Chapter 3

*AWS Certified Solutions Architect Practice Tests: Associate SAA-C01 Exam*
By Brett McLaughlin


# Domain 3: Specify Secure Applications and Architectures

- ✓ **Subdomain: 3.1 Determine how to secure application tiers.**
- ✓ **Subdomain: 3.2 Determine how to secure data.**
- ✓ **Subdomain: 3.3 Define the networking infrastructure for a single VPC application.**

# Review Questions

1. When creating a new security group, which of the following are true? (Choose two.)
   - **A.** All inbound traffic is allowed by default.
   - **B.** All outbound traffic is allowed by default.
   - **C.** Connections that are allowed in must also explicitly be allowed back out.
   - **D.** Connections that are allowed in are automatically allowed back out.
2. You have a government-regulated system that will store a large amount of data on S3 standard. You must encrypt all data and preserve a clear audit trail for traceability and third-party auditing. Security policies dictate that encryption must be consistent across the entire data store. Which of the following encryption approaches would be best?
   - **A.** SSE-C
   - **B.** SSE-KMS
   - **C.** SSE-C
   - **D.** Encrypt the data prior to upload to S3 and decrypt the data when returning it to the client.
3. You are creating a bastion host to allow SSH access to a set of EC2 instances in a private subnet within your organization's VPC. Which of the following should be done as part of configuring the bastion host? (Choose two.)
   - **A.** Ensure that the bastion host is exposed directly to the Internet.
   - **B.** Place the bastion host within the private subnet.
   - **C.** Add a route from the bastion host IP into the private subnet into the subnet's NACLs.
   - **D.** Ensure that the bastion host is within the same security group as the hosts within the private subnet.
4. Which of the following are invalid IAM actions? (Choose two.)
   - **A.** Limiting the root account SSH access to all EC2 instances
   - **B.** Allowing a user account SSH access to all EC2 instances
   - **C.** Removing console access for the root account
   - **D.** Removing console access for all non-root user accounts
5. Which of the following statements is true?
   - **A.** You should store application keys only in your application's `.aws` file.
   - **B.** You should never store your application keys on an instance, in an AMI, or anywhere else permanent on the cloud.
   - **C.** You should only store application keys in an encrypted AMI.
   - **D.** You should only use your application key to log in to the AWS console.

6. Your company is setting up a VPN connection to connect its local network to an AWS VPC. Which of the following components are *not* necessary for this setup? (Choose two.)
   - **A.** A NAT instance
   - **B.** A virtual private gateway
   - **C.** A private subnet in the AWS VPC
   - **D.** A customer gateway

7. You have a private subnet in a VPC within AWS. The instances within the subnet are unable to access the Internet. You have created a NAT gateway to solve this problem. What additional steps do you need to perform to allow the instances Internet access? (Choose two.)
   - **A.** Ensure that the NAT gateway is in the same subnet as the instances that cannot access the Internet.
   - **B.** Add a route in the private subnet to route traffic aimed at 0.0.0.0/0 at the NAT gateway.
   - **C.** Add a route in the public subnet to route traffic aimed at 0.0.0.0/0 at the NAT gateway.
   - **D.** Ensure that the NAT gateway is in a public subnet.

8. Which of the following statements regarding NAT instances and NAT gateways are false? (Choose two.)
   - **A.** Both NAT instances and NAT gateways are highly available.
   - **B.** You must choose the instance type and size when creating a NAT gateway but not when creating a NAT instance.
   - **C.** It is your responsibility to patch a NAT instance and AWS's responsibility to patch a NAT gateway.
   - **D.** You assign a security group to a NAT instance but not to a NAT gateway.

9. Which of the following statements is true?
   - **A.** A VPC's default NACLs allow all inbound and outbound traffic.
   - **B.** NACLs are stateful.
   - **C.** Security groups are stateless.
   - **D.** Traffic allowed into a NACL is automatically allowed back out.

10. You have changed the permissions associated with a role, and that role is assigned to an existing running EC2 instance. When will the permissions you updated take effect for the instance?
    - **A.** Immediately
    - **B.** Within 5 minutes
    - **C.** Within 1 hour
    - **D.** The next time the EC2 instance is restarted

**11.** Which of the following statements is true?

**A.** When creating a new security group, by default, all traffic is allowed in, including SSH.

**B.** If you need inbound HTTP and HTTPS access, create a new security group and accept the default settings.

**C.** You must explicitly allow any inbound traffic into a new security group.

**D.** Security groups are stateless.

**12.** Which of the following statements is not true?

**A.** When creating a new security group, by default, no inbound traffic is allowed.

**B.** When creating a new security group, by default, all traffic is allowed out, including SSH.

**C.** When creating a new security group, by default, all traffic is allowed out, with the exception of SSH.

**D.** When creating a new security group, inbound HTTPS traffic is not allowed.

**13.** How would you enable encryption of your EBS volumes?

**A.** Use the AWS CLI with the aws security command.

**B.** Take a snapshot of the EBS volume and copy it to an encrypted S3 bucket.

**C.** Select the encryption option when creating the EBS volume.

**D.** Encrypt the volume using the encryption tools of the operating system of the EC2 instance that has mounted the EBS volume.

**14.** What types of rules does a security group allow? (Choose two.)

**A.** Allow rules

**B.** Prevent rules

**C.** Deny rules

**D.** Inbound rules

**15.** Which of the following are true about security groups? (Choose two.)

**A.** You can specify deny rules, but not allow rules.

**B.** By default, a security group includes an outbound rule that allows all outbound traffic.

**C.** You can specify specific separate rules for inbound and outbound traffic.

**D.** Security groups are stateless.

**16.** Which of the following are not true about security groups? (Choose two.)

**A.** Allow rules take priority over deny rules.

**B.** Responses to allowed inbound traffic are allowed to flow back out.

**C.** You can specify specific separate rules for inbound and outbound traffic.

**D.** If there are no outbound rules, then all outbound traffic is allowed to flow out.

17. Which of the following must a security group have when you create it? (Choose two.)
    - **A.** At least one inbound rule
    - **B.** A name
    - **C.** A description
    - **D.** At least one outbound rule

18. Which of the following is a security group associated with?
    - **A.** An ELB
    - **B.** A network interface
    - **C.** An ALB
    - **D.** A network access list

19. Which of the following are default rules on a default security group, such as the one that comes with the default VPC? (Choose two.)
    - **A.** Outbound: 0.0.0.0/0 for all protocols allowed
    - **B.** Inbound: 0.0.0.0/0 for all protocols allowed
    - **C.** Outbound: ::/0 for all protocols allowed
    - **D.** Inbound: ::/0 for all protocols allowed

20. Which of the following are parts of a security group rule? (Choose two.)
    - **A.** A protocol
    - **B.** A subnet
    - **C.** An instance ID
    - **D.** A description

21. Which of the following allows you to securely upload data to S3? (Choose two.)
    - **A.** HTTP endpoints using HTTP
    - **B.** SSL endpoints using HTTPS
    - **C.** HTTP endpoints using HTTPS
    - **D.** SSL endpoints using HTTP

22. Which of the following describes client-side encryption for S3 bucket data?
    - **A.** You encrypt and upload data to S3, managing the encryption process yourself.
    - **B.** You encrypt and upload data to S3, allowing AWS to manage the encryption process.
    - **C.** You request AWS to encrypt an object before saving it to S3.
    - **D.** You encrypt an object, but AWS uploads and decrypts the object.

23. Which of the following describes server-side encryption for S3 bucket data?
    - **A.** You encrypt and upload data to S3, managing the encryption process yourself.
    - **B.** You encrypt and upload data to S3, allowing AWS to manage the encryption process.
    - **C.** You request AWS to encrypt an object before saving it to S3.
    - **D.** You encrypt an object, but AWS uploads and decrypts the object.

