SCS-C01 Q&As

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/aws-certified-security-specialty.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 1

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

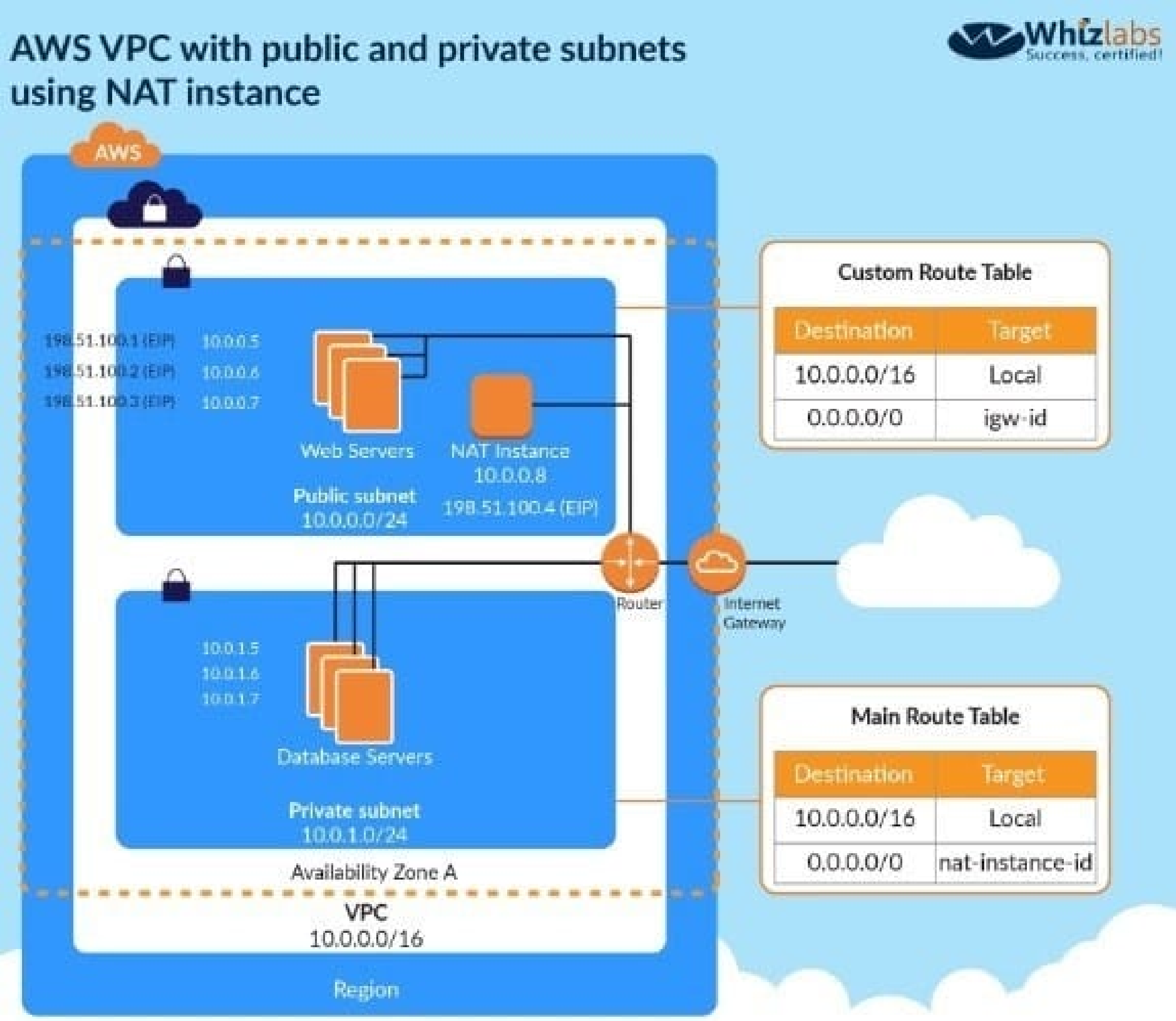
B. Use multiple IAM groups, each group for each department

C. Use multiple IAM roles, each group for each department

D. Use multiple AWS accounts, each account for each department

Correct Answer: D

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



Custom Route Table

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

Main Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	nat-instance-id

QUESTION 2

A company accidentally deleted the private key for an Amazon Elastic Block Store (Amazon EBS)-backed Amazon EC2 instance. A security engineer needs to regain access to the instance. Which combination of steps will meet this requirement? (Choose two.)

