Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

NEW QUESTION 1
You have an Ec2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective
Please select:

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

Answer: A

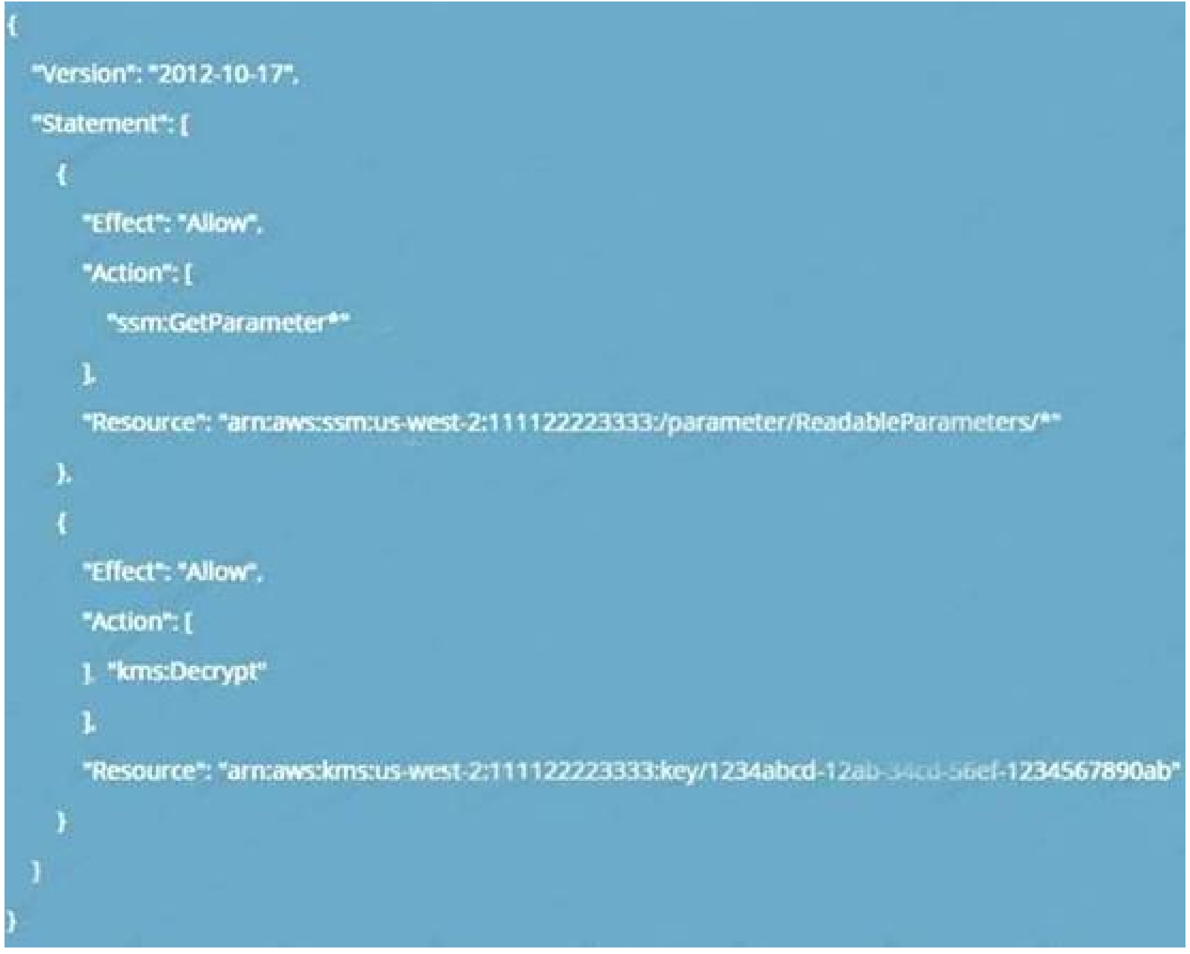
Explanation:
The AWS Documentation mentions the following
You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and AWS KMS is conducted entirely within the AWS network.
Option B is invalid because this could open threats from the internet
Option C is invalid because this is normally used for communication between on-premise environments and AWS.
Option D is invalid because this is normally used for communication between VPCs
For more information on accessing KMS via an endpoint, please visit the following URL https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.htmll
The correct answer is: Use a VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 2
An application running on EC2 instances must use a username and password to access a database. The developer has stored those secrets in the SSM Parameter Store with type SecureString using the default KMS CMK. Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below
Please select:

A. Add the EC2 instance role as a trusted service to the SSM service role.
B. Add permission to use the KMS key to decrypt to the SSM service role.
C. Add permission to read the SSM parameter to the EC2 instance role..
D. Add permission to use the KMS key to decrypt to the EC2 instance role
E. Add the SSM service role as a trusted service to the EC2 instance rol

Answer: CD

Explanation:
The below example policy from the AWS Documentation is required to be given to the EC2 Instance in order to read a secure string from AWS KMS. Permissions need to be given to the Get Parameter API and the KMS API call to decrypt the secret.



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter*"
      ],
      "Resource": "arn:aws:ssm:us-west-2:111122223333:/parameter/ReadableParameters/*"
    },
    {
      "Effect": "Allow",
      "Action": [
      ], "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```

Option A is invalid because roles can be attached to EC2 and not EC2 roles to SSM Option B is invalid because the KMS key does not need to decrypt the SSM service role.
Option E is invalid because this configuration is valid For more information on the parameter store, please visit the below URL:
https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.htmll
The correct answers are: Add permission to read the SSM parameter to the EC2 instance role., Add permission to use the KMS key to decrypt to the EC2 instance role
Submit your Feedback/Queries to our Experts

NEW QUESTION 3
Your company has mandated that all calls to the AWS KMS service be recorded. How can this be achieved?
Please select:

A. Enable logging on the KMS service
B. Enable a trail in Cloudtrail
C. Enable Cloudwatch logs
D. Use Cloudwatch metrics

Answer: B

Explanation:
The AWS Documentation states the following
AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP
address from which the request was made, who made the request when it was made, and so on. Option A is invalid because logging is not possible in the KMS service
Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL https://docs.aws.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html The correct answer is: Enable a trail in Cloudtrail
Jubmit your Feedback/Queries to our Experts

NEW QUESTION 4
You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?
Please select:

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

Answer: C

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

NEW QUESTION 5
Your company is planning on hosting an internal network in AWS. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.
Please select:

A. Consider using Windows Server 2016 Certificate Manager
B. Consider using AWS Certificate Manager
C. Consider using AWS Access keys to generate the certificates
D. Consider using AWS Trusted Advisor for managing the certificates

Answer: B

Explanation:
The AWS Documentation mentions the following
ACM is tightly linked with AWS Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally. Private certificates cannot be publicly trusted
Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", AWS Certificate Manager should be used Option C and D are invalid because these cannot be used for managing certificates.
For more information on ACM, please visit the below URL: https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html
The correct answer is: Consider using AWS Certificate Manager Submit your Feedback/Queries to our Experts

NEW QUESTION 6
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
The correct answer is: Check the Route tables for the VPCs Submit your Feedback/Queries to our Experts

NEW QUESTION 7
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 encryptio

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 8
An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.
Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below
Please select:

A. A network ACL with a rule that allows outgoing traffic on port 443.
B. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports
C. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.
D. A security group with a rule that allows outgoing traffic on port 443
E. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports.
F. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

Answer: BD

Explanation:
Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port.
Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports
Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443 Option E and F are invalid since here you are allowing additional ports on Security groups which are not required
For more information on VPC Security Groups, please visit the below URL:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.htmll
The correct answers are: A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports, A security group with a rule that allows outgoing traffic on port 443
Submit your Feedback/Queries to our Experts

NEW QUESTION 9
A company has a set of resources defined in AWS. It is mandated that all API calls to the resources be monitored. Also all API calls must be stored for lookup purposes. Any log data greater than 6 months must be archived. Which of the following meets these requirements? Choose 2 answers from the options given below. Each answer forms part of the solution.
Please select:

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

Answer: AD

Explanation:
Cloudtrail publishes the trail of API logs to an S3 bucket
Option B is invalid because you cannot put the logs into Glacier from CloudTrail
Option C is invalid because lifecycle policies cannot be used to move data to EBS volumes For more information on Cloudtrail logging, please visit the below URL:
https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/cloudtrail-find-log-files.htmll
You can then use Lifecycle policies to transfer data to Amazon Glacier after 6 months For more information on S3 lifecycle policies, please visit the below URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html
The correct answers are: Enable CloudTrail logging in all accounts into S3 buckets. Ensure a lifecycle policy is defined on the bucket to move the data to Amazon Glacier after 6 months.