**24.** Which of the following are valid steps in enabling client-side encryption for S3? (Choose two.)

**A.** Download the AWS CLI and SSH to your S3 key store.

**B.** Use a KMS-managed customer master key.

**C.** Download an AWS SDK for encrypting data on the client side.

**D.** Turn on bucket encryption for the target S3 buckets.

**25.** Which of the following is not a way to manage server-side encryption keys for S3?

**A.** SSE-S3

**B.** SSE-KMS

**C.** SSE-E

**D.** SSE-C

**26.** Which of the following encryption key management options is best for ensuring strong audit trails?

**A.** SSE-S3

**B.** SSE-KMS

**C.** Client-side encryption keys

**D.** SSE-C

**27.** Which of the following encryption key management options is best for managing keys but allowing S3 to handle the actual encryption of data?

**A.** SSE-S3

**B.** SSE-KMS

**C.** Client-side encryption keys

**D.** SSE-C

**28.** You have a customer that has a legacy security group that is very suspicious of all things security in the cloud. The customer wants to use S3, but doesn't trust AWS encryption, and you need to enable its migration to the cloud. What option would you recommend to address the company's concerns?

**A.** SSE-S3

**B.** SSE-KMS

**C.** Client-side encryption keys

**D.** SSE-C

**29.** You want to begin encrypting your S3 data, but your organization is new to encryption. Which option is a low-cost approach that still offloads most of the work to AWS rather than the organization new to encryption?

**A.** SSE-S3

**B.** SSE-KMS

**C.** Client-side encryption keys

**D.** SSE-C

**30.** You are the architect for a company whose data must comply with current EU privacy restrictions. Which of the following S3 buckets are valid options? (Choose two.)

**A.** Buckets in EU Central 1

**B.** Buckets in US East 2

**C.** Buckets in EU West 1

**D.** Buckets in SA East 1

**31.** Which of the following options could be used to provide availability-zone-resilient fault-tolerant storage that complies with EU privacy laws? (Choose two.)

**A.** S3 buckets in US West 1

**B.** S3 buckets in EU West 2

**C.** S3-IA buckets in EU Central 1

**D.** S3 One Zone-IA buckets in EU-West-1

**32.** What type of replication will your Multi-AZ RDS instances use?

**A.** Offline replication

**B.** Synchronous replication

**C.** Push replication

**D.** Asynchronous replication

**33.** You want to provide maximum protection against data in your S3 object storage being deleted accidentally. What should you do?

**A.** Enable versioning on your EBS volumes.

**B.** Turn on MFA Delete on your S3 buckets.

**C.** Set up a Lambda job to monitor and block delete requests to S3.

**D.** Turn off the DELETE endpoints on the S3 REST API.

**34.** You want to provide maximum protection against data in your S3 object storage being deleted accidentally. What steps should you take? (Choose two.)

**A.** Enable versioning on your S3 buckets.

**B.** Turn on MFA Delete on your S3 buckets.

**C.** Enable versioning in CloudWatch's S3 API.

**D.** Remove IAM permissions for deleting objects for all users.

**35.** You want to enable MFA Delete on your S3 buckets in the US East 1 region. What step must you take before enabling MFA Delete?

**A.** Disable the REST API for the buckets on which you want MFA Delete.

**B.** Enable cross-region replication on the buckets on which you want MFA Delete.

**C.** Move the buckets to a region that supports MFA Delete, such as US West 1.

**D.** Enable versioning on the buckets on which you want MFA Delete.

**36.** What is AWS Trusted Advisor?

- **A.** An online resource to help you improve performance
- **B.** An online resource to help you reduce cost
- **C.** An online resource to help you improve security
- **D.** All of the above

**37.** On which of the following does AWS Trusted Advisor not provide recommendations?

- **A.** Reducing cost
- **B.** Improving fault tolerance
- **C.** Improving security
- **D.** Organizing accounts

**38.** Which of the following are included in the core AWS Trusted Advisor checks? (Choose two.)

- **A.** S3 bucket permissions
- **B.** MFA on root account
- **C.** Quantity of CloudWatch alarms
- **D.** Use of VPC endpoints

**39.** Which of the following recommendations might AWS Trusted Advisor make? (Choose two.)

- **A.** Turn on MFA for the root account.
- **B.** Turn on antivirus protection for EC2 instances.
- **C.** Update S3 buckets with public write access.
- **D.** Update NAT instances to NAT gateways.

**40.** Which of the following is not possible using IAM policies?

- **A.** Requiring MFA for the root account
- **B.** Denying the root account access to EC2 instances
- **C.** Disabling S3 access for users in a group
- **D.** Restricting SSH access to EC2 instances to a specific user

**41.** Which of the following are not true about S3 encryption? (Choose two.)

- **A.** S3 applies AWS-256 encryption to data when server-side encryption is enabled.
- **B.** S3 encryption will use a client key if it is supplied with data.
- **C.** Encrypted EBS volumes can only be stored if server-side encryption is enabled.
- **D.** S3 will accept locally encrypted data if client-side encryption is enabled.

**42.** What types of data are encrypted when you create an encrypted EBS volume? (Choose two.)

**A.** Data at rest inside the volume

**B.** Data moving between the volume and the attached instance

**C.** Data inside S3 buckets that store the encrypted instance

**D.** Data in an EFS on instances attached to the volume

**43.** What types of data are not automatically encrypted when you create an encrypted EBS volume? (Choose two.)

**A.** A snapshot created from the EBS volume

**B.** Any data on additional volumes attached to the same instance as the encrypted volume

**C.** Data created on an instance that has the encrypted volume attached

**D.** Data moving between the volume and the attached instance

**44.** What of the following types of data is not encrypted automatically when an encrypted EBS volume is attached to an EC2 instance?

**A.** Data in transit to the volume

**B.** Data at rest on the volume

**C.** Data in transit from the volume

**D.** All of these are encrypted.

**45.** What encryption service is used by encrypted EBS volumes?

**A.** S3-KMS

**B.** S3-C

**C.** KMS

**D.** Customer-managed keys

**46.** How can you access the private IP address of a running EC2 instance?

**A.** `http://169.254.169.254/latest/user-data/`

**B.** `http://169.254.169.254/latest/instance-data/`

**C.** `http://169.254.169.254/latest/meta-data/`

**D.** `http://169.254.169.254/latest/ec2-data/`

**47.** If you take a snapshot of an encrypted EBS volume, which of the following will be true? (Choose two.)

**A.** The snapshot will be encrypted.

**B.** All data on the bucket on which the snapshot is stored will be encrypted.

**C.** Any instances using the snapshot will be encrypted.

**D.** Any volumes created from the snapshot will be encrypted.

**48.** If you take a snapshot of an encrypted EBS volume, which of the following must you do to use that snapshot as a volume in a separate region? (Choose two.)

**A.** Copy the snapshot to the new region.

**B.** Delete the snapshot from the old region.

**C.** Unencrypt the snapshot once it is in the new region.

**D.** Create a new volume from the snapshot in the new region.

**49.** How do you encrypt an RDS instance?

**A.** Enable encryption on the running instance via the CLI.

**B.** Enable encryption on the running instance via the console.

**C.** Run the encryption process on the running instance via the console.

**D.** Enable encryption when creating the instance.

**50.** Which of the following will ensure that data on your RDS instance is encrypted?

**A.** Use client-side encryption keys.

**B.** Enable encryption on the running RDS instance via the AWS API.

**C.** Encrypt the instance on which RDS is running.

**D.** None of these will encrypt all data on the instance.

**51.** Which of the following will allow you to bring a non-encrypted RDS instance into compliance with an "all data must be encrypted at rest" policy?

