AWS® Certified Developer Official Study Guide
By Nick Alteen, Jennifer Fisher, Casey Gerena, Wes Gruver, Asim Jalis, Heiwad Osman, Marife Pagan, Santosh Patlolla and Michael Roth

Appendix

Answers to Review Questions

Chapter 1: Introduction to AWS Cloud API

1. B. The specific credentials include the access key ID and secret access key. If the access key is valid only for a short-term session, the credentials also include a session token.

   AWS uses the user name and passwords for working with the AWS Management Console, not for working with the APIs. Data encryption uses the customer master keys, not API access.

2. C. Most AWS API services are regional in scope. The service is running and replicating your data across multiple Availability Zones within an AWS Region. You choose a regional API endpoint either from your default configuration or by explicitly setting a location for your API client.

3. A. The AWS SDK relies on access keys, not passwords. The best practice is to use AWS Identity and Access Management (IAM) credentials and not the AWS account credentials. Comparing IAM users or IAM roles, only IAM users can have long-term security credentials.

4. C. Although you can generate IAM users for everyone, this introduces management overhead of a new set of long-term credentials. If you already have an external directory of your organization's users, use IAM roles and identity federation to provide short-term, session-based access to AWS.

5. A. The permissions for `DynamoDBFullAccess` managed policy grant access to *all* Amazon DynamoDB tables in your account. Write a custom policy to scope the access to a specific table. You can update the permissions of a user independently from the lifecycle of the table. DynamoDB does not have its own concept of users, but it uses the AWS API and relies on IAM.

6. B. You can view or manage your AWS resources with the console, AWS CLI, or AWS SDK. The core functionality of each SDK is powered by a common set of web services on the backend. Most AWS services are isolated by AWS Region.

7. B. If you look closely at the URL, the AWS Region string is incorrectly set as `us-east-1a`, which is specific to the Availability Zone. An AWS Region string ends in a number, and the correct configuration is `us-east-1`. If the error was related to API credentials, you would receive a more specific error related to credentials, such as `AccessDenied`.

8. B. This policy allows access to the `s3:ListBucket` operation on `example_bucket` as a specific bucket. This does not grant access to operations on the objects within the bucket. IAM is granular. The date in the `Version` attribute is a specific version of the IAM policy language and not an expiration.

9. D. The long-term credentials are not limited to a single AWS Region. IAM is a global service, and IAM user credentials are valid across different AWS Regions. However, when the API call is made, a signing key is derived from the long-term credentials, and that signing key is scoped to a region, service, and day.

10. B. The `AssumeRole` method of the AWS Security Token Service (AWS STS) returns the security credentials for the role that include the access key ID, secret access key, and session token. AWS Key Management Service (AWS KMS) is not used for API signing. The identity provider may provide a SAML assertion, but AWS STS generates the AWS API credentials.

11. D. The `DynamoDBReadOnlyAccess` policy is a built-in policy that applies to the resource `*` wildcard, which means that it applies to any and all DynamoDB tables accessible from the account regardless of when those tables were created. Because IAM policies are related to the IAM user, not the access key, rotating the key does not affect the policy. IAM policies are also global in scope, so you do not need a custom one per AWS Region. You can add IAM users to IAM groups but not IAM roles. Instead, roles must be assumed for short-term sessions.

12. B. The IAM trust policy defines the principals who can request role credentials from the AWS STS. Access policies define what API actions can be performed with the credentials from the role.

13. C. You can define an IAM user for your new team member and add the IAM user to an IAM group to inherit the appropriate permissions. The best practice is *not* to use *AWS account root user* credentials. Though you can use AWS Directory Service to track users, this answer is incomplete, and the AWS KMS is not related to permissions. Roles can be assumed only for short-term sessions—there are no long-term credentials directly associated with the role.

14. C. The AWS API backend is accessed through web service calls and is operating system– and programming language–agnostic. You do not need to do anything special to enable specific programming languages other than downloading the appropriate SDK.

15. B. The primary latency concern is for customers accessing the data, and there are no explicit dependencies on existing infrastructure in the United States. Physically locating the application resources closer to these users in Australia reduces the distance that the information must travel and therefore decreases the latency.

Chapter 2: Introduction to Compute and Networking

1. B. You launch Amazon Elastic Compute Cloud (Amazon EC2) instances into specific subnets that are tied to specific Availability Zones. You can look up the Availability Zone in which you have launched an Amazon EC2 instance. While an Availability Zone is part of a region, this answer is not the most specific. You do not get to choose the specific data center, and edge locations do not support EC2.

2. B. When you stop an Amazon EC2 instance, its public IP address is released. When you start it again, a new public IP address is assigned. If you require a public IP address to be persistently associated with the instance, allocate an Elastic IP address. SSH key pairs and security group rules do not have any built-in expiration, and SSH is enabled as a service by default. It is available even after restarts. Security groups do not expire.

3. A. A restricted rule that allows RDP from only certain IP addresses may block your request if you have a new IP address because of your location. Because you are trying to connect to the instance, verify that an appropriate inbound rule is set as opposed to an outbound rule. For many variants of Windows, RDP is the default connection mechanism, and it defaults to enabled even after a reboot.

4. A, D. The NAT gateway allows outbound requests to the external API to succeed while preventing inbound requests from the internet. Configuring the security group to allow only inbound requests from your web servers allows outbound requests to succeed because the default rule for the security group allows outbound requests to the APIs that your web service needs. Option B is incorrect because security group rules cannot explicitly deny traffic; they can only allow it. Option C is incorrect because network ACLs are stateless, and this rule would prevent all of the replies to your outbound web requests from entering the public subnet.

5. C. You are in full control over the software on your instance. The default user that was created when the instance launched has full control over the guest operating system and can install the necessary software. Instance profiles are unrelated to the software on the instance.

6. D. You can query the Amazon EC2 metadata service for this information. Networking within the Amazon Virtual Private Cloud (Amazon VPC) is based on private IP addresses, so this rules out options A and B. Because the metadata service is available, you are not required to use a third-party service, which eliminates option C.

7. A. You can implement user data to execute scripts or directives that install additional packages. Even though you can use Amazon Simple Storage Service (Amazon S3) to stage software installations, there is no special bucket. You have full control of EC2 instances, including the software. AWS KMS is unrelated to software installation.

8. A. Amazon EC2 instances are resizable. You can change the RAM available by changing the instance type. Option B is incorrect because you can change this attribute only when the instance is stopped. Although option C is one possible solution, it is not required. Option D is incorrect because the RAM available on the host server does not change the RAM allocation for your EC2 instance.

9. A. AWS generates the default password for the instance and encrypts it by using the public key from the Amazon EC2 key pair used to launch the instance. You do not select a password when you launch an instance. You can decrypt this with the private key. IAM users and IAM roles are not for providing access to the operating system on the Amazon EC2 instance.

10. A, B, E. For an instance to be directly accessible as a web server, you must assign a public IP address, place the instance in a public subnet, and ensure that the inbound security group rules allow HTTP/HTTPS. A public subnet is one in which there is a direct route to an internet gateway. Option C defines a private subnet. Because security groups are stateful, you are not required to set the outbound rules—the replies to the inbound request are automatically allowed.

11. A, D. You can use an AMI as a template for launching any number of Amazon EC2 instances. AMIs are available for various versions of Windows and Linux. Option B is false because AMIs are local to the region in which they were created unless they are explicitly copied. Option C is false because, in addition to AWS-provided AMIs, there are third-party AMIs in the marketplace, and you can create your own AMIs.

12. B, D. Option B is true; Amazon Elastic Block Store (Amazon EBS) provides persistent storage for all types of EC2 instances. Option D is true because hardware accelerators, such as GPU and FGPA, are accessible depending on the type of instance. Option A is false because instance store is provided only for a few Amazon EC2 instance types. Option C is incorrect because Amazon EC2 instances can be resized after they are launched, provided that they are stopped during the resize. Hardware accelerators, such as GPU and FGPA, are accessible depending on the type of instance.

13. B, D. Only instances in the running state can be started, stopped, or rebooted.

14. D. Both the web server and the database are running on the same instance, and they can communicate locally on the instance. Option A is incorrect because security groups apply to only network traffic that leaves the instance. Option C is incorrect because network ACLs apply only to traffic leaving a subnet. Similarly, option B is incorrect because the public IP address is required for inbound requests from the internet but is not necessary for requests local to the same instance.

15. C. A public subnet is one in which there is a route that directs internet traffic (0.0.0.0/0) to an internet gateway. None of the other routes provides a direct route to the internet, which is required to be a public subnet.

16. D. A private subnet that allows outbound internet access must provide an indirect route to the internet. This is provided by a route that directs internet traffic to a NAT gateway or NAT instance. Option C is incorrect because a route to an internet gateway would make this a public subnet with a direct connection to the internet. The remaining options do not provide access to the internet.

17. D. Amazon VPC Flow Logs have metadata about each traffic flow within your Amazon VPC and show whether the connection was accepted or rejected. The other responses do not provide a log of network traffic.

18. C. Amazon CloudWatch is the service that tracks metrics, including CPU utilization for an Amazon EC2 instance. The other services are not responsible for tracking metrics.

19. B. EBS volumes provide persistent storage for an Amazon EC2 instance. The data is persisted until the volume is deleted and therefore persists on the volume when the instance is stopped.