A. Stop the instance. Detach the root volume. Generate a new key pair.

B. Keep the instance running. Detach the root volume. Generate a new key pair.

C. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new public key. Move the volume back to the original instance. Start the instance.

D. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new private key. Move the volume back to the original instance. Start the instance.

E. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new public key. Move the volume back to the original instance that is running.

Correct Answer: DE

QUESTION 3

A company has two software development teams that are creating applications that store sensitive data in Amazon S3. Each team\\'s data must always be separate. The company\\'s security team must design a data encryption strategy for both teams that provides the ability to audit key usage. The solution must also minimize operational overhead.

What should the security team recommend?

A. Tell the application teams to use two different S3 buckets with separate AWS Key Management Service (AWS KMS) AWS managed CMKs. Limit the key policies to allow encryption and decryption of the CMKs to their respective teams only. Force the teams to use encryption context to encrypt and decrypt.

B. Tell the application teams to use two different S3 buckets with a single AWS Key Management Service (AWS KMS) AWS managed CMK. Limit the key policy to allow encryption and decryption of the CMK only. Do not allow the teams to use encryption context to encrypt and decrypt.

C. Tell the application teams to use two different S3 buckets with separate AWS Key Management Service (AWS KMS) customer managed CMKs Limit the key policies to allow encryption and decryption of the CMKs to their respective teams only Force the teams to use encryption context to encrypt and decrypt

D. Tell the application teams to use two different S3 buckets with a single AWS Key Management Service (AWS KMS) customer managed CMK Limit the key policy to allow encryption and decryption of the CMK only Do not allow the teams to use encryption context to encrypt and decrypt

Correct Answer: B

QUESTION 4

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

Correct Answer: C

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

QUESTION 5

A security engineer is attempting to assign a virtual multi-factor authentication (MFA) device to an IAM user whose current virtual MFA device is faulty. The security engineer receives an error message that indicates that the security engineer is not authorized to perform iam:DeleteVirtualMFADevice.

The IAM role that the security engineer is using has the correct permissions to delete, list, and create a virtual MFA device. The IAM user also has permissions to delete their own virtual MFA device, but only if the IAM user is authenticated with MFA.

What should the security engineer do to resolve this issue?

A. Modify the policy for the IAM user to allow the IAM user to delete the virtual MFA device without using MFA authentication.

B. Sign in as the AWS account root user. Modify the MFA device by using the IAM console to generate a new synchronization quick response (QR) code.

C. Use the AWS CLI or AWS API to find the ARN of the virtual MFA device and to delete the device.

D. Sign in as the AWS account root user. Delete the virtual MFA device by using the IAM console.

Correct Answer: D

QUESTION 6

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

Please select:

A. AWS KMS API

B. AWS Certificate Manager

C. API Gateway with STS

D. IAM Access Key

Correct Answer: A

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

KMS is integrated with other AWS services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage Option B is incorrect - The AWS Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest Option C is incorrect is again used for issuing tokens when using API gateway for traffic in transit. Option D is used for secure access to EC2 Instances For more information on AWS KMS, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developereuide/overview.htmll The correct answer is: AWS KMS API

QUESTION 7

A company is migrating one of its legacy systems from an on-premises data center to AWS. The application server will run on AWS, but the database must remain in the on-premises data center for compliance reasons. The database is sensitive to network latency. Additionally, the data that travels between the on-premises data center and AWS must have IPsec encryption.

Which combination of AWS solutions will meet these requirements? (Choose two.)

A. AWS Site-to-Site VPN

B. AWS Direct Connect

C. AWS VPN CloudHub

D. VPC peering

E. NAT gateway

Correct Answer: BD

QUESTION 8

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

A. Create an IAM user and generate encryption keys for that user. Create a policy for Redshift read-only access. Embed th keys in the application.

B. Create an HSM client certificate in Redshift and authenticate using this certificate.

C. Create a Redshift read-only access policy in IAM and embed those credentials in the application.

D. Use roles that allow a web identity federated user to assume a role that allows access to the Redshift table by providing temporary credentials.