**A.** Snapshot the RDS instance and restore it, encrypting the new copy upon restoration.

**B.** Use the AWS Database Migration Service to migrate the data from the instance to an encrypted instance.

**C.** Create a new encrypted instance and manually move data into it.

**D.** None of these will encrypt all data on the instance.

**52.** Which of the following will allow you to bring a non-encrypted EBS volume into compliance with an "all data must be encrypted at rest" policy?

**A.** Stop the volume, snapshot it, and encrypt a copy of the snapshot. Then restore from the encrypted snapshot.

**B.** Stop the volume, select "Turn on encryption," and restart the volume.

**C.** Encrypt the volume via the AWS API and turn on the "encrypt existing data" flag.

**D.** None of these will encrypt all data on the volume.

**53.** Which of the following will allow you to bring a non-encrypted EBS volume into compliance with an "all data must be encrypted at rest" policy?

**A.** Stop the volume, create a snapshot, and restart from the snapshot, selecting "Encrypt this volume."

**B.** Stop the volume, select "Turn on encryption," and restart the volume.

**C.** Encrypt the volume via the AWS API and turn on the "encrypt existing data" flag.

**D.** None of these will encrypt all data on the volume.

**54.** Which of the following will allow you to bring a non-encrypted EBS volume into compliance with an "all data must be encrypted at rest" policy?

**A.** Create a new volume, attach the new volume to an EC2 instance, copy the data from the non-encrypted volume to the new volume, and then encrypt the new volume.

**B.** Create a new volume with encryption turned on, attach the new volume to an EC2 instance, and copy the data from the non-encrypted volume to the new volume.

**C.** Create a new volume, attach the new volume to an EC2 instance, and use the encrypted-copy command to copy the data from the non-encrypted volume to the new volume.

**D.** None of these will encrypt all data on the volume.

**55.** Which of the following are valid options on an EBS volume? (Choose two.)

**A.** Encrypt the volume.

**B.** Encrypt a snapshot of the volume.

**C.** Encrypt a copy of a snapshot of the volume.

**D.** Restore an encrypted snapshot to an encrypted volume.

**56.** Which of the following are not true about EBS snapshots? (Choose two.)

**A.** Snapshots of encrypted volumes are automatically encrypted.

**B.** When you copy an encrypted snapshot, the copy is not encrypted unless you explicitly specify.

**C.** You cannot copy an encrypted snapshot unless you unencrypt the snapshot first.

**D.** Volumes that are created from encrypted snapshots are automatically encrypted.

**57.** Can you copy a snapshot across AWS accounts?

**A.** Yes

**B.** Yes, but you first have to modify the snapshot's access permissions.

**C.** Yes, but you have to be the owner of both AWS accounts.

**D.** No

**58.** You have a snapshot of an EBS volume in US East 2. You want to create a volume from this snapshot in US West 1. Is this possible?

**A.** Yes, create the volume in US West 1 based upon the snapshot in US East 2.

**B.** Yes, but you'll need to copy the snapshot to US West 1 first.

**C.** Yes, but you'll need to create the instance in US East 2 and then move it to US West 1.

**D.** No

**59.** Can you copy an EBS snapshot across regions?

**A.** Yes, as long as the snapshot is not encrypted.

**B.** Yes, as long as the snapshot is marked for multi-region use.

**C.** Yes

**D.** No

**60.** Which of the following does a security group attached to an instance control? (Choose two.)

**A.** Inbound traffic

**B.** HTTP error messages

**C.** Outbound traffic

**D.** Access control lists

**61.** How many security groups can you attach to a single instance in a VPC?

**A.** None, security groups aren't attached to instances.

**B.** 1

**C.** 1 or more

**D.** 2 or more

**62.** Which of the following can be added to a VPC, in addition to security groups on included instances, to further secure the VPC?

