Amazon

AWS-Security-Specialty
AWS Certified Security - Specialty (SCS-C01)

➤**Up to Date products, reliable and verified.**
➤**Questions and Answers in PDF Format.**

For More Information – Visit link below:
https://www.examkill.com/

Version product

Question: 1

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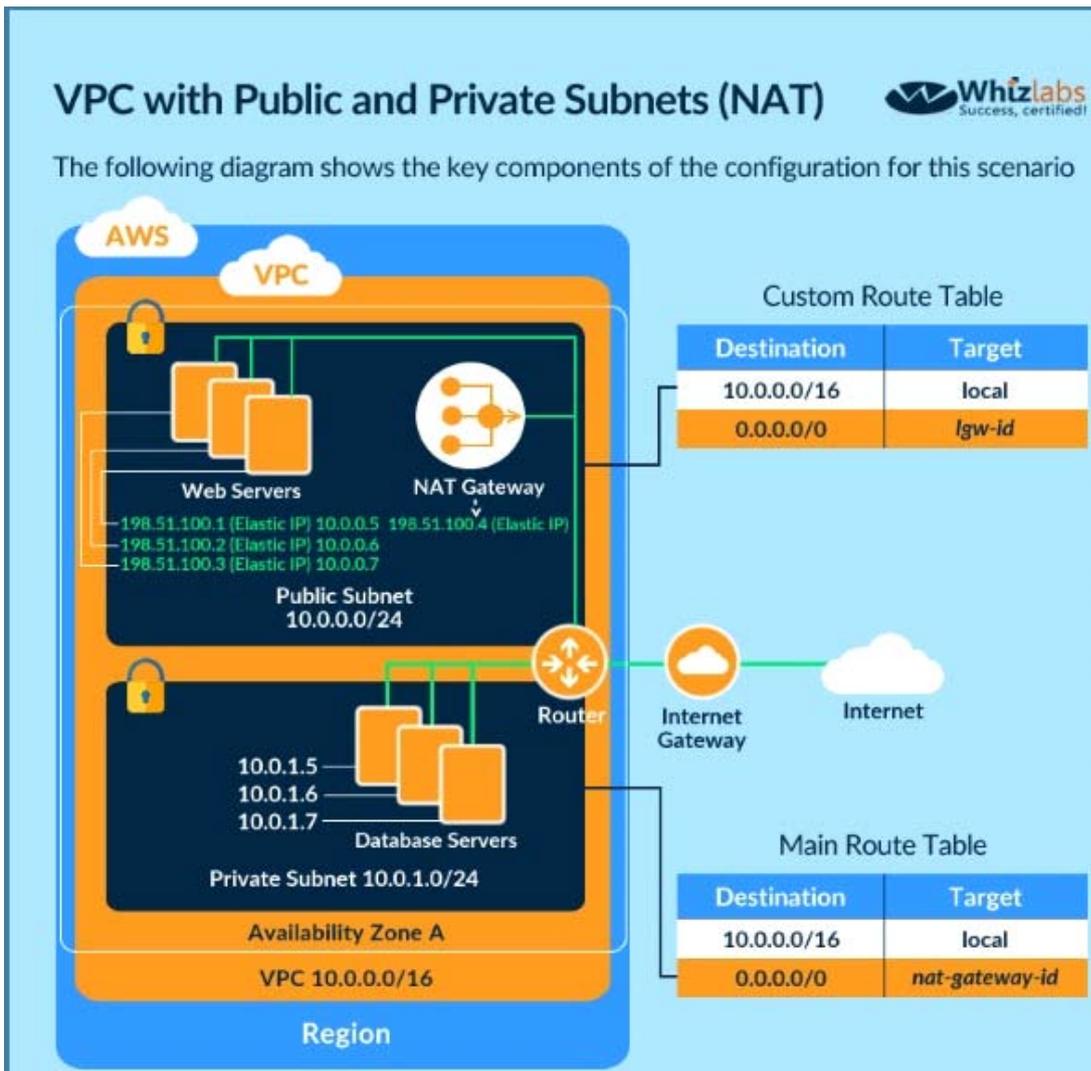Please select:

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

Answer: B

Explanation:
The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet.
The below diagram from the AWS Documentation shows how this can be setup

VPC with Public and Private Subnets (NAT)

The following diagram shows the key components of the configuration for this scenario

Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users Option D is invalid because NAT instances should be present in the public subnet
For more information on public and private subnets in AWS, please visit the following url
.com/AmazonVPC/latest/UserGuide/VPC Scenario2.
The correct answer is: Consider moving the database server to a private subnet Submit your Feedback/Queries to our Experts

