Appendix A
Answers to Review Questions

Chapter 1: Introduction to AWS

1. D. A region is a named set of AWS resources in the same geographical area. A region comprises at least two Availability Zones. Endpoint, Collection, and Fleet do not describe a physical location around the world where AWS clusters data centers.
2. A. An Availability Zone is a distinct location within a region that is insulated from failures in other Availability Zones and provides inexpensive, low-latency network connectivity to other Availability Zones in the same region. Replication areas, geographic districts, and compute centers are not terms used to describe AWS data center locations.
3. B. A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud. An all-in deployment refers to an environment that exclusively runs in the cloud. An on-premises deployment refers to an environment that runs exclusively in an organization's data center.
4. C. Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications organizations run on AWS. It allows organizations to collect and track metrics, collect and monitor log files, and set alarms. AWS IAM, Amazon SNS, and AWS CloudFormation do not provide visibility into resource utilization, application performance, and the operational health of your AWS resources.
5. B. Amazon DynamoDB is a fully managed, fast, and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. Amazon SQS, Amazon ElastiCache, and Amazon RDS do not provide a NoSQL database service. Amazon SQS is a managed message queuing service. Amazon ElastiCache is a service that provides in-memory cache in the cloud. Finally, Amazon RDS provides managed relational databases.
6. A. Auto Scaling helps maintain application availability and allows organizations to scale Amazon Elastic Compute Cloud (Amazon EC2) capacity up or down automatically according to conditions defined for the particular workload. Not only can it be used to help ensure that the desired number of Amazon EC2 instances are running, but it also allows resources to scale in and out to match the demands of dynamic workloads. Amazon Glacier, Amazon SNS, and Amazon VPC do not provide services to scale compute capacity automatically.
7. D. Amazon CloudFront is a web service that provides a CDN to speed up distribution of your static and dynamic web content—for example, `.html`, `.css`, `.php`, image, and media files—to end users. Amazon CloudFront delivers content through a worldwide network of edge locations. Amazon EC2, Amazon Route 53, and AWS Storage Gateway do not provide CDN services that are required to meet the needs for the photo sharing service.
8. A. Amazon EBS provides persistent block-level storage volumes for use with Amazon EC2 instances on the AWS Cloud. Amazon DynamoDB, Amazon Glacier, and AWS CloudFormation do not provide persistent block-level storage for Amazon EC2 instances. Amazon DynamoDB provides managed NoSQL databases. Amazon Glacier provides low-cost archival storage. AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources.

9. C. Amazon VPC lets organizations provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a virtual network that they define. Amazon SWF, Amazon Route 53, and AWS CloudFormation do not provide a virtual network. Amazon SWF helps developers build, run, and scale background jobs that have parallel or sequential steps. Amazon Route 53 provides a highly available and scalable cloud Domain Name System (DNS) web service. Amazon CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources.
10. B. Amazon SQS is a fast, reliable, scalable, fully managed message queuing service that allows organizations to decouple the components of a cloud application. With Amazon SQS, organizations can transmit any volume of data, at any level of throughput, without losing messages or requiring other services to be always available. AWS CloudTrail records AWS API calls, and Amazon Redshift is a data warehouse, neither of which would be useful as an architecture component for decoupling components. Amazon SNS provides a messaging bus complement to Amazon SQS; however, it doesn't provide the decoupling of components necessary for this scenario.

Chapter 2: Amazon Simple Storage Service (Amazon S3) and Amazon Glacier Storage

1. D, E. Objects are stored in buckets, and objects contain both data and metadata.
2. B, D. Amazon S3 cannot be mounted to an Amazon EC2 instance like a file system and should not serve as primary database storage.
3. A, B, D. C and E are incorrect—objects are private by default, and storage in a bucket does not need to be pre-allocated.
4. B, C, E. Static website hosting does not restrict data access, and neither does an Amazon S3 lifecycle policy.
5. C, E. 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. Cross-region replication and migration to the Amazon Glacier storage class do not protect against deletion. Vault locks are a feature of Amazon Glacier, not a feature of Amazon S3.
6. C. Migrating the data to Amazon S3 Standard-IA after 30 days using a lifecycle policy is correct. Amazon S3 RRS should only be used for easily replicated data, not critical data. Migration to Amazon Glacier might minimize storage costs if retrievals are infrequent, but documents would not be available in minutes when needed.
7. B. Data is automatically replicated within a region. Replication to other regions and versioning are optional. Amazon S3 data is not backed up to tape.
8. C. In a URL, the bucket name precedes the string “s3.amazonaws.com/,” and the object key is everything after that. There is no folder structure in Amazon S3.
9. C. Amazon S3 server access logs store a record of what requestor accessed the objects in your bucket, including the requesting IP address.
10. B, C. Cross-region replication can help lower latency and satisfy compliance requirements on distance. Amazon S3 is designed for eleven nines durability for objects in a single region, so a second region does not significantly increase durability. Cross-region replication does not protect against accidental deletion.
11. C. If data must be encrypted before being sent to Amazon S3, client-side encryption must be used.
12. B. Amazon S3 scales automatically, but for request rates over 100 GETS per second, it helps to make sure there is some randomness in the key space. Replication and logging will not affect performance or scalability. Using sequential key names could have a negative effect on performance or scalability.
13. A, D. You must enable versioning before you can enable cross-region replication, and Amazon S3 must have IAM permissions to perform the replication. Lifecycle rules migrate data from one storage class to another, not from one bucket to another. Static website hosting is not a prerequisite for replication.
14. B. Amazon S3 is the most cost effective storage on AWS, and lifecycle policies are a

simple and effective feature to address the business requirements.