Submit your Feedback/Queries to our Experts

NEW QUESTION 10
You are building a large-scale confidential documentation web server on AWSand all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use Cloud Front to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below
Please select:

A. Create an Identity and Access Management (1AM) user for CloudFront and grant access to the objects in your S3 bucket to that 1AM User.
B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAl.
C. Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.
D. Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: B

Explanation:
If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if user's access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront ace logs are less useful because they're incomplete.
Option A is invalid because you need to create a Origin Access Identity for Cloudfront and not an 1AM user
Option C and D are invalid because using policies will not help fulfil the requirement For more information on Origin Access Identity please see the below Link: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contentrestrictine- access-to-s3.htmll
The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
(
Submit your Feedback/Queries to our Experts

NEW QUESTION 10
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 create

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 newCMKand 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 sam CMK to decrypt the dat
A. As long as you keep both
the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK.
Option B is invalid because you also need to point the key alias to the new key Option C is invalid because existing CMK keys cannot be rotated as they are
Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key
For more information on Key rotation please see the below Link: https://docs.aws.amazon.com/kms/latest/developereuide/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 15
A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement?
Please select:

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

Answer: C

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

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

NEW QUESTION 16
When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users? These permissions should be easily managed.
Please select:

A. Use the secure token service to manage the permissions for the different users
B. Use 1AM Policies to create different policies for the different types of users.
C. Use the AWS Config tool to manage the permissions for the different users
D. Use 1AM Access Keys to create sets of keys for the different types of user

Answer: B

Explanation:
The AWS Documentation mentions the following
You control access to Amazon API Gateway with 1AM permissions by controlling access to the following two API Gateway component processes:
* To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.
* To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required 1AM actions supported by the API execution component of API Gateway.
Option A, C and D are invalid because these cannot be used to control access to AWS services. This needs to be done via policies. For more information on permissions with the API gateway, please visit the following URL: https://docs.aws.amazon.com/apisateway/latest/developerguide/permissions.html
The correct answer is: Use 1AM Policies to create different policies for the different types of users. Submit your Feedback/Queries to our Experts

NEW QUESTION 18
A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?
Please select:

A. Use Bucket policies
B. Use the Secure Token service
C. Use 1AM user policies
D. Use AWS Access Keys

Answer: AC

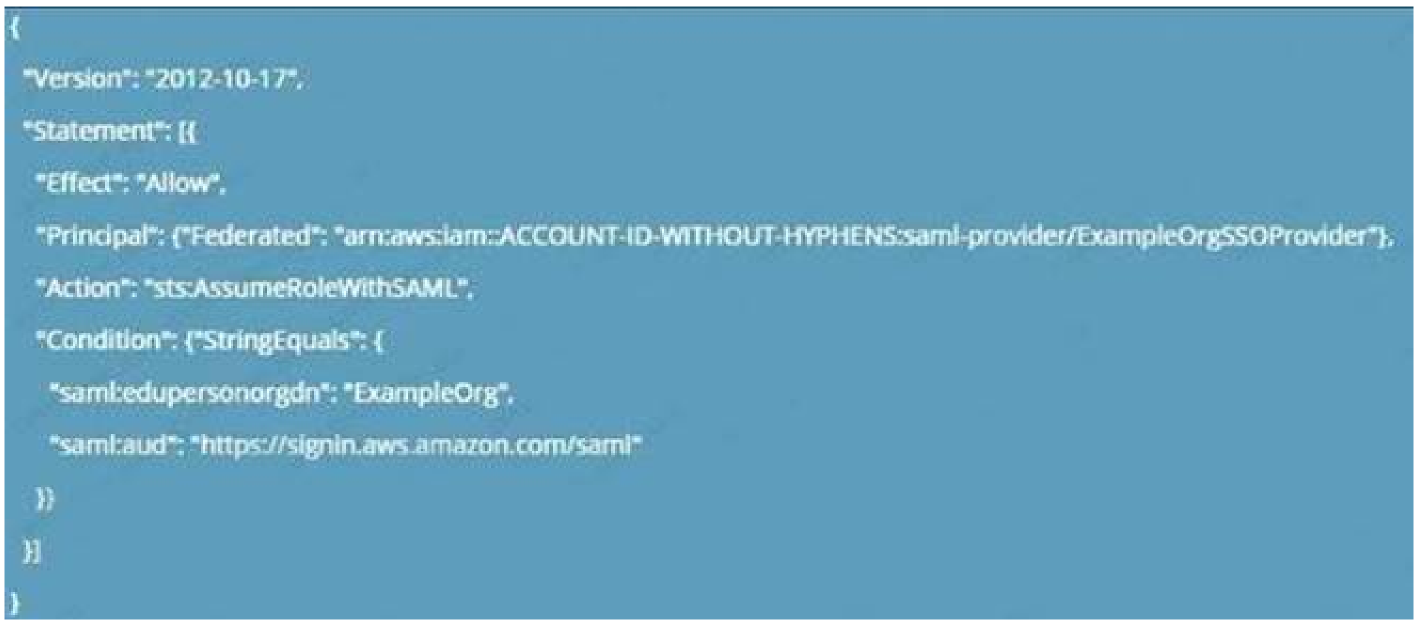
Explanation:
The AWS Documentation mentions the following
Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as
resource-based policies. For example, bucket policies and access control lists (ACLs) are resourcebased policies. You can also attach access policies to users in your account. These are called user
policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.
Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below Link: https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.htmll
The correct answers are: Use Bucket policies. Use 1AM user policies Submit your Feedback/Queries to our Experts

