52. B. ECS is the Elastic Container Service, AWS's service for running applications in containers and managing the starting, stopping, and scaling of those containers.

53. C, D. Containers allow you to reduce startup times, as they are launched into already-running instances in most cases (C). This also touches on AWS's facility to manage and provision the instances on which the containers run (D), another advantage. While you can scale applications in containers (A), you can just as easily scale applications on EC2 instances. Finally, option B is simply false.

54. A. The first thing here is to know these various acronyms. ECR is the Elastic Container Registry, ECS is the Elastic Container Service, EC2 is Elastic Compute Cloud, EMR is Elastic MapReduce, and of course S3 is Simple Storage Service. Given that, only A has all the needed components: the registry (ECR), the management service (ECS), and instances on which to run containers (EC2). Note that even though you might not use EC2 explicitly for your containers, it or Fargate will be required to manage instances at some level, even if only by AWS for you.

55. C. You'll need to know these various acronyms. ECR is the Elastic Container Registry, ECS is the Elastic Container Service, EMR is Elastic MapReduce, and S3 is Simple Storage Service. ECC isn't an AWS acronym, so it is immediately out. Of those left, ECR, the Elastic Container Registry, is most closely associated with ECS.

56. B, C. Containers allow you to co-locate applications on instances and more effectively use your available instances without a lot of overhead, so B is true. C is in a similar vein: Containers reduce the management overhead of instances. A is not true, as containers don't significantly change your cost structure, and D is false, as containers and instances can both scale up and down to meet demand.

57. A, D. Containers are applications (D) that scale based on application load (A). Lambda, in contrast, runs isolated pieces of code and not entire application tiers. Additionally, Lambda launches based on events rather than load. (Note that you could actually set up load monitors in CloudWatch and trigger Lambda based on load, although that is not automatic as it is in containers.)

Practice Test

1. A, C. First, a larger instance with the fastest possible volume type—provisioned IOPS—is generally going to improve overall performance, so A is a good idea. Second, ElastiCache will provide faster responses and reduce database reads over time. A and C are both valid approaches. A Multi-AZ setup is for disaster recovery, and sharding is high overhead and could potentially increase response time, rather than reduce it, in this use case.

2. B. redis and memcached are engines available for use by ElastiCache. reddit is an online information site, and Redshift is a data warehousing and OLAP service.

3. B, C. AWS allows a number of options for encrypting data at rest. In the supplied solutions, AWS Key Management Service (KMS) is an AWS-managed solution for data encryption, and customer-provided keys are allowed as well. In the latter case, customers provide the keys and AWS handles encryption of data using those keys. ElastiCache for memcached does not support encryption and, further, is not a solution for encrypting data but instead a caching service. AWS Encryptic is not an actual AWS service.

4. A, D. AWS Organizations allows the management of multiple accounts in one place and allows tracking of those individual accounts (D). Additionally, in many cases, AWS will allow discounts based on total services used rather than treating each account individually (A).

5. B, C. The biggest issue here is that all the users are using the root account, meaning there's a shared password and that users have far more permissions than they should. These can both be addressed by creating new IAM users for each user (B) and putting those users in predefined groups according to their job function (C). Developers don't need access to IAM in general, so D is incorrect, and while changing the root password is a good idea, A is also incorrect because a financial manager (and possibly support engineers) may not need the AWS CLI as their access mechanism.

6. D. The best choice for I/O intensive applications and databases is provisioned IOPS (D). The only other potentially confusing option is B, throughput optimized HDD. These are not SSD volumes, and they are better for data warehousing rather than intensive I/O.

7. B, C. There are two potential problems here: network throughput and failed transmissions not being retried. Solution B addresses throughput by increasing the ability of the NAT instance to handle large amounts of data from multiple instances. Solution C addresses failed transmissions by treating them as a problem that should be retried by instances.

8. A, B. You cannot encrypt an existing EBS volume (A). Additionally, once a snapshot is encrypted, you cannot create an unencrypted copy of that snapshot (B). You can attach encrypted volumes to instances (C), and you can create an encrypted volume from an unencrypted snapshot (D).

9. C. First, realize that when you see a question asking about writing to S3, you want a URL that is not set up for static website hosting. This means that the bucket name follows the trailing slash and is not part of the domain itself. This means that B and C are the only valid options. Then, remember that the service (s3) and the region (in this case, eu-west-2) are *not* separated by a dot delimiter, but instead a dash. This leaves C as the correct answer.