15. B, C, E. Amazon S3 bucket policies cannot specify a company name or a country or origin, but they can specify request IP range, AWS account, and a prefix for objects that can be accessed.
16. B, C. Amazon S3 provides read-after-write consistency for PUTs to new objects (new key), but eventual consistency for GETs and DELETEs of existing objects (existing key).
17. A, B, D. A, B, and D are required, and normally you also set a friendly CNAME to the bucket URL. Amazon S3 does not support FTP transfers, and HTTP does not need to be enabled.
18. B. Pre-signed URLs allow you to grant time-limited permission to download objects from an Amazon Simple Storage Service (Amazon S3) bucket. Static web hosting generally requires world-read access to all content. AWS IAM policies do not know who the authenticated users of the web app are. Logging can help track content loss, but not prevent it.
19. A, C. Amazon 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.
20. C, D, E. Amazon Glacier stores data in archives, which are contained in vaults. Archives are identified by system-created archive IDs, not key names.

Chapter 3: Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Elastic Block Store (Amazon EBS)

1. C. Reserved Instances provide cost savings when you can commit to running instances full time, such as to handle the base traffic. On-Demand Instances provide the flexibility to handle traffic spikes, such as on the last day of the month.
2. B. Spot Instances are a very cost-effective way to address temporary compute needs that are not urgent and are tolerant of interruption. That's exactly the workload described here. Reserved Instances are inappropriate for temporary workloads. On-Demand Instances are good for temporary workloads, but don't offer the cost savings of Spot Instances. Adding more queues is a non-responsive answer as it would not address the problem.
3. C, D. The Amazon EC2 instance ID will be assigned by AWS as part of the launch process. The administrator password is assigned by AWS and encrypted via the public key. The instance type defines the virtual hardware and the AMI defines the initial software state. You must specify both upon launch.
4. A, C. You can change the instance type only within the same instance type family, or you can change the Availability Zone. You cannot change the operating system nor the instance type family.
5. D. When there are multiple security groups associated with an instance, all the rules are aggregated.
6. A, B, E. These are the benefits of enhanced networking.
7. A, B, D. The other answers have nothing to do with networking.
8. C. Dedicated Instances will not share hosts with other accounts.
9. B, C. Instance stores are low-durability, high-IOPS storage that is included for free with the hourly cost of an instance.
10. A, C. There are no tapes in the AWS infrastructure. Amazon EBS volumes persist when the instance is stopped. The data is automatically replicated within an Availability Zone. Amazon EBS volumes can be encrypted upon creation and used by an instance in the same manner as if they were not encrypted.
11. B. There is no delay in processing when commencing a snapshot.
12. B. The volume is created immediately but the data is loaded lazily. This means 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.
13. A, C. B and D are incorrect because an instance store will not be durable and a magnetic volume offers an average of 100 IOPS. Amazon EBS-optimized instances reserve network bandwidth on the instance for IO, and Provisioned IOPS SSD volumes provide the highest consistent IOPS.
14. D. Bootstrapping runs the provided script, so anything you can accomplish in a script you can accomplish during bootstrapping.

15. C. The public half of the key pair is stored on the instance, and the private half can then be used to connect via SSH.
16. B, C. These are the possible outputs of VM Import/Export.
17. B, D. Neither the Windows machine name nor the Amazon EC2 instance ID can be resolved into an IP address to access the instance.
18. A. None of the other options will have any effect on the ability to connect.
19. 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. Instance stores are not durable, magnetic volumes cannot provide enough IOPS, and to set up a Provisioned IOPS SSD volume to handle the peak would mean spending money for more IOPS than you need.
20. B. There is a very small hourly charge for allocated elastic IP addresses that are not associated with an instance.

Chapter 4: Amazon Virtual Private Cloud (Amazon VPC)

1. C. The minimum size subnet that you can have in an Amazon VPC is /28.
2. C. You need two public subnets (one for each Availability Zone) and two private subnets (one for each Availability Zone). Therefore, you need four subnets.
3. A. Network ACLs are associated to a VPC subnet to control traffic flow.
4. A. The maximum size subnet that you can have in a VPC is /16.
5. D. By creating a route out to the Internet using an IGW, you have made this subnet public.
6. A. When you create an Amazon VPC, a route table is created by default. You must manually create subnets and an IGW.
7. C. When you provision an Amazon VPC, all subnets can communicate with each other by default.
8. A. You may only have one IGW for each Amazon VPC.
9. B. Security groups are stateful, whereas network ACLs are stateless.
10. C. You should disable source/destination checks on the NAT.
11. B, E. In the EC2-Classic network, the EIP will be disassociated with the instance; in the EC2-VPC network, the EIP remains associated with the instance. Regardless of the underlying network, a stop/start of an Amazon EBS-backed Amazon EC2 instance always changes the host computer.
12. D. Six VPC Peering connections are needed for each of the four VPCs to send traffic to the other.
13. B. A DHCP option set allows customers to define DNS servers for DNS name resolution, establish domain names for instances within an Amazon VPC, define NTP servers, and define the NetBIOS name servers.
14. D. A CGW is the customer side of a VPN connection, and an IGW connects a network to the Internet. A VPG is the Amazon side of a VPN connection.
15. A. The default limit for the number of Amazon VPCs that a customer may have in a region is 5.
16. B. Network ACL rules can deny traffic.
17. D. IPsec is the security protocol supported by Amazon VPC.
18. D. An Amazon VPC endpoint enables you to create a private connection between your Amazon VPC and another AWS service without requiring access over the Internet or through a NAT device, VPN connection, or AWS Direct Connect.
19. A, C. The CIDR block is specified upon creation and cannot be changed. An Amazon VPC is associated with exactly one region which must be specified upon creation. You can add a subnet to an Amazon VPC any time after it has been created, provided its address range falls within the Amazon VPC CIDR block and does not overlap with the address range of