NEW QUESTION 23
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 AW
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:



```
{
 "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_enabli 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 24
Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company's EC2 instances?
Please select:

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

Answer: D

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

NEW QUESTION 26
A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database - administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure-
* sgLB - associated with the ELB
* sgWeb - associated with the EC2 instances.
* sgDB - associated with the database
* sgBastion - associated with the bastion host Which security group configuration will allow the application to be secure and functional?
Please select: A.
sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from 0.0.0.0/0 sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range
B.
sgLB :aIlow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgLB sgBastion: allow port 22 traffic from the VPC IP address range C.
sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB
sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the VPC IP address range D.
sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB

sgDB :al!ow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

A.

Answer: D

Explanation:
The Load Balancer should accept traffic on ow port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer
The database should allow traffic from the Web server
And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on AWS Security Groups, please refer to below URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.htmll
The correct answer is: sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB
sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range Submit your Feedback/Queries to our Experts

NEW QUESTION 31
A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working. What is the other step that needs to be followed to ensure that the AD domain join can work as intended
Please select:

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

Answer: C

Explanation:
In addition to VPC peering and setting the right route tables, the security groups for the AD EC2 instance needs to ensure the right rules are put in place for allowing incoming traffic.
Option A and B is invalid because changing the connection type will not help. This is a problem with the Security Groups.
Option D is invalid since the AD should not be placed in a public subnet
For more information on allowing ingress traffic for AD, please visit the following url
|https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html|
The correct answer is: Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets Submit your Feedback/Queries to our Experts

NEW QUESTION 32
You need to inspect the running processes on an EC2 Instance that may have a security issue. How can you achieve this in the easiest way possible. Also you need to ensure that the process does not interfere with the continuous running of the instance.
Please select:

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

Answer: C

Explanation:
The SSM Run command can be used to send OS specific commands to an Instance. Here you can check and see the running processes on an instance and then send the output to an S3 bucket. Option A is invalid because this is used to record API activity and cannot be used to record running
processes.
Option B is invalid because Cloudwatch is a logging and metric service and cannot be used to record running processes.
Option D is invalid because AWS Config is a configuration service and cannot be used to record running processes.
For more information on the Systems Manager Run command, please visit the following URL: https://docs.aws.amazon.com/systems-manaEer/latest/usereuide/execute-remote-commands.htmll The correct answer is: Use the SSM Run command to send the list of running processes information to an S3 bucket. Submit your Feedback/Queries to our Experts

NEW QUESTION 36
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 AP

Answer: ACD

Explanation:
For ensuring that the instances are configured properly you need to ensure the followi .
1) You installed the latest version of the SSM Agent on your instance
2) Your instance is configured with an AWS Identity and Access Management (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-remotecommands. html
The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure that agent is running on the Instances., Check the Instance status by using the Health API.
Submit your Feedback/Queries to our Experts

NEW QUESTION 40
You are trying to use the AWS Systems Manager run command on a set of Instances. The run command on a set of Instances. What can you do to diagnose the issue? Choose 2 answers from the options given
Please select:

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

Answer: AB

Explanation:
The AWS Documentation mentions the following
If you experience problems executing commands using Run Command, there might be a problem with the SSM Agent. Use the following information to help you troubleshoot the agent
View Agent Logs
The SSM Agent logs information in the following files. The information in these files can help you troubleshoot problems.
On Windows
%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log
%PROGRAMDATA%\Amazon\SSM\Logs\error.log
The default filename of the seelog is seelog-xml.template. If you modify a seelog, you must rename the file to seelog.xml.
On Linux
/var/log/amazon/ssm/amazon-ssm-agentlog /var/log/amazon/ssm/errors.log
Option C is invalid because the right AMI has nothing to do with the issues. The agent which is used to execute run commands can run on a variety of AMI'S
Option D is invalid because security groups does not come into the picture with the communication between the agent and the SSM service
For more information on troubleshooting AWS SSM, please visit the following URL: https://docs.aws.amazon.com/systems-manaeer/latest/userguide/troubleshootine-remotecommands. htmll
The correct answers are: Ensure that the SSM agent is running on the target machine. Check the /var/log/amazon/ssm/errors.log file
Submit your Feedback/Queries to our Experts

NEW QUESTION 42
You work as an administrator for a company. The company hosts a number of resources using AWS. There is an incident of a suspicious API activity which occurred 11 days ago. The Security Admin has asked to get the API activity from that point in time. How can this be achieved?
Please select:

A. Search the Cloud Watch logs to find for the suspicious activity which occurred 11 days ago
B. Search the Cloudtrail event history on the API events which occurred 11 days ago.
C. Search the Cloud Watch metrics to find for the suspicious activity which occurred 11 days ago
D. Use AWS Config to get the API calls which were made 11 days ag

Answer: B

Explanation:
The Cloud Trail event history allows to view events which are recorded for 90 days. So one can use a metric filter to gather the API calls from 11 days ago.
Option A and C is invalid because Cloudwatch is used for logging and not for monitoring API activity Option D is invalid because AWSConfig is a configuration service and not for monitoring API activity For more information on AWS Cloudtrail, please visit the following URL:
https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/how-cloudtrail-works.html
Note:
In this question we assume that the customer has enabled cloud trail service.
AWS CloudTrail is enabled by default for ALL CUSTOMERS and will provide visibility into the past seven days of account activity without the need for you to configure a trail in the service to get started. So for an activity that happened 11 days ago to be stored in the cloud trail we need to configure the trail manually to ensure that it is stored in the events history.
• https://aws.amazon.com/blogs/aws/new-amazon-web-services-extends-cloudtrail-to-all-awscustomers/ The correct answer is: Search the Cloudtrail event history on the API events which occurred 11 days ago.

NEW QUESTION 47
You have a requirement to serve up private content using the keys available with Cloudfront. How can this be achieved?
Please select:

A. Add the keys to the backend distribution.
B. Add the keys to the S3 bucket
C. Create pre-signed URL's
D. Use AWS Access keys

Answer: C

Explanation:
Option A and B are invalid because you will not add keys to either the backend distribution or the S3 bucket.
Option D is invalid because this is used for programmatic access to AWS resources
You can use Cloudfront key pairs to create a trusted pre-signed URL which can be distributed to users Specifying the AWS Accounts That Can Create Signed URLs and Signed Cookies (Trusted Signers) Topics
• Creating CloudFront Key Pairs for Your Trusted Signers
• Reformatting the CloudFront Private Key (.NET and Java Only)

- Adding Trusted Signers to Your Distribution
- Verifying that Trusted Signers Are Active (Optional) 1 Rotating CloudFront Key Pairs

To create signed URLs or signed cookies, you need at least one AWS account that has an active CloudFront key pair. This accou is known as a trusted signer.
The trusted signer has two purposes:

- As soon as you add the AWS account ID for your trusted signer to your distribution, CloudFront starts to require that users us signed URLs or signed cookies to access your objects.

' When you create signed URLs or signed cookies, you use the private key from the trusted signer's key pair to sign a portion of the URL or the cookie. When someone requests a restricted object CloudFront compares the signed portion of the URL or cookie with the unsigned portion to verify that the URL or cookie hasn't been tampered with. CloudFront also verifies that the URL or cookie is valid, meaning, for example, that the expiration date and time hasn't passed.