Correct Answer: D

The AWS Documentation mentions the following "When you write such an app, you\\'ll make requests to AWS services that must be signed with an AWS access key. However, we strongly recommend that you do not embed or distribute longterm AWS credentials with apps that a user downloads t device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamica when needed using web identify federation. The supplied

temporary credentials map to an AWS role that has only the permissioi needed to perform the tasks required by the mobile app".

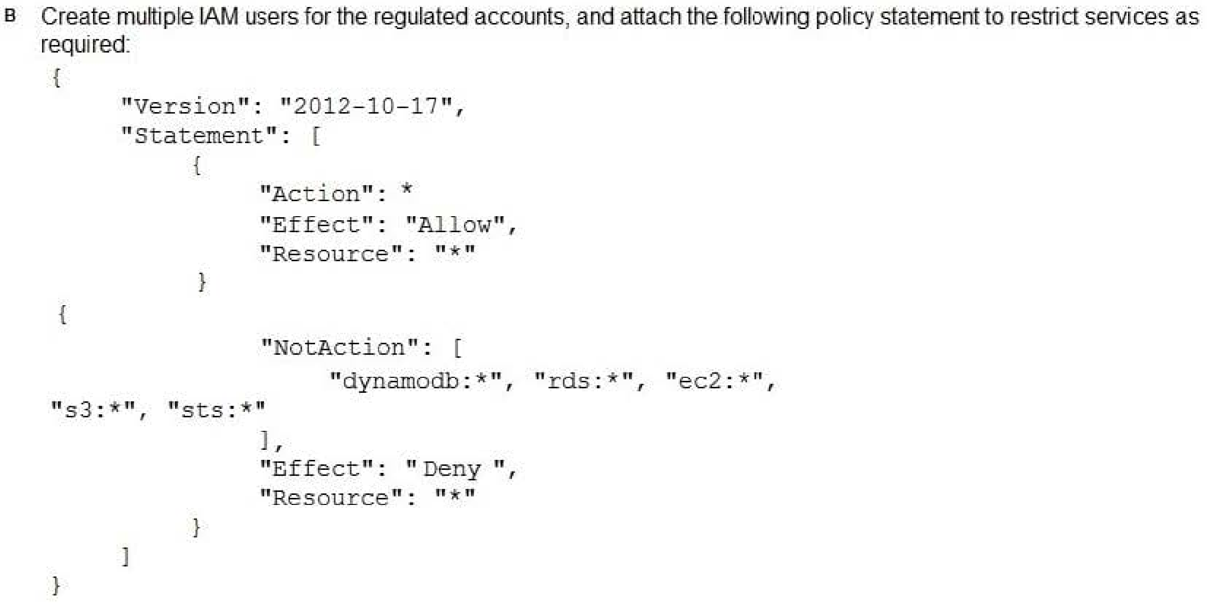
Option A.B and C are all automatically incorrect because you need to use IAM Roles for Secure access to services For more information on web identity federation please refer to the below Link:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html The correct answer is: Use roles that allow a web identity federated user to assume a role that allows access to the RedShift table by providing temporary

credentials.