any existing CIDR block. You can set up peering relationships between Amazon VPCs after they have been created.

20. B. Attaching an ENI associated with a different subnet to an instance can make the instance dual-homed.

Chapter 5: Elastic Load Balancing, Amazon CloudWatch, and Auto Scaling

1. A, D. An Auto Scaling group must have a minimum size and a launch configuration defined in order to be created. Health checks and a desired capacity are optional.
2. B. The load balancer maintains two separate connections: one connection with the client and one connection with the Amazon EC2 instance.
3. D. Amazon CloudWatch metric data is kept for 2 weeks.
4. A. Only the launch configuration name, AMI, and instance type are needed to create an Auto Scaling launch configuration. Identifying a key pair, security group, and a block device mapping are optional elements for an Auto Scaling launch configuration.
5. B. You can use the Amazon CloudWatch Logs Agent installer on existing Amazon EC2 instances to install and configure the CloudWatch Logs Agent.
6. C. You configure your load balancer to accept incoming traffic by specifying one or more listeners.
7. D. The default Amazon EC2 instance limit for all regions is 20.
8. A. An SSL certificate must specify the name of the website in either the subject name or listed as a value in the SAN extension of the certificate in order for connecting clients to not receive a warning.
9. C. When Amazon EC2 instances fail the requisite number of consecutive health checks, the load balancer stops sending traffic to the Amazon EC2 instance.
10. D. Amazon CloudWatch metrics provide hypervisor visible metrics.
11. C. Auto Scaling is designed to scale out based on an event like increased traffic while being cost effective when not needed.
12. B. Auto Scaling will provide high availability across three Availability Zones with three Amazon EC2 instances in each and keep capacity above the required minimum capacity, even in the event of an entire Availability Zone becoming unavailable.
13. B, E, F. Auto Scaling responds to changing conditions by adding or terminating instances, launches instances from an AMI specified in the launch configuration associated with the Auto Scaling group, and enforces a minimum number of instances in the min-size parameter of the Auto Scaling group.
14. D. A, B, and C are all true statements about launch configurations being loosely coupled and referenced by the Auto Scaling group instead of being part of the Auto Scaling group.
15. A, C. An Auto Scaling group may use On-Demand and Spot Instances. An Auto Scaling group may not use already stopped instances, instances running someplace other than AWS, and already running instances not started by the Auto Scaling group itself.
16. A, F. Amazon CloudWatch has two plans: basic, which is free, and detailed, which has an additional cost. There is no ad hoc plan for Amazon CloudWatch.

17. A, C, D. An Elastic Load Balancing health check may be a ping, a connection attempt, or a page that is checked.
18. B, C. When connection draining is enabled, the load balancer will stop sending requests to a deregistered or unhealthy instance and attempt to complete in-flight requests until a connection draining timeout period is reached, which is 300 seconds by default.
19. B, E, F. Elastic Load Balancing supports Internet-facing, internal, and HTTPS load balancers.
20. B, D, E. Auto Scaling supports maintaining the current size of an Auto Scaling group using four plans: maintain current levels, manual scaling, scheduled scaling, and dynamic scaling.

Chapter 6: AWS Identity and Access Management (IAM)

1. B, C. Programmatic access is authenticated with an access key, not with user names/passwords. IAM roles provide a temporary security token to an application using an SDK.
2. A, C. IAM policies are independent of region, so no region is specified in the policy. IAM policies are about authorization for an already-authenticated principal, so no password is needed.
3. A, B, C, E. Locking down your root user and all accounts to which the administrator had access is the key here. Deleting all IAM accounts is not necessary, and it would cause great disruption to your operations. Amazon EC2 roles use temporary security tokens, so relaunching Amazon EC2 instances is not necessary.
4. B, D. IAM controls access to AWS resources only. Installing ASP.NET will require Windows operating system authorization, and querying an Oracle database will require Oracle authorization.
5. A, C. Amazon DynamoDB global secondary indexes are a performance feature of Amazon DynamoDB; Consolidated Billing is an accounting feature allowing all bills to roll up under a single account. While both are very valuable features, neither is a security feature.
6. B, C. Amazon EC2 roles must still be assigned a policy. Integration with Active Directory involves integration between Active Directory and IAM via SAML.
7. A, D. Amazon EC2 roles provide a temporary token to applications running on the instance; federation maps policies to identities from other sources via temporary tokens.
8. A, C, D. Neither B nor E are features supported by IAM.
9. B, C. Access requires an appropriate policy associated with a principal. Response A is merely a policy with no principal, and response D is not a principal as IAM groups do not have user names and passwords. Response B is the best solution; response C will also work but it is much harder to manage.
10. C. An IAM policy is a JSON document.

