Chapter 1: The Cloud

1. C. Having globally distributed infrastructure and experienced security engineers makes a provider's infrastructure more reliable. Metered pricing makes a wider range of workloads possible.

2. A, D. Security and virtualization are both important characteristics of successful cloud workloads, but neither will directly impact availability.

3. B, D. Security and scalability are important cloud elements but are not related to metered pricing.

4. A, B. Security and elasticity are important but are not directly related to server virtualization.

5. D. A hypervisor is software (not hardware) that administrates virtualized operations.

6. B. Sharding, aggregating remote resources, and abstracting complex infrastructure can all be accomplished using virtualization techniques, but they aren't, of themselves, virtualization.

7. C. PaaS products mask complexity, SaaS products provide end-user services, and serverless architectures (like AWS Lambda) let developers run code on cloud servers.

8. A. IaaS products provide full infrastructure access, SaaS products provide end-user services, and serverless architectures (like AWS Lambda) let developers run code on cloud servers.

9. B. IaaS products provide full infrastructure access, PaaS products mask complexity, and serverless architectures (like AWS Lambda) let developers run code on cloud servers.

10. A. Increasing or decreasing compute resources better describes elasticity. Efficient use of virtualized resources and billing models aren't related directly to scalability.

11. C. Preconfiguring compute instances before they're used to scale up an application is an element of scalability rather than elasticity. Efficient use of virtualized resources and billing models aren't related directly to elasticity.

12. A, D. Capitalized assets and geographic reach are important but don't have a direct impact on operational scalability.

Chapter 2: Understanding Your AWS Account

1. D. Only the t2.micro instance type is Free Tier–eligible, and any combination of t2.micro instances can be run up to a total of 750 hours per month.

2. B, C. S3 buckets—while available in such volumes under the Free Tier—are not necessary for an EC2 instance. Since the maximum total EBS space allowed by the Free Tier is 30 GB, two 20 GB would not be covered.

3. B, D. The API calls/month and ECR free storage are available only under the Free Tier.

4. A, B. There is no Top Free Tier Services Dashboard or, for that matter, a Billing Preferences Dashboard.

5. C. Wikipedia pages aren't updated or detailed enough to be helpful in this respect. The AWS CLI isn't likely to have much (if any) pricing information. The TCO Calculator shouldn't be used for specific and up-to-date information about service pricing.

6. A. Pricing will normally change based on the volume of service units you consume and, often, between AWS Regions.

7. B. You can, in fact, calculate costs for a multiservice stack. The calculator pricing is kept up-to-date. You can specify very detailed configuration parameters.

8. C, D. Calculate By Month Or Year is not an option, and since the calculator calculates only cost by usage, Include Multiple Organizations wouldn't be a useful option.

9. A. The calculator covers all significant costs associated with an on-premises deployment but doesn't include local or national tax implications.

10. D. The currency you choose to use will have little impact on price—it's all relative, of course. The guest OS and region will make a difference, but it's relatively minor.

11. B. The correct URL is `https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html`.

12. A. Resource limits exist only within individual regions; the limits in one region don't impact another. There's no logistical reason that customers can't scale up deployments at any rate. There are, in fact, no logical limits to the ability of AWS resources to scale upward.

13. D. While most service limits are soft and can be raised on request, there are some service limits that are absolute.

14. D. The Cost Explorer and Cost and Usage Reports pages provide more in-depth and/or customized details. Budgets allow you to set alerts based on usage.

15. C. Reservation budgets track the status of any active reserved instances on your account. Cost budgets monitor costs being incurred against your account. There is no budget type that correlates usage per unit cost to understand your account cost efficiency.

16. D. You can configure the period, instance type, and start/stop dates for a budget, but you can't filter by resource owner.

17. A. Billing events aren't triggers for alerts. Nothing in this chapter discusses intrusion events.

18. C. Tags are passive, so they can't automatically trigger anything. Resource tags—not cost allocation tags—are meant to help you understand and control deployments. Tags aren't associated with particular billing periods.

19. A, C. Companies with multiple users of resources in a single AWS account would not benefit from AWS Organizations, nor would a company with completely separated units. The value of AWS Organizations is in integrating the administration of related accounts.

20. B. Budgets are used to set alerts. Reports provide CSV-formatted data for offline processing. Consolidated Billing (now migrated to AWS Organizations) is for administrating resources across multiple AWS accounts.

Chapter 3: Getting Support on AWS

1. C. The Basic plan won't provide any personalized support. The Developer plan is cheaper, but there is limited access to support professionals. The Business plan does offer 24/7 email, chat, and phone access to an engineer, so until you actually deploy, this will make the most sense. At a $15,000 monthly minimum, the Enterprise plan won't be cost effective.

2. B. Using the public documentation available through the Basic plan won't be enough to address your specific needs. The Business and Enterprise plans are not necessary as you don't yet have production deployments.

3. D. The lower three support tiers provide limited access to only lower-level support professionals, while the Enterprise plan provides full access to senior engineers and dedicates a technical account manager (TAM) as your resource for all your AWS needs.

4. C. Basic plan customers are given customer support access only for account management issues and not for technical support or security breaches.

5. B. The TAM is available only for Enterprise Support customers. The primary function is one of guidance and advocacy.

6. B. Only the Business and Enterprise plans include help with troubleshooting interoperability between AWS resources and third-party software and operating systems. The Business plan is the least expensive that will get you this level of support.

7. A. The Developer plan costs the greater of $29 or 3 percent of the monthly usage. In this case, 3 percent of the month's usage is $120.