For more information on Cloudfront private trusted content please visit the following URL:

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contenttrusted- s

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

NEW QUESTION 49
Your application currently uses customer keys which are generated via AWS KMS in the US east region. You now want to use the same set of keys from the EU-Central region. How can this be accomplished?
Please select:

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

Answer: D

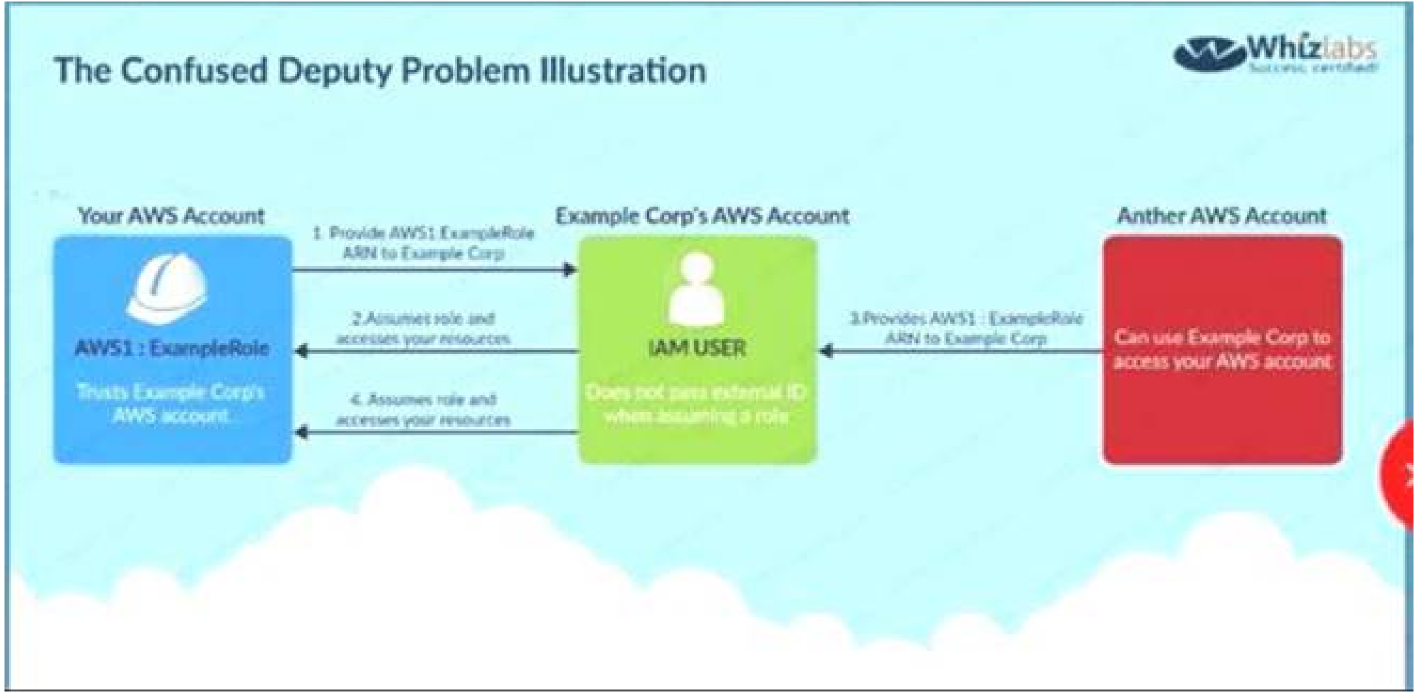
Explanation:
Option A is invalid because keys cannot be exported and imported across regions. Option B is invalid because key rotation cannot be used to export keys
Option C is invalid because the backing key cannot be used to export keys This is mentioned in the AWS documentation
What geographic region are my keys stored in?
Keys are only stored and used in the region in which they are created. They cannot be transferred to another region. For example; keys created in the EU-Central (Frankfurt) region are only stored and used within the EU-Central (Frankfurt) region
For more information on KMS please visit the following URL: https://aws.amazon.com/kms/faqs/
The correct answer is: This is not possible since keys from KMS are region specific Submit your Feedback/Queries to our Experts

NEW QUESTION 51
You currently have an S3 bucket hosted in an AWS Account. It holds information that needs 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 1AM role is created which can be assumed by the partner account.
B. Ensure an 1AM 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 1AM 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 1AM role and external ID is us> access an AWS account resources


The Confused Deputy Problem Illustration
Whizlabs
Success certified!
Your AWS Account
AWS1 : ExampleRole
Trusts Example Corp's AWS account
1. Provide AWS1 ExampleRole ARN to Example Corp
2.Assumes role and accesses your resources
4. Assumes role and accesses your resources
Example Corp's AWS Account
IAM USER
Does not pass external ID when assuming a role
3.Provides AWS1 : ExampleRole ARN to Example Corp
Anther AWS Account
Can use Example Corp to access your AWS account

For more information on creating roles for external ID'S please visit the following URL:
The correct answers are: Ensure an 1AM 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

NEW QUESTION 55
You have a set of Customer keys created using the AWS KMS service. These keys have been used for around 6 months. You are now trying to use the new KMS features for the existing set of key's but are not able to do so. What could be the reason for this.
Please select:

A. You have not explicitly given access via the key policy
B. You have not explicitly given access via the 1AM policy
C. You have not given access via the 1AM roles
D. You have not explicitly given access via 1AM users

Answer: A

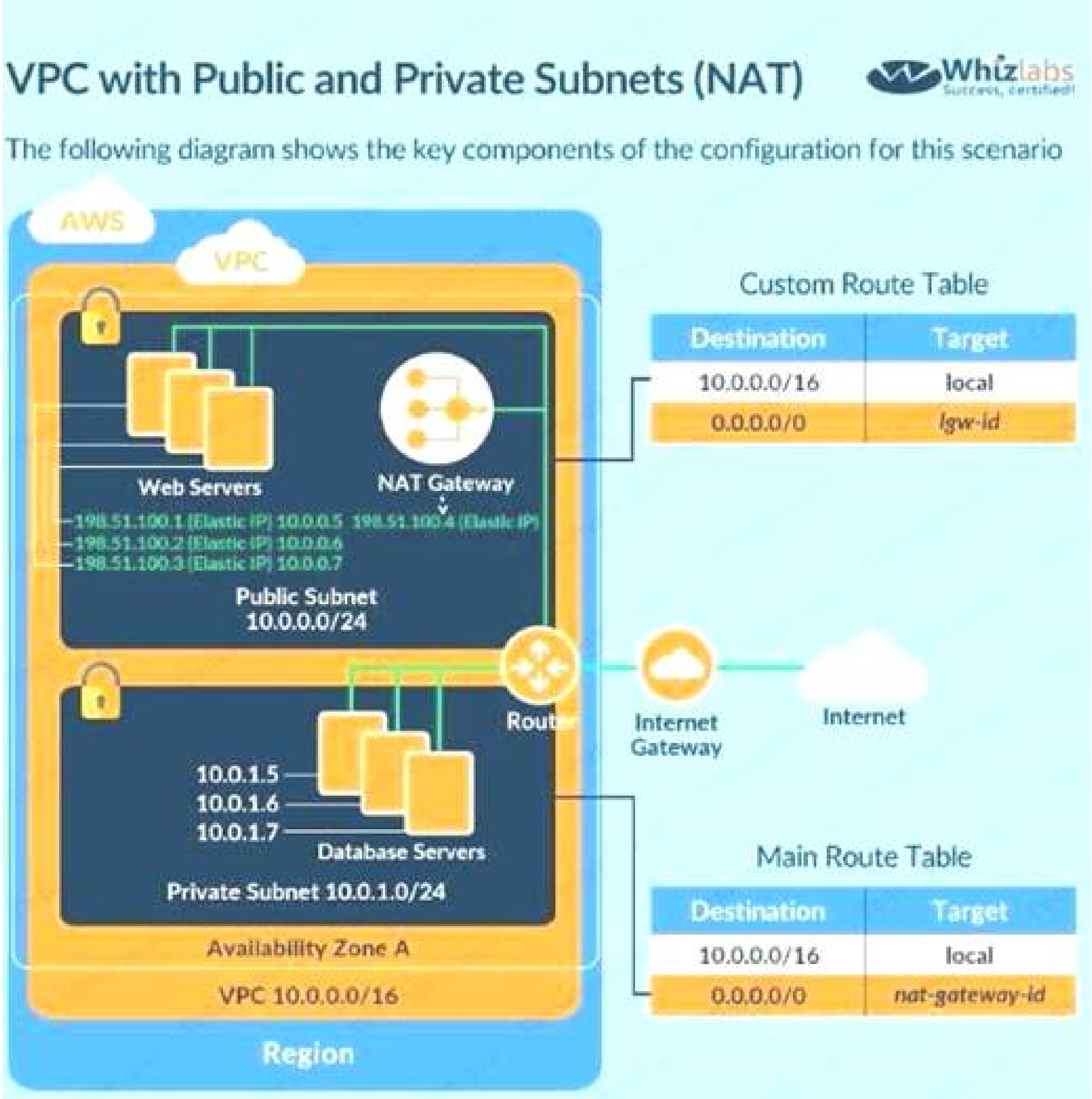
Explanation:
By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explii update the default key policy for these keys.
Option B,C and D are invalid because the key policy is the main entity used to provide access to the keys
For more information on upgrading key policies please visit the following URL: https://docs.aws.ama20n.com/kms/latest/developerguide/key-policy-upgrading.html
(
The correct answer is: You have not explicitly given access via the key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 56
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.


VPC with Public and Private Subnets (NAT)
Whizlabs
Success, certified!
The following diagram shows the key components of the configuration for this scenario
AWS
VPC
Web Servers
NAT Gateway
198.51.100.1 (Elastic IP) 10.0.0.5
198.51.100.2 (Elastic IP) 10.0.0.6
198.51.100.3 (Elastic IP) 10.0.0.7
198.51.100.4 (Elastic IP)
Public Subnet
10.0.0.0/24
Router
Internet Gateway
Internet
10.0.1.5
10.0.1.6
10.0.1.7
Database Servers
Private Subnet 10.0.1.0/24
Availability Zone A
VPC 10.0.0.0/16
Region
Custom Route Table
Main Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-gateway-id

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.
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 57
An EC2 Instance hosts a Java based application that access a DynamoDB table. This EC2 Instance is currently serving production based users. Which of the following is a secure way of ensuring that the EC2 Instance access the Dynamo table
Please select:

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

Answer: A

Explanation:
To always ensure secure access to AWS resources from EC2 Instances, always ensure to assign a Role to the EC2 Instance Option B is invalid because KMS keys are not used as a mechanism for providing EC2 Instances access to AWS services. Option C is invalid Access keys is not a safe mechanism for providing EC2 Instances access to AWS services. Option D is invalid because there is no way access groups can be assigned to EC2 Instances. For more information on 1AM Roles, please refer to the below URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id roles.html
The correct answer is: Use 1AM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 58
Development teams in your organization use S3 buckets to store the log files for various applications hosted ir development environments in AWS. The developers want to keep the logs for one month for troubleshooting purposes, and then purge the logs. What feature will enable this requirement? Please select:

A. Adding a bucket policy on the S3 bucket.
B. Configuring lifecycle configuration rules on the S3 bucket.
C. Creating an 1AM policy for the S3 bucket.
D. Enabling CORS on the S3 bucke

Answer: B

Explanation:
The AWS Documentation mentions the following on lifecycle policies
Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified a« follows:
Transition actions - In which you define when objects transition to another . For example, you may choose to
transition objects to the STANDARDJA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.
Expiration actions - In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.
Option A and C are invalid because neither bucket policies neither 1AM policy's can control the purging of logs Option D is invalid CORS is used for accessing objects across domains and not for purging of logs For more information on AWS S3 Lifecycle policies, please visit the following URL:
.com/AmazonS3/latest/d<
The correct answer is: Configuring lifecycle configuration rules on the S3 bucket. Submit your Feedback/Queries to our Experts

NEW QUESTION 62
A company has a large set of keys defined in AWS KMS. Their developers frequently use the keys for the applications being developed. What is one of the ways that can be used to reduce the cost of accessing the keys in the AWS KMS service.
Please select:

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

Answer: B

Explanation:
The AWS Documentation mentions the following
Data key caching stores data keys and related cryptographic material in a cache. When you encrypt or decrypt data, the AWS Encryption SDK looks for a matching data key in the cache. If it finds a match, it uses the cached data key rather than generatir a new one. Data key caching can improve performance, reduce cost, and help you stay within service limits as your application scales. Option A.C and D are all incorrect since these options will not impact how the key is used.
For more information on data key caching, please refer to below URL: https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-key-cachine.htmll
The correct answer is: Use Data key caching Submit your Feedback/Queries to our Experts

NEW QUESTION 64
Your company use AWS KMS for management of its customer keys. From time to time, there is a requirement to delete existing keys as part of housekeeping activities. What can be done during the deletion process to verify that the key is no longer being used.
Please select:

A. Use CloudTrail to see if any KMS API request has been issued against existing keys
B. Use Key policies to see the access level for the keys
C. Rotate the keys once before deletion to see if other services are using the keys
D. Change the 1AM policy for the keys to see if other services are using the keys

Answer: A

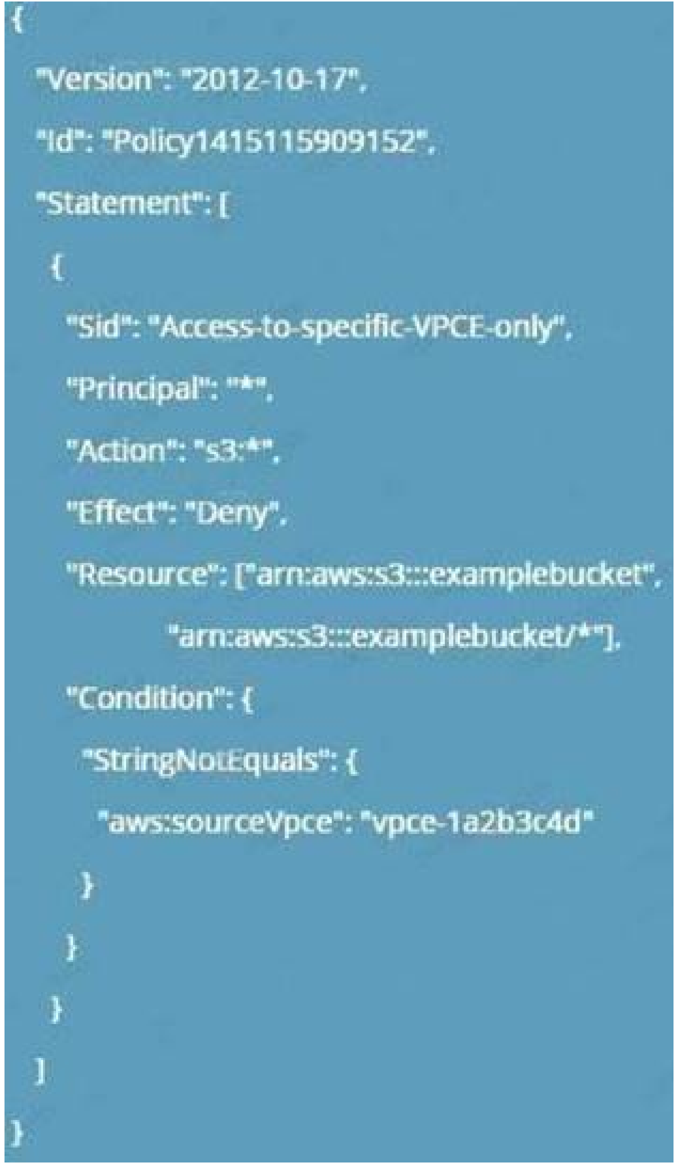
Explanation:
The AWS lentation mentions the following
You can use a combination of AWS CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an alarm that notifies you of AWS KMS API requests that attempt to use a customer master key (CMK) that is pending deletion. If you receive a notification from such an alarm, you might want to cancel deletion of the CMK to give yourself more time to determine whether you want to delete it
Options B and D are incorrect because Key policies nor 1AM policies can be used to check if the keys are being used.
Option C is incorrect since rotation will not help you check if the keys are being used. For more information on deleting keys, please refer to below URL:
https://docs.aws.amazon.com/kms/latest/developereuide/deletine-keys-creatine-cloudwatchalarm. html
The correct answer is: Use CloudTrail to see if any KMS API request has been issued against existing keys Submit your Feedback/Queries to our Experts

NEW QUESTION 69
You have a bucket and a VPC defined in AWS. You need to ensure that the bucket can only be accessed by the VPC endpoint. How can you accomplish this?
Please select:

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

Answer: D

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