Chapter 7: Databases and AWS

1. B. Amazon RDS is best suited for traditional OLTP transactions. Amazon Redshift, on the other hand, is designed for OLAP workloads. Amazon Glacier is designed for cold archival storage.
2. D. Amazon DynamoDB is best suited for non-relational databases. Amazon RDS and Amazon Redshift are both structured relational databases.
3. C. In this scenario, the best idea is to use read replicas to scale out the database and thus maximize read performance. When using Multi-AZ, the secondary database is not accessible and all reads and writes must go to the primary or any read replicas.
4. A. Amazon Redshift is best suited for traditional OLAP transactions. While Amazon RDS can also be used for OLAP, Amazon Redshift is purpose-built as an OLAP data warehouse.
5. B. DB Snapshots can be used to restore a complete copy of the database at a specific point in time. Individual tables cannot be extracted from a snapshot.
6. A. All Amazon RDS database engines support Multi-AZ deployment.
7. B. Read replicas are supported by MySQL, MariaDB, PostgreSQL, and Aurora.
8. A. You can force a failover from one Availability Zone to another by rebooting the primary instance in the AWS Management Console. This is often how people test a failover in the real world. There is no need to create a support case.
9. D. Monitor the environment while Amazon RDS attempts to recover automatically. AWS will update the DB endpoint to point to the secondary instance automatically.
10. A. Amazon RDS supports Microsoft SQL Server Enterprise edition and the license is available only under the BYOL model.
11. B. General Purpose (SSD) volumes are generally the right choice for databases that have bursts of activity.
12. B. NoSQL databases like Amazon DynamoDB excel at scaling to hundreds of thousands of requests with key/value access to user profile and session.
13. A, C, D. DB snapshots allow you to back up and recover your data, while read replicas and a Multi-AZ deployment allow you to replicate your data and reduce the time to failover.
14. C, D. Amazon RDS allows for the creation of one or more read-replicas for many engines that can be used to handle reads. Another common pattern is to create a cache using Memcached and Amazon ElastiCache to store frequently used queries. The secondary slave DB Instance is not accessible and cannot be used to offload queries.
15. A, B, C. Protecting your database requires a multilayered approach that secures the infrastructure, the network, and the database itself. Amazon RDS is a managed service and direct access to the OS is not available.
16. A, B, C. Vertically scaling up is one of the simpler options that can give you additional processing power without making any architectural changes. Read replicas require some

application changes but let you scale processing power horizontally. Finally, busy databases are often I/O- bound, so upgrading storage to General Purpose (SSD) or Provisioned IOPS (SSD) can often allow for additional request processing.

17. C. Query is the most efficient operation to find a single item in a large table.
18. A. Using the Username as a partition key will evenly spread your users across the partitions. Messages are often filtered down by time range, so Timestamp makes sense as a sort key.
19. B, D. You can only have a single local secondary index, and it must be created at the same time the table is created. You can create many global secondary indexes after the table has been created.
20. B, C. Amazon Redshift is an Online Analytical Processing (OLAP) data warehouse designed for analytics, Extract, Transform, Load (ETL), and high-speed querying. It is not well suited for running transactional applications that require high volumes of small inserts or updates.

Chapter 8: SQS, SWF, and SNS

1. D. Amazon DynamoDB is not a supported Amazon SNS protocol.
2. A. When you create a new Amazon SNS topic, an Amazon ARN is created automatically.
3. A, C, D. Publishers, subscribers, and topics are the correct answers. You have subscribers to an Amazon SNS topic, not readers.
4. A. The default time for an Amazon SQS visibility timeout is 30 seconds.
5. D. The maximum time for an Amazon SQS visibility timeout is 12 hours.
6. B, D. The valid properties of an SQS message are Message ID and Body. Each message receives a system-assigned Message ID that Amazon SQS returns to you in the SendMessage response. The Message Body is composed of name/value pairs and the unstructured, uninterpreted content.
7. B. Use a single domain with multiple workflows. Workflows within separate domains cannot interact.
8. A, B, C. In Amazon SWF, actors can be activity workers, workflow starters, or deciders.
9. B. Amazon SWF would best serve your purpose in this scenario because it helps developers build, run, and scale background jobs that have parallel or sequential steps. You can think of Amazon SWF as a fully-managed state tracker and task coordinator in the Cloud.
10. D. Amazon SQS does not guarantee in what order your messages will be delivered.
11. A. Multiple queues can subscribe to an Amazon SNS topic, which can enable parallel asynchronous processing.
12. D. Long polling allows your application to poll the queue, and, if nothing is there, Amazon Elastic Compute Cloud (Amazon EC2) waits for an amount of time you specify (between 1 and 20 seconds). If a message arrives in that time, it is delivered to your application as soon as possible. If a message does not arrive in that time, you need to execute the ReceiveMessage function again.
13. B. The maximum time for an Amazon SQS long polling timeout is 20 seconds.
14. D. The longest configurable message retention period for Amazon SQS is 14 days.
15. B. The default message retention period that can be set in Amazon SQS is four days.
16. D. With Amazon SNS, you send individual or multiple messages to large numbers of recipients using publisher and subscriber client types.
17. B. The decider schedules the activity tasks and provides input data to the activity workers. The decider also processes events that arrive while the workflow is in progress and closes the workflow when the objective has been completed.
18. C. Topic names should typically be available for reuse approximately 30–60 seconds after the previous topic with the same name has been deleted. The exact time will depend on the number of subscriptions active on the topic; topics with a few subscribers will be

available instantly for reuse, while topics with larger subscriber lists may take longer.