**A.** A NACL

**B.** A port filter

**C.** An ALB

**D.** A flow log

**63.** Which of the following statements is true about a custom, user-created NACL?

**A.** A NACL by default allows all traffic out of a VPC.

**B.** A NACL by default allows all traffic into a VPC.

**C.** A NACL is a virtual firewall for associated subnets.

**D.** A NACL functions at the instance level.

**64.** What do you use to permit and restrict control of a NACL?

**A.** VPC

**B.** WAF

**C.** AWS Organizations

**D.** IAM

**65.** Which of these are true about security groups? (Choose two.)

**A.** Support allow and deny rules

**B.** Evaluate all rules before deciding whether to allow traffic

**C.** Operate at the instance level

**D.** Apply to all instances in the associated subnet

**66.** Which of these are true about security groups? (Choose two.)

**A.** Stateful

**B.** Stateless

**C.** Process rules in order

**D.** Associated with an instance

**67.** Which of these are true about NACLs? (Choose two.)

**A.** Stateful

**B.** Stateless

**C.** Process rules in order

**D.** Associated with an instance

**68.** Which of these are true about NACLs? (Choose two.)

**A.** Apply to all instances in an associated subnet

**B.** Only apply if no security group is present

**C.** Support allow and deny rules

**D.** Evaluate all rules before deciding whether to allow or disallow traffic

**69.** In which order are NACLs and security groups evaluated?

**A.** NACLs and security groups are evaluated in parallel.

**B.** A NACL is evaluated first, and then the security group.

**C.** A security group is evaluated first, and then the NACL.

**D.** It depends on the VPC setup.

**70.** Which of these statements are true? (Choose two.)

**A.** A security group can apply to two instances at the same time.

**B.** A NACL applies to all instances within a subnet at the same time.

**C.** A security group can apply to only one instance at the same time.

**D.** A NACL can apply to only one instance at the same time.

**71.** With which of the following is a NACL associated?

**A.** An instance

**B.** A subnet

**C.** A VPC

**D.** A NACL can be associated with all of these.

**72.** Which of the following are true about the default NACL that comes with the default VPC? (Choose two.)

**A.** It allows all inbound traffic.

**B.** It allows all outbound traffic.

**C.** It disallows all inbound traffic.

**D.** It disallows all outbound traffic.

**73.** Which of the following are true about a user-created NACL? (Choose two.)

**A.** It allows all inbound traffic.

**B.** It allows all outbound traffic.

**C.** It disallows all inbound traffic.

**D.** It disallows all outbound traffic.

**74.** In which order are rules in a NACL evaluated?

**A.** From low to high, using the number on the rule

**B.** From high to low, using the number on the rule

**C.** From low to high, using the port of the rule

**D.** From high to low, using the port of the rule

**75.** Which of the following statements is not true? (Choose two.)

**A.** A network ACL has separate inbound and outbound rules.

**B.** Network ACLs are stateful.

**C.** Each subnet in your VPC must be associated with a NACL.

**D.** A network ACL can only be associated with a single subnet.

**76.** With how many subnets can a NACL be associated?

**A.** One

**B.** One or more

**C.** A NACL is associated with instances, not subnets.

**D.** A NACL is associated with VPCs, not subnets.

**77.** With how many NACLs can a subnet be associated?

**A.** One

**B.** One or more

**C.** A subnet is associated with security groups, not NACLs.

**D.** A subnet is associated with VPCs, not NACLs.

**78.** What happens when you associate a NACL with a subnet that already is associated with a different NACL?

**A.** Nothing, both NACLs are associated with the subnet.

**B.** You receive an error. You must remove the first NACL to associate the new one.

**C.** You receive an error. You must first merge the two NACLs to apply them to a subnet.

**D.** The new NACL replaces the previous NACL, and the subnet still only has one NACL association.

**79.** Which of the following are part of a network ACL rule? (Choose two.)

**A.** An ASCII code

**B.** A rule number

**C.** An IAM group

**D.** A protocol

**80.** Which of the following are part of a network ACL rule? (Choose two.)

**A.** An ALLOW or DENY specification

**B.** A CIDR range

**C.** An IP address

**D.** A VPC identifier

**81.** Which of the following inbound rules of a custom NACL would be evaluated first?

**A.** Rule #800 // HTTP // TCP // 80 // 0.0.0.0/0 -> ALLOW.

**B.** Rule #100 // HTTPS // TCP // 443 // 0.0.0.0/0 -> ALLOW.

**C.** Rule * // All // All // All // 0.0.0.0/0 -> DENY.

**D.** Rule #130 // RDP // TCP // 3389 // 192.0.2.0/24 -> ALLOW.

**82.** If all of the following inbound rules existed on a custom NACL, would SSH traffic be allowed?

Rule #800 // HTTP // TCP // 80 // 0.0.0.0/0 -> ALLOW

Rule #100 // HTTPS // TCP // 443 // 0.0.0.0/0 -> ALLOW

Rule * // All // All // All // 0.0.0.0/0 -> DENY

Rule #130 // RDP // TCP // 3389 // 192.0.2.0/24 -> ALLOW

**A.** Yes, SSH is included as a default protocol on NACLs.

**B.** Yes, SSH is included in the HTTPS protocol.

**C.** Only if the SSH access permission in IAM is granted.

**D.** No

**83.** If all of the following inbound rules existed on the default VPC's default NACL, would SSH traffic be allowed?

Rule #800 // HTTP // TCP // 80 // 0.0.0.0/0 -> ALLOW

Rule #100 // HTTPS // TCP // 443 // 0.0.0.0/0 -> ALLOW

**A.** Yes, the default VPC's default NACL allows all inbound traffic by default.

**B.** Yes, SSH is included in the HTTPS protocol.

**C.** Only if the SSH access permission in IAM is granted.

**D.** No

**84.** If all of the following inbound rules existed on a custom NACL, would SSH traffic be allowed?

Rule #800 // HTTP // TCP // 80 // 0.0.0.0/0 -> ALLOW

Rule #100 // HTTPS // TCP // 443 // 0.0.0.0/0 -> ALLOW

Rule #140 // All // All // All // 0.0.0.0/0 -> DENY

Rule #120 // SSH // TCP // 22 // 192.0.2.0/24 -> ALLOW

**A.** Yes

**B.** Yes, but only from the CIDR block 192.0.2.0/24.

**C.** Only if the SSH access permission in IAM is granted.

**D.** No

**85.** If all of the following inbound rules existed on a custom NACL, would SSH traffic be allowed?

Rule #800 // HTTP // TCP // 80 // 0.0.0.0/0 -> ALLOW

Rule #100 // HTTPS // TCP // 443 // 0.0.0.0/0 -> ALLOW

Rule #110 // All // All // All // 0.0.0.0/0 -> DENY

Rule #120 // SSH // TCP // 22 // 192.0.2.0/24 -> ALLOW

**A.** Yes

**B.** Yes, but only from the CIDR block 192.0.2.0/24.

**C.** Only if the SSH access permission in IAM is granted.

**D.** No

**86.** Which of the following is the most accurate statement about what the following inbound rule on a NACL will do?

Rule #120 // SSH // TCP // 22 // 192.0.2.0/24 -> ALLOW

**A.** Allows inbound SSH traffic to the associated subnets

**B.** Allows inbound TCP traffic to the associated subnets

**C.** Allows inbound TCP traffic to the associated subnets from the CIDR block 192.0.2.0/24

**D.** Allows inbound SSH traffic to the associated subnets from the CIDR block 192.0.2.0/24

**87.** Which of the following is the most accurate statement about what the following inbound rule on a NACL will do?

Rule #120 // HTTP // TCP // 80 // 0.0.0.0/0 -> ALLOW

**A.** Allows inbound HTTP traffic to the associated subnets

**B.** Allows inbound IPv4 HTTP traffic to the associated subnets as long as it is not prevented by lower-numbered rules

**C.** Allows inbound IPv4 HTTP traffic to the associated subnets

**D.** Allows inbound IPv4 TCP traffic to the associated subnets

**88.** What does the CIDR block 0.0.0.0/0 represent?

**A.** The entire Internet

**B.** The entire Internet, limited to IPv4 addresses

**C.** The entire Internet, limited to IPv6 addresses

**D.** Inbound traffic from the entire Internet

**89.** What does the CIDR block ::/0 represent?

**A.** The entire Internet

**B.** The entire Internet, limited to IPv4 addresses

**C.** The entire Internet, limited to IPv6 addresses

**D.** Inbound traffic from the entire Internet

**90.** Which of the following rules allows IPv6 outbound traffic to flow to the entire Internet through a NAT gateway with the ID nat-123456789?

**A.** 0.0.0.0/0 -> NAT -> nat-123456789

**B.** ::/0 -> nat-123456789

**C.** 0.0.0.0/0 -> nat-123456789

**D.** ::/0 -> NAT -> nat-123456789

**91.** How many availability zones in a single region does a single VPC span?

**A.** None, VPCs do not span availability zones.

**B.** One

**C.** At least two

**D.** All of them

**92.** Which of these must be specified when creating a new VPC? (Choose two.)

**A.** An availability zone

**B.** A region

**C.** A CIDR block

**D.** A security group

**93.** How many subnets can be added to an availability zone within a VPC?

**A.** None

**B.** One

**C.** One or more

**D.** At least two

**94.** To how many availability zones within a region can a single subnet in a VPC be added?

**A.** None

**B.** One

**C.** One or more

**D.** At least two

**95.** How many availability zones can a subnet span?

**A.** None

**B.** One

**C.** One or more

**D.** At least two

**96.** How many IPv6 CIDR blocks can be assigned to a single VPC?

**A.** None

**B.** One

**C.** One or more

**D.** At least two

**97.** How many IPv4 CIDR blocks can be assigned to a single VPC?

**A.** None

**B.** One

**C.** One or more

**D.** At least two

**98.** You have a VPC in US East 1 with three subnets. One of those subnets' traffic is routed to an internet gateway. What does this make the subnet?

**A.** A private subnet

**B.** A restricted subnet

**C.** The master subnet of that VPC

**D.** A public subnet

**99.** You have a public subnet in a VPC and an EC2 instance serving web traffic within that public subnet. Can that EC2 instance be reached via the Internet?

**A.** Yes

**B.** Yes, as long as it has a public IPv4 address.

**C.** Yes, as long as the VPC is marked as public.

**D.** No

**100.** You have a public subnet within your VPC. Within that subnet are three instances, each running a web-accessible API. Two of the instances are responding to requests from Internet clients, but one is not. What could be the problem?