8. D. The Business plan—when monthly consumption falls between $10,000 and $80,000—costs the greater of $100 or 7 percent of the monthly usage. In this case, 7 percent of a single month's usage ($11,000) is $770. The three month total would, therefore, be $2,310.

9. C. The AWS Professional Services site includes tech talk webinars, white papers, and blog posts. The Basic Support plan includes AWS documentation resources. The Knowledge Center consists of FAQ documentation.

10. A. The TAM is an AWS employee dedicated to guiding your developer and admin teams. There is no such thing as a network appliance for workload testing.

11. B, C. Although DOC and DocBook are both popular and useful formats, neither is used by AWS for its documentation.

12. A, C. The `compare-plans` page provides general information about support plans, and the `professional-services` site describes accessing that particular resource. Neither directly includes technical guides.

13. D. The Knowledge Center is a FAQ for technical problems and their solutions. The main documentation site is much better suited to introduction-level guides. The `https://forums.aws.amazon.com` site is the discussion forum for AWS users.

14. B. The Knowledge Center is a general FAQ for technical problems and their solutions. The `docs.aws.amazon.com` site is for general documentation. There is no `https://aws.amazon.com/security/encryption` page.

15. A. Version numbers are not publicly available, and the word *Current* isn't used in this context.

16. C. Replication is, effectively, a subset of Fault Tolerance and therefore would not require its own category.

17. A. Performance identifies configuration settings that might be blocking performance improvements. Security identifies any failures to use security best-practice configurations. Cost Optimization identifies any resources that are running and unnecessarily costing you money.

18. B. Performance identifies configuration settings that might be blocking performance improvements. Service Limits identifies resource usage that's approaching AWS Region or service limits. There is no Replication category.

19. A. An OK status for a failed state is a false negative. There is no single status icon indicating that your account is completely compliant in Trusted Advisor.

20. B, D. Both the MFA and Service Limits checks are available for all accounts.

Chapter 4: Understanding the AWS Environment

1. B. The letter (a, b…) at the end of a designation indicates an Availability Zone. us-east-1 would never be used for a Region in the western part of the United States.

2. D. The AWS GovCloud Region is restricted to authorized customers only. Asia Pacific (Tokyo) is a normal Region. AWS Admin and US-DOD don't exist (as far as we know, at any rate).

3. D. EC2 instances will automatically launch into the Region you currently have selected. You can manually select the subnet that's associated with a particular Availability Zone for your new EC2 instance, but there's no default choice.

4. B, D. Relational Database Service (RDS) and EC2 both use resources that can exist in only one Region. Route 53 and CloudFront are truly global services in that they're not located in or restricted to any single AWS Region.

5. C. The correct syntax for an endpoint is `<service-designation>.<region-designation>.amazonaws.com`—meaning, in this case, `rds.us-east-1.amazonaws.com`.

6. B, C. For most uses, distributing your application infrastructure between multiple AZs within a single Region gives them sufficient fault tolerance. While AWS services do enjoy a significant economy of scale—bring prices down—little of that is due to the structure of their Regions. Lower latency and compliance are the biggest benefits from this list.

7. A. Sharing a single resource among Regions wouldn't cause any particular security, networking, or latency problems. It's a simple matter of finding a single physical host device to run on.

8. B. Auto Scaling is an important working element of application high availability, but it's not what most directly drives it (that's load balancing). The most effective and efficient way to get the job done is through parallel, load-balanced instances in multiple Availability Zones, not Regions.

9. A. "Data centers running uniform host types" would describe an edge location. The data centers within a "broad geographic area" would more closely describe an AWS Region. AZs aren't restricted to a single data center.

10. C. Imposing virtual networking limits on an instance would be the job of a security group or access control list. IP address blocks are not assigned at the Region level. Customers have no access to or control over AWS networking hardware.

11. B. AWS displays AZs in (apparently) random order to prevent too many resources from being launched in too few zones.

12. D. Auto Scaling doesn't focus on any one resource (physical or virtual) because it's interested only in the appropriate availability and quality of the overall *service*. The job of orchestration is for load balancers, not autoscalers.

13. C. Resource isolation can play an important role in security, but not reliability. Automation can improve administration processes, but neither it, nor geolocation, is the most effective reliability strategy.

14. A, C. RDS database instances and Lambda functions are not qualified CloudFront origins. EC2 load balancers can be used as CloudFront origins.

15. D. CloudFront can't protect against spam and, while it can complement your application's existing redundancy and encryption, those aren't its primary purpose.

16. B. Countering the threat of DDoS attacks is the job of AWS Shield. Protecting web applications from web-based threats is done by AWS Web Application Firewall. Using Lambda to customize CloudFront behavior is for Lambda Edge.

17. A, B. What's *in* the cloud is your responsibility—it includes the administration of EC2-based operating systems.

18. C. There's no one easy answer, as some managed services are pretty much entirely within Amazon's sphere, and others leave lots of responsibility with the customer. Remember, "if you can edit it, you own it."

19. D. The AWS Billing Dashboard is focused on your account billing issues. Neither the AWS Acceptable Use Monitor nor the Service Status Dashboard actually exists. But nice try.

20. B. The correct document (and web page `https://aws.amazon.com/aup/`) for this information is the AWS Acceptable Use Policy.

Chapter 5: Securing Your AWS Resources

1. A. Identity and Access Management (IAM) is primarily focused on helping you control access to your AWS resources. KMS handles access keys. EC2 manages SSH key pairs. While IAM does touch on federated management, that's not its primary purpose.