```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
   {
     "Sid": "Access-to-specific-VPCE-only",
     "Principal": "*",
     "Action": "s3:*",
     "Effect": "Deny",
     "Resource": ["arn:aws:s3:::examplebucket",
                  "arn:aws:s3:::examplebucket/*"],
     "Condition": {
       "StringNotEquals": {
         "aws:sourceVpce": "vpce-1a2b3c4d"
       }
     }
   }
  ]
}
```

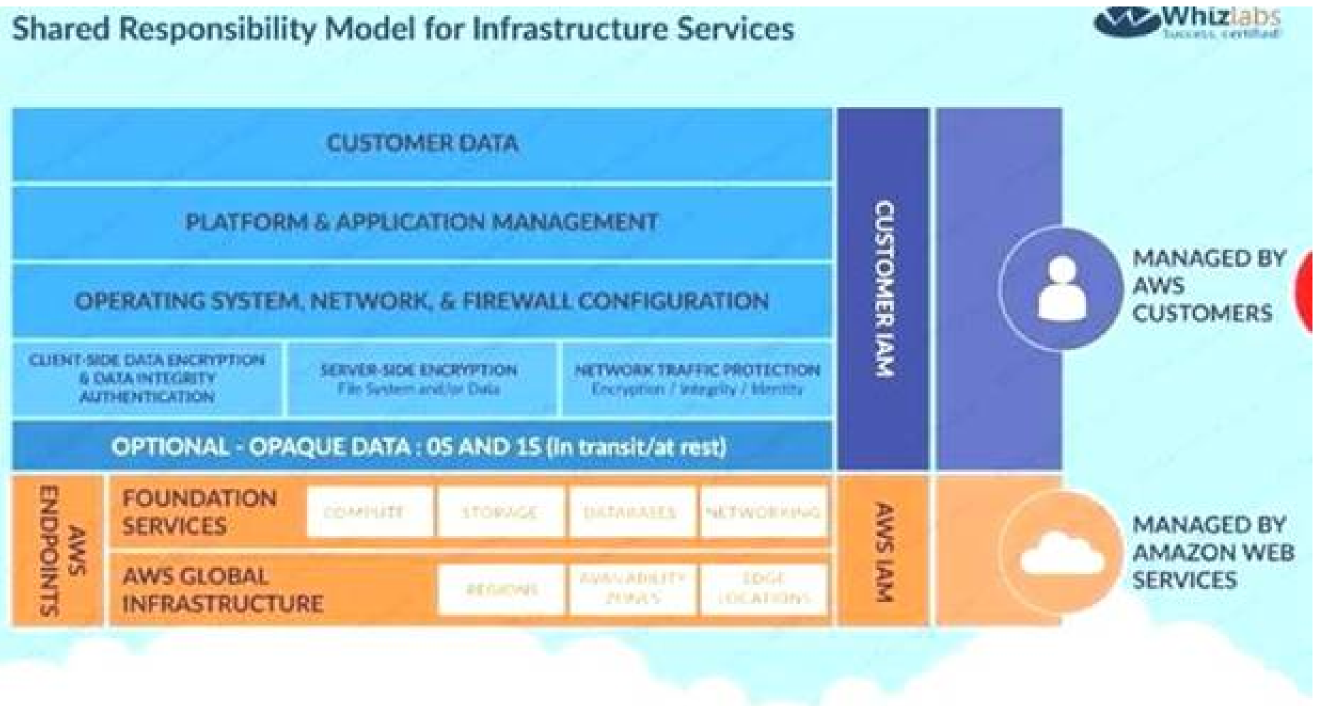
Options A and B are incorrect because using Security Groups nor route tables will help to allow access specifically for that bucke via the VPC endpoint Here you specifically need to ensure the bucket policy is changed.
Option C is incorrect because it is the bucket policy that needs to be changed and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

NEW QUESTION 72
Which of the following is the responsibility of the customer? Choose 2 answers from the options given below.
Please select:

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

Answer: BC

Explanation:
Below is the snapshot of the Shared Responsibility Model


Shared Responsibility Model for Infrastructure Services
Whizlabs
success, certified
CUSTOMER DATA
PLATFORM & APPLICATION MANAGEMENT
OPERATING SYSTEM, NETWORK, & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION
File System and/or Data
NETWORK TRAFFIC PROTECTION
Encryption / Integrity / Identity
OPTIONAL - OPAQUE DATA : 0S AND 1S (In transit/at rest)
CUSTOMER IAM
MANAGED BY AWS CUSTOMERS
AWS ENDPOINTS
FOUNDATION SERVICES
COMPUTE
STORAGE
DATABASES
NETWORKING
AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS
AWS IAM
MANAGED BY AMAZON WEB SERVICES

For more information on AWS Security best practises, please refer to below URL
.awsstatic corn/whitepapers/Security/AWS Practices.
The correct answers are: Encryption of data at rest Protection of data in transit Submit your Feedback/Queries to our Experts

NEW QUESTION 77
You want to track access requests for a particular S3 bucket. How can you achieve this in the easiest possible way?
Please select:

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

Answer: A

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

NEW QUESTION 81
Your company has just started using AWS and created an AWS account. They are aware of the potential issues when root access is enabled. How can they best safeguard the account when it comes to root access? Choose 2 answers fro the options given below
Please select:

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

Answer: BD

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

NEW QUESTION 85
You need to create a Linux EC2 instance in AWS. Which of the following steps is used to ensure secure authentication the EC2 instance from a windows machine. Choose 2 answers from the options given below.
Please select:

A. Ensure to create a strong password for logging into the EC2 Instance
B. Create a key pair using putty
C. Use the private key to log into the instance
D. Ensure the password is passed securely using SSL

Answer: BC

Explanation:
The AWS Documentation mentions the following

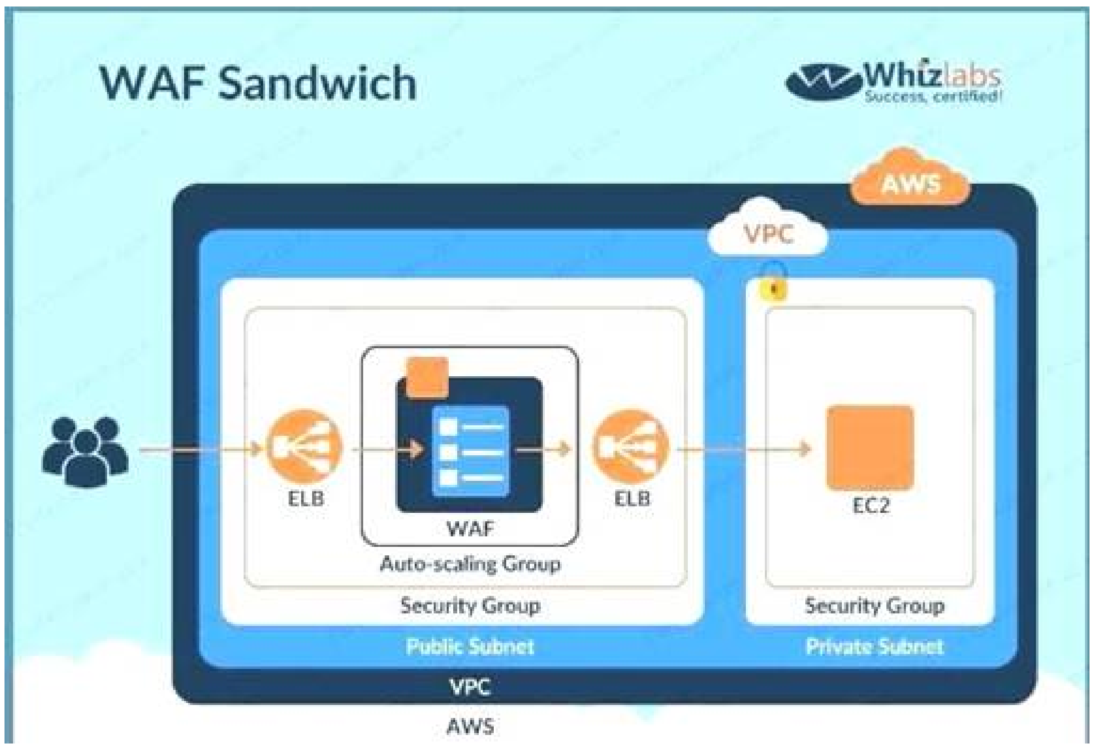
You can use Amazon EC2 to create your key pair. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt login information, so it's important that you store your private keys in a secure place.
Options A and D are incorrect since you should use key pairs for secure access to Ec2 Instances For more information on EC2 key pairs, please refer to below URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html
The correct answers are: Create a key pair using putty. Use the private key to log into the instance Submit your Feedback/Queries to our Experts

NEW QUESTION 88
DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs sit in-line with your application traffic. Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a "WAF sandwich." Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below
Please select:

A. The EC2 instance running your WAF software is placed between your private subnets and any NATed connections to the internet.
B. The EC2 instance running your WAF software is placed between your public subnets and your Internet Gateway.
C. The EC2 instance running your WAF software is placed between your public subnets and your private subnets.
D. he EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.

Answer: D

Explanation:
The below diagram shows how a WAF sandwich is created. Its the concept of placing the Ec2 instance which hosts the WAF software in between 2 elastic load balancers.



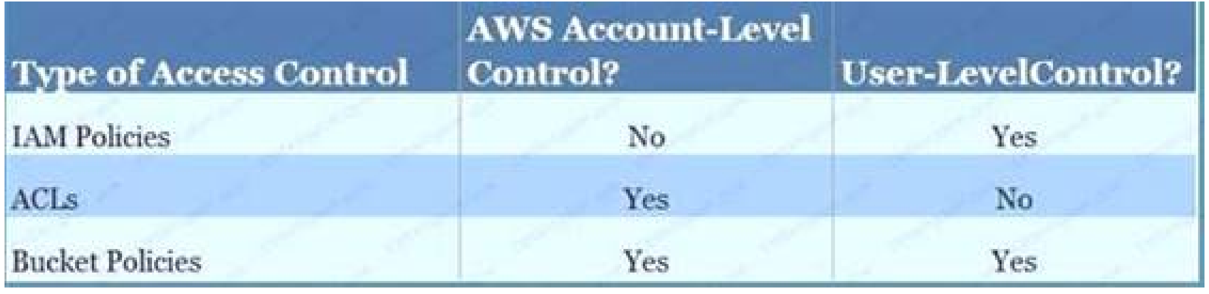
Option A.B and C are incorrect since the EC2 Instance with the WAF software needs to be placed in an Autoscaling Group For more information on a WAF sandwich please refer to the below Link: https://www.cloudaxis.eom/2016/11/2l/waf-sandwich/l
The correct answer is: The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.
Submit your Feedback/Queries to our Experts

NEW QUESTION 92
You have several S3 buckets defined in your AWS account. You need to give access to external AWS accounts to these S3 buckets. Which of the following can allow you to define the permissions for the external accounts? Choose 2 answers from the options given below
Please select:

A. 1AM policies
B. Buckets ACL's
C. 1AM users
D. Bucket policies

Answer: BD

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



Type of Access Control	AWS Account-Level Control?	User-LevelControl?
IAM Policies	No	Yes
ACLs	Yes	No
Bucket Policies	Yes	Yes

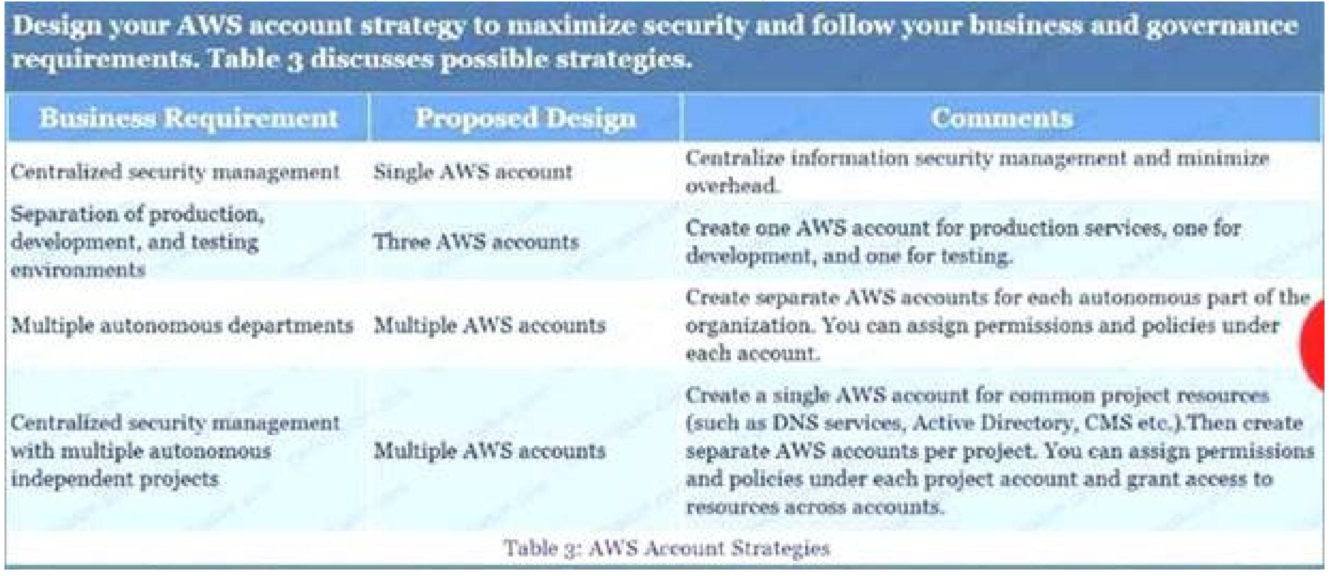
Options A and C are incorrect since for external access to buckets, you need to use either Bucket policies or Bucket ACL's or more information on Security for storage services role please refer to the below URL:
https://d1.awsstatic.com/whitepapers/Security/Security Storage Services Whitepaper.pdf The correct answers are: Buckets ACL's, Bucket policies
Submit your Feedback/Queries to our Experts

NEW QUESTION 95