19. C. The main difference between Amazon SQS policies and IAM policies is that an Amazon SQS policy enables you to grant a different AWS account permission to your Amazon SQS queues, but an IAM policy does not.
20. C. No. After a message has been successfully published to a topic, it cannot be recalled.

Chapter 9: Domain Name System (DNS) and Amazon Route 53

1. C. An AAAA record is used to route traffic to an IPv6 address, whereas an A record is used to route traffic to an IPv4 address.
2. B. Domain names are registered with a domain registrar, which then registers the name to InterNIC.
3. C. You should route your traffic based on where your end users are located. The best routing policy to achieve this is geolocation routing.
4. D. A PTR record is used to resolve an IP address to a domain name, and it is commonly referred to as "reverse DNS."
5. B. You want your users to have the fastest network access possible. To do this, you would use latency-based routing. Geolocation routing would not achieve this as well as latency-based routing, which is specifically geared toward measuring the latency and thus would direct you to the AWS region in which you would have the lowest latency.
6. C. You would use Mail eXchange (MX) records to define which inbound destination mail server should be used.
7. B. SPF records are used to verify authorized senders of mail from your domain.
8. B. Weighted routing would best achieve this objective because it allows you to specify which percentage of traffic is directed to each endpoint.
9. D. The start of a zone is defined by the SOA; therefore, all zones must have an SOA record by default.
10. D. Failover-based routing would best achieve this objective.
11. B. The CNAME record maps a name to another name. It should be used only when there are no other records on that name.
12. C. Amazon Route 53 performs three main functions: domain registration, DNS service, and health checking.
13. A. A TXT record is used to store arbitrary and unformatted text with a host.
14. C. The resource record sets contained in a hosted zone must share the same suffix.
15. B. DNS uses port number 53 to serve requests.
16. D. DNS primarily uses UDP to serve requests.
17. A. The TCP protocol is used by DNS server when the response data size exceeds 512 bytes or for tasks such as zone transfers.
18. B. Using Amazon Route 53, you can create two types of hosted zones: public hosted zones and private hosted zones.
19. D. Amazon Route 53 can route queries to a variety of AWS resources such as an Amazon CloudFront distribution, an Elastic Load Balancing load balancer, an Amazon EC2 instance, a website hosted in an Amazon S3 bucket, and an Amazon Relational Database (Amazon RDS).

20. D. You must first transfer the existing domain registration from another registrar to Amazon Route 53 to configure it as your DNS service.

Chapter 10: Amazon ElastiCache

1. A, B, C. Many types of objects are good candidates to cache because they have the potential to be accessed by numerous users repeatedly. Even the balance of a bank account could be cached for short periods of time if the back-end database query is slow to respond.
2. B, C. Amazon ElastiCache supports Memcached and Redis cache engines. MySQL is not a cache engine, and Couchbase is not supported.
3. C. The default limit is 20 nodes per cluster.
4. A. Redis clusters can only contain a single node; however, you can group multiple clusters together into a replication group.
5. B, C. Amazon ElastiCache is Application Programming Interface (API)-compatible with existing Memcached clients and does not require the application to be recompiled or linked against the libraries. Amazon ElastiCache manages the deployment of the Amazon ElastiCache binaries.
6. B, C. Amazon ElastiCache with the Redis engine allows for both manual and automatic snapshots. Memcached does not have a backup function.
7. B, C, D. Limit access at the network level using security groups or network ACLs, and limit infrastructure changes using IAM.
8. C. Amazon ElastiCache with Redis provides native functions that simplify the development of leaderboards. With Memcached, it is more difficult to sort and rank large datasets. Amazon Redshift and Amazon S3 are not designed for high volumes of small reads and writes, typical of a mobile game.
9. A. When the clients are configured to use AutoDiscovery, they can discover new cache nodes as they are added or removed. AutoDiscovery must be configured on each client and is not active server side. Updating the configuration file each time will be very difficult to manage. Using an Elastic Load Balancer is not recommended for this scenario.
10. A, B. Amazon ElastiCache supports both Memcached and Redis. You can run self-managed installations of Membase and Couchbase using Amazon Elastic Compute Cloud (Amazon EC2).