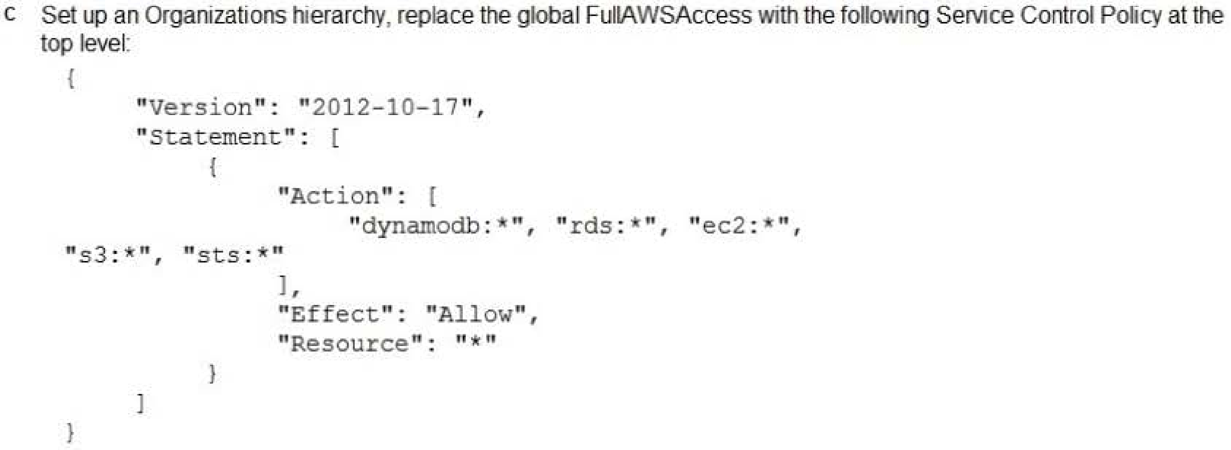
QUESTION 9

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



B Create multiple IAM users for the regulated accounts, and attach the following policy statement to restrict services as required:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": *
               "Effect": "Allow",
               "Resource": "*"
          }
 {
               "NotAction": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": " Deny ",
               "Resource": "*"
          }
     ]
}
```



C Set up an Organizations hierarchy, replace the global FullAWSAccess with the following Service Control Policy at the top level:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Allow",
               "Resource": "*"
          }
     ]
}
```

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

A. Move the bastion host to the VPC with VPN connectivity. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.

B. Create a SSH port forwarding tunnel on the Developer\\'s workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.

C. Move the bastion host to the VPC with VPN connectivity. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.

D. Create an AWS Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

Correct Answer: A

QUESTION 10

A company has a strict policy against using root credentials. The company\\'s security team wants to be alerted as soon as possible when root credentials are used to sign in to the AWS Management Console. How should the security team achieve this goal?

A. Use AWS Lambda to periodically query AWS CloudTrail for console login events and send alerts using Amazon Simple Notification Service (Amazon SNS).

B. Use Amazon EventBridge (Amazon CloudWatch Events) to monitor console logins and direct them to Amazon Simple Notification Service (Amazon SNS).

C. Use Amazon Athena to query AWS SSO logs and send alerts using Amazon Simple Notification Service (Amazon SNS) for root login events.

D. Configure AWS Resource Access Manager to review the access logs and send alerts using Amazon Simple Notification Service (Amazon SNS).

Correct Answer: D

Reference https://aws.amazon.com/blogs/security/how-to-receive-notifications-when-your-aws-accounts-root-access-keys-are-used/

QUESTION 11

A company\\'s database developer has just migrated an Amazon RDS database credential to be stored and managed by AWS Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.

After a short period of time, a number of existing applications have failed with authentication errors.

What is the MOST likely cause of the authentication errors?

A. Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.

B. Enabling rotation in Secrets Manager causes the secret to rotate immediately, and the applications are using the earlier credential.

C. The Secrets Manager IAM policy does not allow access to the RDS database.

D. The Secrets Manager IAM policy does not allow access for the applications.

Correct Answer: B

https://docs.aws.amazon.com/secretsmanager/latest/userguide/enable-rotation-rds.html

QUESTION 12

A company\\'s security engineer must record when specific AWS Lambda functions are invoked. The logs must include the AWS principal that invoked the function. External sources and the company\\'s developers deliver the Lambda function code by using a variety of languages such as Python, Node.js, and Golang. The security engineer has created an AWS CloudTrail trail with default configuration for the AWS account.

Which solution will meet these requirements with the LEAST operational overhead?

A. Update the Lambda function code to extract the AWS principal from the Lambda context and to write a log entry when the function to be monitored is invoked.

B. Use Amazon EventBridge (Amazon CloudWatch Events) to configure a rule and custom pattern for lambda:invoke events with a filter on the functions to monitor. Invoke another Lambda function to write the EventBridge (CloudWatch Events) data to Amazon CloudWatch Logs.

C. Modify the existing CloudTrail trail. Configure the existing CloudTrail trail to monitor Lambda functions as data events.

D. Create a Lambda layer that provides CloudTrail with a log event that includes the Lambda context when the function is invoked. Attach this layer to all Lambda functions that must be monitored.

Correct Answer: C

QUESTION 13

A company has a VPC with several Amazon EC2 instances behind a NAT gateway. The company\\'s security policy states that all network traffic must be logged and must include the original source and destination IP addresses. The existing VPC Flow Logs do not include this information. A security engineer needs to recommend a solution.

Which combination of steps should the security engineer recommend? (Choose two.)