20. F. You can install any software you want on an Amazon EC2 instance, including any interpreters required to run your application code.

21. B, C. Web requests are typically made on port 80 for HTTP and port 443 for HTTPS. Because security groups are stateful, you must set only the inbound rule. Options A and D are unnecessary because the security group automatically allows the outbound replies to the inbound requests.

22. B, D. The customer is responsible for the guest operating system and above. Options C and E fall under AWS responsibility. AWS is responsible for the virtualization layer, underlying host machines, and all the way down to the physical security of the facilities.

Chapter 3: Hello, Storage

1. D. Amazon EC2 instance store is directly attached to the instance, which will give you the lowest latency between the disk and your application. Instance store is also provided at no additional cost on instance types that have it available, so this is the lowest-cost option. Additionally, since the data is being retrieved from somewhere else, it can be copied back to an instance as needed.

   Option A is incorrect because Amazon S3 cannot be directly mounted to an Amazon EC2 instance.

   Options B and C are incorrect because Amazon EBS and Amazon Elastic File System (Amazon EFS) would be a higher-cost option with higher latency than instance store.

2. D, E. Objects are stored in buckets and contain both data and metadata.

   Option A is incorrect because Amazon S3 is object storage, not block storage.

   Option B is incorrect because objects are identified by a URL generated from the bucket name, service region endpoint, and key name.

   Option C is incorrect because Amazon S3 object can range in size from a minimum of 0 bytes to a maximum of 5 TB.

3. B. The volume is created immediately, but the data is loaded lazily, meaning that the volume can be accessed upon creation, and if the data being requested has not yet been restored, it will be restored upon first request.

   Options A and C are incorrect because it does not matter what the size of the volume is or the amount of the data that is stored on the volume. Lazy loading will get data upon first request as needed while the volume is being restored.

   Option D is incorrect because an Amazon EBS-optimized instance provides additional, dedicated capacity for Amazon EBS I/O. This minimizes contention, but it does not increase or decrease the amount of time before the data is made available while restoring a volume.

4. A, B, D. Option C is incorrect because Amazon S3 is accessible through a URL. Amazon EFS is an AWS service that can be mounted to the file system of multiple Amazon EC2 instances. Amazon S3 can be accessible to multiple EC2 instances, but not through a file system mount.

   Option E is incorrect because, unlike Amazon EBS volumes, storage in a bucket does not need to be pre-allocated and can grow in a virtually unlimited manner.

5. A, C. Amazon Simple Storage Service Glacier is optimized for long-term archival storage and is not suited to data that needs immediate access or short-lived data that is erased within 90 days.

6. B. Option B is correct because pre-signed URLs allow you to grant time-limited permission to download objects from an Amazon S3 bucket.

   Option A is incorrect because static web hosting requires world-read access to all content.

   Option C is incorrect because AWS IAM policies do not know who are the authenticated users of your web application, as these are not IAM users.

   Option D is incorrect because logging can help track content loss, but not prevent it.

7. A, D. Option A is correct because the data is automatically replicated within an availability zone.

   Option D is correct because Amazon EBS volumes persist when the instance is stopped.

   Option B is incorrect. There are no tapes in the AWS infrastructure.

   Option C is incorrect because Amazon EBS volumes can be encrypted upon creation and used by an instance in the same manner as if they were not encrypted.

8. C. The Max I/O performance mode is optimized for applications where tens, hundreds, or thousands of EC2 instances are accessing the file system. It scales to higher levels of aggregate throughput and operations per second with a trade-off of slightly higher latencies for file operations.

   Option A is incorrect because the General-Purpose performance mode in Amazon EFS is appropriate for most file systems, and it is the mode selected by default when you create a file system. However, when you need concurrent access from 10 or more instances to the file system, you may need to increase your performance.

   Option B is incorrect. This is an option to increase I/O throughput for Amazon EBS volumes by connecting multiple volumes and setting up RAID 0 to increase overall I/O.

   Option D is incorrect. Changing to a larger instance size will increase your cost for compute, but it will not improve the performance for concurrently connecting to your Amazon EFS file system from multiple instances.

9. A, B, D. Options A, B, and D are required, and optionally you can also set a friendly CNAME to the bucket URL.

   Option C is incorrect because Amazon S3 does not support FTP transfers.

   Option E is incorrect because HTTP does not need to be enabled.

10. C. A short period of heavy traffic is exactly the use case for the bursting nature of general-purpose SSD volumes—the rest of the day is more than enough time to build up enough IOPS credits to handle the nightly task.

    Option A is incorrect because to set up a Provisioned IOPS SSD volume to handle the peak would mean overprovisioning and spending money for more IOPS than you need during off-peak time.

    Option B is incorrect because instance stores are not durable.

    Option D is incorrect because magnetic volumes cannot provide enough IOPS.

11. C, D, E. Option A is incorrect because you store data in Amazon S3 Glacier as an archive. You upload archives into vaults. Vaults are collections of archives that you use to organize your data. Amazon S3 stores data in objects that live in buckets.

Option B is incorrect because archives are identified by system-created archive IDs, not key names like in S3.

12. A. Amazon EFS supports one to thousands of Amazon EC2 instances connecting to a file system concurrently.

Options B and C are incorrect because Amazon EBS and Amazon EC2 instance store can be mounted only to a single instance at a time.

Option D is incorrect because Amazon S3 does not provide a file system connection, but rather connectivity over the web. It cannot be mounted to an instance directly.

13. B. There is no delay in processing when commencing a snapshot.

Options A and C are incorrect because the size of the volume or the amount of the data that is stored on the volume does not matter. The volume will be available immediately.

Option D is incorrect because an Amazon EBS-optimized instance provides additional, dedicated capacity for Amazon EBS I/O. This minimizes contention, but it does not change the fact that the volume will still be available while taking a snapshot.

14. B, C, E. Amazon S3 bucket policies can specify a request IP range, an AWS account, and a prefix for objects that can be accessed.

Options A and D are incorrect because bucket policies cannot be restricted by company name or country of origin.

15. B, D. Option B is incorrect because Amazon S3 cannot be mounted to an Amazon EC2 instance like a file system.

Option D is incorrect because Amazon S3 should not serve as primary database storage because it is object storage, not transactional block-based storage. Databases are generally stored on disk in one or more large files. If you needed to change one row in a database, the entire database file would need to be updated in Amazon S3, and every time you needed to access a record, you'd need to download the whole database.

16. B, C, E. Option A is incorrect because static web hosting does not restrict data access. You can host a website on Amazon S3, but the bucket must have public read access, so everyone in the world will have read access to this bucket.

Option B is correct because creating a presigned URL for an object optionally allows you to share objects with others.

Option C is correct because Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects, defining which AWS accounts or groups are granted access and the type of access.

Option D is incorrect because using an Amazon S3 lifecycle policy does not restrict data access. Lifecycle policies can be used to define actions for Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time).

Option E is correct because a bucket policy is a resource-based AWS IAM policy that allows you to grant permission to your Amazon S3 resources for other AWS accounts or IAM users.

17. C, E. Option A is incorrect because even though you get increased redundancy with using cross-region replication, that does not protect the object from being deleted.

Option B is incorrect because vault locks are a feature of Amazon S3 Glacier, not a feature of Amazon S3.

Option D is incorrect because a lifecycle policy would move the object to Amazon Glacier, moving it out of your intended storage in S3 and reducing the time to access the data, and it does not prevent it from being deleted once it arrives in Amazon S3 Glacier.

C and E are correct. Versioning protects data against inadvertent or intentional deletion by storing all versions of the object, and MFA Delete requires a one-time code from a multi-factor authentication (MFA) device to delete objects.

18. C. To track requests for access to your bucket, enable access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code (if any). Access log information can be useful in security and access audits. It can also help you learn about your customer base and understand your Amazon S3 bill.

19. A, B, D. Option A is correct because cross-region replication allows you to replicate data between distance AWS Regions to satisfy these requirements.

Option B is correct because this can minimize latency in accessing objects by maintaining object copies in AWS Regions that are geographically closer to your users.

Option D is correct because you can maintain object copies in both regions, allowing lower latency by bringing the data closer to the compute.

Option C is incorrect because cross-region replication does not protect against accidental deletion.

Option E is incorrect because Amazon S3 is designed for 11 nines of durability for objects in a single region. A second region does not significantly increase durability.

20. C. If data must be encrypted before being sent to Amazon S3, client-side encryption must be used.

Options A, B, and D are incorrect because they use server-side encryption. This will only encrypt the data at rest in Amazon S3, not prior to transit to Amazon S3.

21. B. Data is automatically replicated across at least three Availability Zones within a single region.

Option A is incorrect because you can optionally choose to replicate data to other regions, but that is not done by default.

Option C is incorrect because versioning is optional, and data in Amazon S3 is durable regardless of turning on versioning.

Option D is incorrect because there are no tapes in the AWS infrastructure.

Chapter 4: Hello, Databases

1. B, D, E. Amazon Relational Database Service (Amazon RDS) manages the work involved in setting up a relational database, from provisioning the infrastructure capacity to installing the database software. After your database is up and running, Amazon RDS automates common administrative tasks, such as performing backups and patching the software that powers your database. Option A is incorrect. Because Amazon RDS provides native database access, you interact with the relational database software as you normally would. This means that you're still responsible for managing the database settings that are specific to your application. Option C is incorrect. You need to build the relational schema that best fits your use case and are responsible for any performance tuning to optimize your database for your application's workflow and query patterns.