A large organization is planning on AWS to host their resources. They have a number of autonomous departments that wish to use AWS. What could be the strategy to adopt for managing the accounts. Please select:

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

Answer: D

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



Design your AWS account strategy to maximize security and follow your business and governance requirements. Table 3 discusses possible strategies.

Business Requirement	Proposed Design	Comments
Centralized security management	Single AWS account	Centralize information security management and minimize overhead.
Separation of production, development, and testing environments	Three AWS accounts	Create one AWS account for production services, one for development, and one for testing.
Multiple autonomous departments	Multiple AWS accounts	Create separate AWS accounts for each autonomous part of the organization. You can assign permissions and policies under each account.
Centralized security management with multiple autonomous independent projects	Multiple AWS accounts	Create a single AWS account for common project resources (such as DNS services, Active Directory, CMS etc.).Then create separate AWS accounts per project. You can assign permissions and policies under each project account and grant access to resources across accounts.

Table 3: AWS Account Strategies

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

NEW QUESTION 96
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 encryptii 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 amoui of dat
A\\ 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/developereuide/concepts.htmll
The correct answers are: Password, RSA Keys Submit your Feedback/Queries to our Experts

NEW QUESTION 100
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 1AM user in the company account
B. Create an 1AM Role in the company account
C. Ensure the 1AM user has access for read-only to the S3 buckets
D. Ensure the 1AM 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 1AM role for each account that you want to share log files with.
For each of these 1AM roles, create an access policy that grants read-only access to the account you want to share the log files with.
Have an 1AM user in each account programmatically assume the appropriate role and retrieve the log files.
Options A and C are invalid because creating an 1AM user and then sharing the 1AM 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-sharine-loes.htmll
The correct answers are: Create an 1AM Role in the company account Ensure the 1AM Role has access for read-only to the S3 buckets
Submit your Feedback/Queries to our Experts

NEW QUESTION 102
The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy Submit your Feedback/Queries to our Experts
You company has mandated that all data in AWS be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below
Please select:

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

Answer: AB

Explanation:
EBS encryption can also be enabled when the volume is created and not for existing volumes. One can use existing tools for OS level encryption.
Option C is incorrect.
AWS Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.
Option D is incorrect
You cannot choose to encrypt a non-encrypted boot volume on instance launch. To have encrypted boot volumes during launch , your custom AMI must have it's boot volume encrypted before launch. For more information on the Security Best practices, please visit the following URL:
.com/whit Security Practices.
The correct answers are: Use Windows bit locker for EBS volumes on Windows instances. Use TrueEncrypt for EBS volumes on Linux instances
Submit your Feedback/Queries to our Experts

NEW QUESTION 107
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 recreated.
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 thelog 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 vour Feedback/Queries to our Experts

NEW QUESTION 109
Your company is planning on developing an application in AWS. This is a web based application. The application user will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this.
Please select:

A. Create an OlDC identity provider in AWS
B. Create a SAML provider in AWS
C. Use AWS Cognito to manage the user profiles
D. Use 1AM users to manage the user profiles

Answer: C

Explanation:
The AWS Documentation mentions the following
A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers. Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.
User pools provide:
Sign-up and sign-in services.
A built-in, customizable web Ul to sign in users.
Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user pool.
User directory management and user profiles.
Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.
Customized workflows and user migration through AWS Lambda triggers. Options A and B are invalid because these are not used to manage users Option D is invalid because this would be a maintenance overhead
For more information on Cognito User Identity pools, please refer to the below Link: https://docs.aws.amazon.com/coenito/latest/developerguide/cognito-user-identity-pools.html
The correct answer is: Use AWS Cognito to manage the user profiles Submit your Feedback/Queries to our Experts

NEW QUESTION 111
Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?
Please select:

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

Answer: B

Explanation:
The AWS Documentation mentions the following
Amazon S3 is integrated with AWS CloudTrail. CloudTrail is a service that captures specific API calls made to Amazon S3 from your AWS account and delivers the log files to an Amazon S3 bucket that you specify. It captures API calls made from the Amazon S3 console or from the Amazon S3 API. Using the information collected by CloudTrail, you can determine what request was made to Amazon S3, the source IP address from which the request was made, who made the request when it was
made, and so on
Options A,C and D are invalid because these services cannot be used to get the source IP address of the calls to S3 buckets
