

# Assessment Test

1. Which of the following describes the cloud design principle of scalability?
  - a. **The ability to automatically increase available compute resources to meet growing user demand → A scalable deployment will automatically “scale up” its capacity to meet growing user demand without the need for manual interference. See Chapter 1.**
  - b. The ability to route incoming client requests between multiple application servers
  - c. The ability to segment physical resources into multiple virtual partitions
  - d. The ability to reduce production costs by spreading capital expenses across many accounts
2. Which of the following best describes the cloud service model known as infrastructure as a service (IaaS)?
  - a. End user access to software applications delivered over the internet
  - b. Access to a simplified interface through which customers can directly deploy their application code without having to worry about managing the underlying infrastructure
  - c. **Customer rental of the use of measured units of a provider’s physical compute, storage, and networking resources → IaaS is a model that gives customers access to virtualized units of a provider’s physical resources. IaaS customers manage their infrastructure much the way they would local, physical servers. See Chapter 1.**
  - d. Abstracted interfaces built to manage clusters of containerized workloads
3. How does AWS ensure that no single customer consumes an unsustainable proportion of available resources?
  - a. AWS allows customers to consume as much as they’re willing to pay for, regardless of general availability.
  - b. **AWS imposes default limits on the use of its service resources but allows customers to request higher limits. → AWS applies usage limits on most features of its services. However, in many cases, you can apply for a limit to be lifted. See Chapter 2.**
  - c. AWS imposes hard default limits on the use of its service resources.
  - d. AWS imposes default limits on the use of its services by Basic account holders; Premium account holders face no limits.
4. The AWS Free Tier is designed to give new account holders the opportunity to get to know how their services work without necessarily costing any money. How does it work?
  - a. You get service credits that can be used to provision and launch a few typical workloads.
  - b. You get full free access to a few core AWS services for one month.
  - c. You get low-cost access to many core AWS services for three months.

- d. **You get free lightweight access to many core AWS services for a full 12 months.**  
→ **The Free Tier offers you free lightweight access to many core AWS services for a full 12 months. See Chapter 2.**
5. AWS customers receive “production system down” support within one hour when they subscribe to which support plan(s)?
- Enterprise.
  - Business and Enterprise. → “Production system down” support within one hour is available only to subscribers to the Business or Enterprise support plans. See Chapter 3.**
  - Developer and Basic.
  - All plans get this level of support.
6. AWS customers get full access to the AWS Trusted Advisor best practice checks when they subscribe to which support plan(s)?
- All plans get this level of support.
  - Basic and Business.
  - Business and Enterprise.
  - Developer, Business, and Enterprise. → All support plans come with full access to Trusted Advisor except for the (free) Basic plan. See Chapter 3.**
7. The AWS Shared Responsibility Model illustrates how AWS itself (as opposed to its customers) is responsible for which aspects of the cloud environment?
- The redundancy and integrity of customer-added data
  - The underlying integrity and security of AWS physical resources → According to the Shared Responsibility Model, AWS is responsible for the underlying integrity and security of AWS physical resources, but not the integrity of the data and configurations added by customers. See Chapter 4.**
  - Data and configurations added by customers
  - The operating systems run on EC2 instances
8. Which of these is a designation for two or more AWS data centers within a single geographic area?
- Availability Zone → An Availability Zone is one of two or more physical data centers located within a single AWS Region. See Chapter 4.**
  - Region
  - Network subnet
  - Geo-unit

9. How, using security best practices, should your organization's team members access your AWS account resources?
- a. Only a single team member should be given any account access.
  - b. Through a jointly shared single account user who's been given full account-wide permissions.
  - c. **Through the use of specially created users, groups, and roles, each given the fewest permissions necessary.** → **Team members should each be given identities (as users, groups, and/or roles) configured with exactly the permissions necessary to do their jobs and no more. See Chapter 5.**
  - d. Ideally, resource access should occur only through the use of access keys.
10. Which of the following describes a methodology that protects your organization's data when it's on-site locally, in transit to AWS, and stored on AWS?
- a. **Client-side encryption** → **End-to-end encryption that protects data at every step of its life cycle is called client-side encryption. See Chapter 5.**
  - b. Server-side encryption
  - c. Cryptographic transformation
  - d. Encryption at rest
11. What authentication method will you use to access your AWS resources remotely through the AWS Command Line Interface (CLI)?
- a. Strong password
  - b. Multifactor authentication
  - c. SSH key pairs
  - d. **Access keys** → **AWS CLI requests are authenticated through access keys. See Chapter 6.**
12. Which of these is the primary benefit from using resource tags with your AWS assets?
- a. Tags enable the use of remote administration operations via the AWS CLI.
  - b. **Tags make it easier to identify and administrate running resources in a busy AWS account.** → **Resource tags—especially when applied with consistent naming patterns—can make it easier to visualize and administrate resources on busy accounts. See Chapter 6.**
  - c. Tags enhance data security throughout your account.
  - d. Some AWS services won't work without the use of resource tags.
13. What defines the base operating system and software stack that will be available for a new Elastic Compute Cloud (EC2) instance when it launches?
- a. The Virtual Private Cloud (VPC) into which you choose to launch your instance.
  - b. The instance type you select.
  - c. **The Amazon Machine Image (AMI) you select.** → **The AMI you select while configuring your new instance defines the base OS. See Chapter 7.**

