223. C. Here, the determining factor is the requirement of instant access. S3 One Zone-IA will give you that access, at a lower cost than S3 standard and S3-IA. According to AWS, all three classes have the same first byte latency (milliseconds).

224. D. Glacier takes 3–5 hours to deliver the first byte.

225. D. This is easy to miss, and often is. All three of these S3 storage classes share the same first-byte latency: milliseconds.

226. D. Spot instances offer you significant costs savings as long as you have flexibility and application processes can be stopped and started.

Domain 3: Specify Secure Applications and Architectures

1. B, D. Option A is false, but option B is true. Default security groups prevent all traffic in and allow all traffic out. Options C and D are about whether or not a security group is stateful: whether an incoming connection automatically can get back out. Security groups *are* stateful, so D is true. If the subject of the question was a NACL, then option C would be true, as NACLs are stateless.

2. B. D is not a good answer because relying on encryption outside of S3 does not best address the concerns around consistency. It is generally better to allow AWS to handle encryption in cases where you want to ensure all encryption is the same across a data store. SSE-C, SSE-KMS, and SSE-C all provide this. However, among those three, KMS is the best option for providing clear audit trails.

3. A, C. A bastion host is a publicly accessible host that allows traffic to connect to it. Then, an additional connection is made from the bastion host into a private subnet and the hosts within that subnet. Because the bastion must be accessed by public clients, it must be exposed to the Internet (A). If it is within a private subnet (B), it will not be accessible, making that answer incorrect. There also must be an explicit route from the bastion host into the private subnet (C); this is usually within a NACL. Finally, the security of the bastion *must* be different from the hosts in the private subnet. The bastion host should be hardened significantly as it is public, but also accessible; this is in many ways the *opposite* of the security requirements of hosts within a private subnet.

4. A, C. AWS sometimes asks questions like this to ensure that you understand that the root account is truly a root account and you cannot restrict that account's access. Anything that involves removing access for the root account is always invalid.

5. B. This is a "gimme question" that AWS will often ask on exams. You should never store your application keys on an instance, in an AMI, or anywhere else permanent on the cloud—meaning option B is true. Additionally, D makes no sense; application keys are for programmatic access, not console access.

6. A, C. Site-to-site VPN connections require a virtual private gateway (on the AWS side) and a customer gateway (on the local side). A private subnet is optional, but not required, as is a NAT instance.

7. B, D. There are two pairs of answers here, and you need to choose the correct pair in each case. For private subnet instances, you need a route out to a NAT gateway, and that NAT gateway must be in a public subnet—otherwise, it would not itself be able to provide outbound traffic access to the Internet. That means option D is correct, as is answer B: 0.0.0.0/0 means "traffic with a destination in the Internet at large," more or less.

8. A, B. The easiest way to handle this question is by thinking of a NAT gateway as essentially a managed service and a NAT instance as an instance (which you manage) for networking. That helps identify B as false (you never choose instance types and sizes for managed services) and C as true (AWS patches managed services). Further, since AWS manages NAT gateways, they are automatically highly available and do not need you to associate security groups. This means that A is false—NAT instances *can be* made highly available, but not without your manual intervention—and D is true.

9. A. Option A is true, and if you know that, this is an easy question. However, it doesn't seem obvious, as all custom NACLs *disallow* all inbound and outbound traffic. It is only a VPC's default NACL that has an "allow all" policy. As for B and C, these are both reversed: NACLs are stateless (allowing independent configuration of inbound and outbound traffic) and security groups are stateful. This also explains why D is false: NACLs are stateless.

10. A. Permission changes to a role now take place immediately and apply to all instances using that role.

11. C. If an allow-everything doesn't set off alarm bells, the reference to SSH should. Security groups, by default, don't allow any traffic in. They require you to explicitly allow inbound traffic (C); the other options are all false. And security groups are stateful—remember this, as it will come up in almost every single exam.

12. C. All outbound traffic is allowed to pass out of a VPC by default, although no inbound traffic is allowed.

13. C. EBS volumes can be encrypted when they are created. All other options typically affect snapshots of the volume, but not the volume itself.

14. A, D. Security groups only contain allow rules, not deny rules (and prevent rules are not an actual rule type). Then, you can create both inbound and outbound rules.

15. B, C. You specify allow rules for security groups, so A is false. B and C are true: Default security groups allow all outbound traffic, and you specify separate inbound and outbound rules. Finally, security groups are stateful, not stateless, so D is false.

16. A, D. A is false, as security groups don't provide for deny rules. B and C are both true (and therefore are not correct answers). D is false, because without specific outbound rules, nothing is allowed to flow out. (Note that by default, there is an allowance for all outgoing traffic in security groups, although that can be removed.)

17. B, C. A security group can actually have no inbound or outbound rules, so A and D are not required. A security group does require a name and description, though.

18. B. A security group can be attached to multiple constructs, like an EC2 instance, but is ultimately associated with a network interface, which in turn is attached to individual instances. This is a tough question and probably at the very edge of what the exam might ask.