For more information on Cloudtrail logging, please refer to the below Link:
https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logeins.htmll
The correct answer is: Monitor the S3 API calls by using Cloudtrail logging Submit your Feedback/Queries to our Experts

NEW QUESTION 113
You have private video content in S3 that you want to serve to subscribed users on the Internet. User
IDs, credentials, and subscriptions are stored in an Amazon RDS database. Which configuration will allow you to securely serve private content to your users?
Please select:

A. Generate pre-signed URLs for each user as they request access to protected S3 content
B. Create an 1AM user for each subscribed user and assign the GetObject permission to each 1AM user
C. Create an S3 bucket policy that limits access to your private content to only your subscribed users'credentials
D. Crpafp a Cloud Front Clriein Identity user for vnur suhsrrihprl users and assign the GptOhiprt oprmissinn to this user

Answer: A

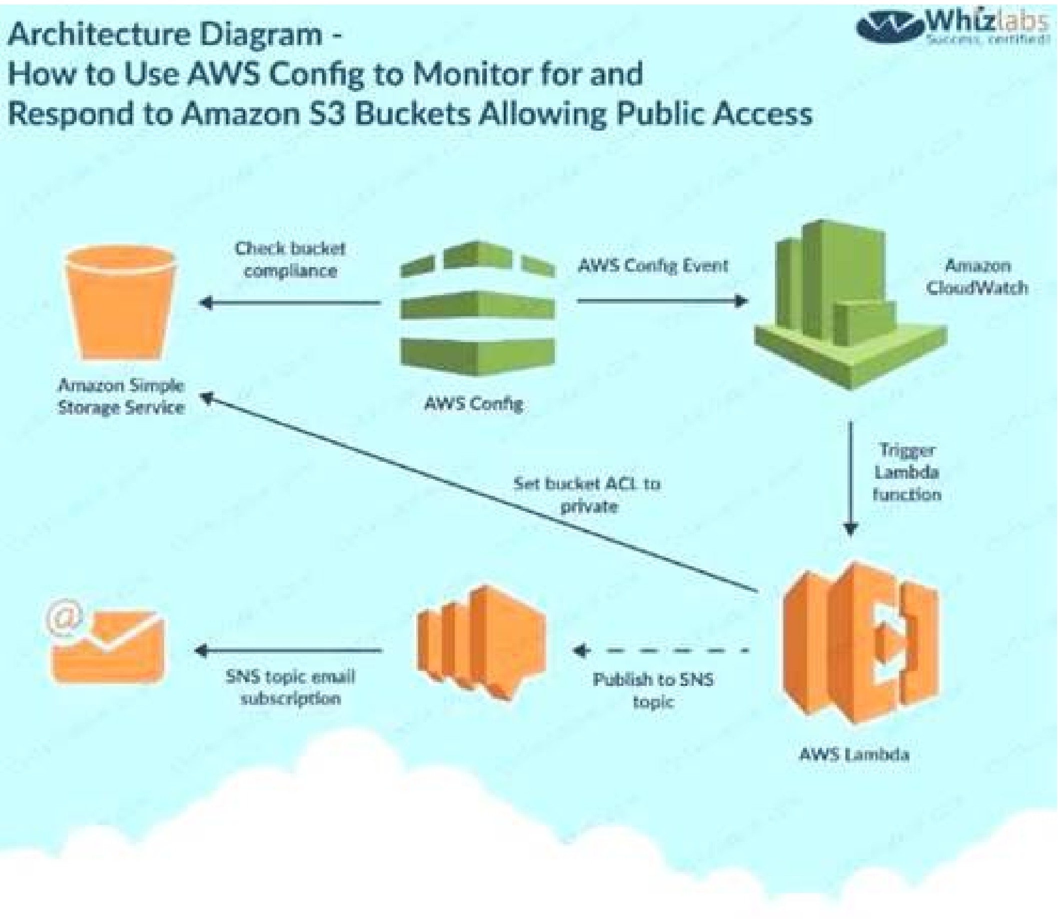
Explanation:
All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able upload a specific object to your bucket but you don't require them to have AWS security credentials or permissions. When you create a pre-signed URL, you must provide your security credentials, specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The pre-signed URLs are valid only for the specified duration.
Option B is invalid because this would be too difficult to implement at a user level. Option C is invalid because this is not possible
Option D is invalid because this is used to serve private content via Cloudfront For more information on pre-signed urls, please refer to the Link:
http://docs.aws.amazon.com/AmazonS3/latest/dev/PresienedUrlUploadObiect.htmll
The correct answer is: Generate pre-signed URLs for each user as they request access to protected S3 content Submit your Feedback/Queries to our Experts

NEW QUESTION 118
A company is hosting sensitive data in an AWS S3 bucket. It needs to be ensured that the bucket always remains private. How can this be ensured continually? Choose 2 answers from the options given below
Please select:

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

Answer: AD

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


Architecture Diagram -
How to Use AWS Config to Monitor for and
Respond to Amazon S3 Buckets Allowing Public Access
Whizlabs
Success, certified!
Check bucket compliance
AWS Config Event
Amazon CloudWatch
Amazon Simple Storage Service
AWS Config
Trigger Lambda function
Set bucket ACL to private
SNS topic email subscription
Publish to SNS topic
AWS Lambda

ption C is invalid because the Trusted Advisor API cannot be used to monitor changes to the AWS Bucket Option B doesn't seems to be the most appropriate.
1. If the object is in a bucket in which all the objects need to be private and the object is not private anymore, the Lambda function makes a PutObjectAcl call to S3 to make the object private.
|https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintendedpermissions- in-amazon-s3-bbiect-acls-with-cloudwatch-events/
The following link also specifies that
Create a new Lambda function to examine an Amazon S3 buckets ACL and bucket policy. If the bucket ACL is found to al public access, the Lambda function overwrites it to be private. If a bucket policy is found, the Lambda function creatt an SNS message, puts the policy in the message body, and
publishes it to the Amazon SNS topic we created. Bucket policies can be complex, and overwriting your policy may cause unexpected loss of access, so this Lambda function doesn't attempt to alter your policy in any way.
https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-toamazon- s3-buckets-allowinj
Based on these facts Option D seems to be more appropriate then Option B.
For more information on implementation of this use case, please refer to the Link: https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-toamazon- s3-buckets-allowinj
The correct answers are: Use AWS Config to monitor changes to the AWS Bucket Use AWS Lambda function to change the bucket ACL

NEW QUESTION 121
You currently operate a web application In the AWS US-East region. The application runs on an autoscaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has
tasked you to develop a reliable and durable logging solution to track changes made to your EC2.IAM and RDS resources. The solution must ensure the integrity and confidentiality of your log dat

A. Which of these solutions would you recommend? Please select:
B. Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selecte
C. Use 1AM roles S3 bucket policies and Mufti Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
D. Create a new CloudTrail with one new S3 bucket to store the log
E. Configure SNS to send log file delivery notifications to your management syste
F. Use 1AM roles and S3 bucket policies on the S3 bucket that stores your logs.
G. Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selecte
H. Use S3 ACLsand Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
I. Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tool
J. Use 1AM roles and S3 bucket policies on the S3 buckets that store your logs.

Answer: A

Explanation:
AWS Identity and Access Management (1AM) is integrated with AWS CloudTrail, a service that logs AWS events made by or on behalf of your AWS account. CloudTrail logs authenticated AWS API calls and also AWS sign-in events, and collects this event information in files that are delivered to Amazon S3 buckets. You need to ensure that all services are included. Hence option B is partially correct. Option B is invalid because you need to ensure that global services is select
Option C is invalid because you should use bucket policies
Option D is invalid because you should ideally just create one S3 bucket For more information on Cloudtrail, please visit the below URL:
http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-inteeration.html