2. B. Amazon Neptune is a fast, reliable, fully managed graph database to store and manage highly connected datasets. Option A is incorrect because Amazon Aurora is a managed SQL database that is meant for transactional workloads that are ACID-compliant. Option C is incorrect because this is a managed NoSQL database service, which is meant for more key-value datasets with no relationships. Option D is incorrect because Amazon Redshift is a data warehouse that can be used for running analytical queries (OLAP) on data warehouses that are petabytes in scale.

3. B. NoSQL databases, such as Amazon DynamoDB, excel at scaling to hundreds of thousands of requests with key-value access to user profile and session. Option A is incorrect because the session state is typically suited for small amounts of data, and DynamoDB can scale more effectively with this type of dataset. Option C is incorrect because Amazon Redshift is a data warehouse service that is used for analytical queries on petabyte scale datasets, so it would not be a good solution. Option D is incorrect because DynamoDB provides scale, whereas MySQL on Amazon EC2 eventually becomes bottlenecked. Additionally, NoSQL databases are much faster and more scalable for this type of dataset.

4. A. 1 RCU = One strongly consistent read per second of 4 KB.

   15 KB is four complete chunks of 4 KB (4 × 4 = 16).

   So you need 25 × 4 = 100 RCUs.

5. C. 1 RCU = Two eventually consistent reads per second of 4 KB.

   15 KB is four complete chunks of 4 KB (4 × 4 = 16).

   So you need (25 × 4) / 2 = 50 RCUs.

6. D. 1 WCU = 1 write per second of 1 KB (1024 bytes).

   512 bytes uses one complete chunk of 1 KB (512/1024 = 0.5, rounded up to 1).

   So you need 100 × 1 = 100 WCUs.

7. B. Amazon DynamoDB Accelerator (DAX) is a write-through caching service that quickly integrates with DynamoDB with a few quick code changes. DAX will seamlessly intercept the API call, and your caching solution will be up and running in a short amount of

time. Option A is incorrect because you could implement your own solution; however, this would likely take a significant amount of development time. Option C is incorrect because your company would like to get the service up and running quickly. Implementing Redis on Amazon EC2 to meet your application's needs would take additional time. Option D is incorrect for many of the same reasons as option C, as time is a factor here. Additionally, your company would like to refrain from managing more EC2 instances, if possible.

8. B. With Amazon ElastiCache, only Redis can be run in a high-availability configuration. Option A is incorrect because this would add complexity to your architecture. It would also likely introduce additional latency, as the company is already using Amazon RDS. Option C is incorrect because ElastiCache for Memcached does not support a high-availability configuration. Option D is incorrect because DAX is a caching mechanism that is used for DynamoDB, not Amazon RDS.

9. C. Amazon Redshift is the best option. It is a managed AWS data warehouse service that allows you to scale up to petabytes worth of data, which would definitely meet their needs. Option A is incorrect because Amazon RDS cannot store that much data; the limit of Amazon RDS for Aurora is 64 TB. Option B is incorrect because DynamoDB is not meant for analytical-type queries—it is meant for simple queries and key-value pair data, which is more transactional based. You can query based on only the partition and sort key in DynamoDB. Option D is incorrect because Amazon ElastiCache is a caching solution that is meant for temporary data. However, you could store queries that ran in Amazon Redshift inside ElastiCache. This would improve the performance of frequently run queries, but by itself is not a solution.

10. A. Scans are less efficient than queries. When possible, always use queries with DynamoDB. Option B is incorrect because doing nothing isn't a good solution; the problem is unlikely to go away. Option C is incorrect because a strongly consistent read would actually be a more expensive query in terms of compute and cost. Strongly consistent reads cost twice as much as eventually consistent reads. Option D is incorrect because the concern is with reading data, not writing data. WCUs are write capacity units.

Chapter 5: Encryption on AWS

1. B, D, E. Option A is incorrect because data can be encrypted in any location (on-premises or in the AWS Cloud). Option C is incorrect because encryption keys should be stored in a secured hardware security module (HSM). Option B is correct because there must be data to encrypt in order to use an encryption system. Option D is correct because tools and a process must be in place to perform encryption. Option E is correct because encryption requires a defined algorithm.

2. A, C. Option B is incorrect because KMI does not have a concept of a data layer. Option D is incorrect because KMI does not have a concept of an encryption layer. Option A is correct because the storage layer is responsible for storing encryption keys. Option C is correct because the management layer is responsible for allowing authorized users to access the stored keys.

3. A, C, D. Option A is correct because this is a common method to offload the responsibility of key storage while maintaining customer-owned management processes. Option C is correct because customers can use this approach to fully manage their keys and KMI. Option D is correct because AWS Key Management Service (AWS KMS) supports both encryption and KMI. Option B is incorrect because this would imply significant overhead to manage the storage while not providing customer benefits.

4. D. Option A is incorrect; with SSE-S3, Amazon S3 is responsible for encrypting the objects, not AWS KMS. Option B is incorrect because the customer provides the key to the Amazon S3 service. Option C is incorrect because the question specifically states that server-side encryption is used. Option D is correct because none of the other options listed server-side encryption with AWS KMS (SSE-KMS), whereby AWS KMS manages the keys.

5. B. Option A is incorrect. AWS KMS does not currently support asymmetric encryption. Option B is correct because AWS CloudHSM supports both asymmetric and symmetric encryption. Options C and D are incorrect because CloudHSM supports asymmetric encryption.

6. A, B. Option A is correct because AWS KMS uses AES-256 as its encryption algorithm. Option B is correct because CloudHSM supports a variety of symmetric encryption options. Options C and D are incorrect because AWS KMS and CloudHSM support symmetric encryption options.

7. C. Option A is incorrect because the organization does *not* want to manage any of the encryption keys. With AWS KMS, it will have to create customer master keys (CMKs). Option B is incorrect because by using customer-provided keys, the organization would have to manage the keys. Option C is correct because Amazon S3 manages the encryption keys and performs rotations periodically. Option D is incorrect because SSE-S3 provides this option.

8. C. Option A is incorrect because AWS KMS provides a centralized key management dashboard; however, this feature does not leverage CloudHSM. Option B is incorrect because you want to use AWS KMS *with* CloudHSM and not use it as a replacement for AWS KMS. Option C is correct because custom key stores allow AWS KMS to store keys in an CloudHSM cluster. Option D is incorrect because S3DistCp is a feature for Amazon Redshift whereby it copies data from Amazon S3 to the cluster.

9. A. Option A is correct because AWS KMS provides the simplest solution with little development time to implement encryption on an Amazon EBS volume. Option B is incorrect because even though you can use open source or third-party tooling to encrypt volumes, there would be some setup and configuration involved. Using CloudHSM would also require some configuration and setup, so option C is incorrect. Option D is incorrect because AWS KMS enables you to encrypt Amazon EBS volumes.

10. D. Options A, B, and C are incorrect because AWS KMS integrates with all these services.

Chapter 6: Deployment Strategies

1. D. Option D is correct because AWS CodePipeline is a continuous delivery service for fast and reliable application updates. It allows the developer to model and visualize the software release process. CodePipeline automates your build, test, and release process when there is a code change.

   Option A is incorrect because AWS CodeCommit is a secure, highly scalable, managed source control service that hosts private Git repositories.

   Option B is incorrect because AWS CodeDeploy automates code deployments to any instance and handles the complexity of updating your applications.

   Option C is incorrect because AWS CodeBuild compiles source code, runs tests, and produces ready-to-deploy software packages.

2. A, B, C, D. A, B, C, and D are correct because you can use them all to create a web server environment with AWS Elastic Beanstalk.

   Option E is incorrect because AWS Lambda is an event-driven, serverless computing platform that runs code in response to events. Lambda automatically manages the computing resources required by that code.

3. C. Elastic Beanstalk supports Java, Node.js, and Go, so options A, B, and D are incorrect. It does not support Objective C, so option C is the correct answer.

4. A. Elastic Beanstalk deploys application code and the architecture to support an environment for the application to run.

5. A, C. Elastic Beanstalk supports Linux and Windows. No support is available for an Ubuntu-only operating system, Fedora, or Jetty.

6. A, B. Elastic Beanstalk can run Amazon EC2 instances and build queues with Amazon SQS.

7. A, B. Elastic Beanstalk can access Amazon S3 buckets and connect to Amazon RDS databases. It cannot install Amazon GuardDuty agents or create or manage Amazon WorkSpaces.

8. C. By using IAM policies, you can control access to resources attached to users, groups, and roles.

9. B, C. Elastic Beanstalk creates a service role to access AWS services and an instance role to access instances.

10. C. Elastic Beanstalk runs at no additional charge. You incur charges only for services deployed.

11. D. Charges are incurred for all accounts that use the allocated resources.

12. C. An existing Amazon RDS instance is deleted if the environment is deleted. There is no auto-retention of the database instance. You must create a snapshot to retain the data and to restore the database.

Chapter 7: Deployment as Code

1. A. Options B and D are incorrect because the deployment is already in progress, and this would not be possible if the AWS CodeDeploy agent had not been installed and running properly. The CodeDeploy agent sends progress reports to the CodeDeploy service. The service does not attempt to query instances directly, and the Amazon EC2 API does not interact with instances at the operating system level. Thus, option C is incorrect, and option A is correct.