19. A, C. The easiest way to work this is to recognize that default security groups never allow broad inbound traffic. That eliminates B and D and leaves rules that allow all outbound traffic for both IPv4 (A) and IPv6 (C).

20. A, D. Security group rules have a protocol and a description. They do not have a subnet, although they can have CIDR blocks or single IP addresses. Instances can associate with a security group, but a security group does not itself refer to a specific instance.

21. B, C. They key here is not the endpoint, but the actual protocol used to access the endpoint. In this case, HTTPS is secure, while HTTP is not, so the answers using HTTPS—B and C—are correct.

22. A. Client-side encryption involves the client (you, in this example) managing the entire encryption and decryption process. AWS only provides storage.

23. C. With server-side encryption, AWS handles all the object encryption and decryption.

24. B, C. For client-side encryption, you'll need a master key, which can either be a KMS-managed key (option B) or a client-side master key. You'll also need an SDK for encrypting the client-side data (C).

25. C. You'll probably simply need to memorize this one. SSE-S3, SSE-KMS, and SSE-C are all valid approaches to S3 encryption; SSE-E is made up.

26. B. The word *audit* should be a trigger for you: always choose KMS when you see a need for strong auditing. SSE-KMS provides a very good audit trail and security, perhaps the best of all these options for most use cases.

27. D. SSE-C allows the customer (the C in SSE-C) to manage keys, but S3 then handles the actual encryption of data.

28. C. Client-side encryption allows the customer to manage keys and encrypt data themselves, then store the data on S3 already encrypted. There's a lot of overhead with this approach, but it's ideal for the use case described.

29. A. In general, SSE-S3 is the "starter" option for encryption. It's by no means a simple or amateur approach to security, but it is low cost compared to KMS and has much less overhead than client-side or SSE-C encryption keys.

30. A, C. Here, you must recognize that EU West and EU Central are both EU regions and the other two options are not.

31. B, C. Option A isn't valid because US-West isn't an EU region. Options B and C are valid as they both provide EU regions, and S3 and S3-IA both can survive the loss of an availability zone; option D would *not* survive the loss of an AZ.

32. B. Multi-AZ RDS instances use synchronous replication to push changes.

33. B. MFA Delete is the most powerful anti-deletion protection you can provide without disabling delete via IAM roles. Option A doesn't affect your object storage—EBS is block storage. Options C and D both won't help; delete requests can't be blocked by Lambda, and there is no "DELETE endpoint" on the S3 API.

34. A, B. MFA Delete is the right option here (B), but A is a required step to enable MFA Delete. Option C doesn't actually make sense, and while option D would technically prevent all deletions, it isn't what the question is asking: You must prevent accidental deletions, not remove the ability to delete objects altogether.

35. D. You must enable versioning to enable MFA Delete. The region of the bucket doesn't have any effect here (B and C), and there is no way to disable the REST API (A), although you could remove programmatic access via IAM or removal of access keys.

36. D. AWS Trusted Advisor does all three of the above: improve performance, reduce cost, and improve security.

37. D. AWS Trusted Advisor provides advice on cost, fault tolerance, performance, and security but does not address account organization.

38. A, B. Here, it's not reasonable to memorize the seven core AWS Trusted Advisor checks. Instead, consider which of these are valid improvements that Trusted Advisor might make. A and B relate to security and permissions, while both C and D are pretty far afield of cost, security, or performance suggestions.

39. A, C. This is tricky. First, MFA on the root account is a standard recommendation, so you can select that. For the remaining three answers, the one that is most directly a "common security recommendation" would have to be S3 buckets with write access, and that is the correct answer.

40. B. The only one of these that's not possible with IAM is denying the root account access to EC2 instances. That's not possible—with IAM or any other mechanism.

41. B, C. A is true, and D is true; if you know this, choosing B and C is simple. Otherwise, you need to recognize that just supplying a client key to S3 is not enough; some form of client-side encryption or server-side encryption using client keys must be enabled. EBS volumes can be encrypted outside of S3 and stored regardless of how S3 is encrypting data.

42. A, B. There are four types of data encrypted when an EBS volume is encrypted: data at rest on the volume, data moving between the volume and the instance, any snapshots created from the volume, and any volumes created from those snapshots.

43. B, C. This is tricky, as both answers that involve unencrypted data have some tricky wording. First, B is not a case of encryption; if data never touches the encrypted volume, it is not automatically encrypted. Second, for C, data that is on the instance but never moves to the encrypted volume is also not automatically encrypted.

44. D. All of these are encrypted. Data moving to and from the volume as well as data at rest on the volume are all encrypted.

45. C. KMS is used as the encryption service, but this is not the S3-KMS that is specific to S3 encryption. You will also sometimes see this KMS referenced as AWS-KMS.

46. C. This is a case of pure memorization. The URL is always `http://169.254.169.254` and the metadata, which is what you want, is at `/latest/meta-data/`.

