SCS-C02 Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

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

https://www.pass4itsure.com/scs-c02.html

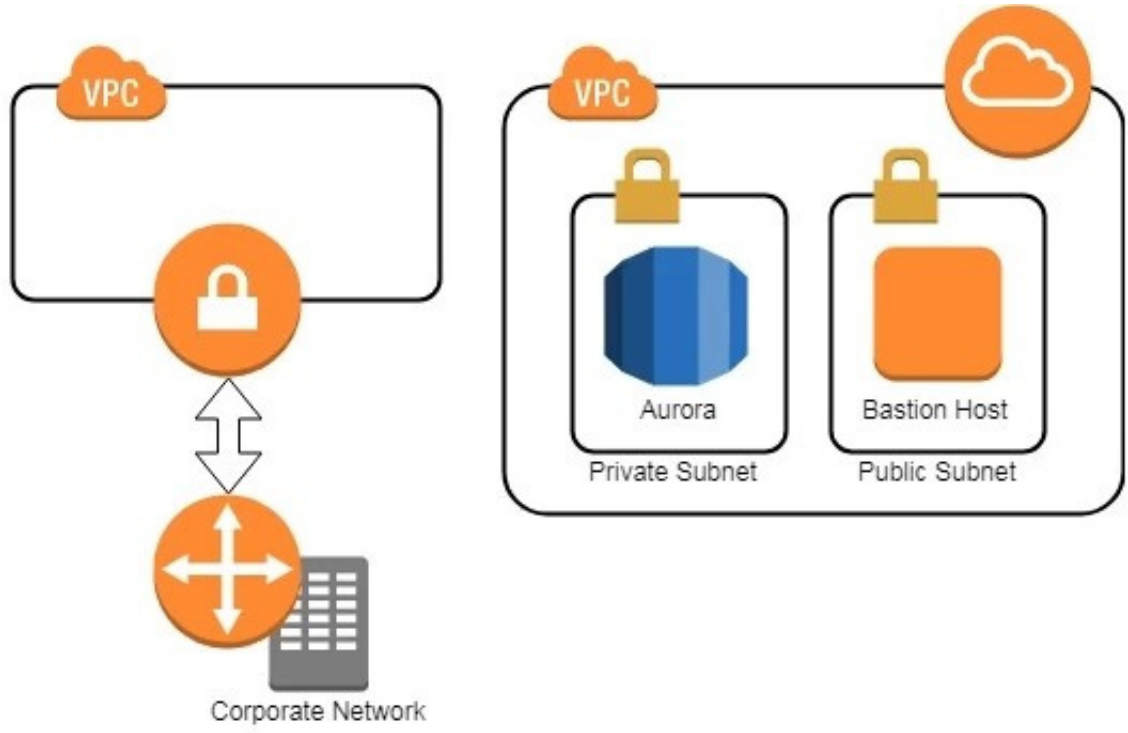
100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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



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

A. Move the bastion host to the VPC with VPN connectivity. 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 IAM Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

Correct Answer: A

QUESTION 2

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 :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

Correct 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 IAM Security Groups, please refer to below URL: https://docs.IAM.amazon.com/IAMEC2/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 3

Which option for the use of the IAM Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

A. Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.

B. Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.

C. Change the CMK alias every 90 days, and update key-calling applications with the new key alias.

D. Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

Correct Answer: A

"automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key. You might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it\\'s often thought of as manually rotating the key."
https://docs.aws.amazon.com/kms/ latest/developerguide/rotate-keys.html
https://docs.IAM.amazon.com/kms/latest/developerguide/rotate-keys.html#rotate-keys- manually for IAM standards

QUESTION 4

A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet with port 80 and a Database server in the private subnet with port 3306. The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). Which of the below mentioned entries is required in the private subnet database security group DBSecGrp?

Please select:

A. Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp.

B. Allow Inbound on port 3306 from source 20.0.0.0/16

C. Allow Outbound on port 3306 for Destination Web Server Security Group WebSecGrp.

D. Allow Outbound on port 80 for Destination NAT Instance IP

Correct Answer: A

Explanation: Since the Web server needs to talk to the database server on port 3306 that means that the database server should allow incoming traffic on port 3306. The below table from the IAM documentation shows how the security groups should be set up.

DBServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group.
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet over IPv4 (for example, for software updates).
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet over IPv4 (for example, for software updates).

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

Option B is invalid because you need to allow incoming access for the database server from the WebSecGrp security group.

Options C and D are invalid because you need to allow Outbound traffic and not inbound traffic For more information on security groups please visit the below Link:

http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuide/VPC Scenario2.html The correct answer is: Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp. Submit your Feedback/Queries to our Experts

QUESTION 5

A company\\'s security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance. What combination of actions should the Engineer take? (Choose two.)

A. Create an IAM Lambda function that determines whether Flow Logs are enabled for a given VPC.

B. Create an IAM Config configuration item for each VPC in the company IAM account.

C. Create an IAM Config managed rule with a resource type of IAM:: Lambda:: Function.

D. Create an Amazon CloudWatch Event rule that triggers on events emitted by IAM Config.

E. Create an IAM Config custom rule, and associate it with an IAM Lambda function that contains the evaluating logic.

Correct Answer: AE

Explanation: https://medium.com/mudita-misra/how-to-audit-your-aws-resources-for- security-compliance-by-using-custom-IAM-config-rules-2e53b09006de