2. A, B, D. Including a space or null character is not a password policy option.

3. C, D. The root user should *not* be used for day-to-day admin tasks—even as part of an "admin" group. The goal is to protect root as much as possible.

4. D. MFA requires at least two ("multi") authentication methods. Those will normally include a password (something you know) and a token sent to either a virtual or physical MFA device (something you have).

5. B. The `-i` argument should point to the name (and location) of the key stored on the local (client) machine. By default, the admin user on an Amazon Linux instance is named `ec2-user`.

6. B. While assigning permissions and policy-based roles will work, it's not nearly as efficient as using groups, where you need to set or update permissions only once for multiple users.

7. C. An IAM role is meant to be assigned to a trusted entity (like another AWS service or a federated identity). A "set of permissions" could refer to a policy. A set of IAM users could describe a group.

8. A, D. Federated identities are for permitting authenticated entities access to AWS resources and data. They're not for importing anything from external accounts—neither data nor guidance.

9. C, D. Secure Shell (SSH) is an encrypted remote connectivity protocol, and SSO (single sign-on) is an interface feature—neither is a standard for federated identities.

10. D. The credential report focuses only on your users' passwords, access keys, and MFA status. It doesn't cover actual activities or general security settings.

11. B. The credential report is saved to the comma-separated values (spreadsheet) format.

12. A. Your admin user will need broad access to be effective, so AmazonS3FullAccess and AmazonEC2FullAccess—which open up only S3 and EC2, respectively—won't be enough. There is no AdminAccess policy.

13. D. "Programmatic access" users don't sign in through the AWS Management Console; they access through APIs or the AWS CLI. They would therefore not need passwords or MFA. An access key ID alone without a matching secret access key is worthless.

14. B. When the correct login page (such as `https://291976716973.signin.aws.amazon.com/console`) is loaded, an IAM user only needs to enter a username and a valid password. Account numbers and secret access keys are not used for this kind of authentication.

15. C. In-transit encryption requires that the data be encrypted on the remote client before uploading. Server-side encryption (either SSE-S3 or SSE-KMS) only encrypts data within S3 buckets. DynamoDB is a NoSQL database service.

16. A. You can only encrypt an EBS volume at creation, not later.

17. D. A client-side master key is used to encrypt objects before they reach AWS (specifically S3). There are no keys commonly known as either SSH or KMS master keys.

18. C. SSE-KMS are KMS-managed server-side keys. FedRAMP is the U.S. government's Federal Risk and Authorization Management Program (within which transaction data protection plays only a relatively minor role). ARPA is the Australian Prudential Regulation Authority.

19. B. SOC isn't primarily about guidance or risk assessment, and it's definitely not a guarantee of the state of your own deployments. SOC reports are reports of audits *on* AWS infrastructure that you can use as part of your own reporting requirements

20. A, B. AWS Artifact documents are about AWS infrastructure compliance with external standards. They tangentially can also provide insight into best practices. They do *not* represent internal AWS design or policies.

Chapter 6: Working with Your AWS Resources

1. D. You can sign in as the root user or as an IAM user. Although you need to specify the account alias or account ID to log in as an IAM user, those are not credentials. You can't log in to the console using an access key ID.

2. B. Once you're logged in, your session will remain active for 12 hours. After that, it'll expire and log you out to protect your account.

3. A. If a resource that should be visible appears to be missing, you may have the wrong Region selected. Since you're logged in as the root, you have view access to all resources in your account. You don't need an access key to use the console. You can't select an Availability Zone in the navigation bar.

4. C. Each resource tag you create must have a key, but a value is optional. Tags don't have to be unique within an account, and they are case-sensitive.

5. A. The AWS CLI requires an access key ID and secret key. You can use those of an IAM user or the root user. Outbound network access to TCP port 443 is required, not port 80. Linux is also not required, although you can use the AWS CLI with Linux, macOS, or Windows. You also can use the AWS Console Mobile Application with Android or iOS devices.

6. A, D. You can use Python and the pip package manager or (with the exception of Windows Server 2008) the MSI installer to install the AWS CLI on Windows. AWS SDKs don't include the AWS CLI. Yum and Aptitude are package managers for Linux only.

7. B. The `aws configure` command walks you through setting up the AWS CLI to specify the default Region you want to use as well as your access key ID and secret key. The `aws --version` command displays the version of the AWS CLI installed, but running this command isn't necessary to use the AWS CLI to manage your resources. Rebooting is also not necessary. Using your root user to manage your AWS resources is insecure, so there's no need to generate a new access key ID for your root user.

8. C. The AWS CLI can display output in JSON, text, or table formats. It doesn't support CSV or TSV.

9. B, D, E. AWS offers SDKs for JavaScript, Java, and PHP. There are no SDKs for Fortran. JSON is a format for representing data, not a programming language.

10. A, B. The AWS Mobile SDK for Unity and the AWS Mobile SDK for .NET and Xamarin let you create mobile applications for both Android and Apple iOS devices. The AWS SDK for Go doesn't enable development of mobile applications for these devices. The AWS Mobile SDK for iOS supports development of applications for Apple iOS devices but not Android.

11. A, B. AWS IoT device SDKs are available for C++, Python, Java, JavaScript, and Embedded C. There isn't one available for Ruby or Swift.

12. A, B. The AWS CLI is a program that runs on Linux, macOS, or Windows and allows you to interact with AWS services from a terminal. The AWS SDKs let you use your favorite programming language to write applications that interact with AWS services.

