



# ANS-C00<sup>Q&As</sup>

AWS Certified Advanced Networking - Specialty (ANS-C00)

## Pass Amazon ANS-C00 Exam with 100% Guarantee

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

<https://www.passapply.com/aws-certified-advanced-networking-specialty.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

Your website utilizes EC2, S3, ELB-Classical, and CloudFront. Your manager has shifted focus to security and wants you to ensure the site is as secure as possible. What two items could you recommend? (Choose two.)

- A. An NACL that blocks all ports to your subnets.
- B. A restricted bucket policy.
- C. A WAF on the load balancer.
- D. A WAF on your CloudFront distribution.

Correct Answer: BD

Explanation:

A WAF on CloudFront and a restricted bucket policy to ensure the only access is from CloudFront. You cannot apply a WAF to a classic load balancer and an NACL that blocks all ports would block access to the load balancer.

---

### QUESTION 2

What service is used to store the log files generated by CloudTrail?

- A. EC2
- B. EBS
- C. S3
- D. VPC

Correct Answer: C

Explanation:

The AWS CloudTrail uses Amazon's Simple Storage Service (S3) to store log files. It also supports the use of S3 life cycle configuration rules to reduce storage costs.

Reference: <https://aws.amazon.com/cloudtrail/>

---

### QUESTION 3

You have two public applications on different domains that use two front-end servers and two back-end servers each. You wish to achieve high availability for both applications. What two options should you configure? (Choose two.)

- A. Route 53: 2 public zones and 2 private zones.



- B. Route 53: 2 public zones and 1 private zone.
- C. 3 load balancers: 2 public and 1 internal.
- D. 4 load balancers: 2 public and 2 internal.

Correct Answer: AD

Explanation:

Route 53: 2 public zones and 2 private zones and 4 load balancers: 2 public and 2 internal. This will allow one domain to be balanced over two application servers which will then have traffic balanced to the two backend servers.

---

#### QUESTION 4

You currently use a single security group assigned to all nodes in a clustered NoSQL database. Only your cluster members in one region must be able to connect to each other. This security group uses a self-referencing rule using the cluster security group's group-id to make it easier to add or remove nodes from the cluster. You need to make this database comply with out-of-region disaster recovery requirements and ensure that the network traffic between the nodes is encrypted when travelling between regions. How should you enable secure cluster communication while deploying additional cluster members in another AWS region?

- A. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group rules that reference each other's security group-id in each region.
- B. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
- C. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
- D. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group rules that reference each other's security group-id in each region.

Correct Answer: D

---

#### QUESTION 5

Your website is under attack and a malicious party is stealing large amounts of data. You have default NACL rules. Stopping the attack is the ONLY priority in this case. Which two commands should you use? (Choose two.)

- A. `aws ec2 delete-network-acl-entry -network-acl-id acl-5fb84d47 -ingress -rule-number 32768`
- B. `aws ec2 delete-network-acl-entry -network-acl-id acl-5fb84d47 -egress rule-number 100`
- C. `aws ec2 delete-network-acl-entry -network-acl-id acl-5fb84d47 -ingress rule-number 100`
- D. `aws ec2 create-network-acl-entry -network-acl-id acl-5fb84d47 -ingress rule-number 100 -protocol -1 port-range`



From =-1,To =-1 -cidr-block 0.0.0.0/0 -rule-action deny

Correct Answer: BC

Explanation:

You should remove the default allow rules in your NACL and a default deny will be the only rule left for inbound and outbound. If you attempt to create a rule number 100, it will encounter an error as there is already a rule 100.

[ANS-C00 PDF Dumps](#)

[ANS-C00 VCE Dumps](#)

[ANS-C00 Practice Test](#)