10. C. CloudWatch is the AWS preferred solution for monitoring events. While data from flow logs could be handled by RDS and analyzed by Redshift, neither of these are as targeted a solution for monitoring as CloudWatch.

11. C. Lambda is best for writing custom code without the overhead of provisioning EC2 instances, so both A and C are potentially correct answers. While SQS does offer queuing of code, SWF (the Simple Workflow Service) offers you prebuilt tracking of application-level events and tasks. Attach Lambda to this and you have a ready-to-use event-driven service.

12. B, D. Non-default VPCs do not have an internet gateway attached, so B provides that remedy. Attaching an internet gateway to the VPC will provide public instances with a path out to the Internet. Solution D is also correct; NACLs on non-default VPCs will not allow HTTP or HTTPS traffic in (nor will security groups, for that matter) and need to explicitly allow in HTTP/S traffic.

13. D. Most of these answers will not help the problem. The NAT instance should be in a public subnet, so A is not useful. The EBS volume of the NAT can be an issue, but not in providing Internet access for connecting instances (B). The subnet containing the EC2 instances using the NAT instance should be private, so C is both incorrect and a bad design decision. This leaves D: NAT instances must have Source/Destination Check disabled to function properly.

14. D. All S3 storage classes share the same durability: 11 9s (99.999999999%). That's often unintuitive, so it's best to recall that all S3 classes have durability in common and decrease in availability from S3 to S3-IA to S3 One Zone-IA.

15. C. The keys here are that cost is a driver and that the image processing code is fast and inexpensive. That effectively means that if images were lost after processing, they could be reprocessed without affecting the overall system cost. As a result, it's possible to pick an S3 class where images post-processing might be lost, *if* that results in a lower overall cost. This allows for S3 One Zone-IA, the cheapest of the provided S3 classes aside from Glacier, which has load times much longer than would be acceptable. S3 One Zone-IA might lose your processed images, but since they can easily be re-created, this isn't a deterrent.

16. C. EFS, the Elastic File System, is effectively a NAS in the cloud and can provide storage accessible to multiple EC2 instances at one time.

17. C, D. Non-default VPCs do not have an internet gateway attached and will need one to host any public subnets, so C is required. Then, with the internet gateway attached, instances within the subnet will need a route through this gateway for Internet traffic (D).

18. A, B. AWS defines several custom request headers, and all begin with x-amz rather than x-aws. This will help you eliminate incorrect answers; in this case, it means that A is valid and C is not. Then, you'll simply have to memorize the other request headers; Content-Length (C) is valid, while Content-Size (D) is not.

19. A, C. There are four AWS support levels: basic, developer, business, and enterprise. Neither professional nor corporate is a valid support level.

20. B, D. RDS supports a number of database options: MariaDB, Aurora, PostgreSQL, MySQL, Oracle, and SQL Server. DynamoDB is not a relational database, and DB2 is not supported.

21. B. Scaling in is the process by which an Auto Scaling group removes instances. You can think of scaling in as "moving *in* the boundaries of the group" and scaling out as "moving *out* the boundaries of the group." Of the available choices, only B—5 instances—represents a reduction of instances.

22. B, D. CloudFormation templates can be written in JSON and YAML.

23. C. Only geolocation routing will ensure that the location of the user is the primary factor. While latency-based routing would seem to translate to location-based, it is conceivable that network traffic to a nearby region could cause latency to be lower for a user in (for example) Australia to be routed to US regions. Therefore, only geolocation routing would ensure that the closest region geographically is used by the major user bases.

24. C. A CNAME record allows you to direct traffic to a DNS name, and in this case, that DNS name would be the ELB. ELBs do not provide an IP address, so an A record would not work. An MX record is for email, and an AAAA record is for IPv6 addresses.

25. A, C. The key here is that you are not creating new users (and B is therefore incorrect); instead, you need to use an existing Active Directory setup. That requires an identity provider (A). Then, you can issue temporary tokens (C) to get users started, and they can update credentials from there.

26. D. This is a question with a relatively easy answer, but lots of red herring answers as well. When you have a specific recurring traffic period, scheduled scaling is an easy solution (D). All the other options are much more complex and may not work at all.

