86. A. Lambda allows you to "ignore" the underlying resources required for running code. You simply give Lambda the code to run, and Lambda will handle provisioning resources in a scalable and cost-effective manner.

87. D. CloudWatch provides monitoring of applications and is a low-cost solution for AWS monitoring.

88. A. CloudTrail is the AWS service for logging and is particularly helpful for auditing and compliance.

89. C. Almost all of these add unnecessary steps and involve multiple instances or either Oracle or PostgreSQL. The easiest, most cost-effective option is to migrate directly from Oracle to PostgreSQL using DMS, the Database Migration Service.

90. A. S3 is the AWS choice for durability and flat-file (non-relational data) storage.

91. A. IAM is the best option for handling users, groups, and permissions within AWS.

92. A, B. IAM is the best option for handling users, groups, and permissions within AWS. You can then add Cognito to offer single sign-on capabilities to your applications.

93. B. Trusted Advisor is a great start to find glaring holes or deficiencies in an AWS environment.

94. C. OpsWorks is a configuration management tool that actually can use Chef, so many of the existing modules would plug right in and existing expertise would translate directly over.

Domain 5: Define Operationally Excellent Architectures

1. B. AWS does guarantee that all SQS messages will be delivered *at least* once, but the message *may be* delivered more than once (making option A incorrect). This is not related to the number of requests to the queue or the applications using the queue; therefore, both C and D are incorrect. This leaves B, the correct answer.

2. B, C. This is a common question AWS often asks to ensure that you understand that managed services like RDS and DynamoDB are indeed completely *managed*: You cannot access the underlying operating system of the service. This leaves EC2 and EMR as the remaining, and correct, answers. While EMR does provide you with a lot of functionality "out of the box," it still allows root level access, as do EC2 instances.

3. C. SQS queues have a visibility timeout that controls how long a message in the queue is marked as "invisible" while being processed. This accounts for the message "disappearing." Then, if application processing fails—as in option C—the message is remarked as visible and is available for processing again. Option A correctly notes this timeout, but reducing the timeout would not cause the message to be processed correctly. It would just reduce the time that the message is "invisible." Option B is not how queues work; they cannot ask a sender to resend a message. Option D is incorrect as well, as the queue is operating as intended with regard to visibility of messages and timeouts.

4. D. Snapshots are accessible through the console via username/password and through AWS CLI and APIs via application key.

5. B. SNS is the Simple Notification Service and functions like a mailer, sending out notifications that can be subscribed to by other applications.

6. A. SNS sends out notifications to subscribed listeners, and SWF pushes out messages as they arrive. Only SQS holds messages until the queue is polled. Redshift is not a messaging service at all but rather a data warehousing solution.

7. B. SNS and SWF operate on a push approach. SQS holds messages until they are pulled out of the queue. S3 is not a message store.

8. D. Both SWF and SQS deliver a message at least once, but only SWF guarantees that a message will *only* be delivered a single time.

9. B. Messages in SWF are tasks; messages in SQS are messages; messages in SNS are notifications. S3 is a storage solution, not a messaging solution.

10. C. Messages in SWF are tasks; messages in SQS are messages; messages in SNS are notifications. S3 is not a messaging solution at all.

11. D. Messages in SWF are tasks; messages in SQS are messages; messages in SNS are notifications. S3 is not a message store. Since SQS is not an option, the answer is D, none of these.

12. C. SWF is more than a simple queue. It automates workflow, moving a task (what SWF calls its messages) from one application component to the next in a predetermined order.

13. B. SWF is not exactly a true acronym. It stands for Simple Workflow Service but is not represented by SWS. Instead, the *WF* refers to *workflow*.

14. A, D. Both EC2 and ECS provide environments on which your custom code can run, and both are compute services. S3 is a storage service, and Redshift is a data warehousing solution. While Redshift can be helpful in analysis of data, it is not suitable for running custom scripts.

15. B. Of the choices available, Amazon Lightsail is the easiest solution for getting simple applications running quickly. EC2 and ECS are both much more complex. While S3 website hosting is a web hosting solution, it does require quite a bit of AWS knowledge (security, permissions, etc.).

16. B, D. An EBS snapshot cannot be deleted if it is the root device of a registered AMI while that AMI is in use. You'll need to deregister the AMI first (B), and then you can delete the EBS volume and any snapshots and stop using the AMI.

17. A. EBS is considered a subset of EC2 functionality. Therefore, you use the `aws ec2` commands; for example, `aws ec2 delete-snapshot`.

18. C. A records are used to point a specific domain or subdomain to an IP address. CNAMEs point to a different URL, which in turn can be resolved further by DNS. In this case, you'd want to create a CNAME record for `applestoapples.com` and point that record to `applestoapples.net` and then let DNS resolve that domain. Using an A record means you'd have to lock the record to a specific IP rather than the domain name for `applestoapples.net`. That's a problem, though, as over time, the domain may be served by different resources with different IP addresses, making the A record dated and incorrect.

19. A. A records are used to point a specific domain or subdomain to an IP address. CNAMEs point to URLs or other domain names. In this case, since you're pointing at an ELB, you'd need to use a CNAME, as ELBs don't expose a public IP address.

20. A. This is a little trickier in terms of picking the *best* answer. It is possible to set a CNAME up and point that at the ALB's URL (B). However, AWS prefers that you use an A record and configure it as an alias record, allowing you to direct traffic to the ALB. This is different than a standard A record, which can only point at an IP address. Option C is incorrect because ALBs don't expose an IP address, and D doesn't even make sense in this context.