Question: 2

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

A. Apply Multi-AZ for the underlying 53 bucket
B. Copy the data to an EBS Volume in another Region

C. Create a snapshot of the S3 bucket and copy it to another region
D. Enable Cross region replication for the S3 bucket

Answer: D

Explanation:
This is mentioned clearly as a use case for S3 cross-region replication
You might configure cross-region replication on a bucket for various reasons, including the following:
• Compliance requirements - Although, by default Amazon S3 stores your data across multiple geographically distant Availability Zones, compliance requirements might dictate that you store data at even further distances. Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these compliance requirements.
Option A is invalid because Multi-AZ cannot be used to S3 buckets
Option B is invalid because copying it to an EBS volume is not a recommended practice
Option C is invalid because creating snapshots is not possible in S3
For more information on S3 cross-region replication, please visit the following URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.htmll
The correct answer is: Enable Cross region replication for the S3 bucket
Submit your Feedback/Queries to our Experts

Question: 3

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 users.

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

Question: 4

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: A, C

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 resource-based 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

Question: 5

You are responsible to deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Also there is a need to monitor web application logs to identify any malicious activity. Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below
Please select:

A. Amazon Cloudwatch Logs
B. Amazon VPC Flow Logs
C. Amazon AWS Config
D. Amazon Cloudtrail

Answer: A, D

Explanation:

The AWS Documentation mentions the following about these services

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

Option B is incorrect because VPC flow logs can only check for flow to instances in a VPC

Option C is incorrect because this can check for configuration changes only

For more information on Cloudtrail, please refer to below URL:

https://aws.amazon.com/cloudtrail;

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Amazon Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs.

For more information on Cloudwatch logs, please refer to below URL:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/loes/WhatisCloudWatchLoES.htmll

The correct answers are: Amazon Cloudwatch Logs, Amazon Cloudtrail

Question: 6

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

A. Create a Direct Connect connection between on-premise network and AWS. Use an AD connector for connecting AWS with on-premise active directory.
B. Create 1AM policies that can be mapped to group memberships in the corporate directory.
C. Create a Lambda function to assign 1AM roles to the temporary security tokens provided to the users.
D. Create 1AM users that can be mapped to the employees' corporate identities
E. Create an 1AM role that establishes a trust relationship between 1AM and the corporate directory identity provider (IdP)

Answer: A, E

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

Question: 7

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

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

Answer: A

Explanation:
You can use a Lambda function to create a new key and then update the S3 bucket to use the new key. Remember not to delete the old key, else you will not be able to decrypt the documents stored in the S3 bucket using the older key.
Option B is incorrect because AWS KMS cannot rotate keys on a monthly basis
Option C is incorrect because deleting the old key means that you cannot access the older objects
Option D is incorrect because rotating key material is not possible.
For more information on AWS KMS keys, please refer to below URL:
https://docs.aws.amazon.com/kms/latest/developereuide/concepts.htmll
The correct answer is: Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.
Submit your Feedback/Queries to our Experts

Question: 8

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-behavior-analysis.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

Question: 9

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 :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 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

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

Question: 10

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

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

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

VPN Connections	
VPN connectivity option	**Description**
AWS managed VPN	You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a *virtual private gateway* provides two VPN endpoints (tunnels) for automatic failover. You configure your *customer gateway* on the remote side of the VPN connection. For more information, see AWS Managed VPN Connections, and the Amazon VPC Network Administrator Guide.
AWS VPN CloudHub	If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks. For more information, see Providing Secure Communication Between Sites Using VPN CloudHub.
Third party software VPN appliance	You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a third party software VPN appliance. AWS does not provide or maintain third party software VPN appliances; however, you can choose from a range of products provided by partners and open source communities. Find third party software VPN appliances on the AWS Marketplace.

You can also use AWS Direct Connect to create a dedicated private connection from a remote network to your VPC. You can combine this connection with an AWS managed VPN connection to create an IPsec-encrypted connection. For more information, see What is AWS Direct Connect? in the *AWS Direct Connect User Guide*. For more information about the different VPC and VPN connectivity options, see the Amazon Virtual Private Cloud Connectivity Options whitepaper.

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

Question: 11

How can you ensure that instance in an VPC does not use AWS DNS for routing DNS requests. You want to use your own managed DNS instance. How can this be achieved?
Please select:

A. Change the existing DHCP options set
B. Create a new DHCP options set and replace the existing one.
C. Change the route table for the VPC
D. Change the subnet configuration to allow DNS requests from the new DNS Server

Explanation:
In order to use your own DNS server, you need to ensure that you create a new custom DHCP options set with the IP of th custom DNS server. You cannot modify the existing set, so you need to create a new one.
Option A is invalid because you cannot make changes to an existing DHCP options Set.
Option C is invalid because this can only be used to work with Routes and not with a custom DNS solution.