Chapter 11: Additional Key Services

1. B, C, E. Amazon CloudFront can use an Amazon S3 bucket or any HTTP server, whether or not it is running in Amazon EC2. A Route 53 Hosted Zone is a set of DNS resource records, while an Auto Scaling Group launches or terminates Amazon EC2 instances automatically. Neither can be specified as an origin server for a distribution.
2. A, C. The site in A is “popular” and supports “users around the world,” key indicators that CloudFront is appropriate. Similarly, the site in C is “heavily used,” and requires private content, which is supported by Amazon CloudFront. Both B and D are corporate use cases where the requests come from a single geographic location or appear to come from one (because of the VPN). These use cases will generally not see benefit from Amazon CloudFront.
3. C, E. Using multiple origins and setting multiple cache behaviors allow you to serve static and dynamic content from the same distribution. Origin Access Identifiers and signed URLs support serving private content from Amazon CloudFront, while multiple edge locations are simply how Amazon CloudFront serves any content.
4. B. Amazon CloudFront OAI is a special identity that can be used to restrict access to an Amazon S3 bucket only to an Amazon CloudFront distribution. Signed URLs, signed cookies, and IAM bucket policies can help to protect content served through Amazon CloudFront, but OAIs are the simplest way to ensure that only Amazon CloudFront has access to a bucket.
5. C. AWS Storage Gateway allows you to access data in Amazon S3 locally, with the Gateway-Cached volume configuration allowing you to expand a relatively small amount of local storage into Amazon S3.
6. B. Simple AD is a Microsoft Active Directory-compatible directory that is powered by Samba 4. Simple AD supports commonly used Active Directory features such as user accounts, group memberships, domain-joining Amazon Elastic Compute Cloud (Amazon EC2) instances running Linux and Microsoft Windows, Kerberos-based Single Sign-On (SSO), and group policies.
7. C. AWS KMS CMKs are the fundamental resources that AWS KMS manages. CMKs can never leave AWS KMS unencrypted, but data keys can.
8. D. AWS KMS uses envelope encryption to protect data. AWS KMS creates a data key, encrypts it under a Customer Master Key (CMK), and returns plaintext and encrypted versions of the data key to you. You use the plaintext key to encrypt data and store the encrypted key alongside the encrypted data. You can retrieve a plaintext data key only if you have the encrypted data key and you have permission to use the corresponding master key.
9. A. AWS CloudTrail records important information about each API call, including the name of the API, the identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS Cloud service.
10. B, C. Encryption context is a set of key/value pairs that you can pass to AWS KMS when you call the Encrypt, Decrypt, ReEncrypt, GenerateDataKey, and

GenerateDataKeyWithoutPlaintext APIs. Although the encryption context is not included in the ciphertext, it is cryptographically bound to the ciphertext during encryption and must be passed again when you call the Decrypt (or ReEncrypt) API. Invalid ciphertext for decryption is plaintext that has been encrypted in a different AWS account or ciphertext that has been altered since it was originally encrypted.

11. B. Because the Internet connection is full, the best solution will be based on using AWS Import/Export to ship the data. The most appropriate storage location for data that must be stored, but is very rarely accessed, is Amazon Glacier.
12. C. Because the job is run monthly, a persistent cluster will incur unnecessary compute costs during the rest of the month. Amazon Kinesis is not appropriate because the company is running analytics as a batch job and not on a stream. A single large instance does not scale out to accommodate the large compute needs.
13. D. The Amazon Kinesis services enable you to work with large data streams. Within the Amazon Kinesis family of services, Amazon Kinesis Firehose saves streams to AWS storage services, while Amazon Kinesis Streams provide the ability to process the data in the stream.
14. C. Amazon Data Pipeline allows you to run regular Extract, Transform, Load (ETL) jobs on Amazon and on-premises data sources. The best storage for large data is Amazon S3, and Amazon Redshift is a large-scale data warehouse service.
15. B. Amazon Kinesis Firehose allows you to ingest massive streams of data and store the data on Amazon S3 (as well as Amazon Redshift and Amazon Elasticsearch).
16. C. AWS OpsWorks uses Chef recipes to start new app server instances, configure application server software, and deploy applications. Organizations can leverage Chef recipes to automate operations like software configurations, package installations, database setups, server scaling, and code deployment.
17. A. With AWS CloudFormation, you can reuse your template to set up your resources consistently and repeatedly. Just describe your resources once and then provision the same resources over and over in multiple stacks.
18. B. AWS Trusted Advisor inspects your AWS environment and makes recommendations when opportunities exist to save money, improve system availability and performance, or help close security gaps. AWS Trusted Advisor draws upon best practices learned from the aggregated operational history of serving hundreds of thousands of AWS customers.
19. A. AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. With AWS Config, you can discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing.
20. D. AWS Elastic Beanstalk is the fastest and simplest way to get an application up and running on AWS. Developers can simply upload their application code, and the service automatically handles all the details such as resource provisioning, load balancing, Auto Scaling, and monitoring.

Chapter 12: Security on AWS

1. B. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.
2. C. The administrator password is encrypted with the public key of the key pair, and you provide the private key to decrypt the password. Then log in to the instance as the administrator with the decrypted password.
3. C. By default, network access is turned off to a DB Instance. You can specify rules in a security group that allows access from an IP address range, port, or Amazon Elastic Compute Cloud (Amazon EC2) security group.
4. A. Amazon S3 SSE uses one of the strongest block ciphers available, 256-bit AES.
5. C. IAM permits users to have no more than two active access keys at one time.
6. B. The shared responsibility model is the name of the model employed by AWS with its customers.
7. D. When you choose AWS KMS for key management with Amazon Redshift, there is a four-tier hierarchy of encryption keys. These keys are the master key, a cluster key, a database key, and data encryption keys.
8. D. Elastic Load Balancing supports the Server Order Preference option for negotiating connections between a client and a load balancer. During the SSL connection negotiation process, the client and the load balancer present a list of ciphers and protocols that they each support, in order of preference. By default, the first cipher on the client's list that matches any one of the load balancer's ciphers is selected for the SSL connection. If the load balancer is configured to support Server Order Preference, then the load balancer selects the first cipher in its list that is in the client's list of ciphers. This ensures that the load balancer determines which cipher is used for SSL connection. If you do not enable Server Order Preference, the order of ciphers presented by the client is used to negotiate connections between the client and the load balancer.
9. C. Amazon WorkSpaces uses PCoIP, which provides an interactive video stream without transmitting actual data.
10. C. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures.
11. A. A virtual MFA device uses a software application that generates six-digit authentication codes that are compatible with the TOTP standard, as described in RFC 6238.
12. B, D. Amazon DynamoDB does not have a server-side feature to encrypt items within a table. You need to use a solution outside of DynamoDB such as a client-side library to encrypt items before storing them, or a key management service like AWS Key Management Service to manage keys that are used to encrypt items before storing them in DynamoDB.