**A.** The VPC needs to be marked as public-facing.

**B.** The three instances should be moved into an Auto Scaling group.

**C.** There is no internet gateway available for the VPC.

**D.** The unavailable instance needs an elastic IP.

**101.** Which of the following are allowed when creating a new VPC? (Choose two.)

**A.** An IPv4 CIDR block

**B.** VPC description

**C.** An IPv6 CIDR block

**D.** A security group

**102.** Which of the following is not a required part of creating a custom VPC? (Choose two.)

**A.** An IPv6 CIDR block

**B.** A VPC name

**C.** A set of VPC tags

**D.** An IPv4 CIDR block

**103.** Which of the following defines a subnet as a public subnet? (Choose two.)

**A.** A security group that allows inbound public traffic

**B.** A routing table that routes traffic through the internet gateway

**C.** Instances with public IP addresses

**D.** An internet gateway

**104.** Which of the following defines a VPN-only subnet? (Choose two.)

**A.** A routing table that routes traffic through the internet gateway

**B.** A routing table that routes traffic through the virtual private gateway

**C.** A virtual private gateway

**D.** An internet gateway

**105.** Which of the following are required components in a VPN-only subnet? (Choose two.)

**A.** A routing table

**B.** A virtual private gateway

**C.** An elastic IP address

**D.** An internet gateway

**106.** By default, how many VPCs can you create per region?

**A.** 1

**B.** 5

**C.** 20

**D.** 200

**107.** By default, how many subnets can you create per VPC?

**A.** 1

**B.** 5

**C.** 20

**D.** 200

**108.** By default, how many IPv4 CIDR blocks can you create per VPC?

**A.** 1

**B.** 5

**C.** 20

**D.** 200

**109.** By default, how many elastic IPs can you create per region?

**A.** 1

**B.** 5

**C.** 20

**D.** 200

**110.** Which of the following is not true? (Choose two.)

**A.** A subnet can have the same CIDR block as the VPC within which it exists.

**B.** A subnet can have a larger CIDR block than the VPC within which it exists.

**C.** A subnet can have a smaller CIDR block than the VPC within which it exists.

**D.** A subnet does not have to have a CIDR block specified.

**111.** A VPC peering connection connects a VPC to which of the following?

**A.** A subnet within another VPC

**B.** A specific instance within another VPC

**C.** Another VPC

**D.** A virtual private gateway

**112.** An Amazon VPC VPN connection links your on-site network to which of the following?

**A.** A customer gateway

**B.** An internet gateway

**C.** An Amazon VPC

**D.** A virtual private gateway

**113.** Which of the following are required for a VPC VPN connection? (Choose two.)

**A.** A customer gateway

**B.** An internet gateway

**C.** A virtual private gateway

**D.** A public subnet

**114.** Which of the following would you use to secure a VPC and its instances? (Choose two.)

**A.** A customer gateway

**B.** A NACL

**C.** A virtual private gateway

**D.** A security group

**115.** You want to ensure that no incoming traffic reaches any instances in your VPC. Which of the following is your best option to prevent this type of traffic?

**A.** A blacklist

**B.** A NACL

**C.** A virtual private gateway

**D.** A security group

**116.** You want to ensure that no incoming traffic reaches just the database instances in a particular subnet within your VPC. Which of the following is your best option to prevent this type of traffic?

**A.** A blacklist

**B.** A NACL

**C.** A virtual private gateway

**D.** A security group

**117.** You have a subnet with five instances within it. Two are serving public APIs and three are providing backend compute power through database instances. What is the best way to secure these instances? (Choose two.)

**A.** Apply NACLs at the subnet level.

**B.** Attach a single security group to all the instances.

**C.** Move the two backend database instances into a different subnet.

**D.** Attach an internet gateway to the VPC.

**118.** Security groups operate most like which of the following?

**A.** A blacklist

**B.** A NACL

**C.** A whitelist

**D.** A greylist

**119.** If you have a NACL and a security group, at what two levels is security functioning? (Choose two.)

**A.** The VPN level

**B.** The service level

**C.** The subnet level

**D.** The instance level

**120.** What type of filtering does a security group perform?

**A.** Stateful

**B.** Synchronous

**C.** Whitelist

**D.** Stateless

**121.** What type of filtering does a network ACL perform?

**A.** Stateful

**B.** Synchronous

**C.** Whitelist

**D.** Stateless

**122.** With which of the following can you create a VPC peering connection?

**A.** A VPC in the same AWS account and same region

**B.** A VPC in another AWS account

**C.** A VPC in the same AWS account but in another region

**D.** All of these

**123.** With which of the following can you not create a VPC peering connection? (Choose two.)

**A.** A VPC in another AWS account

**B.** An instance in the same region

**C.** A VPC in the same region

**D.** An internet gateway

**124.** You have an instance within a custom VPC, and that instance needs to communicate with an API published by an instance in another VPC. How can you make this possible? (Choose two.)

**A.** Enable cross-VPC communication via the AWS console.

**B.** Configure routing from the source instance to the API-serving instance.

**C.** Add a security group to the source instance.

**D.** Add an internet gateway or virtual private gateway to the source VPC.

**125.** Which of the following could be used to allow instances within one VPC to communicate with instances in another region? (Choose two.)

**A.** VPN connections

**B.** NACLs

**C.** Internet gateways

**D.** Public IP addresses

**126.** Which region does not currently support VPCs?

**A.** US East 1

**B.** EU West 1

**C.** SA East 1

**D.** VPC is supported in all AWS regions.

**127.** How many availability zones can a VPC span?

**A.** None, VPCs don't exist within availability zones.

**B.** One

**C.** Two or more

**D.** All the availability zones within a region

**128.** When you launch an instance within a VPC, in which availability zone is it launched?

**A.** The default availability zone

**B.** You must specify an availability zone.

**C.** The first availability zone without an instance

**D.** The availability zone with the least resources utilized

**129.** You are the architect at a company that requires all data at rest to be encrypted. You discover several EBS-backed EC2 instances that will be commissioned in the next week. How can you ensure that data on these volumes will be encrypted?

**A.** Use OS-level tools on the instance to encrypt the volumes.

**B.** Specify via the AWS console that the volumes should be encrypted when they are created.

**C.** You cannot enable encryption on a specific EBS volume.

**D.** Start the instances with the volumes and then encrypt them via the AWS console.

**130.** Which of the following is required to use a VPC endpoint?

**A.** An internet gateway

**B.** A VPN connection

**C.** A NAT instance

**D.** A VPC endpoint does not require any of these.

**131.** Which of the following is not true about a VPC endpoint?

**A.** A VPC endpoint can attach to an S3 bucket.

**B.** A VPC endpoint is a hardware device.

**C.** A VPC endpoint does not require an internet gateway.

**D.** Traffic to a VPC endpoint does not travel over the Internet.

**132.** To which of the following can a VPC endpoint *not* attach?

**A.** S3

**B.** SNS

**C.** Internet gateway

**D.** DynamoDB

**133.** Which of the following might you need to create for using a VPC endpoint attached to S3?

**A.** A NAT instance

**B.** A NAT gateway

**C.** An IAM role

**D.** A security group

**134.** Is it possible to SSH into a subnet with no public instances?

**A.** Yes

**B.** Yes, as long as you have a bastion host and correct routing.

**C.** Yes, as long as you have an AWS Direct Connect.

**D.** No

**135.** Where should a bastion host be located?

**A.** In a private subnet

**B.** In a public subnet

**C.** In a private VPC

**D.** In a VPC with a virtual private gateway

**136.** What is another name for a bastion host?

**A.** A remote host

**B.** A box host

**C.** A jump server

**D.** A bastion connection

**137.** To which of the following might a bastion host be used to connect?

**A.** A public instance in a public subnet

**B.** A public instance in a private subnet

**C.** A private instance in a public subnet

**D.** A private instance in a private subnet

**138.** Which of these would you use to secure a bastion host?

**A.** A network ACL

**B.** A security group

**C.** OS hardening

**D.** All of the above

**139.** For a bastion host intended to provide shell access to your private instances, what protocols should you allow via a security group?