47. A, D. Encryption of a volume affects snapshots of the volume and instances created from that snapshot, but nothing else.

48. A, D. The only steps required here are to copy the snapshot to the new region (usually via the console), and then create a new volume from it.

49. D. You cannot encrypt a running instance; you have to create the instance with encryption enabled.

50. D. You cannot encrypt a running RDS instance, so B is incorrect, and you have no access to the underlying instance for RDS, so C is also incorrect. Option A sounds possible, but it will not address any data created by the database itself (such as indices, references to other data in the database, etc.). The only way to encrypt an RDS instance is to encrypt it at creation of the instance.

51. C. The only option here is the manual one. You must set up encryption when creating a new instance from scratch (snapshots won't work) and then move data into it so that this data is encrypted as it moves into the new instance.

52. A. You cannot encrypt an existing volume "on the fly." You must create a snapshot and then encrypt that snapshot as you copy it to another, encrypted snapshot. You can then restore from that new snapshot.

53. D. None of these will work. The important thing to remember for a question like this is that you must make a *copy* of an unencrypted snapshot to apply encryption. There is no in-place encryption mechanism for volumes or snapshots.

54. B. The only way to encrypt an EBS volume is to encrypt it *at creation time*. Remembering this one detail will help on lots of questions in this vein.

55. C, D. You cannot encrypt an existing EBS volume, so A is incorrect. And you cannot encrypt a snapshot that is unencrypted, so B is incorrect. You *can* encrypt a copy of a snapshot and restore an encrypted snapshot to a volume that is encrypted (C and D).

56. B, C. Snapshots of encrypted volumes stay encrypted—whether you copy them (B and C) or create volumes from them (D). So A and D are true, while B and C are false.

57. B. You can copy snapshots across accounts, but the default permissions do not allow this. So you have to modify those permissions, and then the snapshot can be copied to any other AWS account, regardless of account owner.

58. B. You can only create volumes from snapshots in the same region. Since the instance is desired in US West 1, a copy of the snapshot must be made in that region first, so B is correct.

59. C. You can copy a snapshot to a different region without any special considerations.

60. A, C. Security groups control the inbound and outbound traffic allowed into and out of instances.

61. C. An instance must have a security group but can have more than that.

62. A. In addition to security groups, NACLs (network access control lists) can be used to further refine inbound and outbound routing into and out of a VPC. Security groups are attached to instances, and NACLs to VPCs, building a complete security picture of your VPC and its instances.

63. C. NACLs are virtual firewalls, and they operate at the subnet and VPC level rather than at an individual instance level. Also note the words *custom, user-created*. The default NACL does allow in and out all traffic; created NACLs do not.

64. D. IAM roles and permissions control access to NACLs.

65. B, C. Security groups support only allow rules (A is false). They do evaluate all rules (B is true) and operate at the instance level (C is true). D is false, as security groups aren't associated with a subnet.

66. A, D. Security groups are stateful and are associated with an instance (or instances), so A and D are true. They are not stateless, and they process all rules rather than processing rules in order.

67. B, C. NACLs are stateless; rules must be specified for traffic going both in and out (so A is false, and B is true). They also process rules in order (C is true). They're associated with subnets, not a particular instance (so D is false).

68. A, C. NACLs are associated with a subnet (A) and support both allow and deny rules (C). B is false; NACLs and security groups work together. D is false, as rules are processed in order.

69. B. NACLs are always evaluated first because they exist at the border of a subnet. As security groups are attached to instances, they are not processed until traffic passes through the NACL and into the instance's subnet.

70. A, B. Both security groups and NACLs can—and usually do—apply to multiple instances in a subnet. The NACL applies to all instances within the associate subnet, and a security group can be associated with multiple instances.

71. B. NACLs are associated with subnets.

72. A, B. The default NACL allows in and out all traffic, which is somewhat unintuitive. Keep in mind that the default *security group* disallows inbound traffic, but the default NACL allows that traffic in.

73. C, D. Unlike the default NACL that comes with the default VPC, custom NACLs disallow all inbound and outbound traffic by default.

74. A. Each rule in a NACL has a number, and those rules are evaluated using those numbers, moving from low to high.

75. B, D. A and C are true. B is false; NACLs are stateless. D is false, because a NACL can be associated with multiple subnets.

76. B. A NACL is associated with a subnet, not an instance or VPC. It can be associated with a single subnet or multiple subnets.

77. A. A subnet is associated with a NACL. However, a subnet can only be associated to a single NACL at a time.

78. D. A subnet is associated with a NACL but can only be associated to a single NACL at a time.

79. B, D. NACL rules have a rule number, a protocol, a choice of ALLOW or DENY, and a CIDR range and port or port range for inbound and outbound traffic.

80. A, B. NACL rules have a rule number, a protocol, a choice of ALLOW or DENY, and a CIDR range and port or port range for inbound and outbound traffic.