Option D is invalid because this needs to be done at the VPC level and not at the Subnet level
For more information on DHCP options set, please visit the following url
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC DHCP Options.html
The correct answer is: Create a new DHCP options set and replace the existing one. Submit your Feedback/Queries to our Experts

Question: 12

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

Question: 13

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

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

Answer: A, D

Explanation:
AWS Key Management Service (KMS) now uses FIPS 140-2 validated hardware security modules (HSM) and supports FIPS 140-2 validated endpoints, which provide independent assurances about the confidentiality and integrity of your keys.
All master keys in AWS KMS regardless of their creation date or origin are automatically protected using FIPS 140-2 validated
HSMs. defines four levels of security, simply named "Level 1'' to "Level 4". It does not specify in detail what level of security is required by any particular application.
• FIPS 140-2 Level 1 the lowest, imposes very limited requirements; loosely, all components must be "production-grade" anc various egregious kinds of insecurity must be absent
• FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
• FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
• FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks.
AWSCIoudHSM provides you with a FIPS 140-2 Level 3 validated single-tenant HSM cluster in your Amazon Virtual Private Cloud (VPQ to store and use your keys. You have exclusive control over how your keys are used via an authentication mechanism independent from AWS. You interact with keys in your AWS CloudHSM cluster similar to the way you interact with your applications running in Amazon EC2.
AWS KMS allows you to create and control the encryption keys used by your applications and supported AWS services in multiple regions around the world from a single console. The service uses a FIPS 140-2 validated HSM to protect the security of your keys. Centralized management of all your keys in AWS KMS lets you enforce who can use your keys under which conditions, when they get rotated, and who can manage them.
AWS KMS HSMs are validated at level 2 overall and at level 3 in the following areas:
• Cryptographic Module Specification
• Roles, Services, and Authentication
• Physical Security
• Design Assurance
So I think that we can have 2 answers for this question. Both A & D.
• https://aws.amazon.com/blo15s/security/aws-key-management-service- now-ffers-flps-140-2-validated-cryptographic-m< enabling-easier-adoption-of-the-service-for-regulated-workloads/
• https://a ws.amazon.com/cloudhsm/faqs/
• https://aws.amazon.com/kms/faqs/
• https://en.wikipedia.org/wiki/RPS
The AWS Documentation mentions the following
AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions ()CE). and Microsoft CryptoNG (CNG) libraries. CloudHSM is also standards-compliant and enables you to export all of your keys to most other commercially-available HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups. CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs.

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

For more information on CloudHSM, please visit the following url

https://aws.amazon.com/cloudhsm;

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

Question: 14

You need to have a requirement to store objects in an S3 bucket with a key that is automatically managed and rotated. Which of the following can be used for this purpose?
Please select:

A. AWS KMS
B. AWS S3 Server side encryption
C. AWS Customer Keys
D. AWS Cloud HSM

Answer: B

Explanation:

The AWS Documentation mentions the following

Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

All other options are invalid since here you need to ensure the keys are manually rotated since you manage the entire key set Using AWS S3 Server side encryption, AWS will manage the rotation of keys automatically.

For more information on Server side encryption, please visit the following URL:

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsineServerSideEncryption.htmll

The correct answer is: AWS S3 Server side encryption Submit your Feedback/Queries to our Experts

Question: 15

A company stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket. In addition , it should be ensured that objects are available in a secondary region if the primary one goes down. Which of the following can help fulfil these requirements? Choose 2 answers from the options given below
Please select:

A. Enable bucket versioning and also enable CRR
B. Enable bucket versioning and enable Master Pays

C. For the Bucket policy add a condition for {"Null": {"aws:MultiFactorAuthAge": true}}
i
D. Enable the Bucket ACL and add a condition for {"Null": {"aws:MultiFactorAuthAge": true}}

Answer: A, C

Explanation:
The AWS Documentation mentions the following
Adding a Bucket Policy to Require MFA
Amazon S3 supports MFA-protected API access, a feature that can enforce multi-factor authentication (MFA) for access to your Amazon S3 resources. Multi-factor authentication provides an extra level of security you can apply to your AWS environment. It is a security feature that requires users to prove physical possession of an MFA device by providing a valid MFA code. For more information, go to AWS Multi-Factor Authentication. You can require MFA authentication for any requests to access your Amazoi. S3 resources.
You can enforce the MFA authentication requirement using the aws:MultiFactorAuthAge key in a bucket policy. 1AM users car access Amazon S3 resources by using temporary credentials issued by the AWS Security Token Service (STS). You provide the MFA code at the time of the STS request.
When Amazon S3 receives a request with MFA authentication, the aws:MultiFactorAuthAge key provides a numeric value indicating how long ago (in seconds) the temporary credential was created. If the temporary credential provided in the request was not created using an MFA device, this key value is null (absent). In a bucket policy, you can add a condition to check this value, as shown in the following example bucket policy. The policy denies any Amazon S3 operation on the /taxdocuments folder in the examplebucket bucket if the request is not MFA authenticated. To learn more about MFA authentication, see Using Multi-Factor Authentication (MFA) in AWS in the 1AM User Guide.

```
{
  "Version": "2012-10-17",
  "Id": "123",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/taxdocuments/*",
      "Condition": { "Null": { "aws:MultiFactorAuthAge": true }}
    }
  ]
}
```