2. B. Option B is correct because the `ApplicationStop` lifecycle event occurs before any new deployment files download. For this reason, it will not run the first time a deployment occurs on an instance. Option C is incorrect, as this is a valid lifecycle event. Option A is incorrect. Option D is incorrect because lifecycle hooks are not aware of the current state of your application. Lifecycle hook scripts execute any listed commands.

3. A. Option B requires precise timing that would be overly burdensome to add to a CI/CD workflow. Option C would not include edge cases where both sources are updated within a small time period and would require separate release cadences for both sources. Option D is incorrect, as AWS CodePipeline supports multiple sources. When multiple sources are configured for the same pipeline, the pipeline will be triggered when any source is updated.

4. C. Option A is incorrect because storing large binary objects in a Git-based repository can incur massive storage requirements. Any time a binary object is modified in a repository, a new copy is saved. Comparing cost to Amazon S3 storage, it is more expensive to take this approach. By building the binary objects into an Amazon Machine Image (AMI), you are required to create a new AMI any time changes are made to the objects; thus, option B is incorrect. Option D and E introduce unnecessary cost and complexity into the solution. By using both an AWS CodeCommit repository and Amazon S3 archive, the lowest cost and easiest management is achieved.

5. D. Option A is incorrect because rolling deployments without an additional batch would result in less than 100 percent availability, as one batch of the original set of instances would be taken out of circulation during the deployment process. Option B is incorrect because if you add an additional batch, it would ensure 100 percent availability at the lowest cost but would require a longer update process than replacing all instances at once. Option C is incorrect because, by default, blue/green deployments will leave the original environment intact, accruing charges until it is manually deleted. Option D is correct as immutable updates would result in the fastest deployment for the lowest cost. In an immutable update, a new Auto Scaling group is created and registered with the load balancer. Once health checks pass, the existing Auto Scaling group is terminated.

6. D. Option C is incorrect because Amazon S3 does not have a concept of service roles. When a pipeline is initiated, it is done in response either to a change in a source or when a previous change is released by an authorized AWS IAM user or role. However, after the pipeline has been initiated, the AWS CodePipeline service role is used to perform pipeline actions. Thus, options A and B are incorrect. Option D is correct, because the pipeline's service role requires permissions to download objects from Amazon S3.

7. B. Option A is incorrect because this output is used only in the CodeBuild console. Option D is incorrect because CodeBuild natively supports this functionality. Though option C would technically work, CodeBuild supports output artifacts in the `buildspec.yml` specification. The BuildSpec includes a `files` directive to indicate any files from the build environment that will be passed as output artifacts. Thus, option B is correct.

8. C. Option A is incorrect because a custom build environment would expose the secrets to any user able to create new build jobs using the same environment. Option B is also incorrect. Though uploading the secrets to Amazon S3 would provide some protection, administrators with Amazon S3 access may still be able to view the secrets. Option D is incorrect because AWS does not recommend storing sensitive information in source control repositories, as it is easily viewed by anyone with access to the repository. Option D is correct. By encrypting the secrets with AWS KMS and storing them in AWS Systems Manager Parameter Store, you ensure that the keys are protected both at rest and in transit. Only AWS IAM users or roles with permissions to both the key and parameter store would have access to the secrets.

9. A. Options B, C, D, and E are incorrect. AWS Lambda functions can execute as part of a pipeline only with the Invoke action type.

10. A, B. Options D and E are incorrect because FIFO/LIFO are not valid pipeline action configurations. Option C is incorrect because pipeline stages support multiple actions. Pipeline actions can be specified to occur both in series and in parallel within the same stage. Thus, options A and B are correct.

11. D. Option A is incorrect because it will only create or update a stack, not delete the existing stack. Option B is incorrect because the desired actions are in the wrong order. Option C is incorrect because the final action, "Replace a failed stack," is not needed. Option D is correct. Only two actions are required. First, the stack must be deleted. Second, the replacement stack can be created. Unless otherwise required, however, both actions can be essentially accomplished by using one "Create or update a stack" action.

12. D. Option A is incorrect. AWS CodeCommit is fully compatible with existing Git tools, and it also supports authentication with AWS Identity and Access Management (IAM) credentials. Options B and C are incorrect. These are the only protocols over which you can interact with a repository. You can use the CodeCommit credential helper to convert an IAM access key and secret access key to valid Git credentials for SSH and HTTPS authentication. Thus, option D is correct.

13. C. Options A, B, and D are all valid Amazon Simple Notification Service (Amazon SNS) notification event sources for CodeCommit repositories. Option C is correct because Amazon SNS notifications cannot be configured to send when a commit is made to a repository.

14. C, E. Options A, B, and D are incorrect because these action types do not support CodeBuild projects. Options C and E are correct because CodeBuild projects can be executed in a pipeline as part of build and test actions.

15. D. Environment variables in CodeBuild projects are not encrypted and are visible using the CodeBuild API. Thus, options A, B, and C are incorrect. If you need to pass sensitive information to build containers, use Systems Manager Parameter Store instead. Thus, option D is correct.

16. A. Because AWS does not have the ability to create or destroy infrastructure in customer data centers, options B, C, and D are incorrect. Option A is correct because on-premises instances support only in-place deployments.

17. C. Options A and B are incorrect because AWS CodeDeploy will not modify files on an instance that were not created by a deployment. Option D is incorrect because this approach could result in failed deployments because of missing settings in your configuration file. Option C is correct. By default, CodeDeploy will not remove files that it does not manage. This is maintained as a list of files on the instance.

18. C. Option A is incorrect because function versions cannot be modified after they have been published. Option B is also incorrect because function version numbers cannot be changed. Aliases can be used to point to different function versions; however, the alias itself cannot be overwritten (it is a pointer to a function version). Thus, option D is incorrect. AWS Lambda does not support in-place deployments. This is because, after a function version has been published, it cannot be updated. Option C is correct.

19. C. AWS CodePipeline requires that every pipeline contain a source stage and at least one build or deploy stage. Thus, the minimum number of stages is 2.

20. C. Option A is not correct because deleting the old revisions will temporarily resolve the issue. However, future deployments will continue to consume disk space. The same reasoning applies to options B and D, which are also temporary solutions to the problem. The CodeDeploy agent configuration file includes a number of useful settings. Among these, a limit can be set on how many revisions to store on an instance at any point in time. Thus, option C is correct.

Chapter 8: Infrastructure as Code

1. D. Only the `Resources` section of a template is required. If this section is omitted, AWS CloudFormation has no resources to manage. However, a template does not require `Parameters`, `Metadata`, or `AWSTemplateFormatVersion`. Thus, options A, B, C, and E are incorrect.

2. E. The return value of the `Ref` intrinsic function for an `AWS::ElasticLoadBalancing::LoadBalancer` resource is the load balancer name, which is not valid in a URL, so option A is incorrect. Since the application server instances are in a private subnet, neither will have a public DNS name; thus, option B is incorrect. Option C uses incorrect syntax for the `Ref` intrinsic function. Option D attempts to output a URL for the database instance. Thus, option E is correct.

3. A, C, D. If account limits were preventing the launch of additional instances, the stack creation process would fail as soon as AWS CloudFormation attempts to launch the instance (the Amazon EC2 API would return an error to AWS CloudFormation in this case). Thus, option B is incorrect. Any issues preventing the instance from calling `cfn-signal` and sending a success/failure message to AWS CloudFormation would cause the creation policy to time out. Thus, options A, C, and D are correct answers.

4. C. Option A is incorrect because AWS CloudFormation does not monitor the status of your database and would not be able to determine whether the database is corrupted. It also does not track whether there are currently running transactions before attempting updates. Thus, option E is incorrect. If an invalid update is submitted, the stack generates an error message when attempting the database update. Thus, option D is incorrect. Though option B would work, it is not needed to remove the database from the stack and manage it separately. Option C is correct because an AWS CloudFormation service role extends the default timeout value for stack actions to allow you to manage resources with longer update periods.

5. A. Custom resource function permissions are obtained by a function execution role, not the service role invoking the stack update; thus, option B is incorrect. When the AWS Lambda function corresponding to a custom resource no longer exists, the custom resource will fail to update immediately; thus, option C is incorrect. However, if the custom resource function is executed but does not provide a response to the AWS CloudFormation service endpoint, the resource times out with the aforementioned error. Thus, option A is correct.

6. A. AWS CloudFormation processes transformations by creating a change set, which generates an AWS CloudFormation supported template. Without the `AWS::Serverless` transform, AWS CloudFormation cannot process the AWS SAM template. For any stack in your account, the current template can be downloaded using the `get-stack-template` AWS CLI command. This command will return templates as processed by AWS CloudFormation; thus, option B is incorrect. Option C is also incorrect, because the original template is not saved before executing the transform. Option D is also incorrect, as AWS CloudFormation saves the current template for all stacks.

7. E. AWS SAM supports other AWS CloudFormation resources, and it is not limited to defining only `AWS::Serverless::*` resource types; thus, option D is incorrect, and option A is correct. However, the `AWS::Serverless` transform will not automatically associate serverless functions with `AWS::ApiGateway::RestApi` resources. The transform will automatically associate any functions with the serverless API being declared, or it will create a new one when the transform is executed. Thus, option B is also correct. Option C is also correct because AWS Serverless also supports Swagger definitions to outline the endpoints of your OpenAPI specification.