**A.** SSH and RDP

**B.** Just SSH

**C.** Just RDP

**D.** Just HTTPS

**140.** Which of the following statements about internet gateways is false?

**A.** They scale horizontally.

**B.** They are automatically redundant.

**C.** They are automatically highly available.

**D.** They scale vertically.

**141.** To which of the following does an internet gateway attach?

**A.** An AWS account

**B.** A subnet within a VPC

**C.** A VPC

**D.** An instance within a subnet

**142.** Which of the following destination routes would be used for routing IPv4 traffic to an internet gateway?

**A.** 0.0.0.0/24

**B.** 0.0.0.0/0

**C.** ::/0

**D.** 192.168.1.1

**143.** Which of the following destination routes would be used for routing IPv6 traffic to an internet gateway?

**A.** 0.0.0.0/24

**B.** 0.0.0.0/0

**C.** ::/0

**D.** 192.168.1.1

**144.** Which of the following is not necessary for an instance to have IPv6 communication over the Internet?

**A.** A VPC with an associated IPv6 CIDR block

**B.** A public IPv6 assigned to the instance

**C.** A subnet with an associated IPv6 CIDR block

**D.** A virtual private gateway with IPv6 enabled

**145.** Which of the following are possible options for assigning to an instance that needs public access? (Choose two.)

**A.** A public IP address

**B.** An elastic IP address

**C.** An IAM role

**D.** A NACL

**146.** Which of the following will have internet gateways available? (Choose two.)

**A.** A public subnet

**B.** An IPv6 elastic IP address

**C.** The default VPC

**D.** An ALB

**147.** What does ALB stand for?

**A.** Access load balancer

**B.** Application load balancer

**C.** Adaptive load balancer

**D.** Applied load balancer

**148.** At what OSI layer does an application load balancer operate?

**A.** 4

**B.** 7

**C.** 4 and 7

**D.** 6

**149.** At what OSI layer does a network load balancer operate?

**A.** 4

**B.** 7

**C.** 4 and 7

**D.** 6

**150.** At what OSI layer does a classic load balancer operate?

**A.** 4

**B.** 7

**C.** 4 and 7

**D.** 6

**151.** Which type of load balancer operates at the Transport layer?

**A.** Classic load balancer

**B.** Application load balancer

**C.** Network load balancer

**D.** Both classic and network load balancers

**152.** Which type of load balancer operates at the Application layer?

**A.** Classic load balancer

**B.** Application load balancer

**C.** Network load balancer

**D.** Both classic and application load balancers

**153.** What type of subnets are the default subnets in the default VPC?

**A.** Private

**B.** Hybrid

**C.** Public

**D.** Transport

**154.** What type of subnets are the default subnets in a custom VPC?

**A.** Private

**B.** Hybrid

**C.** Public

**D.** Transport

**155.** Which of the following is not automatically created for an instance launched into a non-default subnet?

**A.** A private IPv4 address

**B.** A security group

**C.** A public IPv4 address

**D.** A route to other instances in the subnet

**156.** Which of the following would be needed to allow an instance launched into a non-default subnet Internet access? (Choose two.)

**A.** A private IPv4 address

**B.** A security group

**C.** An elastic IP address

**D.** An internet gateway

**157.** Which of the following would you need to add or create to allow an instance launched into a default subnet in the default VPC Internet access?

**A.** A public IPv4 address

**B.** An internet gateway

**C.** An elastic IP address

**D.** None of these

**158.** Which of the following would you use to allow outbound Internet traffic while preventing unsolicited inbound connections?

**A.** A NAT device

**B.** A bastion host

**C.** A VPC endpoint

**D.** A VPN

**159.** What does a NAT device allow?

**A.** Incoming traffic from the Internet to reach private instances

**B.** Incoming traffic from other VPCs to reach private instances

**C.** Outgoing traffic to other VPCs from private instances

**D.** Outgoing traffic to the Internet from private instances

**160.** Which of the following are NAT devices offered by AWS? (Choose two.)

**A.** NAT router

**B.** NAT instance

**C.** NAT gateway

**D.** NAT load balancer

**161.** Which of the following requires selecting an AMI? (Choose two.)

**A.** Launching an EC2 instance

**B.** Backing up an EBS volume

**C.** Creating an EBS volume

**D.** Launching a NAT instance

**162.** For which of the following do you not need to worry about operating system updates?

**A.** NAT instance

**B.** NAT gateway

**C.** EC2 instance

**D.** ECS container

**163.** Which of the following does not automatically scale to meet demand?

**A.** DynamoDB

**B.** NAT instance

**C.** SNS topic

**D.** NAT gateway

**164.** Which of the following, without proper security, could be most dangerous to your private instances?

**A.** Bastion host

**B.** VPC endpoint

**C.** Internet gateway

**D.** NAT instance

**165.** Which of the following could be used as a bastion host?

**A.** NAT gateway

**B.** VPC endpoint

**C.** Internet gateway

**D.** NAT instance

**166.** You are building out a site-to-site VPN connection from an on-site network to a private subnet within a custom VPC. Which of the following might you need for this connection to function properly? (Choose two.)

**A.** An internet gateway

**B.** A public subnet

**C.** A virtual private gateway

**D.** A customer gateway

**167.** You are building out a site-to-site VPN connection from an on-site network to a custom VPC. Which of the following might you need for this connection to function properly? (Choose two.)

**A.** A NAT instance

**B.** A DynamoDB instance

**C.** A private subnet

**D.** An internet gateway

**168.** With which of the following is an egress-only internet gateway most closely associated?

**A.** IPv4

**B.** IPv6

**C.** A NAT instance

**D.** A NAT gateway

**169.** You are responsible for securing an EC2 instance with an IPv6 address that resides in a public subnet. You want to allow traffic from the instance to the Internet but restrict access to the instance. Which of the following would you suggest?

**A.** VPC endpoint

**B.** Internet gateway

**C.** Egress-only internet gateway

**D.** A NAT gateway

**170.** You have just created a NAT instance and want to launch the instance into a subnet. Which of these need to be true of the subnet into which you want to deploy? (Choose two.)

**A.** The subnet is public.

**B.** The subnet is private.

**C.** The subnet has routing into the private subnets in your VPC.

**D.** The subnet has routing to the public subnets in your VPC.

**171.** Which of the following are true about an egress-only internet gateway? (Choose two.)

**A.** It only supports IPv4 traffic.

**B.** It is stateful.

**C.** It only supports IPv6 traffic.

**D.** It is stateless.

**172.** Which of these would be used as the destination address in a routing table for a VPC that uses an egress-only internet gateway?

**A.** 0.0.0.0/0

**B.** 0.0.0.0/16

**C.** ::/0

**D.** ::/24

**173.** Which of the following are true about IPv6 addresses? (Choose two.)

**A.** They are globally unique.

**B.** They are in the format x.y.z.w.

**C.** They require underlying IPv4 addresses.

**D.** They are public by default.

**174.** What is an elastic network interface? (Choose two.)

**A.** A hardware network interface on an EC2 instance

**B.** A virtual network interface

**C.** An interface that can have one or more IPv6 addresses

**D.** An interface that does not have a MAC address

**175.** Which of the following is not part of an elastic network interface?

**A.** A primary IPv4 address

**B.** A MAC address

**C.** A source/destination check flag

**D.** A NACL

**176.** How many network interfaces can a single instance have?

**A.** None

**B.** One and only one

**C.** One or more

**D.** At least two, up to five

**177.** If an elastic network interface is moved from one instance to another, what happens to network traffic directed at the interface?