A. Edit the existing VPC Flow Logs. Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.

B. Delete and recreate the existing VPC Flow Logs. Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.

C. Change the destination to Amazon CloudWatch Logs.

D. Include the pkt-srcaddr and pkt-dstaddr fields in the log format.

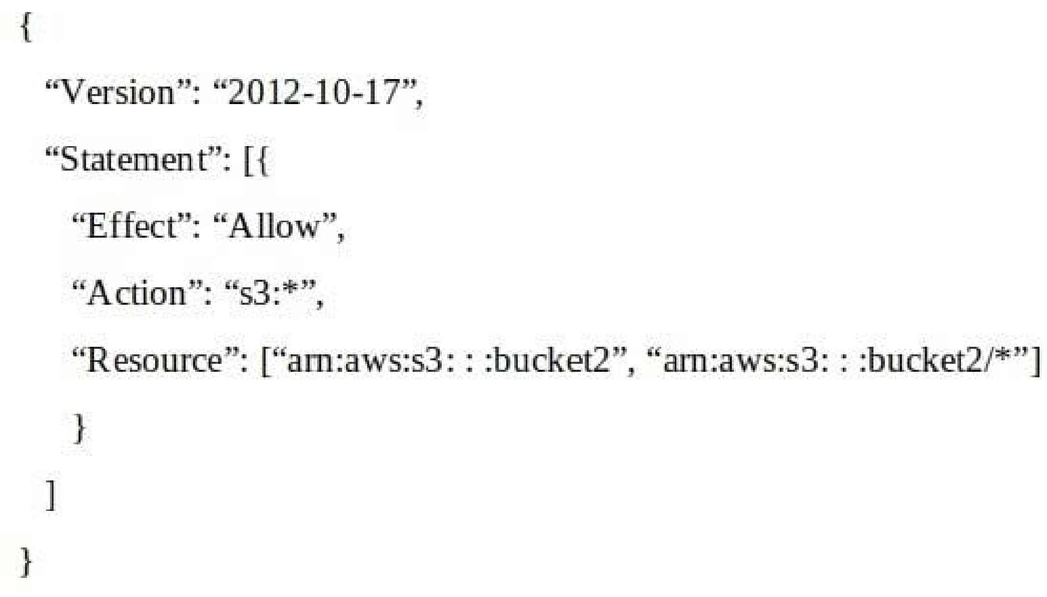
E. Include the subnet-id and instance-id fields in the log format.

Correct Answer: BD

Reference: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

QUESTION 14

A company has multiple VPCs in their account that are peered, as shown in the diagram. A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs. How can this be accomplished? (Choose two.)



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

A. Deploy a pre-authorized scanning engine from the AWS Marketplace into VPC B, and use it to scan instances in all three VPCs. Do not complete the penetration test request form.

B. Deploy a pre-authorized scanning engine from the Marketplace into each VPC, and scan instances in each VPC from the scanning engine in that VPC. Do not complete the penetration test request form.

C. Create a VPN connection from the data center to VPC A. Use an on-premises scanning engine to scan the instances in all three VPCs. Complete the penetration test request form for all three VPCs.

D. Create a VPN connection from the data center to each of the three VPCs. Use an on- premises scanning engine to scan the instances in each VPC. Do not complete the penetration test request form.

E. Create a VPN connection from the data center to each of the three VPCs. Use an on- premises scanning engine to scan the instances in each VPC. Complete the penetration test request form for all three VPCs.

Correct Answer: BD

https://aws.amazon.com/security/penetration-testing/

QUESTION 15

A company uses AWS Organizations to manage several AWs accounts. The company processes a large volume of sensitive data. The company uses a serverless approach to microservices. The company stores all the data in either Amazon

S3 or Amazon DynamoDB. The company reads the data by using either AWS lambda functions or container-based services that the company hosts on Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate.

The company must implement a solution to encrypt all the data at rest and enforce least privilege data access controls. The company creates an AWS Key Management Service (AWS KMS) customer managed key.

What should the company do next to meet these requirements?

A. Create a key policy that allows the kms:Decrypt action only for Amazon S3 and DynamoDB. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.

B. Create an IAM policy that denies the kms:Decrypt action for the key. Create a Lambda function than runs on a schedule to attach the policy to any new roles. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

C. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.

D. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

Correct Answer: B