27. D. DynamoDB is a prototypical example of an AWS managed service. It handles its resources and does not provide controls for these to the user (answer D). In the case of proactivity, DynamoDB and AWS will handle scaling up. Additionally, DynamoDB already uses SSDs and multiple instances, without user intervention.

28. B. The default settings for CloudWatch specify a 5-minute interval at which metrics are collected.

29. B, C. The issue here is CPU, which you can essentially convert in your head to "too many things are being asked of the database at one time." The easiest way to reduce CPU on any database is to decrease requests and reads, and both an ElastiCache instance and read replicas do just that: reduce load on the primary database instance.

30. A. The Simple Workflow Service is ideal for tasks that need to execute based on steps within an application. Additionally, SWF has hooks built into applications that you get automatically without custom infrastructure code.

31. B. SQS queues in standard configuration are FIFO, but ordering is not guaranteed. If ordering must be preserved, the queue should be set as a FIFO (first-in, first-out) queue (B). With a LIFO queue (D), ordering is reversed and wouldn't meet the requirements of the question.

32. C. Route 53 has a number of valid routing policies: simple, failover, geolocation, geoproximity, latency-based, multivalue answer, and weighted. Of the provided answers, only load-balancing is not valid.

33. D. The only potentially useful answers here are B and D: you need more processing power to handle requests, and you need to deal with nonresponsive instances at peak times. The spot market will do nothing to help here, and pre-warming the load balancer will still not handle traffic when that traffic is sudden and produces a large spike. Of B and D, only D addresses nonresponsiveness. By having requests go to a queue, you should not have users experience a nonresponsive application at all; the SQS queue will scale as needed, and then instances can handle requests as they become available in the queue.

34. A, B. Processes suitable for the spot market must be able to run at any time (B) because the spot market makes instances available unpredictably, and the process must be able to stop and start and continue work (A) because spot instances can stop at any time.

35. D. All of the S3 storage classes offer 11 9s of durability (99.999999999%).

36. A, C. EBS uses block-level storage, while S3 uses object-based storage (A). Additionally, EBS volumes by default are deleted when the attached instance is stopped. While this can be changed, it does result in EBS volumes being ephemeral by default, as compared with S3, which does not disappear by default.

37. B. The key here is the requirement to manage costs. Option C is not cost-effective, as it requires expensive Oracle licenses. Option D is going to require larger instances, which will also incur new costs. Option A might be effective, but running a custom database installation will likely cost more than RDS and also incur significant overhead costs. Only option C provides an "in-place" cost option. Aurora typically outperforms MySQL in an apples-to-apples comparison, although there will be some overhead in migrating from MySQL to Aurora.

38. C, D. Both ELBs (elastic load balancers) and DynamoDB provide fault tolerance, and ELBs provide load balancing. Further, both services are automatically redundant without user intervention. Lightsail and AWS Organizations are services used for deployment and management of AWS rather than for providing redundancy and high availability.

39. A, D. EC2 instances are not automatically redundant; you would need to do additional work as the architect to ensure that applications on EC2 instances are redundant across AZs. While RDS as a service is fault tolerant, it is not automatically highly available. A Multi-AZ setup would address that need, for example. On the contrary, both S3 (B) and SQS (C) are automatically highly available across availability zones.

40. D. AWS does not allow vulnerability scans to be run without advance notice. There are some preapproved scans using AWS-approved tools, but in general, you'll need to contact your AWS account manager or support team in advance of running vulnerability scans.

41. A, D. Although cost is an important factor, the solutions here would remain the same even if it were not explicitly mentioned. First, an SQS queue is ideal for capturing what needs to be accomplished, independent of running queries. That queue will need to be accessible from EC2 instances that will run those queries. Additionally, spot instances are ideal for long-running queries that can be interrupted and restarted. Even better, the spot market also addresses the cost concerns mentioned in the question.

42. D. Spot instances terminate when the maximum set bid price is reached. Increasing the bid price will effectively raise the threshold for termination, causing them to run longer. This will cost more but, overall, keeps the application design intact.

43. B. A cached volume gateway stores your data in S3 while caching frequently accessed data. While a stored volume gateway would keep all data locally, it would not address the on-site storage costs mentioned in the question.