81. B. Almost none of this detail actually matters. The only key parameter is the rule number. NACLs evaluate lowest-numbered rules first, so Rule #100 would go first, option B.

82. D. SSH is not explicitly mentioned, so it is not allowed on a custom NACL. Every protocol must explicitly be mentioned.

83. A. SSH is not explicitly mentioned, but because the question asks about the *default* NACL on the *default* VPC, all traffic is allowed in unless explicitly denied.

84. B. SSH is allowed here, but only from a specific CIDR block.

85. D. While there is a rule allowing SSH from the CIDR block 192.0.2.0/24, that rule would be evaluated after the lower-numbered rule 110, which disallows any traffic not allowed in from lower-numbered rules (in this case, just rule #100).

86. D. Technically, B and C are correct; SSH is a type of TCP traffic. However, that is not the most specific answer, which is what the question asks. A is partially correct but does not call out the CIDR block limitation that D does. Therefore, D is the most accurate answer.

87. B. The *most accurate* answer here includes several components: the type of TCP traffic (HTTP), the allowed source CIDR block (the entire Internet), and IPv4. This rule does *not* explicitly allow IPv6 traffic. Further, this rule is only effective if there are no lower-numbered rules that short-circuit this rule.

88. B. 0.0.0.0/0 represents IPv4 addresses, and the entire Internet. However, a CIDR block does not represent any type of traffic, inbound or outbound.

89. C. ::/0 represents IPv6 addresses, and the entire Internet. However, a CIDR block does not represent any type of traffic, inbound or outbound.

90. B. ::/0 represents IPv6 addresses, so the answer must be either B or D. The route should go from all IPv6 addresses to the ID of the NAT gateway, which is nat-123456789. There is no intermediate -> NAT that should be inserted into the routes.

91. D. A VPC spans all the availability zones in a region.

92. B, C. You must always select a region to create a VPC, and you must always provide a CIDR block. VPCs span all the AZs in a region, so that is not required, and security groups are associated at the instance level rather than at the VPC level.

93. C. For a single VPC, you can add one or more subnets to each availability zone within that VPC.

94. B. A subnet cannot span availability zones. It can be added to a single AZ.

95. B. A subnet cannot span availability zones. It can be added to a single AZ and can only exist within that single AZ.

96. B. A VPC can have a single primary CIDR block assigned to it for IPv4 addresses and an optional IPv6 CIDR block. While you can add secondary IPv4 CIDR blocks, you *cannot* add additional CIDR blocks for IPv6 at this time.

97. C. A VPC can have a single primary CIDR block assigned to it for IPv4 addresses and an optional IPv6 CIDR block. However, you can add *additional* secondary CIDR blocks to a VPC (up to four).

98. D. Any subnet that routes traffic through an internet gateway is a public subnet by definition.

99. B. Instances in a public subnet are not automatically reachable. They must have either a public IPv4 or IPv6 address (B) or an elastic IP address.

100. D. A public subnet, as well as existing Internet-accessible instances, indicates a working internet gateway, so C is not correct. A is not an actual AWS option, and B—Auto Scaling—would not address public accessibility. This leaves D, which is correct: Instances in a public subnet that are intended to be Internet accessible need either a public IP address or an elastic IP address assigned to the instance.

101. A, C. When creating a VPC, you can specify an option name, a required IPv4 CIDR block, and an optional IPv6 CIDR block.

102. A, C. When creating a VPC, you can specify an option name, a required IPv4 CIDR block, and an optional IPv6 CIDR block. You cannot assign tags to a VPC at creation time.

103. B, D. A public subnet is one in which traffic is routed (via a routing table, B) to an internet gateway (D).

104. B, C. A VPN-only subnet routes traffic through a virtual private gateway rather than an internet gateway.

105. A, B. At a minimum, a VPC-only subnet must have a routing table routing traffic and a virtual private gateway to which traffic is routed. Neither elastic IP addresses nor internet gateways are required.

106. B. You can only create 5 VPCs per region by default. Creating more requires a request to AWS.

107. D. This is a high number, but accurate: You can create 200 subnets per VPC.

108. B. This is a very hard question, but it can come up, albeit rarely. This limit is your primary CIDR block and then, in addition, 4 secondary CIDR blocks.

109. B. You're allowed 5 elastic IP addresses per region, unless you have the default limits raised by AWS.

110. B, D. Subnets must have CIDR blocks (so D is false), and the block must be the same as or smaller than the CIDR block for the VPC within which it exists, so while A and C are true, B is false.

111. C. A VPC peering connection connects one VPC to another VPC via networking and routing.

112. C. A VPC VPN connection links your on-site network to a VPC within the AWS cloud.

113. A, C. A VPC VPN connection requires a customer gateway, a VPN connection, and a virtual private gateway.

114. B, D. Customer gateways (A) and virtual private gateways (C) are used in VPN connections. For security, a NACL (B) is used at the subnet level, and a security group (D) can be used at the instance level.