**A.** It is redirected to the elastic network interface that has moved to the new instance.

**B.** It is redirected to the primary network interface on the original instance.

**C.** It is redirected to the primary network interface on the new instance.

**D.** It is lost and must be re-sent to the elastic network interface on the new instance.

**178.** To how many instances can an elastic network interface be attached?

**A.** One and only one

**B.** One or more

**C.** One at a time, but it can be moved from one instance to another.

**D.** Up to five

**179.** Which of these is not a reason to attach multiple network interfaces to an instance?

**A.** You are creating a management network.

**B.** You are attempting to increase network throughput to the instance.

**C.** You need a high-availability solution and have a low budget.

**D.** You need dual-homed instances.

**180.** Which of the following can you not do with regard to network interfaces?

**A.** Detach a secondary interface from an instance.

**B.** Attach an elastic network interface to an instance with an existing interface.

**C.** Detach a primary interface from an instance.

**D.** Attach an elastic network interface to a different instance than originally attached.

**181.** Which of the following is not a valid attribute for an elastic network interface?

**A.** An IPv6 address

**B.** An IPv4 address

**C.** A source/destination check flag

**D.** A routing table

**182.** Why might you use an elastic IP address?

**A.** You need an IPv4 address for a specific instance.

**B.** You need an IPv6 address for a specific instance.

**C.** You want to mask the failure of an instance to network clients.

**D.** You want to avoid making changes to your security groups.

**183.** Which of the following can you not do with an elastic IP address?

**A.** Change the IP address associated with it while it is in use.

**B.** Move it from one instance to another.

**C.** Move it across VPCs.

**D.** Associate it with a single instance in a VPC.

**184.** Which of the following are advantages of an elastic IP? (Choose two.)

**A.** Reduces the number of IP addresses your VPC uses

**B.** Provides protection in case of an instance failure

**C.** Allows all attributes of a network interface to be moved at one time

**D.** Provides multiple IP addresses for a single instance

**185.** Which of the following would you need to do to create an elastic IP address? (Choose two.)

**A.** Allocate an elastic IP address for use in a VPC.

**B.** Allocate an IP address in Route 53.

**C.** Detach the primary network interface on an instance.

**D.** Associate the elastic IP to an instance in your VPC.

**186.** Which of these is not a valid means of working with an Amazon EBS snapshot?

**A.** The AWS API

**B.** The AWS CLI

**C.** The AWS console

**D.** The AWS EBS management tool

**187.** Where are individual instances provisioned?

**A.** In a VPC

**B.** In a region

**C.** In an availability zone

**D.** In an Auto Scaling group

**188.** How are EBS snapshots backed up to S3?

**A.** Incrementally

**B.** In full, every time they are changed

**C.** EBS snapshots are backed up to RDS.

**D.** Sequentially

**189.** You have an existing IAM role in use by several instances in your VPC. You make a change in the role, removing permissions to access S3. When does this change take effect on the instances already attached to the role?

**A.** Immediately

**B.** Within 60 seconds

**C.** The next time the instances are restarted

**D.** The instances preserve the pre-change permissions indefinitely.

**190.** How many IAM roles can you attach to a single instance?

**A.** One

**B.** One or two

**C.** As many as you want

**D.** None, roles are not assigned to instances.

**191.** How can you attach multiple IAM roles to a single instance? (Choose two.)

**A.** You can attach as many roles as you want to an instance.

**B.** You cannot, but you can combine the policies each role uses into a single new role and assign that.

**C.** You can assign two IAM roles to an instance, but no more than that.

**D.** You cannot; only one role can be assigned to an instance.

**192.** You need to make a change to a role attached to a running instance. What do you need to do to ensure the least amount of downtime? (Choose two.)

**A.** Update the IAM role via the console or AWS API or CLI.

**B.** Re-attach the updated role to the instance.

**C.** Restart the instance.

**D.** Other than updating the role, no additional changes are needed.

**193.** You have a new set of permissions that you want to attach to a running instance. What do you need to do to ensure the least amount of downtime? (Choose two.)

**A.** Remove the instance's IAM role via the console or AWS API or CLI.

**B.** Create a new IAM role with the desired permissions.

**C.** Stop the instance, assign the role, and restart the instance.

**D.** Attach the new role to the running instance.

**194.** How can you delete a snapshot of an EBS volume when it's used as the root device of a registered AMI?

**A.** You can't.

**B.** You can, but only using the AWS API or CLI.

**C.** Delete the snapshot using the AWS console.

**D.** Ensure that you have correct IAM privileges and delete the AMI.

**195.** Which of these is the best option for encrypting data at rest on an EBS volume?

**A.** Configure the volume's encryption at creation time.

**B.** Configure AES 256 encryption on the volume once it's been started.

**C.** Configure encryption using the OS tools on the attached EC2 instance.

**D.** Back up the data in the volume to an encrypted S3 bucket.

**196.** How can you ensure that an EBS root volume persists beyond the life of an EC2 instance, in the event that the instance is terminated?

**A.** The volume will persist automatically.

**B.** Configure the EC2 instance to not terminate its root volume and the EBS volume to persist.

**C.** You cannot; root volumes always are deleted when the attached EC2 instance is terminated.

**D.** Ensure that encryption is enabled on the volume and it will automatically persist.

**197.** Which of the following is not part of the well-architected framework?

**A.** Apply security at all layers.

**B.** Enable traceability.

**C.** Use defaults whenever possible.

**D.** Automate responses to security events.

**198.** Which of the following should you attempt to automate, according to the AWS well-architected framework? (Choose two.)

**A.** Security best practices

**B.** Scaling instances

**C.** Responses to security events

**D.** IAM policy creation

**199.** Which of the following statements are true? (Choose two.)

**A.** You are responsible for security in the cloud.

**B.** AWS is responsible for security of the cloud.

**C.** AWS is responsible for security in the cloud.

**D.** You are responsible for security of the cloud.

**200.** For which of the following is AWS responsible for security? (Choose two.)

**A.** Edge locations

**B.** Firewall configuration

**C.** Network traffic

**D.** Availability zones

**201.** For which of the following is AWS not responsible for security?

**A.** Networking infrastructure

**B.** RDS database installations

**C.** S3 buckets

**D.** Networking traffic

**202.** For which of the following are you not responsible for security?

**A.** DynamoDB

**B.** Operating system configuration

**C.** Server-side encryption

**D.** Application keys

**203.** Which of the following is not included in the well-architected framework's definition of security?

**A.** Data protection

**B.** Infrastructure protection

**C.** Reduction of privileges

**D.** Defective controls

**204.** Which of the following is a principle of the well-architected framework's security section?

**A.** Encrypt the least amount of data possible.

**B.** Always encrypt the most important data.

**C.** Encrypt everything where possible.

**D.** Encrypt data at rest.

**205.** Which of the following are principles of the well-architected framework's security section? (Choose two.)

**A.** Encrypt data at rest.

**B.** Encrypt data in transit.

**C.** Encrypt data in groups rather than individually.

**D.** Encrypt data at the destination.

**206.** Who is responsible for encrypting data in the cloud?

**A.** You

**B.** AWS

**C.** AWS provides mechanisms such as key rotation for which they are responsible, but you are responsible for appropriate usage of those mechanisms.

**D.** AWS provides an API, but you are responsible for security when using that API.

**207.** What is the term used to represent the resiliency of data stored in S3?

**A.** 9 9s

**B.** 11 9s

**C.** 7 9s

**D.** 99th percentile

**208.** Which of these statements is not true?

**A.** AWS recommends encrypting data at rest and in transit.

**B.** AWS will never move data between regions unless initiated by the customer.

**C.** AWS will initiate moving data between regions if needed.

**D.** Customers move data between regions rather than AWS.

**209.** Which of the following can be part of a strategy to avoid accidental data overwriting of S3 data?

**A.** IAM roles

**B.** MFA Delete

**C.** Versioning

**D.** All of these

**210.** Which of the following should always be done to protect your AWS environment? (Choose two.)

**A.** Enable MFA on the root account.

**B.** Enable MFA Delete on your S3 buckets.

**C.** Set a password rotation policy for users.

**D.** Create custom IAM roles for all users.

**211.** At what level does infrastructure protection exist in AWS?

- **A.** The physical hardware layer
- **B.** OSI layer 4
- **C.** The VPC layer
- **D.** OSI layer 7

**212.** Which of the following might be used to detect or identify a security breach in AWS? (Choose two.)

- **A.** CloudWatch
- **B.** CloudFormation
- **C.** CloudTrail
- **D.** Trusted Advisor

**213.** Which of the following AWS services is associated with privilege management?

- **A.** AWS Config
- **B.** RDS
- **C.** IAM
- **D.** VPC

**214.** Which of the following AWS services is associated with privilege management?

- **A.** Internet gateway
- **B.** S3-IA
- **C.** CloudTrail
- **D.** MFA

**215.** Which of the following AWS services is associated with identifying potential security holes?

- **A.** Trusted Advisor
- **B.** CloudFormation
- **C.** Security Detector
- **D.** Security Advisor

**216.** Which of the following is not one of the five pillars in the cloud defined by the AWS well-architected framework?