8. A. The `cfn-init` helper script is used to define which packages, files, and other configurations will be performed when an instance is first launched. The `cfn-signal` helper script is used to signal back to AWS CloudFormation when a resource creation or update has completed, so options B and C are incorrect. Option D is incorrect because `cfn-update`, is not a valid helper script. The `cfn-hup` helper script performs updates on an instance when its parent stack is updated. Thus, option A is correct.

9. C. Wait conditions accept only one signal and will not track additional signals from the same resource; thus, options A and B are incorrect. `WaitCount` is an invalid option type, so option D is incorrect. Option C is correct because creation policies enable you to specify a count and timeout.

10. A. Options B and C will affect resources in your account. Option D would let you see the syntax differences between two template versions, but this does not indicate what type of updates will happen on the resources themselves. Thus, option D is incorrect. Change sets create previews of infrastructure changes without actually executing them. After reviewing the changes that will be performed, the change set can be executed on the target stack.

11. B. Option A is incorrect, as this is a supported feature of nested stacks. Option C creates a circular dependency between the parent and child stacks (the parent stack needs to import the value from the child stack, which cannot be created until the parent begins creation). Option D is incorrect because cross-stack references are not possible without exporting and importing outputs. Option B uses intrinsic functions to access resource properties in the same manner as any other stack resource.

12. B. AWS CloudFormation does not assume full administrative control on your account, and it requires permissions to interact with resources you own. AWS CloudFormation can operate using a service role; however, this must be explicitly passed as part of the stack operation. Otherwise, it will execute with the same permissions as the user performing the stack operation. Thus, option B is the correct answer.

13. C. Because the reference to the Amazon DynamoDB table is made as part of an arbitrary string (the function code), AWS CloudFormation does not recognize this as a dependency between resources. To prevent any potential errors, you would need to declare explicitly that the function depends on the table. Thus, option C is correct.

14. E. Replacing updates results in the deletion of the original resource and the creation of a replacement. AWS CloudFormation creates the replacement first with a new physical ID and verifies it before deleting the original. Because of this, option E is correct (all of the above).

15. B, C. Option A is incorrect, as it states that no interruption will occur. Options D and E are not valid update types. Replacing updates delete the original resource and provision a replacement. Updates with some interruption have resource downtime, but the original resource is not replaced. Thus, options B and C are correct.

16. A. The export does not need to be removed from the stack before it can be deleted, so option B is incorrect. Options C and D are also incorrect, as the stack does not need to be deleted. However, the stack cannot be deleted until any other stacks that import the value remove the import. Thus, option A is correct.

17. B, D, E. If a stack update fails for any reason, the next state would be `UPDATE_ROLLBACK_IN_PROGRESS`, which must occur before the rollback fails or completes. A stack that is currently updating can either complete the update, fail to update, or complete and clean up old resources. Thus, options B, D, and E are correct.

18. B. Because the stack status shows the update has completed, you know that the update did not fail. This means that options A and D are incorrect. When a stack updates and resources are created, they will not be deleted unless the update fails. Thus, option C is incorrect. Old resources that are no longer required are removed during the cleanup phase. Thus, option B is correct.

19. A, C. AWS CloudFormation currently supports JSON and YAML template formats only.

20. E. AWS CloudFormation provides a number of benefits over procedural scripting. The risk of human error is reduced because templates are validated by AWS CloudFormation before deployment. Infrastructure is repeatable and versionable using the same process as application code development. Individual users provisioning infrastructure need a reduced scope of permissions when using AWS CloudFormation service roles. Thus, option E is correct.

21. B. Option C is incorrect because, though on-premises servers can be part of a custom resource's workflow, they do not receive requests directly. Options D and E are incorrect because specific actions are not declared in custom resource properties. Option A is incorrect because AWS services themselves do not process custom resource requests. Specifically, Amazon SNS topics and AWS Lambda functions can act as recipients to custom resource requests. Thus, option B is correct.

22. C. Options A and B are incorrect because they would require interacting with other AWS services using the AWS CLI. For certain situations, such as running arbitrary commands in Amazon EC2 instance user data scripts, this would work. However, not all resource types have this ability. Option D is incorrect, as this is a built-in functionality of AWS CloudFormation. Option C is correct because any data that is declared in a custom resource response is accessible to the remainder of the template using the `Fn::GetAtt` intrinsic function.

Chapter 9: Configuration as Code

1. E. You can raise all of the limits listed by submitting a limit increase request to AWS Support.

2. D. Option A is incorrect because instances do not attempt to download new cookbooks when performing Chef runs. Option B is incorrect because AWS OpsWorks Stacks does not have a concept of cookbook caching. Option C is incorrect because lifecycle events do not allow you to specify cookbook versions. Option D is correct because after updating a custom cookbook repository, any currently online instances will not automatically receive the updated cookbooks. To upload the modified cookbooks to the instances, you must first run the `Update Custom Cookbooks` command.

3. B. Options A, C, and D are incorrect because OpsWorks Stacks provides integration with Elastic Load Balancing to handle automatic registration and deregistration. Option B is correct as the Elastic Load Balancing layers for OpsWorks Stacks automatically register instances when they come online and deregister them when they move to a different state. You can also enable connection draining to prevent deregistration until any active sessions end.

4. A, B. Option C is incorrect because changing the cluster capacity will not affect service scaling. Option D is incorrect because submitting a replacement will result in the same behavior. If there are insufficient resources to launch replacement tasks when a service updates, Amazon Elastic Container Service (Amazon ECS) will continue to attempt to launch the tasks until it is able to do so. If you increase the cluster size, additional resources add to the pool to allow the new task to start. After it has done so, the old task will terminate. After it terminates, the cluster can scale back to its original size. If the downtime of this service does not concern you, set the minimum in-service percentage to 0 percent to allow Amazon ECS to terminate the currently running task before it launches the new one. Thus, options A and B are correct.

5. B. Options A, C, and D are incorrect because no other parties have access to the underlying clusters in AWS Fargate. When you use the Fargate launch type, AWS provisions and manages underlying cluster instances for your containers. You do not need to manage maintenance and patching. Thus, option B is correct.

6. A. Option B is incorrect, as this is a matter of personal preference. Option C is also incorrect because instances can be stopped and started individually, not only in layers at a time. Option D is incorrect because the configure lifecycle event runs on all instances in a stack, regardless of layer. Assigning recipes is performed at the layer level, meaning that all instances in the same layer will run the same configuration code. Organizing instances into layers based on purpose removes the need to add complex conditional logic. Thus, option A is correct.

7. C. Option A is incorrect because AWS OpsWorks Stacks does not include a central Chef Server. Option B is incorrect because storing recipes as part of an AMI would introduce considerable complexity for regular recipe code updates. Option D is incorrect because Amazon EC2 is not a valid storage location for cookbooks. A custom cookbook repository location is configured for a stack. When instances in the stack are first launched, they will download cookbooks from this location and run them as part of lifecycle events. Thus, option C is correct.

8. A. Option B is incorrect because you cannot associate a single Amazon RDS database instance with multiple stacks at the same time. Option C is incorrect because this approach would require manual snapshotting and data migration that is not necessary. Option D is incorrect. Migration of database instances between stacks is a common workflow. To migrate an Amazon RDS layer, you must remove it from the first layer before you add it to the second. Thus, option A is correct.

9. C. Option A is incorrect because 24/7 instances are normally recommended for constant demand. Option B is incorrect because load-based instances are recommended for variable, unpredictable demand changes. Option D is incorrect because On-Demand is an Amazon ECS instance type, not an OpsWorks Stacks instance type. You configure time-based instances to start and stop on a specific schedule. AWS recommends this for a predictable increase in workload throughout a day. Thus, option C is correct.

10. B. Option A is incorrect because 24/7 instances are normally recommended for constant demand. Option C is incorrect because time-based instances are recommended for changes in load that are predictable over time. Option D is incorrect because Spot is an Amazon ECS instance type, not an OpsWorks Stacks instance type. Option B is correct because load-based instances are recommended for unpredictable changes in demand.

11. A. Option B is incorrect because the Amazon ECS service role is used to create and manage AWS resources on behalf of the customer. Option C is incorrect because AWS Systems Manager is not part of Amazon ECS. Option D is incorrect because Amazon ECS automates the process of stopping and starting containers within a cluster. The Amazon ECS agent is responsible for all on-instance tasks such as downloading container images and starting or stoping containers. Thus, option A is correct.

12. B. Option A is incorrect. Though high availability is a tenet of SOA, it is not a requirement. Option C is incorrect because SOA does not define how development teams are organized. Option D is incorrect because SOA does not define what should or should not be procured from vendors. Service-oriented architecture involves using containers to implement discrete application components separately from one another to ensure availability and durability of each component. Thus, option B is correct.

13. D. A single task definition can describe up to 10 containers to launch at a time. To launch more containers, you need to create multiple task definitions. Task definitions should group containers by similar purpose, lifecycle, or resource requirements. Thus, option D is correct.