115. B. A NACL is best for dealing with all traffic at a subnet or VPC level, as it is associated at the subnet level.

116. D. Anytime you are protecting or limiting traffic to or from specific instances, a security group is your best choice. Security groups are associated with specific instances, so they can effectively limit traffic to some instances while allowing other instances—using different security groups—to still be accessible.

117. A, C. This takes a little careful reading. First, it is not considered a good practice to mix private and public instances within a subnet—although this is not a hard-and-fast rule. So C, moving the private database instances into a different subnet, is at least worth considering. D is not helpful in this case. If you have two subnets, one private and one public, then A is a good idea: NACLs can protect one subnet and keep another public. Finally, B is *not* valid, because of the word *single*. You cannot have a single security group that allows traffic to one instance but not to another. This leaves A and C as the best combined solution.

118. C. A security group denies all traffic unless explicitly allowed. This means it functions as a whitelist: Only specific rules allow in traffic, and all other traffic is denied.

119. C, D. A security group operates at the instance level, and a NACL operates at the subnet level.

120. A. A security group performs stateful filtering, meaning that traffic allowed in is automatically allowed back out, without the need for an explicit outbound rule.

121. D. Network ACLs are stateless. Inbound traffic is not automatically allowed back out; an explicit rule must be present for traffic to move from within a subnet back out of that subnet.

122. D. VPC peering allows a VPC to connect with any other VPC: in the same region, in a different region, or in a different account altogether.

123. B, D. VPC peering allows a VPC to connect with any other VPC, so the options that don't involve VPCs are incorrect: B and D.

124. B, D. As long as there is a gateway (internet or virtual private) on the source VPC, and routing through that gateway, an instance in a VPC can communicate with other instances. So in this case, you'd want B and D. There is no "cross-VPC communication" option, and security groups won't actually help this scenario.

125. A, D. This is a little difficult, but it comes down to accessibility: How can the target instance be reached? Of the answers available, a public IP would make the target available, as would a VPN connection.

126. D. VPCs are fundamental to AWS networking and are available in all AWS regions.

127. D. A VPC automatically spans all the availability zones within the region in which it exists.

128. B. When you launch an instance, you must specify an availability zone. This could be as simple as accepting the AWS default, but it is your choice.

129. B. EBS volumes can be encrypted, but it must be done at launch time (B).

130. D. A VPC endpoint is a connection to an AWS service and explicitly does *not* use internet gateways, VPN connections, or NAT devices.

131. B. A VPC endpoint is a virtual device, not a physical one.

132. C. A VPC endpoint is for attaching to AWS services and explicitly does *not* require an internet gateway (C).

133. C. By default, IAM users don't have permissions to work with endpoints. You may need to create an IAM role. You would *not* need a NAT device (A or B) or a security group (D) to use a VPC endpoint.

134. B. A private subnet is not accessible without a bastion host or other connection and routing from the public Internet to an accessible host and finally into private instances.

135. B. Bastion hosts should be in a public subnet so that they can be accessed via the public Internet. They can then route traffic into a private subnet.

136. C. Bastion hosts are also sometimes called jump servers, because they allow a connection to "jump" to the bastion and then into a private subnet.

137. D. Bastion hosts are intended to provide access to private instances in private subnets; in other words, instances inaccessible via the public Internet in any other way.

138. D. Bastion hosts are publicly accessible and have access to your private hosts. Therefore, they must be the *most* secure hosts on your network. Use a network ACL for the subnet in which it resides, a security group for the instance, and OS hardening to reduce access within the instance itself.

139. B. Shell access only requires SSH, and you should therefore only allow that protocol. Always allow *only what is absolutely required* for bastion hosts.

140. D. Internet gateways scale horizontally, not vertically. They are also redundant and highly available automatically.

141. C. Internet gateways attach to VPCs and serve multiple subnets (if needed).

142. B. The route 0.0.0.0/0 catches all IPv4 traffic intended for the public Internet. ::/0 is for IPv6, 0.0.0.0/24 limits traffic to a certain CIDR block, and D is an internal IP address.

143. C. The route ::/0 catches all IPv6 traffic intended for the public Internet. 0.0.0.0/0 is for IPv6, 0.0.0.0/24 limits traffic to a certain CIDR block, and D is an internal IP address.

144. D. An instance must have IPv6 communication from itself (with a public IP address) through a subnet with IPv6 addresses, in a VPC with IPv6 addresses, to reach the Internet via IPv6. A virtual private gateway is not connected with any of these.

145. A, B. For an instance to reach and be reached to and from the public Internet, the instance must have either a public IP address or an elastic IP address associated with it. IAM roles do not provide public access, and NACLs are attached to subnets, not instances.

146. A, C. A public subnet, by definition, is a subnet with an internet gateway attached. And the default VPC has an internet gateway automatically attached.

147. B. ALB stands for application load balancer.

148. B. Application load balancers operate at the Application layer, which is layer 7 of the OSI model. ELBs (classic load balancers) operate at the Transport layer, layer 4, as well as layer 7, and network load balancers operate at layer 4 as well.