- **A.** Operational excellence
- **B.** Performance efficiency
- **C.** Organizational blueprint
- **D.** Cost optimization

**217.** Which of the following is not one of the five pillars in the cloud defined by the AWS well-architected framework?

**A.** Performance efficiency

**B.** Usability

**C.** Security

**D.** Reliability

**218.** Which of the following is not one of the security principles recommended by AWS's well-architected framework?

**A.** Automate security best practices.

**B.** Enable traceability.

**C.** Apply security at the highest layers.

**D.** Protect data in transit and at rest.

**219.** Which of the following is one of the security principles recommended by AWS's well-architected framework?

**A.** Make sure all users have passwords.

**B.** Only protect data at rest.

**C.** Turn on MFA Delete for S3 buckets.

**D.** Keep people away from data.

**220.** The AWS's well-architected framework defines five areas to consider with respect to security. Choose the two that are part of this set. (Choose two.)

**A.** Identity and Access Management

**B.** User management

**C.** Virtual private networks

**D.** Incident response

**221.** Who is responsible for physically securing the infrastructure that supports cloud services?

**A.** AWS

**B.** You

**C.** Your users

**D.** AWS and you have joint responsibility.

**222.** Which of the following statements about the root account in an AWS account are true? (Choose two.)

**A.** It is the first account created.

**B.** It is ideal for everyday tasks.

**C.** It is intended primarily for creating other users and groups.

**D.** It has access keys that are important to keep.

**223.** Which of the following are appropriate password policy requirements? (Choose two.)

**A.** Maximum length

**B.** Recovery

**C.** Minimum length

**D.** Complexity

**224.** What additional requirements should users that can access the AWS console have?

**A.** Users with console access should have more stringent password policy requirements.

**B.** Users with console access should have to use their access keys to log in.

**C.** Users with console access should be required to use MFA.

**D.** None. These users should be treated the same as other users.

**225.** Which of the following provide a means of federating users from an existing organization? (Choose two.)

**A.** SAML 2.0

**B.** Web identities

**C.** LDAP

**D.** UML 2.0

**226.** Which of the following principles suggests ensuring that authenticated identities are only permitted to perform the most minimal set of functions necessary?

**A.** Principle of lowest privilege

**B.** Principle of least priority

**C.** Principle of least privilege

**D.** Principle of highest privilege

**227.** What is an AWS Organizations OU?

**A.** Orchestration unit

**B.** Organizational unit

**C.** Operational unit

**D.** Offer of urgency

**228.** What is an AWS Organizations SCP?

**A.** Service control policy

**B.** Service control permissions

**C.** Standard controlling permissions

**D.** Service conversion policy

**229.** To which of the following constructs is an AWS Organizations SCP applied?

**A.** To a service control policy

**B.** To an IAM role

**C.** To an organizational unit

**D.** To a SAML user store

**230.** Which of the following can be used to centrally control AWS services across multiple AWS accounts?

**A.** A service control policy

**B.** An organizational unit

**C.** An LDAP user store

**D.** IAM roles

**231.** What AWS service would you use for managing and enforcing policies for multiple AWS accounts?

**A.** AWS Config

**B.** AWS Trusted Advisor

**C.** AWS Organizations

**D.** IAM

**232.** Which of the following does AWS provide to increase privacy and control network access?

**A.** Network firewalls built into Amazon VPC

**B.** Encryption in transit with TLS across all services

**C.** Connections that enable private and dedicated connections from an on-premises environment

**D.** All of these

**233.** You have an application that uses S3 standard for storing large data. Your company wants to ensure that all data is encrypted at rest while avoiding adding work to your current development sprints. Which S3 encryption solution should you use?

**A.** SSE-C

**B.** SSE-S3

**C.** SSE-KMS

**D.** Amazon S3 Encryption Client

**234.** You are the architect of an application that allows users to send private messages back and forth. You want to ensure encryption of the messages when stored in S3 and a strong auditing trail in case of a breach. You also want to capture any failed attempts to access data. What Amazon encryption solution would you use?

**A.** SSE-C

**B.** SSE-S3

**C.** SSE-KMS

**D.** Amazon S3 Encryption Client

**235.** Your company has just hired three new developers. They need immediate access to a suite of AWS services. What is the best approach to giving these developers access?

**A.** Give the developers the admin credentials and change the admin password when they are finished for the day.

**B.** Create a new IAM user for each developer and assign the required permissions to each user.

**C.** Create a new IAM user for each developer, create a single group with the required permissions, and assign each user to that group.

**D.** Create a new SCP and assign the SCP to an OU with each user's credentials within that OU.

**236.** Your application requires a highly available storage solution. Further, the application will serve customers in the EU and must comply with EU privacy laws. What should you do to provide this storage?

**A.** Create a new EC2 instance in EU-Central-1 and set up EBS volumes in a RAID configuration attached to that instance.

**B.** Create a new S3 standard bucket in EU-West-1.

**C.** Create a new Glacier vault in EU-South-1.

**D.** Create a new Auto Scaling group in EU-West-1 with at least three EC2 instances, each with an attached Provisioned IOPS EBS volume.

**237.** Which of the following provides SSL for data in transit?

**A.** S3 standard

**B.** S3 One Zone-IA

**C.** Glacier

**D.** All of these

**238.** Which of the following does not provide encryption of data at rest?

**A.** S3 standard

**B.** S3 One Zone-IA

**C.** Glacier

**D.** All of these encrypt data at rest.

**239.** What is the AWS shared responsibility model?

**A.** A model that defines which components AWS secures and which you as an AWS customer must secure

**B.** A model that defines which components you secure and which components your customers must secure

**C.** A model that defines how connections between offices or on-premises data centers and the cloud must work together to secure data that moves between the two

**D.** A model that defines how the five pillars of the AWS well-architected framework interact

**240.** Which of the following is not one of the types of services that AWS offers, according to the shared responsibility model?

**A.** Infrastructure services

**B.** Managed services

**C.** Containers services

**D.** Abstracted services

**241.** For which of the following are you not responsible for security?

**A.** Operating systems

**B.** Credentials

**C.** Virtualization infrastructure

**D.** AMIs

**242.** Which of the following is used to allow EC2 instances to access S3 buckets?

**A.** IAM role

**B.** IAM policy

**C.** IAM user

**D.** AWS organizational unit

**243.** You have a task within a Docker container deployed via AWS ECS. The application cannot access data stored in an S3 bucket. What might be the problem? (Choose two.)

**A.** The IAM role associated with the task doesn't have permissions to access S3.

**B.** The task is not in a security group with inbound access allowed from S3.

**C.** The task does not have access to an S3 VPC endpoint.

**D.** There is no policy defined to allow ECS tasks to access S3.

**244.** What is the default security on a newly created S3 bucket?

**A.** Read-only

**B.** Read and write is permitted from EC2 instances in the same region.

**C.** Completely private, reads and writes are disallowed.

**D.** There is no policy defined to allow ECS tasks to access S3.