13. B. CloudWatch metrics store performance data from AWS services. Logs store text-based logs from applications and AWS services. Events are actions that occur against your AWS resources. Alarms monitor metrics. Metric filters extract metric information from logs.

14. D. A CloudWatch alarm monitors a metric and triggers when that metric exceeds a specified threshold. It will not trigger if the metric doesn't change. Termination of an EC2 instance is an event, and you can't create a CloudWatch alarm to trigger based on an event. You also can't create an alarm to trigger based on the presence of an IP address in a web server log. But you could create a metric filter to look for a specific IP address in the log and increment a custom metric when that IP address appears in the log.

15. A, C. SNS supports the SMS and SQS protocols for sending notifications. You can't send a notification to a CloudWatch event. There is no such thing as a mobile pull notification.

16. C, D. CloudWatch Events monitors events that cause changes in your AWS resources as well as AWS Management Console sign-in events. In response to an event, CloudWatch

Events can take an action including sending an SNS notification or rebooting an EC2 instance. CloudWatch Events can also perform actions on a schedule. It doesn't monitor logs or metrics.

17. B, D. Viewing an AWS resource triggers an API action regardless of whether it's done using the AWS Management Console or the AWS CLI. Configuring the AWS CLI doesn't trigger any API actions. Logging into the AWS Management Console doesn't trigger an API action.

18. A. The CloudTrail event history log stores the last 90 days of management events for each Region. Creating a trail is overkill and not as cost-effective since it would involve storing logs in an S3 bucket. Streaming CloudTrail logs to CloudWatch would require creating a trail. CloudWatch Events doesn't log management events.

19. A, D. Creating a trail in the Region where the bucket exists will generate CloudTrail logs, which you can then stream to CloudWatch for viewing and searching. CloudTrail event history doesn't log data events. CloudTrail logs global service events by default, but S3 data events are not included.

20. B. Log file integrity validation uses cryptographic hashing to help you assert that no CloudTrail log files have been deleted from S3. It doesn't prevent tampering or deletion and can't tell you how a file has been tampered with. Log file integrity validation has nothing to do with CloudWatch.

21. D. The costs and usage reports show you your monthly spend by service. The reserved instances reports and reserved instance recommendations don't show actual monthly costs.

22. A. RDS lets you purchase reserved instances to save money. Lambda, S3, and Fargate don't use instances.

23. B. The reservation utilization report shows how much you have saved using reserved instances. The reservation coverage report shows how much you could have potentially saved had you purchased reserved instances. The daily costs and monthly EC2 running hours costs and usage reports don't know how much you've saved using reserved instances.

24. D. Cost Explorer will make reservation recommendations for EC2, RDS, ElastiCache, Redshift, and Elasticsearch instances. You need to select the service you want it to analyze for recommendations. But Cost Explorer will not make recommendations for instances that are already covered by reservations. Because your Elasticsearch instances have been running continuously for at least the past seven days, that usage would be analyzed.

Chapter 7: The Core Compute Services

1. C. An instance's hardware profile is defined by the instance type. High-volume (or low-volume) data processing operations and data streams can be handled using any storage volume or on any instance (although some may be better optimized than others).

2. A. The Quick Start includes only the few dozen most popular AMIs. The Community tab includes thousands of publicly available AMIs—whether verified or not. The My AMIs tab only includes AMIs created from your account.

3. B, C. AMIs can be created that provide both a base operating system and a pre-installed application. They would not, however, include any networking or hardware profile information—those are largely determined by the instance type.

4. B, D. c5d.18xlarge and t2.micro are the names of EC2 instance types, not instance type families.

5. D. A virtual central processing unit (vCPU) is a metric that roughly measures an instance type's compute power in terms of the number of processors on a physical server. It has nothing to do with resilience to high traffic, system memory, or the underlying AMI.

6. A. An EC2 instance that runs on a physical host reserved for and controlled by a single AWS account is called a dedicated host. A dedicated host is not an AMI, nor is it an instance type.

7. C. A virtualized partition of a physical storage drive that is directly connected to the EC2 instance it's associated with is known as an instance store volume. A software stack archive packaged to make it easy to copy and deploy to an EC2 instance describes an EC2 AMI. It's possible to encrypt EBS volumes, but encryption doesn't define them.

8. C, D. Instance store volumes cannot be encrypted, nor will their data survive an instance shutdown. Those are features of EBS volumes.

9. B. Spot instances are unreliable for this sort of usage since they can be shut down unexpectedly. Reserved instances make economic sense where they'll be used 24/7 over long stretches of time. "Dedicated" isn't a pricing model.

10. D. Reserved instances will work here because your "base" instances will need to run 24/7 over the long term. Spot and spot fleet instances are unreliable for this sort of usage since they can be shut down unexpectedly. On-demand instances will incur unnecessarily high costs over such a long period.

11. A. There's no real need for guaranteed available capacity since it's extremely rare for AWS to run out. You choose how you'll pay for a reserved instance. All Upfront, Partial Upfront, and No Upfront are available options, and there is no automatic billing. An instance would never be launched automatically in this context.

12. A, C. Because spot instances can be shut down, they're not recommended for applications that provide any kind of always-on service.

13. C, D. Elastic Block Store provides storage volumes for Lightsail and Beanstalk (and for EC2, for that matter). Elastic Compute Cloud (EC2) provides application deployment, but no one ever accused it of being simple.