14. A. Option B is incorrect because PAT cannot be configured within your VPC (it must be configured using a proxy instance of some kind). Option C is incorrect because containers can be configured to bind to a random port instead of a specific one. Dynamic host port mapping allows you to launch multiple copies of the same container listening on different ports. Classic Load Balancers do not support dynamic host port mapping. Thus, option D is incorrect. Option A is correct because the Application Load Balancer is then responsible for mapping requests on one port to each container's specific port.

15. A. Options B and C are incorrect because they do not consider the Availability Zone of each cluster instance when placing tasks. Option D is incorrect because least cost is not a valid placement policy. The spread policy distributes tasks across multiple availability zones and cluster instances. Thus, option A is correct.

Chapter 10: Authentication and Authorization

1. D. You need to use a third-party IdP as the confirmation of identity. Based on that confirmation, a policy can be assigned. Option A is incorrect because roles cannot be assigned to users outside of your account. Option B is incorrect because you cannot assign an IAM user ID to a user that is external to AWS. Option C is incorrect because it makes provisioning an identity a manual process.

2. D. An identity provider (IdP) answers the question "Who are you?" Based on this answer, policies are assigned. Those policies control the level of access to the AWS infrastructure and applications (if using AWS for managed services).

   Option A is incorrect; it is one of the functions of a service provider—to control access to applications. Option B is incorrect; policies are used to control access to APIs, which is how access to the AWS infrastructure is controlled. Option C is incorrect; identity providers do no error checking on policy assignment.

3. A. Where possible, using multi-factor authentication (MFA) minimizes the impact of lost or compromised credentials. Option B is incorrect in that embedding credentials is both a security risk and makes credential administration much more difficult. Option C would decrease the opportunity for misuse. It would not address any misuse that was a result of internal users. Option D is a good step but not as secure as option A.

4. D. If you want to use Security Assertion Markup Language (SAML) as an identity provider (IdP), use SAML 2.0. With Amazon Cognito, you can use Google (option A), Microsoft Active Directory (option B), and your own identity store (option C) as identity providers.

5. C. By using AWS Cloud services, such as Amazon Cognito, you are able to view the API calls in AWS CloudTrail. Amazon CloudWatch Logs are generated if you are using Amazon Cognito to control access to AWS resources. Option A is incorrect as AWS can act as an IdP for non-AWS services. Option B is incorrect in that Amazon CloudWatch allows you to monitor the creation and modification of identity pools. It will not show activity. Option D is incorrect because the service provider assigns the policies, not the identity provider (IdP).

6. A, C. AD Connecter is easy to set up, and you continue to use the existing AD console to do configuration changes on Active Directory. Option B is incorrect because you cannot connect to multiple Active Directory domains with AD Connector, only a single one. AD Connector requires a one-to-one relationship with your on-premises domains. You can use AD Connector for AWS-created applications and services. Option D is incorrect because AD Connector is used to support AWS services.

7. A. To use AWS Single Sign-On (AWS SSO), you must set up AWS Organizations Service and enable all the features. AWS SSO uses Microsoft Active Directory (either AWS Managed Microsoft Active Directory or Active Directory Connector [AD Connector] but not Simple Active Directory). AWS SSO does not support Amazon Cognito. Option B is incorrect because AWS SSO does not use SAML. Options C and D are incorrect because you do not need to deploy either Simple AD or Amazon Cognito as a prerequisite for using AWS SSO.

8. C. Option C is correct because `GetFederationToken` returns a set of temporary security credentials (consisting of an access key ID, a secret access key, and a security token) for a federated user. You call the `GetFederationToken` action using the long-term security credentials of an IAM user. This is appropriate in contexts where those credentials can be safely stored, usually in a server-based application. Option D is incorrect because `GetSessionToken` provides only temporary security credentials. Option A is incorrect because AssumeRole is shorter lived (the default is 60 minutes; can be extended to 720 minutes). Options B and D are incorrect because `GetUserToken` and `GetSessionToken` are nonexistent APIs.

9. B. Because it is a managed service, you are not able to access the Amazon EC2 instances directly running AWS Managed Microsoft AD. AWS Managed Microsoft AD provides for daily snapshots, monitoring, and the ability to sync with an existing on-premises Active Directory.

10. A. Amazon Active Directory Connector (AD Connector) allows you to use your existing RADIUS-based multi-factor authentication (MFA) infrastructure to provide authentication.

Chapter 11: Refactor to Microservices

1. B. Option B is correct because a `Parallel` state enables you to execute several different execution paths at the same time in parallel. This is useful if you have activities or tasks that do not depend on each other and can execute in parallel. This can make your workflow complete faster. Option A is incorrect because it executes only one of the branches, not all. Option C is incorrect because it can execute one task, not multiple. Option D is incorrect because it waits and does not execute any tasks.

2. B. The messages move to the dead-letter queue if they have met the `Maximum Receives` parameter (the number of times that a message can be received before being sent to a dead-letter queue) and have not been deleted.

3. A. Amazon Simple Queue Service (Amazon SQS) attributes supports 256 KB messages. Refer to Table 11.2, Table 11.3, and Table 11.4.

4. B. Option B is correct because to send a message larger than 256 KB, you use Amazon SQS to save the file in Amazon S3 and then send a link to the file on Amazon SQS. Option A is incorrect because using the technique in option B, this is possible. Option C is incorrect because AWS Lambda cannot push messages to Amazon SQS that exceed the size limit of 256 KB. Option D is incorrect because it does not address the question.

5. C. Option C is correct if you need to send messages to other users. Create an Amazon SQS queue and subscribe all the administrators to this queue. Configure an Amazon CloudWatch event to send a message on a daily cron schedule into the Amazon SQS queue. Option A is not correct because Amazon SQS queues do not support subscriptions. Option B is not correct because the message is sent without any status information. Option D is not correct because AWS Lambda does not allow sending outgoing email messages on port 22. Email servers use port 22 for outgoing messages. Port 22 is blocked on Lambda as an anti-spam measure.

6. A. Amazon SNS supports the same attributes and parameters as Amazon SQS. Refer to Table 11.2, Table 11.3, and Table 11.4.

7. D. Option D is correct because there is no limit on the number of consumers as long as they stay within the capacity of the stream, which is based on the number of shards. For a single shard, the capacity is 2 MB of read or five transactions per second. Options A and B are incorrect because there is no limit on the number of consumers that can consume from the stream. Option C is incorrect because together the consumers can consume only 2 MB per second or five transactions per second.

8. C. Option C is correct because Amazon Kinesis Data Streams is a service for ingesting large amounts of data in real time and for performing real-time analytics on the data. Option A is not correct because you use Amazon SQS to ingest events, but it does not provide a way to aggregate them in real time. Option B is incorrect because Amazon SNS is a notification service that does not support ingesting. Option D is incorrect because Amazon Kinesis Data Firehose provides analytics; however, it has a latency of at least 60 seconds.

9. A. Options B, C, and D are incorrect because there are no guarantees about where the records for Washington and Wyoming will be relative to each other. They could be on the same shard, or they could be on different shards. Option A is correct because the records for Washington will not be distributed across multiple shards.

10. E. Option E is correct because all the options from A through D are correct. Options A, B, C, and D are all valid options for writing Amazon Kinesis Data Streams producers.

Chapter 12: Serverless Compute

1. D. Option D is correct because it enables the company to keep their existing AWS Lambda functions intact and create new versions of the AWS Lambda function. When they are ready to update the Lambda function, they can assign the `PROD` alias to the new version. Option A is possible; however, this adds a lot of unnecessary work, because developers would have to update all of their code everywhere. Option B is incorrect because moving regions would require moving all other services or introducing latency into the architecture, which is not the best option. Option C is possible; however, creating new AWS accounts for each application version is not a best practice, and it complicates the organization of such accounts unnecessarily.

2. B. At the time of this writing, the maximum amount of memory for a Lambda function is 3008 MB.

3. A. At the time of this writing, the default timeout value for a Lambda function is 3 seconds. However, you can set this to as little as 1 second or as long as 300 seconds.

4. C. Options A, B, and D are all viable answers; however, the question asks what is the best *serverless* option. Lambda is the only serverless option in this scenario; therefore, option C is the best answer.

5. D. At the time of this writing, the maximum execution time for a Lambda function is 300 seconds (5 minutes).

6. A. At the time of this writing, Ruby is not supported for Lambda functions.

7. A. At the time of this writing, the default limit for concurrent executions with Lambda is set to 1000. This is a soft limit that can be raised. To do this, you must open a case through the AWS Support Center page and send a Server Limit Increase request.

8. C. There are two types of policies with Lambda: a function policy and an execution policy, or AWS role. A function policy defines which AWS resources are allowed to invoke your function. The execution role defines which AWS resources your function can access. Here, the function is invoked successfully, but the issue is that the Lambda function does not have access to process objects inside Amazon S3. Option A is not correct because a function policy is responsible for invoking or triggering the function; here, the function is invoked and executes properly. Option B is not correct, as the scenario states that the trust policy is valid. The execution policy or AWS role is responsible for providing Lambda with access to other services; thus, the correct answer is option C.

9. A. Option A is correct because Lambda automatically retries failed executions for asynchronous invocations. You can also configure Lambda to forward payloads that were not processed to a DLQ, which can be an Amazon SQS queue or Amazon SNS topic. Option B is incorrect because a VPC network is an AWS service that allows you to define your own network in the AWS Cloud. Option C is incorrect because this is dealing with concurrency issues, and here you have no problems with Lambda concurrency. Additionally, concurrency is enabled by default with Lambda. Option D is incorrect because Lambda does support SQS.