The correct answer is: Create a new CloudTrail trail with one new S3 bucket to store the logs and with
the global services o selected. Use 1AM roles S3 bucket policies and Mulrj Factor Authentication (MFA) Delete on the S3 bucket that stores your l(
Submit your Feedback/Queries to our Experts

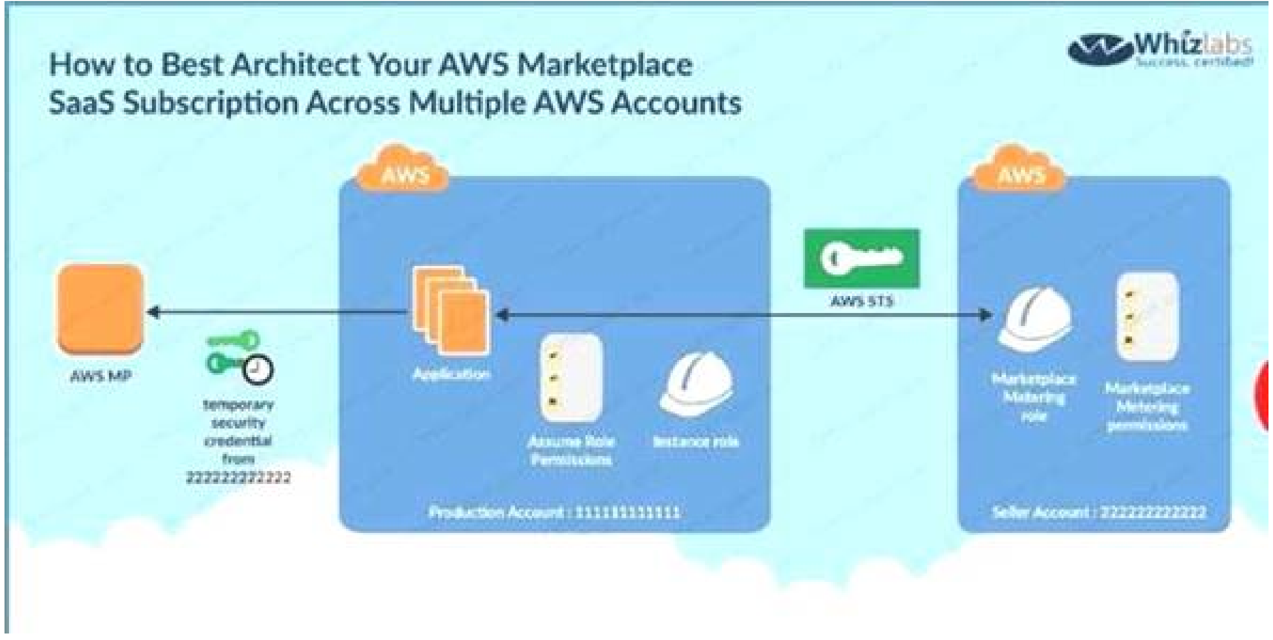
NEW QUESTION 124
An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions?
Please select:

A. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.

B. Create an 1AM user within the enterprise account assign a user policy to the 1AM user that allows only the actions required by the SaaS applicatio
C. Create a new access and secret key for the user and provide these credentials to the SaaS provider.
D. Create an 1AM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
E. Create an 1AM role for EC2 instances, assign it a policy that allows only the actions required tor the Saas application to work, provide the role ARN to the SaaS provider to use when launching their application instances.

Answer: C

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


How to Best Architect Your AWS Marketplace SaaS Subscription Across Multiple AWS Accounts
Whizlabs
Success, certified!
AWS
AWS
AWS STS
AWS MP
temporary security credential from 222222222222
Application
Assume Role Permissions
Instance role
Marketplace Metering role
Marketplace Metering permissions
Production Account : 111111111111
Seller Account : 222222222222

Options A and B are invalid because you should not user 1AM users or 1AM Access keys Options D is invalid because you need to create a role for cross account access
For more information on Allowing access to external accounts, please visit the below URL:
|https://aws.amazon.com/blogs/apn/how-to-best-architect-your-aws-marketplace-saassubscription- across-multiple-aws-accounts;
The correct answer is: Create an 1AM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
Submit your Feedback/Queries to our Experts

NEW QUESTION 128
You have an S3 bucket defined in AWS. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this.
Please select:

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

Answer: B

Explanation:
One can use the AWS Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL: https://aws.amazonxom/blogs/securirv/how4o-encrvpt-and-decrypt-your-data-with-the-awsencryption- cl
The correct answer is: Use the AWS Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

NEW QUESTION 132
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 134
There is a requirement for a company to transfer large amounts of data between AWS and an onpremise location. There is an additional requirement for low latency and high consistency traffic to
AWS. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below

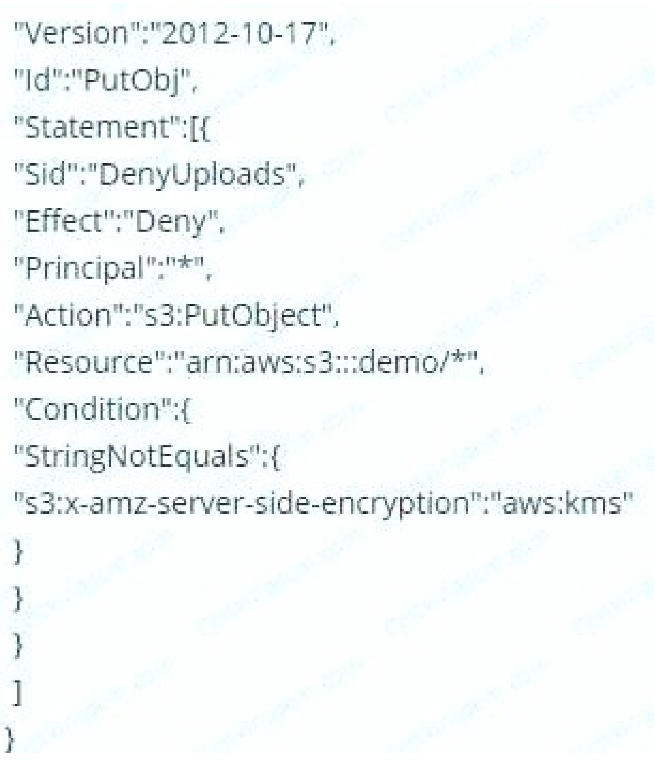
Please select:

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

Answer: A

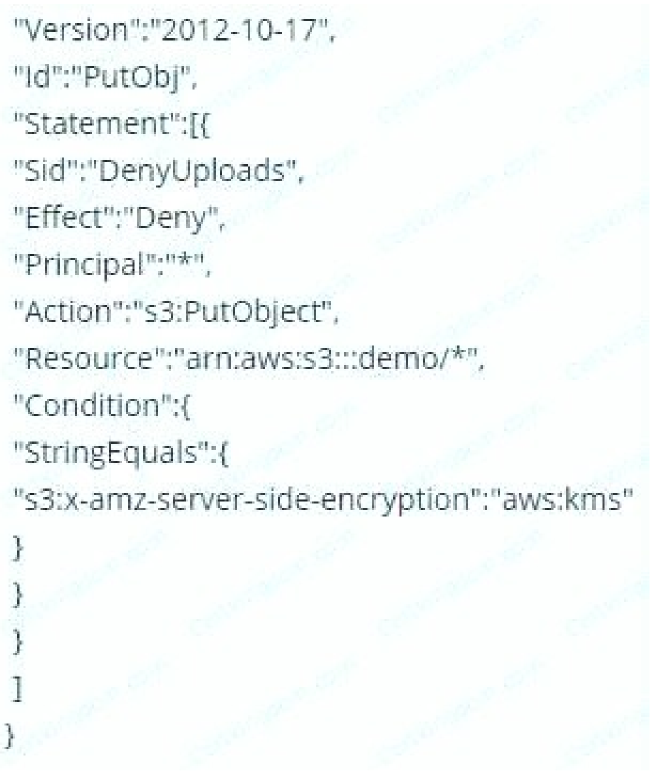
Explanation:
AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect you can establish private connectivity between AWS and your datacenter, office, or colocation environment which in many cases can reduce your network costs,
increase bandwidth throughput and provide a more consistent network experience than InternetQuestions
& Answers PDF P-140 based connections.
Options B and C are invalid because these options will not reduce network latency Options D is invalid because this is only used to connect 2 VPC's
For more information on AWS direct connect, just browse to the below URL: https://aws.amazon.com/directconnect
The correct answer is: Provision a Direct Connect connection to an AWS region using a Direct Connect partner. omit your Feedback/Queries to our Experts

NEW QUESTION 138
Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.
Please select:
A.



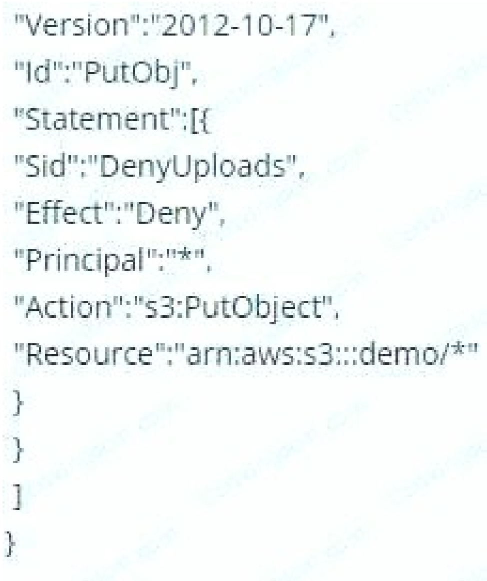
```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*",
"Condition":{
"StringNotEquals":{
"s3:x-amz-server-side-encryption":"aws:kms"
}
}
}
]
}
```

B.



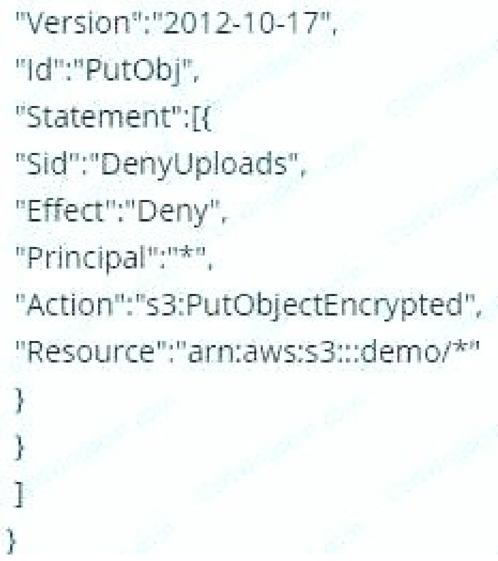
```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*",
"Condition":{
"StringEquals":{
"s3:x-amz-server-side-encryption":"aws:kms"
}
}
}
]
}
```

C.



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

D.

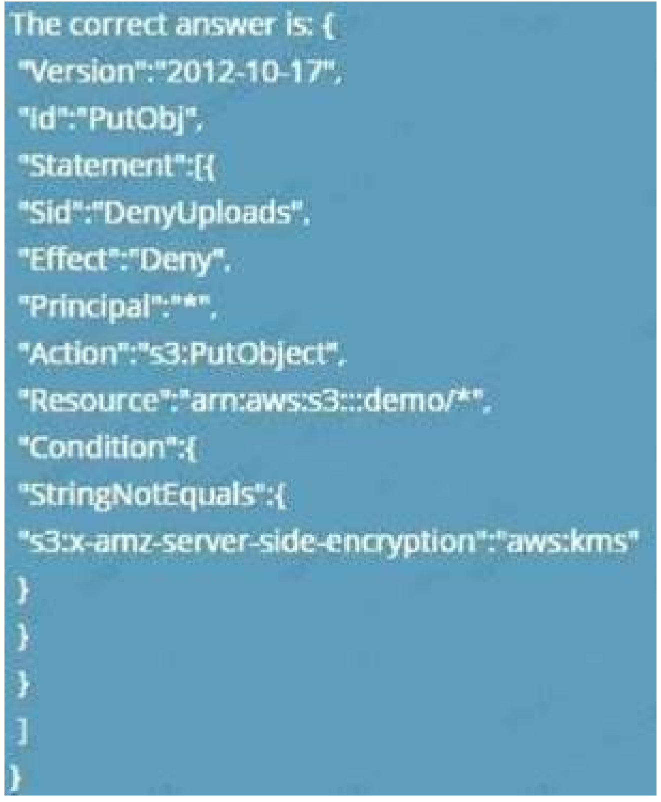


```
 "Version":"2012-10-17",
 "Id":"PutObj",
 "Statement":[{
 "Sid":"DenyUploads",
 "Effect":"Deny",
 "Principal":"*",
 "Action":"s3:PutObjectEncrypted",
 "Resource":"arn:aws:s3:::demo/*"
 }
 }
 ]
}
```

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 ns3:x-amz-server-sideencryption":" 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-praaices.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"
 }
 }
 }
 ]
}
```

Submit your Feedback/Queries to our Expert

NEW QUESTION 140
A company's AWS account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?
Please select:

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

Answer: B

Explanation:
Option A is incorrect since you don't add a user to the 1AM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach
An 1AM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group
For more information on 1AM Groups, just browse to the below URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the 1AM groups and add users, based upon their role, to different groups and apply the policy to group
Submit your Feedback/Queries to our Experts

NEW QUESTION 142
You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?
Please select:

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

Answer: D

Explanation:
Options A and B are incorrect since you need to add an inline policy just for the user Option C is invalid because you don't assign an 1AM role to a user
The AWS Documentation mentions the following
An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.
For more information on 1AM Access and Inline policies, just browse to the below URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/access
The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

NEW QUESTION 145
......