14. A. Beanstalk, EC2 (non-reserved instances), and RDS all bill according to actual usage.

15. B, D. Ubuntu is an OS, not a stack. WordPress is an application, not an OS.

16. B, C. Elastic Block Store is, for practical purposes, an EC2 resource. RDS is largely built on its own infrastructure.

17. A, C. While you could, in theory at least, manually install Docker Engine on either a Lightsail or EC2 instance, that's not their primary function.

18. A, B. Both Lambda and Lightsail are compute services that—while they might possibly make use of containers under the hood—are not themselves container technologies.

19. D. Python is, indeed, a valid choice for a function's runtime environment. There is no one "primary" language for Lambda API calls.

20. A. While the maximum time was, at one point, 5 minutes, that's been changed to 15.

Chapter 8: The Core Storage Services

1. B. Bucket names must be globally unique across AWS, irrespective of Region. The length of the bucket name isn't an issue since it's between 3 and 63 characters long. Storage classes are configured on a per-object basis and have no impact on bucket naming.

2. A, C. STANDARD_IA and GLACIER storage classes offer the highest levels of redundancy and are replicated across at least three Availability Zones. Due to their low level of availability (99.9 and 99.5 percent, respectively), they're the most cost-effective for infrequently accessed data. ONEZONE_IA stores objects in only one Availability Zone, so the loss of that zone could result in the loss of all objects. The STANDARD and INTELLIGENT_TIERING classes provide the highest levels of durability and cross-zone replication but are also the least cost-effective for this use case.

3. A, D. S3 is an object storage service, while EBS is a block storage service that stores volumes. EBS snapshots are stored in S3. S3 doesn't store volumes, and EBS doesn't store objects.

4. A, B, D. Object life cycle configurations can perform transition or expiration actions based on an object's age. Transition actions can move objects between storage classes, such as between STANDARD and GLACIER. Expiration actions can delete objects and object versions. Object life cycle configurations can't delete buckets or move objects to an EBS volume.

5. A, B. You can use bucket policies or access control lists (ACLs) to grant anonymous users access to an object in S3. You can't use user policies to do this, although you can use them to grant IAM principals access to objects. Security groups control access to resources in a virtual private cloud (VPC) and aren't used to control access to objects in S3.

6. C, D. Both S3 and Glacier are designed for durable, long-term storage and offer the same level of durability. Data stored in Glacier can be reliably retrieved within eight hours using the Expedited or Standard retrieval options. Data stored in S3 can be retrieved even faster than Glacier. S3 can store objects up to 5 TB in size, and Glacier can store archives up to 40 TB. Both S3 or Glacier will meet the given requirements, but Glacier is the more cost-effective solution.

7. B. You can create or delete vaults from the Glacier service console. You can't upload, download, or delete archives. To perform archive actions, you must use the AWS Command Line Interface, an AWS SDK, or a third-party program. Glacier doesn't use buckets.

8. D. The Standard retrieval option typically takes 3 to 5 hours to complete. Expedited takes 1 to 5 minutes, and Bulk takes 5 to 12 hours. There is no Provisioned retrieval option, but you can purchase provisioned capacity to ensure Expedited retrievals complete in a timely manner.

9. A. A Glacier archive can be as small as 1 byte and as large as 40 TB. You can't have a zero-byte archive.

10. B, D. The tape gateway and volume gateway types let you connect to iSCSI storage. The file gateway supports NFS. There's no such thing as a cached gateway.

11. B. All AWS Storage Gateway types—file, volume, and tape gateways—primarily store data in S3 buckets. From there, data can be stored in Glacier or EBS snapshots, which can be instantiated as EBS volumes.

12. A, B, D, E. The AWS Storage Gateway allows transferring files from on-premises servers to S3 using industry-standard storage protocols. The AWS Storage Gateway functioning as a file gateway supports the SMB and NFS protocols. As a volume gateway, it supports the iSCSI protocol. AWS Snowball and the AWS CLI also provide ways to transfer data to S3, but using them requires installing third-party software.

13. A, C, E. The volume gateway type offers two configurations: stored volumes and cached volumes. Stored volumes store all data locally and asynchronously back up that data to S3 as EBS snapshots. Stored volumes can be up to 16 TB in size. In contrast, cached volumes locally store only a frequently used subset of data but do not asynchronously back up the data to S3 as EBS snapshots. Cached volumes can be up to 32 TB in size.

14. C. The 80 TB Snowball device offers 72 TB of usable storage and is the largest available. The 50 TB Snowball offers 42 TB of usable space.

15. A, B. AWS Snowball enforces encryption at rest and in transit. It also uses a TPM chip to detect unauthorized changes to the hardware or software. Snowball doesn't use NFS encryption, and it doesn't have tamper-resistant network ports.

16. C. If AWS detects any signs of tampering or damage, it will not replace the TPM chip or transfer customer data from the device. Instead, AWS will securely erase it.

17. B. The Snowball Client lets you transfer files to or from a Snowball using a machine running Windows, Linux, or macOS. It requires no coding knowledge, but the S3 SDK Adapter for Snowball does. Snowball doesn't support the NFS, iSCSI, or SMB storage protocols.

18. A, D. Snowball Edge offers compute power to run EC2 instances and supports copying files using the NFSv3 and NFSv4 protocols. Snowball devices can't be clustered and don't have a QFSP+ port.

19. B. The Snowball Edge—Compute Optimized with GPU option is optimized for machine learning and high-performance computing applications. Although the Compute Optimized and Storage Optimized options could work, they aren't the best choices. There's no Network Optimized option.