149. A. Application load balancers operate at the Application layer, which is layer 7 of the OSI model. ELBs (classic load balancers) operate at the Transport layer, layer 4, as well as layer 7, and network load balancers operate at layer 4 as well.

150. C. Application load balancers operate at the Application layer, which is layer 7 of the OSI model. ELBs (classic load balancers) operate at the Transport layer, layer 4, as well as layer 7, and network load balancers operate at Level 4 as well.

151. D. Both network and classic load balancers operate at the Transport layer. Classic load balancers also operate at layer 7, the Application layer. Application load balancers operate at the Application layer, which is layer 7 of the OSI model.

152. D. Both classic and application load balancers operate at the Application layer. Classic load balancers also operate at layer 4, the Transport layer. Network load balancers operate at the Transport layer, which is layer 4 of the OSI model.

153. C. By default, subnets in the default VPC are public. The default VPC has an internet gateway attached and the default subnets are public as a result.

154. A. By default, subnets in custom VPCs are private. Other than the default VPC, custom VPCs don't have internet gateways attached by default, and created subnets don't have public access.

155. C. Instances launched into non-default subnets have a private IPv4 address, but not a public one, so C is correct. All instances have a security group created or associated, and instances can always talk to other instances in the subnet by default.

156. C, D. Instances launched into non-default subnets have a private IPv4 address, but not a public one, so they need an elastic IP address, as answer C indicates. (A public IP address would work as well.) You'd also need an internet gateway for the instance (D).

157. D. Instances launched into default subnets in the default VPC can automatically reach out to the public Internet, as that VPC has an internet gateway and instances get a public IPv4 address.

158. A. A NAT device—network address translation—provides routing for instances to an internet gateway but can prevent undesired inbound traffic.

159. D. A NAT device provides access to the Internet from private instances—they allow outgoing traffic rather than incoming traffic.

160. B, C. AWS offers two NAT devices: a NAT instance and a NAT gateway.

161. A, D. Instances always require an AMI. In this question, the two instances are EC2 instances (A) and NAT instances (D).

162. B. A NAT gateway is an entirely managed device from AWS. All the other options require maintenance by the user of OS-level patches and updates.

163. B. A NAT instance does not provide automatic scaling, whereas DynamoDB and NAT gateways are managed services and do. There is really no such thing as "scaling" of an SNS topic, although SNS as a service does do some scaling in the background to ensure that demand is met.

164. A. Of these options, only bastion hosts and NAT instances are unmanaged services, making them the only two possible answers. A bastion host typically has SSH routing and permissions to private instances, making it the most important to properly secure. While a NAT instance is usually available to private instances, traffic flows out from the NAT instance and not into the private instances.

165. D. A NAT instance is a candidate for a bastion server. The other options are all managed services.

166. C, D. A site-to-site VPN connection requires a virtual private gateway on the VPC side (C) and a customer gateway on the on-site side (D).

167. A, C. A site-to-site connection is going to require a private subnet on the AWS side (C), with private instances within it. Further, you'll need a NAT instance (A) or similar device to route traffic and receive traffic as a static IP holder.

168. B. An egress-only gateway is for use with IPv6 traffic only.

169. C. An egress-only gateway is for use with IPv6 traffic and only allows outbound traffic. A VPC endpoint connects to managed AWS services, and an internet gateway (that isn't egress only) allows both inbound and outbound traffic. A NAT gateway is for allowing outbound traffic from a private subnet rather than a public subnet.

170. A, C. A NAT instance must be in a public subnet so that it is accessible from the Internet. It also must have access to private instances in private subnets in your VPC.

171. B, C. Egress-only internet gateways are stateful and support IPv6 traffic. This is a matter of memorization, although you can somewhat reason that the gateway—absent a NACL—allows responses to come back to instances that use it to communicate with the public Internet.

172. C. The most important thing here is to remember that egress-only internet gateways only work with IPv6 addresses. This eliminates A and B. Then, only C addresses the entire public Internet in an IPv6 format.

173. A, D. IPv6 addresses are public by default (D) *because* they are globally unique. There is no need to have private IPv6 addresses because the range is so large.

174. B, C. An elastic network interface is virtual and can have multiple IPv4 and IPv6 addresses as well as security groups, a MAC address, and a source/destination check flag.

175. D. An elastic network interface is virtual and can have multiple IPv4 and IPv6 addresses as well as security groups, a MAC address, and a source/destination check flag. NACLs apply to subnets, though, not network interfaces on instances.

176. C. An instance has a primary network interface in all cases but can have additional network interfaces attached, so the answer is C, one or more.

177. A. Traffic follows the network interface rather than sticking to any particular instance. So in this case, traffic is redirected to the new instance but stays targeted at the elastic network interface (A).

178. C. An elastic network interface can only be attached to a single instance at one time but can be moved from one instance to another.