13. B. If your private key can be read or written to by anyone but you, then SSH ignores your key.
14. D. Amazon Cognito Identity supports public identity providers—Amazon, Facebook, and Google—as well as unauthenticated identities.
15. A. An instance profile is a container for an IAM role that you can use to pass role information to an Amazon EC2 instance when the instance starts.
16. B. A network ACL is an optional layer of security for your Amazon VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your Amazon VPC.
17. D. The Signature Version 4 signing process describes how to add authentication information to AWS requests. For security, most requests to AWS must be signed with an access key (Access Key ID [AKI] and Secret Access Key [SAK]). If you use the AWS Command Line Interface (AWS CLI) or one of the AWS Software Development Kits (SDKs), those tools automatically sign requests for you based on credentials that you specify when you configure the tools. However, if you make direct HTTP or HTTPS calls to AWS, you must sign the requests yourself.
18. B. Dedicated instances are physically isolated at the host hardware level from your instances that aren't dedicated instances and from instances that belong to other AWS accounts.
19. C. Amazon EMR starts your instances in two Amazon Elastic Compute Cloud (Amazon EC2) security groups, one for the master and another for the slaves. The master security group has a port open for communication with the service. It also has the SSH port open to allow you to securely connect to the instances via SSH using the key specified at startup. The slaves start in a separate security group, which only allows interaction with the master instance. By default, both security groups are set up to prevent access from external sources, including Amazon EC2 instances belonging to other customers. Because these are security groups in your account, you can reconfigure them using the standard Amazon EC2 tools or dashboard.
20. A. When you create an Amazon EBS volume in an Availability Zone, it is automatically replicated within that Availability Zone to prevent data loss due to failure of any single hardware component. An EBS Snapshot creates a copy of an EBS volume to Amazon S3 so that copies of the volume can reside in different Availability Zones within a region.

Chapter 13: AWS Risk and Compliance

1. A, B, C. Answers A through C describe valid mechanisms that AWS uses to communicate with customers regarding its security and control environment. AWS does not allow customers' auditors direct access to AWS data centers, infrastructure, or staff.
2. C. The shared responsibility model can include IT controls, and it is not just limited to security considerations. Therefore, answer C is correct.
3. A. AWS provides IT control information to customers through either specific control definitions or general control standard compliance.
4. A, B, D. There is no such thing as a SOC 4 report, therefore answer C is incorrect.
5. A. IT governance is still the customer's responsibility.
6. D. Any number of components of a workload can be moved into AWS, but it is the customer's responsibility to ensure that the entire workload remains compliant with various certifications and third-party attestations.
7. B. An Availability Zone consists of multiple discrete data centers, each with their own redundant power and networking/connectivity, therefore answer B is correct.
8. A, C. AWS regularly scans public-facing, non-customer endpoint IP addresses and notifies appropriate parties. AWS does not scan customer instances, and customers must request the ability to perform their own scans in advance, therefore answers A and C are correct.
9. B. AWS publishes information publicly online and directly to customers under NDA, but customers are not required to share their use and configuration information with AWS, therefore answer B is correct.
10. C. AWS has developed a strategic business plan, and customers should also develop and maintain their own risk management plans, therefore answer C is correct.
11. B. The collective control environment includes people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of AWS control framework. Energy is not a discretely identified part of the control environment, therefore B is the correct answer.
12. D. Customers are responsible for ensuring all of their security group configurations are appropriate for their own applications, therefore answer D is correct.
13. C. Customers should ensure that they implement control objectives that are designed to meet their organization's own unique compliance requirements, therefore answer C is correct.