20. B. Snowball Edge with the Compute Optimized configuration includes a QSFP+ network interface that supports up to 100 Gbps. The Storage Optimized configuration has a QSFP+ port that supports only up to 40 Gbps. The 80 TB Snowball supports only up to 10 Gbps. A storage gateway is a virtual machine, not a hardware device.

Chapter 9: The Core Database Services

1. B. A relational database stores data in columns called attributes and rows called records. Nonrelational databases—including key-value stores and document stores—store data in collections or items but don't use columns or rows.

2. B. The SQL `INSERT` statement can be used to add data to a relational database. The `QUERY` command is used to read data. `CREATE` can be used to create a table but not add data to it. `WRITE` is not a valid SQL command.

3. D. A nonrelational database is schemaless, meaning that there's no need to predefine all the types of data you'll store in a table. This doesn't preclude you from storing data with a fixed structure, as nonrelational databases can store virtually any kind of data. A primary key is required to uniquely identify each item in a table. Creating multiple tables is allowed, but most applications that use nonrelational databases use only one table.

4. C. A no-SQL database is another term for a nonrelational database. By definition, nonrelational databases are schemaless and must use primary keys. There's no such thing as a schemaless relational database. No-SQL is never used to describe a relational database of any kind.

5. B. RDS instances use EBS volumes for storage. They no longer can use magnetic storage. Instance volumes are for temporary, not database storage. You can take a snapshot of a database instance and restore it to a new instance with a new EBS volume, but an RDS instance can't use a snapshot directly for database storage.

6. B, D. PostgreSQL and Amazon Aurora are options for RDS database engines. IBM dBase and the nonrelational databases DynamoDB and Redis are not available as RDS database engines.

7. A, B. Aurora is Amazon's proprietary database engine that works with existing PostgreSQL and MySQL databases. Aurora doesn't support MariaDB, Oracle, or Microsoft SQL Server.

8. B, C. Multi-AZ and snapshots can protect your data in the event of an Availability Zone failure. Read replicas don't use synchronous replication and may lose some data. IOPS is a measurement of storage throughput. Vertical scaling refers to changing the instance class but has nothing to do with preventing data loss.

9. B. Amazon Aurora uses a shared storage volume that automatically expands up to 64 TB. The Microsoft SQL Server and Oracle database engines don't offer this. Amazon Athena is not a database engine.

10. A. Multi-AZ lets your database withstand the failure of an RDS instance, even if the failure is due to an entire Availability Zone failing. Read replicas are a way to achieve horizontal scaling to improve performance of database reads but don't increase availability. Point-in-time recovery allows you to restore a database up to a point in time but doesn't increase availability.

11. B, D. A partition is an allocation of storage backed by solid-state drives and replicated across multiple Availability Zones. Tables are stored across partitions, but tables do not

contain partitions. A primary key, not a partition, is used to uniquely identify an item in a table.

12. A. The minimum monthly availability for DynamoDB is 99.99 percent in a single Region. It's not 99.95 percent, 99.9 percent, or 99.0 percent.

13. D. Items in a DynamoDB table can have different attributes. For example, one item can have five attributes, while another has only one. A table can store items containing multiple data types. There's no need to predefine the number of items in a table. Items in a table can't have duplicate primary keys.

14. C, E. Increasing WCU or enabling Auto Scaling will improve write performance against a table. Increasing or decreasing RCU won't improve performance for writes. Decreasing WCU will make write performance worse.

15. C. A scan requires reading every partition on which the table is stored. A query occurs against the primary key, enabling DynamoDB to read only the partition where the matching item is stored. Writing and updating an item are not read-intensive operations.

16. D. A primary key must be unique within a table. A full name, phone number, or city may not be unique, as some customers may share the same name or phone number. A randomly generated customer ID number would be unique and appropriate for use as a primary key.

17. B. Dense compute nodes use magnetic disks. Dense storage nodes use SSDs. There are no such nodes as dense memory or cost-optimized.

18. A. Redshift Spectrum can analyze structured data stored in S3. There is no such service as Redshift S3. Amazon Athena can analyze structured data in S3, but it's not a feature of Redshift. Amazon RDS doesn't analyze data stored in S3.

19. B. A data warehouse stores large amounts of structured data from other relational databases. It's not called a data storehouse or a report cluster. Dense storage node is a type of Redshift compute node.

20. A. Dense storage nodes can be used in a cluster to store up to 2 PB of data. Dense compute nodes can be used to store up to 326 TB of data.

Chapter 10: The Core Networking Services

1. B, D. For each account, AWS creates a default VPC in each Region. A VPC spans all Availability Zones within a Region. VPCs do not span Regions.

2. A. A VPC or subnet CIDR can have a size between /16 and /28 inclusive, so 10.0.0.0/28 would be the only valid CIDR.

3. B, C. A subnet exists in only one Availability Zone, and it must have a CIDR that's a subset of CIDR of the VPC in which it resides. There's no requirement for a VPC to have two subnets, but it must have at least one.

4. C. When you create a security group, it contains an outbound rule that allows access to any IP address. It doesn't contain an inbound rule by default. Security group rules can only permit access, not deny it, so any traffic not explicitly allowed will be denied.

5. B, D. A network access control list is a firewall that operates at the subnet level. A security group is a firewall that operates at the instance level.

6. B. A VPC peering connection is a private connection between only two VPCs. It uses the private AWS network, and not the public internet. A VPC peering connection is different than a VPN connection.