Option B is invalid because just enabling bucket versioning will not guarantee replication of objects Option D is invalid because the condition for the bucket policy needs to be set accordingly For more information on example bucket policies, please visit the following URL: •
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html
Also versioning and Cross Region replication can ensure that objects will be available in the destination region in case the primary region fails.
For more information on CRR, please visit the following URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html
The correct answers are: Enable bucket versioning and also enable CRR, For the Bucket policy add a condition for {"Null": { "aws:MultiFactorAuthAge": true}}
Submit your Feedback/Queries to our Experts

Question: 16

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

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

Explanation:

The AWS Documentation mentions the following on AWS Inspector

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

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

Option C is invalid because the AWS Inspector service is not used to patch servers

For more information on AWS Inspector, please visit the following URL:

https://aws.amazon.com/inspector>

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

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

https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html

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

(

Question: 17

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

Question: 18

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

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

Answer: A, C, D

Explanation:
For ensuring that the instances are configured properly you need to ensure the followi .
1)   You installed the latest version of the SSM Agent on your instance
2)   Your instance is configured with an AWS Identity and Access Management (1AM) role that enables
the instance to communicate with the Systems Manager API
3)   You can use the Amazon EC2 Health API to quickly determine the following information about
Amazon EC2 instances The status of one or more instances
The last time the instance sent a heartbeat value
The version of the SSM Agent
The operating system
The version of the EC2Config service (Windows)
The status of the EC2Config service (Windows)
Option B is invalid because 1AM users are not supposed to be directly granted permissions to EC2
Instances For more information on troubleshooting AWS SSM, please visit the following URL:
https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-remote-
commands.html
The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure
that agent is running on the Instances., Check the Instance status by using the Health API.
Submit your Feedback/Queries to our Experts

Question: 19

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: A, B

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-remote-commands.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

Question: 20

You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between AWS and their On-premise Active Directory. Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below.
Please select:

A. Ensure the right match is in place for On-premise AD Groups and 1AM Roles.
B. Ensure the right match is in place for On-premise AD Groups and 1AM Groups.
C. Configure AWS as the relying party in Active Directory
D. Configure AWS as the relying party in Active Directory Federation services

Explanation:

The AWS Documentation mentions some key aspects with regards to the configuration of On-premise AD with AWS

One is the Groups configuration in AD

Active Directory Configuration

Determining how you will create and delineate your AD groups and 1AM roles in AWS is crucial to how you secure access to your account and manage resources. SAML assertions to the AWS environment and the respective 1AM role access will be managed through regular expression (regex) matching between your on-premises AD group name to an AWS 1AM role.

One approach for creating the AD groups that uniquely identify the AWS 1AM role mapping is by selecting a common group naming convention. For example, your AD groups would start with an identifier, for example, AWS-, as this will distinguish your AWS groups from others within the organization. Next include the 12-digitAWS account number. Finally, add the matching role name within the AWS account. Here is an example:

And next is the configuration of the relying party which is AWS

ADFS federation occurs with the participation of two parties; the identity or claims provider (in this case the owner of the identity repository - Active Directory) and the relying party, which is another application that wishes to outsource authentication to the identity provider; in this case Amazon Secure Token Service (STS). The relying party is a federation partner that is represented by a claims provider trust in the federation service.

Option B is invalid because AD groups should not be matched to 1AM Groups

Option C is invalid because the relying party should be configured in Active Directory Federation services

For more information on the federated access, please visit the following URL:

1   https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-ad-fs/

The correct answers are: Ensure the right match is in place for On-premise AD Groups and 1AM Roles., Configure AWS as the relying party in Active Directory Federation services

Submit your Feedback/Queries to our Experts

FEATURES:

➢ 100% Pass Guarantee

➢ 30 DaysMoney Back Guarantee

➢ 24/7 Live Chat Support(Technical & Sales)

➢ Instant download after purchase

➢ 50,000 +ve Reviews

➢ 100% Success Rate

➢ Discounts Available for Bulk Orders

➢ Updates are free for 90 days

➢ Verified answers by experts