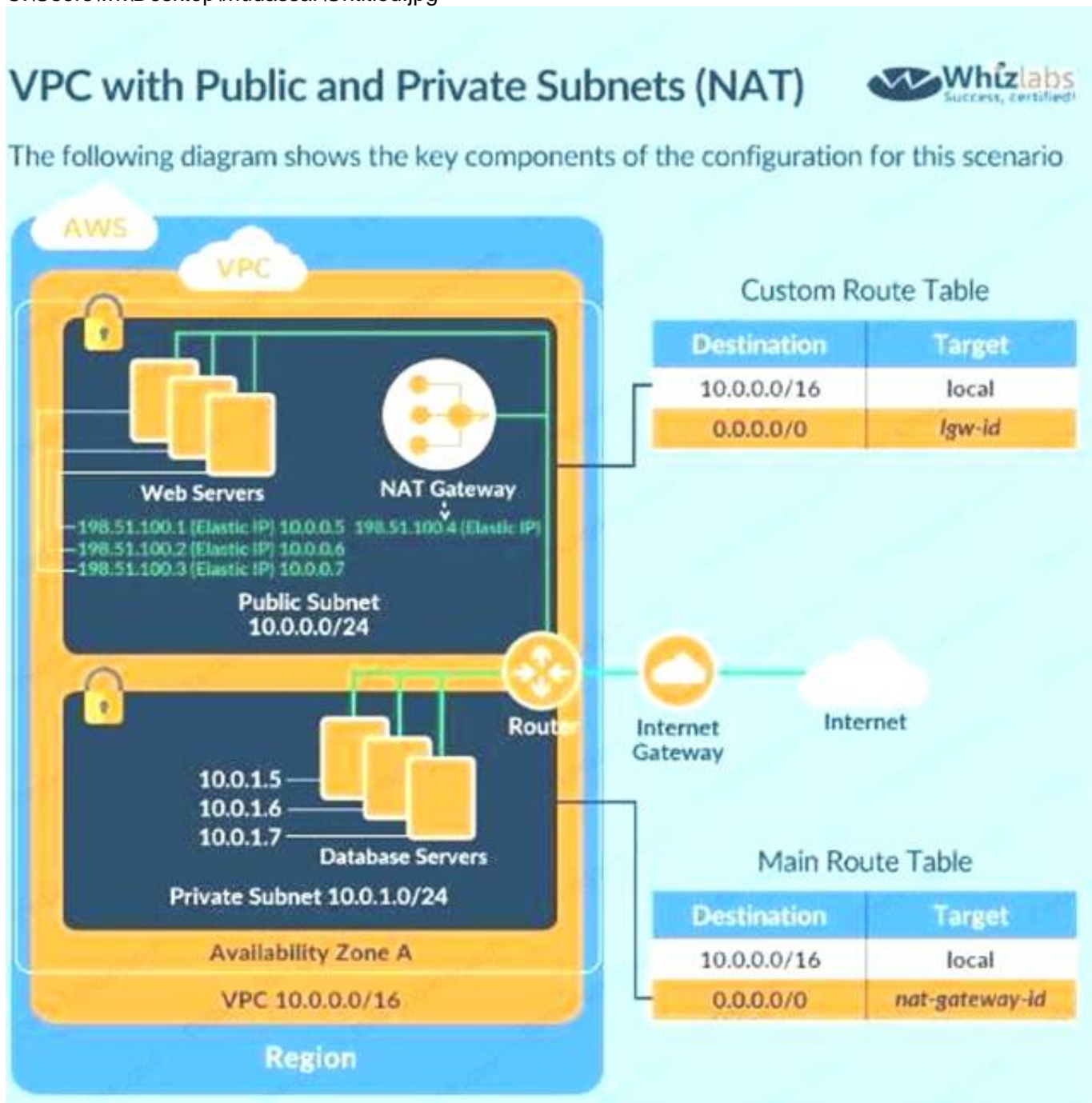
You are planning on hosting a web application on AWS. You create an EC2 Instance in a public subnet. This instance needs to connect to an EC2 Instance that will host an Oracle database. Which of the following steps should be followed to ensure a secure setup is in place? Select 2 answers.  
Please select:

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

**Answer:** BC

**Explanation:**

The best secure option is to place the database in a private subnet. The below diagram from the AWS Documentation shows this setup. Also ensure that access is not allowed from all sources but just from the web servers.  
C:\Users\wk\Desktop\mudassar\Untitled.jpg



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

Option D is invalid because the database security group should not allow traffic from the internet For more information on this type of setup, please refer to the below URL:

[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC\\_Scenario2](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_Scenario2).

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

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 246

A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair.

How can this task be accomplished?

- A. Obtain the list of instances by directly querying Amazon EC2 using: `aws ec2 describe-instances --filters "Name=key-name,Values=KEYNAMEHERE"`.
- B. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in the Amazon Inspector logs.
- C. Obtain the output from the EC2 instance metadata using: `curl http://169.254.169.254/latest/meta-data/public-keys/0/`.
- D. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in Amazon CloudWatch Logs using: `aws logs filter-log-events`.

**Answer: D**

#### NEW QUESTION 248

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

A.

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
    "Bool": {"aws:MultiFactorAuthPresent": true}
  }
}
```

B.

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
    "Bool": {"aws:MultiFactorAuthPresent": false}
  }
}
```

C.

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
    "aws:MultiFactorAuthPresent": false
  }
}
```

D.



```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
    "aws:MultiFactorAuthPresent":true
  }
}
```

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 252**

In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an AWS Auto Scaling group, your instances are constantly being re-created. What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below

Please select:

- A. Give only the necessary access to the Apache servers so that the developers can gain access to the log files.
- B. Give root access to your Apache servers to the developers.
- C. Give read-only access to your developers to the Apache servers.
- D. Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

**Answer:** D

**Explanation:**

One important security aspect is to never give access to actual servers, hence Option A.B and C are just totally wrong from a security perspective.

The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3.

Options A,B and C are all invalid because you should not give access to the developers on the Apache se For more information on S3, please refer to the below link

<https://aws.amazon.com/documentation/s3j>

The correct answer is: Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

Submit your Feedback/Queries to our Experts

**NEW QUESTION 255**

One of the EC2 Instances in your company has been compromised. What steps would you take to ensure that you could apply digital forensics on the Instance.

Select 2 answers from the options given below

Please select:

- A. Remove the role applied to the Ec2 Instance
- B. Create a separate forensic instance
- C. Ensure that the security groups only allow communication to this forensic instance
- D. Terminate the instance

**Answer:** BC

**Explanation:**

Option A is invalid because removing the role will not help completely in such a situation

Option D is invalid because terminating the instance means that you cannot conduct forensic analysis on the instance

One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance.

For more information on security scenarios for your EC2 Instance, please refer to below URL: <https://d1.awsstatic.com/Marketplace/scenarios/security/SEC 11 TSB Final.pdf>

The correct answers are: Create a separate forensic instance. Ensure that the security groups only allow communication to this forensic instance

Submit your Feedback/Queries to our Experts

**NEW QUESTION 259**

.....



## Relate Links

**100% Pass Your SCS-C01 Exam with Exam Bible Prep Materials**

<https://www.exambible.com/SCS-C01-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>