7. A, B. A Direct Connect link uses a dedicated link rather than the internet to provide predictable latency. Direct Connect doesn't use encryption but provides some security by means of a private link. A VPN connection uses the internet for transport, encrypting data with AES 128- or 256-bit encryption. A VPN connection doesn't require proprietary hardware.

8. B, D. When you register a domain name, you can choose a term between 1 year and 10 years. If you use Route 53, it will automatically create a public hosted zone for the domain. The registrar and DNS hosting provider don't have to be the same entity, but often are.

9. B. A Multivalue Answer routing policy can return a set of multiple values, sorted randomly. A simple record returns a single value. A Failover routing policy always routes users to the primary resource unless it's down, in which case it routes users to the secondary resource. A Latency routing policy sends users to the resource in the AWS Region that provides the least latency.

10. C. All Route 53 routing policies except for Simple can use health checks.

11. C. An Endpoint health check works by connecting to the monitored endpoint via HTTP, HTTPS, or TCP. A CloudWatch alarm health check simply reflects the status of a CloudWatch alarm. A Calculated health check derives its status from multiple other health checks. There is no such thing as a Simple health check.

12. A. A Weighted routing policy lets you distribute traffic to endpoints according to a ratio that you define. None of the other routing policies allows this.

13. B. A private hosted zone is associated with a VPC and allows resources in the VPC to resolve private domain names. A public hosted zone is accessible by anyone on the internet. Domain name registration is for public domain names. Health checks aren't necessary for name resolution to work.

14. A. Route 53 private hosted zones provide DNS resolution for a single domain name within multiple VPCs. Therefore, to support resolution of one domain names for two VPCs, you'd need one private hosted zone.

15. B. CloudFront has edge locations on six continents (Antarctica is a hard place to get to).

16. B. A CloudFront origin is the location that a distribution sources content from. Content is stored in edge locations. A distribution defines the edge locations and origins to use.

17. B. The RTMP distribution type is for delivering streaming content and requires you to provide a media player. A Web distribution can also stream audio or video

content but doesn't require you to provide a media player. Streaming and Edge are not distribution types.

18. A. The more edge locations you use for a distribution, the more you'll pay. Selecting the minimum number of locations will be the most cost effective.

19. B. There are more than 150 edge locations throughout the world.

20. A, B. An origin can be an EC2 instance or a public S3 bucket. You can't use a private S3 bucket as an origin.

Chapter 11: Automating Your AWS Workloads

1. C. CloudFormation can create AWS resources and manages them collectively in a stack. Templates are written in the CloudFormation language, not Python. CloudFormation can't create resources outside of AWS. It also doesn't prevent manual changes to resources in a stack.

2. B, D. CloudFormation templates are written in the YAML or JSON format.

3. A. Parameters let you input customizations when creating a CloudFormation stack without having to modify the underlying template. Parameters don't prevent stack updates or unauthorized changes. A template can be used to create multiple stacks, regardless of whether it uses parameters.

4. A, B. Resources CloudFormation creates are organized into stacks. When you update a stack, CloudFormation analyzes the relationships among resources in the stack and updates dependent resources as necessary. This does not, however, mean that any resource you create using CloudFormation will work as you expect. Provisioning resources using CloudFormation is not necessarily faster than using the AWS CLI.

5. A, C. CodeCommit is a private Git repository that offers versioning and differencing. It does not perform deployments.

6. B. Differencing lets you see the differences between two versions of a file, which can be useful when figuring out what change introduced a bug. Versioning, not differencing, is what allows reverting to an older version of a file. Differencing doesn't identify duplicate lines of code or tell you when an application was deployed.

7. D. Continuous integration is the practice of running code through a build or test process as soon as it's checked into a repository. Continuous delivery and continuous deployment include continuous integration but add deployment to the process. Differencing only shows the differences between different versions of a file but doesn't perform any testing.

8. B, D. Build.general1.medium and build.general1.large support Windows and Linux operating systems. Build.general1.small supports Linux only. The other compute types don't exist.

9. A, B. A CodeBuild build environment always contains an operating system and a Docker image. It may contain the other components but doesn't have to.

10. A, B, C. CodeDeploy can deploy application files to Linux or Windows EC2 instances and Docker containers to ECS. It can't deploy an application to smartphones, and it can't deploy files to an S3 bucket.

11. B. At the very least, a CodePipeline must consist of a source stage and a deploy stage.

12. D. A launch template can be used to launch instances manually and with EC2 Auto Scaling. A launch configuration can't be used to launch instances manually. An instance role is used to grant permissions to applications running on an instance. Auto Scaling can't provision instances using a CloudFormation template.

13. A, D. The maximum and minimum group size values limit the number of instances in an Auto Scaling group. The desired capacity (also known as the group size) is the number of instances that Auto Scaling will generally maintain, but Auto Scaling can launch or terminate instances if dynamic scaling calls for it.

14. B. Auto Scaling will use self-healing to replace the failed instance to maintain the desired capacity of 7. Terminating an instance or failing to replace the failed one will result in 6 instances. Auto Scaling won't ever change the desired capacity in response to a failed instance.

15. A. Predictive scaling creates a scheduled scaling action based on past usage patterns. Scheduled scaling and dynamic scaling do not create scheduled scaling actions. There is no such thing as pattern scaling.

16. B. A Command document can execute commands on an EC2 instance. An Automation document can perform administrative tasks on AWS, such as starting or stopping an instance. There is no such thing as a Script document or a Run document.

17. D. An Automation document can perform administrative tasks on AWS, such as starting or stopping an instance. A Command document can execute commands on an EC2 instance. There is no such thing as a Script document or a Run document.