Chapter 14: Architecture Best Practices

1. B, E. Amazon Kinesis is a platform for streaming data on AWS, offering powerful services to make it easy to load and analyze streaming data. Amazon SQS is a fast, reliable, scalable, and fully managed message queuing service. Amazon SQS makes it simple and cost-effective to decouple the components of a cloud application.
2. B, C. Launching instances across multiple Availability Zones helps ensure the application is isolated from failures in a single Availability Zone, allowing the application to achieve higher availability. Whether you are running one Amazon EC2 instance or thousands, you can use Auto Scaling to detect impaired Amazon EC2 instances and unhealthy applications and replace the instances without your intervention. This ensures that your application is getting the compute capacity that you expect, thereby maintaining your availability.
3. A, E. Amazon DynamoDB runs across AWS proven, high-availability data centers. The service replicates data across three facilities in an AWS region to provide fault tolerance in the event of a server failure or Availability Zone outage. Amazon S3 provides durable infrastructure to store important data and is designed for durability of 99.999999999% of objects. Your data is redundantly stored across multiple facilities and multiple devices in each facility. While Elastic Load Balancing and Amazon ElastiCache can be deployed across multiple Availability Zones, you must explicitly take such steps when creating them.
4. A, D. Auto Scaling enables you to follow the demand curve for your applications closely, reducing the need to provision Amazon EC2 capacity manually in advance. For example, you can set a condition to add new Amazon EC2 instances in increments to the Auto Scaling group when the average CPU and network utilization of your Amazon EC2 fleet monitored in Amazon CloudWatch is high; similarly, you can set a condition to remove instances in the same increments when CPU and network utilization are low.
5. B, D, E. There is no direct way to encrypt an existing unencrypted volume. However, you can migrate data between encrypted and unencrypted volumes.
6. A, C, D. The attack surface is composed of the different Internet entry points that allow access to your application. The strategy to minimize the attack surface area is to (a) reduce the number of necessary Internet entry points, (b) eliminate non-critical Internet entry points, (c) separate end user traffic from management traffic, (d) obfuscate necessary Internet entry points to the level that untrusted end users cannot access them, and (e) decouple Internet entry points to minimize the effects of attacks. This strategy can be accomplished with Amazon VPC.
7. C. Amazon RDS read replicas provide enhanced performance and durability for Amazon RDS instances. This replication feature makes it easy to scale out elastically beyond the capacity constraints of a single Amazon RDS instance for read-heavy database workloads. You can create one or more replicas of a given source Amazon RDS instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput.
8. A. An alias resource record set can point to an ELB. You cannot create a CNAME record

at the top node of a Domain Name Service (DNS) namespace, also known as the zone apex, as the case in this example. Alias resource record sets can save you time because Amazon Route 53 automatically recognizes changes in the resource record sets to which the alias resource record set refers.

9. D. An instance profile is a container for an AWS Identity and Access Management (IAM) role that you can use to pass role information to an Amazon EC2 instance when the instance starts. The IAM role should have a policy attached that only allows access to the AWS Cloud services necessary to perform its function.
10. B. Amazon API Gateway is a fully managed service that makes it easy for developers to publish, maintain, monitor, and secure APIs at any scale. You can create an API that acts as a "front door" for applications to access data, business logic, or functionality from your code running on AWS Lambda. Amazon API Gateway handles all of the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management.
11. C. Amazon EFS is a file storage service for Amazon EC2 instances. Multiple Amazon EC2 instances can access an Amazon EFS file system at the same time, providing a common data source for the content of the WordPress site running on more than one instance.
12. A. Amazon DynamoDB is a NoSQL database store that is a great choice as an alternative due to its scalability, high-availability, and durability characteristics. Many platforms provide open-source, drop-in replacement libraries that allow you to store native sessions in Amazon DynamoDB. Amazon DynamoDB is a great candidate for a session storage solution in a share-nothing, distributed architecture.
13. B. Amazon SQS is a fast, reliable, scalable, and fully managed message queuing service. Amazon SQS should be used to decouple the large volume of inbound transactions, allowing the back-end services to manage the level of throughput without losing messages.
14. B, C, E. You should protect AWS user access keys like you would your credit card numbers or any other sensitive secret. Use different access keys for different applications so that you can isolate the permissions and revoke the access keys for individual applications if an access key is exposed. Remember to change access keys on a regular basis. For increased security, it is recommended to configure MFA for any sensitive operations. Remember to remove any IAM users that are no longer needed so that the user's access to your resources is removed. Always avoid having to embed access keys in an application.
15. A, B, E. You can enable AWS CloudTrail in your AWS account to get logs of API calls and related events' history in your account. AWS CloudTrail records all of the API access events as objects in an Amazon S3 bucket that you specify at the time you enable AWS CloudTrail. You can take advantage of Amazon S3's bucket notification feature by directing Amazon S3 to publish object-created events to AWS Lambda. Whenever AWS CloudTrail writes logs to your Amazon S3 bucket, Amazon S3 can then invoke your AWS Lambda function by passing the Amazon S3 object-created event as a parameter. The AWS Lambda function code can read the log object and process the access records logged by AWS CloudTrail.

16. B. Amazon Glacier enables businesses and organizations to retain data for months, years, or decades, easily and cost effectively. With Amazon Glacier, customers can retain more of their data for future analysis or reference, and they can focus on their business instead of operating and maintaining their storage infrastructure. Customers can also use Amazon Glacier Vault Lock to meet regulatory and compliance archiving requirements.
17. A. Many companies that distribute content via the Internet want to restrict access to documents, business data, media streams, or content that is intended for selected users, such as users who have paid a fee. To serve this private content securely using Amazon CloudFront, you can require that users access your private content by using special Amazon CloudFront-signed URLs or signed cookies.
18. B. Amazon S3 provides highly durable and available storage for a variety of content. Amazon S3 can be used as a big data object store for all of the videos. Amazon S3's low cost combined with its design for durability of 99.999999999% and for up to 99.99% availability make it a great storage choice for transcoding services.
19. A. An Availability Zone consists of one or more physical data centers. Availability zones within a region provide inexpensive, low-latency network connectivity to other zones in the same region. This allows you to distribute your application across data centers. In the event of a catastrophic failure in a data center, the application will continue to handle requests.
20. C. You can use a NAT gateway to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances. If you have resources in multiple Availability Zones and they share one NAT gateway, resources in the other Availability Zones lose Internet access in the event that the NAT gateway's Availability Zone is down. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.