44. C. Network access control lists (NACLs) and security groups are the primary mechanisms within AWS that replace traditional firewalls.

45. A, C. By default, AWS creates a VPC with a public subnet, and that subnet by definition must have an internet gateway. NAT devices (instances and gateways) and virtual private gateways must explicitly be set up and are not created by AWS by default.

46. B. Auto Scaling groups scale in using a very specific set of criteria. Highest priority is the availability zone with the most instances, then the age of the launch configuration of instances, and finally, the nearness of instances to the next billing hour.

47. B. This is a tough question, and right on the edges of what might be asked on the exam. Hardware virtualization is fully virtualized (compared to "para" virtualization, partly virtualized) and therefore works with all instance types (making C false) and all hardware extensions (making B true). Since B is advantageous for hardware virtualization, it is the correct answer.

48. A. Provisioned IOPS is the fastest class of drive for high performance. It is built upon SSD (solid-state drives) and provides mission-critical low-latency workloads.

49. A. Changes to security groups take place immediately, regardless of whether the updates affect instances, ELBs, or any other AWS constructs.

50. C. A read replica would provide an additional database instance to service the queries (C). A Multi-AZ setup handles failover (B), and the secondary instance would not be in service normally. Adding memory would not address the CPU issue (A). The implicit assumption here is that the data requested and processed each night is new data, so an ElastiCache instance (D) would have little to cache and therefore affect little.

51. C. Only the bucket owner of an S3 bucket can completely delete a file once versioning has been enabled.

52. B. While in many cases SSE-S3 is perfectly adequate (C), the additional auditing and compliance requirements indicate that SSE-KMS is a better option (B). Anytime you see a need for audit trails, you should think KMS. This is a common exam question, so memorize the association between auditing and KMS and you'll probably get a free correct answer out of it!

53. B. Read replicas are updated asynchronously (B), and this is not configurable (so C is not an option). While network latency could be an issue (D), you still won't be able to avoid the occasional lag in updating due to asynchronous replication.

54. C. You can create 100 buckets in a single AWS account before you need to contact AWS support and ask for a limit increase.

55. B. There is no requirement to use an elastic IP in creating a public subnet. It is just as possible to create public IP addresses for instances in the subnet without using elastic IPs. However, you do need an internet gateway and routes to that gateway for Internet traffic.

56. C. The SSD volumes types, as well as optimized HDD and cold HDD, can all be as large as 16TiB.

57. A. Only A is false: You cannot attach multiple EC2 instances to a single EBS volume at one time.

58. D. This one should be pretty simple: RDS is a Relational Database Service and does not use key-value pairs.

59. A, B. The HDD options for EBS are generally less expensive than SSD options, so anytime lowering cost is a priority, HDD options are ideal; this makes A a valid answer. Data throughput for a throughput optimized HDD is actually greater than that of a general-purpose SSD (HDDs can go up to 500 MiB/s versus only 160 MiB/s on General Purpose SSDs), so B is another valid answer. Performance-critical workloads (answer C) are best served by provisioned IOPS SSDs, and the environment is not a factor in this case (answer D).

60. D. Of these options, only InnoDB is not supported by RDS.

61. A, C. AWS automatically creates a public subnet with new accounts. This public subnet will have instances that are public by default (A) via public IP addresses, but those IPs are *not* elastic IPs (so B is false). The instances will all access the Internet through an internet gateway (C), but the containing VPC will not have a virtual private gateway attached (so D is false).

62. A, D. Classic load balancers do support HTTP and HTTPS, but they do not support SSH or any flavor of FTP that does not use HTTP (or HTTPS) as an underlying protocol.

63. C. RRS, or reduced redundancy storage, is the predecessor to One Zone-IA but is less durable and currently deprecated. However, it can still show up on exams at odd times. Both its durability and availability are 99.99%. Another way to recall this is to note that all current S3 classes of storage have 11 9s durability, leaving only S3-RRS as a possibility here.

64. B, C. Delete protection is best accomplished through versioning and MFA Delete. Also note this is a rare time when the word *audit* does *not* pair with KMS as encryption is never discussed in the question.

65. B. If you know that you will use instances over a long period, reserved instances are always going to be cheaper than on-demand instances. Spot instances, however, will start and stop often and are not candidates for steady usage.