179. B. You actually can't increase network throughput with multiple interfaces, making B false. All three other options are legitimate reasons to attach multiple interfaces to an instance.

180. C. An instance's primary network interface cannot be detached (C), making that the correct answer. You can detach secondary interfaces (A), attach multiple interfaces (B), and move network interfaces (D).

181. D. Elastic network interfaces do not have routing tables, but they do have (or can have) IPv4 and IPv6 addresses and a source/destination check flag.

182. C. Elastic IP addresses are specifically for avoiding being tied to a specific instance, so A and B are not correct. Security groups are typically not associated with a specific IP address (D). This leaves C, a valid reason for an elastic IP address: It can move from one instance (if the instance fails) to another.

183. A. Elastic IP addresses are, by definition, an IP address that will not change, so A is correct—you cannot change the IP address while it is in use. You can move elastic IPs (B), including across VPCs (C), and you absolutely would associate it with a single instance (D).

184. B, C. An elastic IP can mask the failure of an instance (B) by moving traffic to another running instance transparently. It also allows all the network interface attributes to be moved at one time (C).

185. A, D. To use an elastic IP, you must first allocate it for use in a VPC and then associate it with an instance in that VPC (A and D). Route 53 is not involved at this stage, and you cannot detach the primary network interface on an instance.

186. D. There is not such thing as an "EBS management tool" separate from the AWS API, CLI, and console.

187. C. Although instances exist in a region and VPC, and can be part of an Auto Scaling group, they are provisioned into specific availability zones (C).

188. A. EBS snapshots are backed up to S3 incrementally.

189. A. Changes to IAM roles take place immediately.

190. A. You can only assign a single role to an instance.

191. B, D. You can only assign a single role to an instance (D), but you can also create a new role that combines the desired policies (B).

192. A, D. You always need to make the actual role changes (A). There are then no more actions required for these changes to take effect on the instances.

193. B, D. You'll first need to create an IAM role with the desired permissions (B). Then, you can attach the role to a running instance to avoid downtime completely (D). Note that this is relatively new; older versions of AWS required restarting the instance.

194. A. If a snapshot is the root device of a registered AMI, it cannot be deleted.

195. A. Encryption can only be applied to EBS volumes at creation time, so A is correct.

196. B. By default, root volumes do get deleted when the associated instance terminates. However, you can configure this to not be the case using the AWS console or CLI (B).

197. C. Using defaults is not part of the well-architected framework, and it often is not the most secure approach.

198. A, C. The well-architected framework recommends automating security best practices and responses to security events.

199. A, B. AWS is responsible for securing the cloud itself, and then you as a customer are responsible for securing your resources and data in the cloud.

200. A, D. AWS is responsible for securing the cloud itself, which means anything that is infrastructure, such as edge locations and availability zones.

201. D. AWS is responsible for networks, but not the actual traffic across those networks (D).

202. A. AWS manages DynamoDB as a managed service. All the other options are your responsibility as a customer of AWS.

203. C. The well-architected framework includes four areas for security in the cloud: data protection, infrastructure protection, privilege management, and defective controls.

204. C. The well-architected framework suggests encrypting everything where possible, whether it is at rest or in transit.

205. A, B. The well-architected framework suggests encrypting everything where possible, whether the data is at rest or in transit.

206. C. While you are ultimately responsible for the security of your data, AWS provides and accepts responsibility for tools to enable security.

207. B. S3 durability is 99.999999999%, which is often called "11 9s" (or sometimes "11 nines") of durability.

208. C. AWS will never initiate the movement of data between regions. Content in a region must be moved by the customer or moved in response to a customer action.

209. D. S3 data can be protected via MFA Delete and versioning, both of which provide a layer of protection against accidental deletes. Additionally, IAM roles can ensure that only those who *should* be able to delete data *can* delete data.

210. A, C. All of these options are valid, but only two should be done for all environments: enabling MFA on the root account and setting a password rotation policy. Enabling MFA Delete on S3 is a good idea but may not apply to all situations. Further, not all users may need an IAM role; some, for example, are fine with the default roles.

211. C. AWS infrastructure operates at the VPC layer and is almost entirely virtual.

212. A, C. CloudWatch and CloudTrail both provide monitoring and logging, both of which can identify security breaches. CloudFormation is a deployment mechanism, and Trusted Advisor can identify potential holes, but not actual breaches.

213. C. IAM provides access management through users, roles, and permissions, all of which are related to privileges.

214. D. MFA is Multi-Factor Authentication, which adds a layer of protection related to privilege management.

215. A. Trusted Advisor is AWS's service for looking at your system and finding standard "holes" in your infrastructure that might allow for security breaches and then to suggest remediation.

216. C. AWS's well-architected framework provides for five pillars: operational excellence, security, reliability, performance efficiency, and cost optimization. Organizational issues are considered outside of this framework (C).

217. B. AWS's well-architected framework provides for five pillars: operational excellence, security, reliability, performance efficiency, and cost optimization. Usability is not a key concern of the cloud (B), although it is important for applications hosted within the cloud.