18. B. AWS OpsWorks Stacks uses Chef recipes, while AWS OpsWorks for Puppet Enterprise uses Puppet modules. There is no service called AWS OpsWorks Layers or AWS OpsWorks for Automation.

19. B, D. OpsWorks supports the Puppet Enterprise and Chef configuration management platforms. It doesn't support SaltStack, Ansible, or CFEngine.

20. C. Only an OpsWorks layer contains at least one EC2 instance. There's no such thing as an EC2 Auto Scaling layer.

Chapter 12: Common Use-Case Scenarios

1. C. The five pillars of the Well-Architected Framework are reliability, performance efficiency, security, cost optimization, and operational excellence. Resiliency is not one of them.

2. A, D. Security is about protecting the confidentiality, integrity, and availability of data. Granting each AWS user their own IAM username and password makes it possible to ensure the confidentiality of data. Enabling S3 versioning protects the integrity of data by maintaining a backup of an object. Deleting an empty S3 bucket doesn't help with any of these. It's not possible to create a security group rule that denies access to unused ports since security groups deny any traffic that's not explicitly allowed.

3. C, D. Preventing the accidental termination of an EC2 instance in the Auto Scaling group can avoid overburdening and causing performance issues on the remaining instance, especially during busy times. Using CloudFront can help improve performance for end users by caching the content in an edge location close to them. Doubling the number of instances might improve performance, but because performance is already acceptable, doing this would be inefficient. Monitoring for unauthorized access alone won't improve performance or performance efficiency.

4. A, C. Deleting unused S3 objects and unused application load balancers can reduce costs since you're charged for both. Deleting unused VPCs and empty S3 buckets won't reduce costs since they don't cost anything.

5. B. Operational excellence is concerned with strengthening the other four pillars of reliability, performance efficiency, security, and cost optimization; automation is the key to achieving each of these. Improving bad processes and making people work longer hours run counter to achieving operational excellence. Adding more security personnel may be a good idea, but it isn't a key component of operational excellence.

6. B. In a default VPC, AWS creates a subnet for each Availability Zone in the Region. Hence, if there are three subnets in the default VPC, there must be three Availability Zones.

7. A. Application load balancer listeners use security groups to control inbound access, so you need to apply a security group that has an inbound rule allowing HTTP access. Applying the security group rule to the database instance won't help, since users don't connect directly to the database instance. You can't apply a security group to a subnet, only a network access control list.

8. A. An application load balancer can use health checks to identify failed instances and remove them from load balancing. This can prevent a user from ever reaching a failed instance. A load balancer can't replace a failed instance, but Auto Scaling can. An application load balancer distributes traffic to instances using a round-robin algorithm, not based on how busy those instances are. An application load balancer doesn't cache content.

9. D. A launch template tells Auto Scaling how to configure the instances it provisions. A dynamic scaling policy controls how Auto Scaling scales in and out based on CloudWatch metrics. There's no such thing as a launch directive. Auto Scaling does not reference a CloudFormation template, but you can use a CloudFormation template to create a stack that contains a launch template.

10. B. The maximum group size limits the number of instances in the group. Setting the group size (also known as the desired capacity) or minimum group size to 5 would increase the number of instances to 5 but would not stop Auto Scaling from subsequently adding more instances. Deleting the target tracking policy would not necessarily prevent the number of instances in the group from growing, as another process such as a scheduled scaling policy could add more instances to the group.

11. B. A static website serves content just as it's stored without changing the content on the fly. A WordPress blog, a social media website, and a web-based email application all compile content from a database and mix it in with static content before serving it up to the user.

12. A, C. Objects you upload to an S3 bucket are not public by default, nor are they accessible to all AWS users. Even if you try to make an object public using an ACL, S3 will immediately remove the ACL, but you can disable this behavior. S3 never removes objects by default.

13. A. To have S3 host your static website, you need to enable bucket hosting in the S3 service console. It's not necessary to disable or enable default encryption or object versioning. There's also no need to make all objects in the bucket public, but only those that you want S3 to serve up.

14. B. Purchasing and using a custom domain name is the best option for a friendly URL. You need to name the bucket the same as the domain name. Creating a bucket name with only words is unlikely to work, regardless of Region, as bucket names must be globally unique. A bucket name can't start with a number.

15. A. Websites hosted in S3 are served using unencrypted HTTP, not secure HTTPS. The content is publicly readable, but that doesn't mean the public can modify it. You don't have to use a custom domain name, as S3 provides an endpoint URL for you. A website hosted in S3 is stored in a bucket, and a bucket exists in only one Region.

16. C. The reliability of an application can be impacted by the failure of resources the application depends on. One way a resource can fail is if it's misconfigured. Taking EBS snapshots of an instance or provisioning more instances than you need won't impact reliability. The user interface being difficult to use might be an annoyance for the user but doesn't affect the actual reliability of the application.

17. C. You may have control over your VPC, but the rest of the network between your application and users on the internet is not under your control. Compute, storage, and any database your application uses are, or at least theoretically could be, under your control.

18. D. An Auto Scaling group can use an ELB health check to determine whether an instance is healthy. There is no such thing as an S3 health check, a VPC health check, or an SNS health check.

19. B. You're responsible for S3 charges related to your static website. You're not charged for compute with S3. No one may modify the content of your site unless you give them permission. The S3 Standard storage class keeps objects in multiple Availability Zones, so the outage of one won't affect the site.

20. A. The format of the URL is the bucket name, followed by s3-website-, the Region identifier, and then `amazonaws.com`.