10. C. Option C is correct because the environment variables enable you to pass settings dynamically to your function code and libraries without changing your code. Option A is not correct, because dead-letter queries are used for events that could not be processed by Lambda and need to be investigated later. Option B is not correct because it can be done. Option D is incorrect because this can be accomplished through environment variables.

Chapter 13: Serverless Applications

1. D. Option A is incorrect. While AWS CloudFormation can help you provision infrastructure, AWS Serverless Application Model (AWS SAM) is optimized for deploying AWS serverless resources by making it easy to organize related components and resources that operate on a single stack; therefore, option A is not the best answer. Option C is incorrect because AWS OpsWorks is managed by Puppet or Chef, which you can use to deploy infrastructure. However, these are not the optimal answers given that you are specifically looking for serverless technologies. The same is true for Ansible in option B. Option D is correct because AWS SAM is an open-source framework that you can use to build serverless applications on AWS.

2. B. CORS is responsible for allowing cross-site access to your APIs. Without it, you will not be able to call the Amazon API Gateway service. You use a stage to deploy your API, and a resource is a typed object that is part of your API's domain. Each resource may have an associated data model and relationships to other resources and can respond to different methods. Option A is incorrect because you do need to enable CORS. Option B is correct because CORS is responsible for allowing one server to call another server or service. For more information on CORS, see: `https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS`. Option C is incorrect, as deploying a stage allows you to deploy your API. Option D is incorrect, as a resource is where you can define your API, but it is not yet deployed to a stage and "live."

3. A, C. There are three benefits to serverless stacks: no server management, flexible scaling, and automated high availability. Costs vary case by case. For these reasons, option A and option C are the best answers.

4. D. Option A is incorrect; API Gateway only supports HTTPS endpoints. Option B is incorrect because API Gateway does not support creating FTP endpoints. Option C is incorrect; API Gateway does not support SSH endpoints. API Gateway only creates HTTPS endpoints.

5. C. Option A is incorrect because Amazon CloudFront supports a variety of sources, including Amazon S3. Option B is incorrect, because serverless applications contain both static and dynamic data. Additionally, CloudFront supports both static and dynamic data. Option C is correct because CloudFront supports a variety of origins. For the serverless stack, it supports Amazon S3. Option D is incorrect because Amazon S3 is a valid origin for CloudFront.

6. D. Option A, option B, and option C are each not the only language/platform supported. Option D is correct because all of these languages/platforms are supported.

7. C. Option C is correct because Amazon Cognito supports SMS-based MFA.

8. D. Options A, B, and C are incorrect because Amazon Cognito supports device tracking and remembering.

9. A. Option A is correct because the `events` property allows you to assign Lambda to an event source. Option B is incorrect because `handler` is the function handler in an Lambda function. Option C is incorrect because `context` is the context object for a Lambda function. Option D is incorrect because `runtime` is the language that your Lambda function runs as.

10. D. Option A is incorrect. You can run React in an AWS service. Option B is incorrect. You can run your web server with Amazon S3. With option C, you do not need to load balance Lambda functions because Lambda scales automatically. Option D is correct. You can run a fully dynamic website in a serverless fashion. You can also use JavaScript frameworks such as Angular and React. The NoSQL database may need to be refactored to run in Amazon DynamoDB.

Chapter 14: Stateless Application Patterns

1. B. Option B is correct because the maximum size of an item in an DynamoDB table is 400 KB. Option C is incorrect because 4 KB is the capacity of a strongly consistent read per second, or two eventually consistent reads per second, for an item up to 4 KB in size. Option D is incorrect because 1,024 KB is not the size limit of an DynamoDB item. The maximum item size is 400 KB.

2. C. Option C is correct because when creating a new bucket, the bucket name must be globally unique. Option A is incorrect because versioning is disabled by default. Option B is incorrect because the maximum size for an object stored in Amazon S3 is 5 TB, not 5 GB. Option D is incorrect because you cannot change a bucket name after you have created the bucket.

3. B. Option B is correct because storage class is the only factor that is not considered when determining which region to choose. Option A is incorrect because latency is a factor when choosing a bucket region. Option C is incorrect because prices are different between regions; thus, you might consider cost when choosing a bucket region. Option D is incorrect because you may be required to store your data in a bucket in a particular region based on legal requirements or compliance.

4. C. Option C is correct because the recommended technique for protecting your table data at rest is the server-side encryption. Option A is incorrect because fine-grained access controls are a mechanism for providing access to resources and API calls, but the mechanism is not used to encrypt or protect data at rest. Option B is incorrect because TLS protects data in transit, not data at rest. Option D is incorrect because client-side encryption is applied to data before it is transmitted from a user device to a server.

5. D. Option D is correct because versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite. Option A is incorrect because lifecycle policies are used to transition data to a different storage class and do not protect objects against accidental overwrites or deletions. Option B is incorrect because enabling `MFA Delete` on the bucket requires an additional method of authentication before allowing a deletion. Option C is incorrect because using a path-style URL is unrelated to protecting overwrites or accidental deletions.

6. C, D. Options C and D are correct because Amazon S3 stores objects in buckets, and each object that is stored in a bucket is made up of two parts: the object itself and the metadata. Option A is incorrect because Amazon S3 stores data as objects, not in fixed blocks. Option B is incorrect because the size limit of an object is 5 TB.

7. C. Option C is correct because DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table, and the service stores this information in a log for up to 24 hours. Options A, B, and D are incorrect because 24 hours is the maximum time that data persists on an Amazon DynamoDB stream.

8. B. Option B is correct because DynamoDB Streams ensures that each stream record appears exactly once in the stream. Options A and C are incorrect because each stream record appears exactly once. Option D is incorrect because you cannot set the retention period.

9. A. Option A is correct because your bucket can be in only one of three versioning states: versioning-enabled, versioning-disabled, or versioning-suspended. Thus, versioning-paused is a state that is not a valid configuration. Options A, B, and C are incorrect—they are all valid bucket states for versioning.

10. A. Option A is correct because `QueryTable` is the DynamoDB operation used to find items based on primary key values. Option B is incorrect because `UpdateTable` is the DynamoDB operation used to modify the provisioned throughput settings, global secondary indexes, or DynamoDB Streams settings for a given table. Option C is incorrect because DynamoDB does not have a `Search` operation. Option D is incorrect because `Scan` is the DynamoDB operation used to read every item in a table.

11. A, B, C. Option D is incorrect because when compared to the other options, a bank balance is not likely to be stored in a cache; it is probably not data that is retrieved as frequently as the others are fetched. Options A, B, and C are all better data candidates to cache because multiple users are more likely to access them repeatedly. Although, you could also cache the bank account balance for shorter periods if the database query is not performing well.

12. A, D. Options A and D are correct because Amazon ElastiCache supports both the Redis and Memcached open-source caching engines. Option B is incorrect because MySQL is not a caching engine—it is a relational database engine. Option C is incorrect because Couchbase is a NoSQL database and not one of the caching engines that ElastiCache supports.

13. C. Option C is correct because the default limit is 20 nodes per cluster.

14. C. Option C is correct because ElastiCache is a managed in-memory caching service. Option A is incorrect because the description aligns more closely to the Elasticsearch Service. Option B is incorrect because this is not an accurate description of the ElastiCache service. Option D is incorrect because, as a managed service, ElastiCache does not manage Amazon EC2 instances.

15. B, D, E. Option B is correct because DynamoDB is a NoSQL low-latency transactional database that you can use to store state. Option D is correct because Amazon Elastic File System (Amazon EFS) is an elastic file system that you can also use to store state. Option E is correct because ElastiCache is an in-memory cache that is also a good solution for storing state. Option A is incorrect because Amazon CloudFront is a content delivery network that is used more for object caching, not in-memory caching. Option C is incorrect because Amazon CloudWatch is a metric repository and does not provide any kind of user-accessible storage. Option F is incorrect because Amazon SQS is used for exchanging messages.

16. C. Option C is correct because Amazon DynamoDB is a nonrelational database that delivers reliable performance at any scale. Option A is incorrect because Amazon S3 Glacier is for data archiving and long-term backup. It is also an object store and not a database store. Option B is incorrect because Amazon RDS is designed for relational workloads. Option D is incorrect because Amazon Redshift is a data warehousing service.

17. D. Option D is correct because local secondary indexes on a table are created when the table is created. Options A and C are incorrect because you can have five local secondary indexes or five global secondary indexes per table. Option B is incorrect because you can create global secondary indexes after you have created the table.

Chapter 15: Monitoring and Troubleshooting

1. B. Option A is incorrect because you do not want to scale in to reduce your capacity when you are experiencing a high load. Option C is incorrect because you do not want to scale in to reduce your capacity when your application is taking a long time to respond. Option D is incorrect because metrics are required for triggering AWS Auto Scaling events. Option B is correct because scaling out should occur when more resources are being consumed than normal, and scaling in should occur when less resources are being consumed.

2. D. Options A, B, C, and D are all incorrect because data points with a period of 300 seconds are stored for 63 days in Amazon CloudWatch.