218. C. C is a misstatement of the correct principle; apply security at *all* layers. Security should be present at all layers, not just at the highest layers.

219. D. While A and C are both good ideas, they are more specific than the well-architected framework's principles. B is a part of a principle, but data should be protected at rest and in transit. This leaves D, and people should be kept away from direct access to data. Instead, tools and APIs should provide a layer between users and data.

220. A, D. The five areas are Identity and Access Management (A), detective controls, infrastructure protection, data protection, and incident response (D).

221. A. AWS takes responsibility for physically securing cloud infrastructure.

222. A, C. The root account is the first account in every account (A), but it should only be used for creating other users and groups (C). It is *not* intended for everyday tasks (B), and once account setup is complete, you are encouraged by AWS to delete any access keys (D).

223. C, D. A good password policy has minimum length and complexity requirements.

224. C. Users with console access are more privileged users and should be required to use MFA (C). Password policies apply to all users, so A is incorrect. Further, passwords are the mechanism for logging into the console, so B is wrong in that access keys are not used for console login.

225. A, B. SAML 2.0 and web identities both provide a means of working with an existing organizational identity provider.

226. C. The principle of least privilege suggests that users only be allowed to do what they have to in order to perform their job functions.

227. B. AWS Organizations groups accounts into organizational units (OUs), allowing for groupings of permissions and roles.

228. A. An SCP in AWS Organizations is a service control policy and can be applied to an organizational unit (OU) to affect all users within that OU. It effectively applies permissions at an organizational level, much the way that a group applies them at a user level.

229. C. Service control policies (SCPs) are applied to OUs (organizational units) in AWS Organizations.

230. A. Service control policies (SCPs) provide for working across AWS accounts (A). Organizational units (OUs) are groupings of accounts, and IAM roles are applied to users and groups, not cross-account structures.

231. C. AWS Organizations offers a means of organizing and managing policies that span AWS accounts.

232. D. AWS provides all of the above options as a means of providing security of the AWS environment.

233. B. SSE-S3 offers encryption at rest while deferring key management to AWS. SSE-KMS does the same but has a higher cost and is more suitable for stringent auditing. The other two options involve work on the client side, which the question states is undesirable.

234. C. SSE-KMS is the best solution for any encryption problem that requires a strong audit trail.

235. C. New users should be given a new IAM user, and when permissions are the same across users, a group should be used instead of individually assigning permissions.

236. B. Most of these answers are overly complicated. S3 is highly available by default, so simply setting up a bucket in an EU region is sufficient.

237. D. All S3 storage classes provide SSL for data at transit as well as encryption of data at rest.

238. D. All S3 storage classes provide SSL for data at transit as well as encryption of data at rest.

239. A. The shared responsibility model defines the portions of the cloud that AWS secures, and the portions that you, the AWS customer, must secure.

240. B. This is pretty tough unless you've read the AWS shared responsibility white papers and FAQs. It's really a matter of memorization and knowing that while AWS uses the term *managed services* in lots of areas, that term is *not* used in the shared responsibility model as one of the core types of services.

241. C. AWS is responsible for the security of virtualization infrastructure. All other items in this list are your responsibility. As a hint on questions like this and related to the AWS shared responsibility model, AWS is typically responsible for anything with the word *infrastructure*, although there are some exclusions (for example, *application infrastructure*).

242. A. An IAM role is assumed by an EC2 instance when it needs to access other AWS services, and that role has permissions associated with it. While these permissions are formally defined in a policy (B), it is the role that is used by the instance for actual service access.

243. A, D. Just as is the case with a compute instance (EC2), a task in a container needs an IAM role with permissions to access S3 (A), which in turn requires a policy specifying a permission that lets ECS tasks access S3 (D). Both of these are required to ensure access. Security groups apply to network traffic and would not affect S3 access, and while a VPC endpoint could be used (C), it is not required.

244. C. By default, newly created S3 buckets are private. They can only be accessed by a user that has been granted explicit access.

Domain 4: Design Cost-Optimized Architectures

1. A, B. When instance cost is the issue, the answers are almost always to consider some form of lowered instance pricing. AWS provides reserved instances and spot instances and the spot market for this purpose. Further, paying for reserved instances all up front is the most cost-effective means of getting reserved instances. Therefore, A and B are correct. C is problematic, as running a smaller instance for longer is not necessarily any cheaper than running a large instance for shorter amounts of time. Option D has some validity, but AWS is almost certainly going to point you back to either reserved instances or the spot market (A and B).

2. C, D. Reserved instances can be paid for in no up-front, partial up-front, and all up-front models, where all up-front is the least expensive and no up-front is the most expensive.

3. D. Reserved instances are locked to the region in which they are created, so D is correct. You would need to create a new reserved instance in the new region.

4. C. This should be an easy correct answer: Spot instances via the spot market are the potentially least expensive option, given that your compute has flexible timing and needs.