21. A. AWS supports zone apex records for all domains. A zone apex record is a DNS record at the root, or apex, of a DNS zone. So `amazon.com` is an apex record (sometimes called a naked domain record). Route 53 absolutely will support zone apex records and allows alias records (of A type) at this level as well.

22. A, D. First, A is false. A zone apex record is a DNS record at the root, or apex, of a DNS zone. So `amazon.com` is an apex record (sometimes called a naked domain record). Route 53 absolutely will support zone apex records and allows alias records (of A type) at this level as well. D is also false; Route 53 supports zone apex records for AWS and non-AWS domains and services.

23. A, D. Route 53 is scalable by design, so there are no steps required to make it highly available; this makes D true. Additionally, it supports all AWS services, including auto-scaling, so A is true.

24. D. By default, a single account can manage 50 domains using Route 53. However, this is a default, and AWS will raise it pretty willingly if you call and explain your need for management of additional domains.

25. D. RDS is a managed system by AWS and does not allow any access to its underlying operating system.

26. C, D. VPC peering is a networking connection between two VPCs but is not limited to a single region (so A is false) and is neither VPN nor gateway-based (so B is false). This leaves C and D, both of which are true: VPCs can be used to share data and can peer across regions.

27. B. AWS calls a connection between two VPCs via peering across regions an inter-region VPC peering connection.

28. C. When a VPC peering connection is set up, each VPC will need a route manually added to allow communication to the peered VPC.

29. D. Most of these statements are false: VPCs in different regions (A) and in different accounts (B) can be peered, and if both VPCs are in the same account, they can share a security group (C). However, two peered VPCs *cannot* have overlapping CIDR blocks (D).

30. B. A VPC can have multiple subnets, so a VPC peering relationship is a one-to-one relationship between two VPCs (B).

31. C. While it is true that transitive peering relationships are not allowed (A), you can still peer VPCs B and C to allow traffic to flow between the two VPCs.

32. B, C. VPCs with overlapping CIDR blocks cannot be removed as is (B), and therefore the overlap must be removed (C). Changing either VPC to IPv6 *might* be a working solution (D) but is not a requirement.

33. A. Regardless of subnet, NACL, or any other networking consideration, you can only create one VPC connection between two VPCs at a time.

34. B. A VPC can be a part of an unlimited number of VPC connections, as long as those connections are all with different VPCs and you stay within AWS's overall account limits. Only one peering connection between two specific VPCs is possible; for example, only one connection can exist between VPC A and VPC B. But VPC A can have as many peering connections–each with a different VPC–as there are VPCs with which you can connect.

35. C. Transitive VPC relationships are not allowed in AWS. Most of these answers are complete gibberish!

36. B, D. First, AWS does not support IPv6 inter-region communication. This means that for IPv6 communication to work, the two VPCs must be in the same region (D). Then, you must ensure that both VPCs have IPv6 addresses and that routing is set up to use those addresses (B).

37. A, C. EC2-Classic was a flat network that offered very little in the way of multiple options. With VPCs, you can assign multiple IP addresses as well as multiple network interfaces (A and C).

38. A, D. Default VPCs come with both an internet gateway and public subnets. If you think through this, these two go hand in hand: A public subnet would need an internet gateway to function as public.

39. A, D. The default VPC has public subnets within it. Further, it provides a default routing table that provides access to and from these instances and the public Internet (A). Additionally, an internet gateway is added to the VPC by default (D).

40. C. Non-default subnets and their instances are not public by default. Therefore, they are assigned a private IPv4 address (C) rather than a public one.

41. B, C. Non-default subnets are private by default. Therefore, you need an internet gateway on the containing VPC (C) as well as giving the instance a public IP address (B). While a NAT instance *might* work (D), it would need to be in a different, public subnet rather than in the same subnet as the instance trying to reach the Internet.

42. D. SAML, the Security Assertion Markup Language, allows you to provide federated single sign-on access to the AWS management console.

43. C. Remember that AWS provides a principle of least privilege and always wants to limit access to only what a user (or service) needs. Therefore, new IAM users do not have any access to AWS services and must be granted access to any service explicitly.

44. B. IAM stands for Identity and Access Management.

45. A, C. IAM users logging into the AWS console will need a username, password, and the sign-in URL. If the user needs access to AWS APIs or the SDK, then they will need their access key ID and secret access key. Keep in mind that these credential pairs are *not* interchangeable.

46. A. Of these groups, only the Administrator group provides write access to all AWS services. The Power User group provides access to developer-related services, but not *all* services (like IAM). The Support User group is for creating and viewing support cases.

47. D. New users will need a customized sign-in link for accessing the console (D). They will then use this link to sign in using their username and password.

48. B. There are two key parts to this question: the mobile client that must have an endpoint to which it can send data and the receiver for a huge amount of data, as the question indicates millions of users. Mobile SDK is a bit of a giveaway for the mobile component. This also helpfully narrows the answer choices down to A and B. Of the two options, Kinesis and EC2, only Kinesis is built to handle a massive data stream. While you could theoretically scale up enough EC2 instances to serve an API for that volume of requests, it really makes no sense. Kinesis is built for incoming data streams, so is the better option.

49. B. A new AWS account requires the company email (or account owner email) for the root account holder, or a generic email for the company as a whole.

50. A, D. Both the Administrators and the Power Users default policies provide read and write access to most AWS services. Power Users limits access to IAM, but that would not affect access to S3 or EC2.

51. C. A policy is AWS's document type for describing a set of permissions.

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.