3. D. Option A is incorrect because AWS CloudTrail events show who made the request. Option B is incorrect because CloudTrail shows when the request was made, and option C is incorrect because CloudTrail shows what was requested. Option E is incorrect because CloudTrail shows what resource was acted on. Option D is correct because CloudTrail can provide no insight into why a request was made.

4. C. Option A would work; however, it is not the most cost-effective way because logs stored in CloudWatch cost more than logs stored in Amazon S3. Option B is incorrect because CloudWatch cannot ingest logs without access to your servers. Option C is correct because archiving logs from CloudWatch to Amazon S3 reduces overall data storage costs.

5. A, B, D. Option C is incorrect because CloudWatch has no way to access data in your applications or servers. You must push the data either by using the CloudWatch SDK or AWS CLI or by installing the CloudWatch agent. Option A is correct because the CloudWatch agent is required to send operating system and application logs to CloudWatch. Option B is likewise correct because metrics logs are sent to CloudWatch using the `PutMetricData` and `PutLogEvents` API actions. Option D is also correct because the AWS CLI can be used to send metrics to CloudWatch using the `put-metric-data` and `put-log-events` commands.

6. C. Options A and B are incorrect because the strings must match a filter pattern equal to 404. Option C is correct because 404 matches the error code present in the example logs.

7. A. AWS X-Ray color-codes the response types you get from your services. For 4XX, or client-side errors, the circle is orange. Thus, option B is incorrect. Application failures or faults are red, and successful responses, or 2XX, are green. Thus, options C and D are incorrect. For throttling, or 5XX series errors, the circle is purple. Thus, option A is correct.

8. C. Option A is incorrect because CloudTrail logs list security-related events and do not provide a dashboard feature. Option B is incorrect because CloudWatch alarms are used to notify you when something isn't operating based on your specifications. Option D is incorrect because Amazon CloudWatch Logs are for sending and storing server logs to the CloudWatch service; however, you could use these logs to create a metric and then place it on the CloudWatch dashboard. Option C is the correct answer. Use CloudWatch dashboards to create a single interface where you can monitor all the resources.

9. D. CloudTrail stores the CloudTrail event history for 90 days; however, if you would like to store this information permanently, you can create an CloudTrail trail, which stores the logs in Amazon S3.

10. D. Option C is incorrect because the `LookupEvents` API action can be used to query event data. Options A and B are also incorrect because the AWS CLI and the AWS Management Console use the same CloudTrail APIs to query event data. Thus, option D is correct.

11. B, D. Management events are operations performed on resources in your AWS account. Data events are operations performed on data stored in AWS resources. For example, modifying an object in Amazon S3 would qualify as a data event, and changing a bucket policy would qualify as a management event. Because options A, C, and E involve sending or receiving data, not modifying or creating AWS resources, they are data events. Thus, options B and D are correct.

12. A, C, D. When installing the CloudWatch Logs agent, no additional networking configuration is required as long as your instance can reach the CloudWatch API endpoint. Therefore, option B is incorrect. You can use AWS Systems Manager to install and start the agent, but it is not required to install the Systems Manager agent alongside the CloudWatch Logs agent; thus, option E is incorrect. When installing the agent, you must configure the specific logs to send. The agent must be started before new log data is sent to CloudWatch Logs.

13. A. CloudWatch alarms support triggering actions in Amazon EC2, EC2 Auto Scaling, and Amazon SNS. Thus, options B, C, and D are incorrect. It is possible to trigger AWS Lambda functions from an alarm, but only by first sending the alarm notification to an Amazon SNS topic. Thus, option A is correct.

14. D. CPU, network, and disk activity are metrics that are visible to the underlying host for an instance. Thus, options A, B, and C are incorrect. Because memory is allocated in a single block to an instance and is managed by the guest OS, the underlying host does not have visibility into consumption. This metric would have to be delivered to CloudWatch as a custom metric by using the agent. Thus, option D is correct.

15. A. No namespace starts with an `Amazon` prefix; therefore, options B and D are incorrect. Option C is incorrect because namespaces are specific to a service (Amazon EC2), not a resource (an instance). Option A is correct because the Amazon EC2 service uses the `AWS` prefix, followed by `EC2`.

Chapter 16: Optimization

1. D. Amazon EC2 instance store is directly attached to the instance, which gives you the lowest latency between the disk and your application. Instance store is also provided at no additional cost on instance types that have it available, so this is the lowest-cost option. Additionally, because the data is being retrieved from somewhere else, it can be copied back to an instance as needed. Option A is incorrect because Amazon S3 cannot be directly mounted to an Amazon EC2 instance. Options B and C are incorrect because Amazon EBS and Amazon EFS would be higher-cost options, with a higher latency than an instance store.

2. C. `GetItem` retrieves a single item from a table. This is the most efficient way to read a single item because it provides direct access to the physical location of the item. Options A and B are incorrect. `Query` retrieves all the items that have a specific partition key. Within those items, you can apply a condition to the sort key and retrieve only a subset of the

data. `Query` provides quick, efficient access to the partitions where the data is stored. `Scan` retrieves all of the items in the specified table, and it can consume large amounts of system resources based on the size of the table. Option D is incorrect. DynamoDB is a nonrelational NoSQL database, and it does not support table joins. Instead, applications read data from one table at a time.

3. C. Option C is a fault-tolerance check. By launching instances in multiple Availability Zones in the same region, you help protect your applications from a single point of failure. Options A and B are performance checks. Provisioned IOPS volumes in the Amazon EBS are designed to deliver the expected performance only when they are attached to an Amazon EBS optimized instance. Some headers, such as Date or User-Agent, significantly reduce the cache hit ratio (the proportion of requests that are served from a CloudFront edge cache). This increases the load on your origin and reduces performance because CloudFront must forward more requests to your origin. Option D is a cost check. Elastic IP addresses are static IP addresses designed for dynamic cloud computing. A nominal charge is imposed for an Elastic IP address that is not associated with a running instance.

4. B. Options A, C, and D are incorrect because partition keys used in these options could cause "hot" (heavily requested) partition keys because of lack of uniformity. Design your application for uniform activity across all logical partition keys in the table and its secondary indexes. Use distinct values for each item.

5. D. Option A is incorrect because SQS is a messaging service. Option B is incorrect because SNS is a notification service. Option C is incorrect because CloudFront is a web distribution service. Option D is correct because ElastiCache improves the performance of your application by retrieving data from high throughput and low latency in-memory data stores. For details, see `https://aws.amazon.com/elasticache`.

6. C. Option C is correct because CloudFront optimizes performance if your workload is mainly sending `GET` requests. There are also fewer direct requests to Amazon S3, which reduces cost. For details, see `https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html`.

7. D. Option A is incorrect because AWS Auto Scaling is optimal for unpredictable workloads. Option B is incorrect because cross-region replication is better for disaster recovery scenarios. Option C is incorrect because DynamoDB streams are better suited to stream data to other sources. Option D is correct because Amazon DynamoDB Accelerator (DAX) provides fast in-memory performance. For details, see `https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.html`.

8. C. Option A is incorrect because EC2 instance store is too volatile to be optimal. Option B is incorrect because this is a security solution and will not impact performance positively. Option C is correct because ElastiCache is ideal for handling session state. You can abstract the HTTP sessions from the web servers by using Redis and Memcached. Option D is incorrect because compression is not the optimal solution given the choices. For details, see `https://aws.amazon.com/caching/session-management/`.

9. B. Option B is correct because lazy loading only loads data into the cache when necessary. This avoids filling up the cache with data that isn't requested. Options A, C, and D are

incorrect because they do not match the requirement of the question. For details, see https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/Strategies.html.

10. A. Option A is correct because information about the instance, such as private IP, is stored in the instance metadata. Option B is incorrect because private IP information is not stored in the instance user data. Option C is incorrect because running `ifconfig` is manual and not automated. Option D is incorrect because it is not clear on what type of instance the application is running. For details, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html.

11. D. Options A, B, and C are incorrect because they are not recommended best practices. Option D is correct because it is one of the recommendations in the best practices documentation, "Avoid using recursive code." For details, see https://docs.aws.amazon.com/lambda/latest/dg/best-practices.html.

12. C. Option A is incorrect because changing the entire architecture is not ideal. Option B is incorrect because Multi-AZ is used for fault tolerance. Option C is correct because loads can be reduced by routing read queries from your application to the read replica. Option D is incorrect because using an Elastic Load Balancing load balancer will not reduce the query load. For details, see https://aws.amazon.com/rds/details/read-replicas/.

13. C. Option A is incorrect because this is relevant only when you need a static website. Option B is incorrect because changing the storage class does not help with latency. Option C is correct because cross-region replication maintains object copies in regions that are geographically closer to your users, reducing latency. Option D is incorrect because encryption is necessary only for securing data at rest. For details, see https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html.

14. B. Options A, C, and D are incorrect because they are not optimal for handling large object uploads to Amazon S3. Option B is correct because a multipart upload enables you to upload large objects in parts to Amazon S3. For details, see https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html.

15. C. Option A is incorrect because this is not the optimal approach for bootstrapping. Option B is incorrect because, while possible, bootstrapping in the user data is optimal. Option C is correct because instance user data is used to perform common automated configuration tasks and run scripts after boot. Option D is incorrect because bootstrapping is done in instance user data, not instance metadata. For details, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html.