- d. You don't need to define the base OS—you can install that once the instance launches.

14. Which of the following AWS compute services offers an administration experience that most closely resembles the way you would run physical servers in your own local data center?

- a. Simple Storage Service (S3)
- b. Elastic Container Service (ECS)
- c. **Elastic Compute Cloud (EC2) → You can administrate EC2 instances using techniques that are similar to the way you'd work with physical servers. See Chapter 7.**
- d. Lambda

15. Which of the following AWS object storage services offers the lowest ongoing charges, but at the cost of some convenience?

- a. **Glacier → Amazon Glacier can reliably store large amounts of data for a very low price but requires CLI or SDK administration access, and retrieving your data can take hours. See Chapter 8.**
- b. Storage Gateway
- c. Simple Storage Service (S3)
- d. Elastic Block Store (EBS)

16. Which of the following AWS storage services can make the most practical sense for petabyte-sized archives that currently exist in your local data center?

- a. Saving to a Glacier Vault
- b. Saving to a Simple Storage Service (S3) bucket
- c. Saving to an Elastic Block Store (EBS) volume
- d. **Saving to an AWS Snowball device → You can transfer large data stores to the AWS cloud (to S3 buckets) by having Amazon send you a Snowball device to which you copy your data and which you then ship back to Amazon. See Chapter 8.**

17. Which of the following will provide the most reliable and scalable relational database experience on AWS?

- a. **Relational Database Service (RDS) → RDS offers a managed and highly scalable database environment for most popular relational database engines (including MySQL, MariaDB, and Oracle). See Chapter 9.**
- b. Running a database on an EC2 instance
- c. DynamoDB
- d. Redshift

18.What's the best and simplest way to increase reliability of an RDS database instance?

- a. Increase the available IOPS.
- b. Choose the Aurora database engine when you configure your instance.
- c. **Enable Multi-AZ.** → **Multi-AZ will automatically replicate your database in a second Availability Zone for greater reliability. It will, of course, also double your costs. See Chapter 9.**
- d. Duplicate the database in a second AWS Region.

19.How does AWS describe an isolated networking environment into which you can launch compute resources while closely controlling network access?

- a. Security group
- b. **Virtual private cloud (VPC)** → **A VPC is an isolated networking environment into which you can launch compute resources while closely controlling network access. See Chapter 10.**
- c. Availability Zone
- d. Internet gateway

20.What service does AWS use to provide a content delivery network (CDN) for its customers?

- a. VPC peering
- b. Internet gateway
- c. Route 53
- d. **CloudFront** → **CloudFront is a content delivery network (CDN) that distributes content through its global network of edge locations. See Chapter 10.**

21.What is Amazon's Git-compliant version control service for integrating your source code with AWS resources?

- a. **CodeCommit** → **CodeCommit is a Git-compliant version control service for integrating your source code with AWS resources. See Chapter 11.**
- b. CodeBuild
- c. CodeDeploy
- d. Cloud9

22.Which AWS service allows you to build a script-like template representing complex resource stacks that can be used to launch precisely defined environments involving the full range of AWS resources?

- a. LightSail
- b. EC2
- c. CodeDeploy
- d. **CloudFormation** → **CloudFormation templates can represent complex resource stacks that can be used to launch precisely defined environments involving the full range of AWS resources. See Chapter 11.**

23.What is Amazon Athena?

- a. **A service that permits queries against data stored in Amazon S3 → Amazon Athena is a managed service that permits queries against S3-stored data. See Chapter 13.**
- b. A service that permits processing and analyzing of real-time video and data streams
- c. A NoSQL database engine
- d. A Greece-based Amazon Direct Connect service partner

24.What is Amazon Kinesis?

- a. A service that permits queries against data stored in Amazon S3
- b. **A service that permits processing and analyzing of real-time video and data streams → Amazon Kinesis allows processing and analyzing of real time video and data streams. See Chapter 13.**
- c. A NoSQL database engine
- d. A Greece-based Amazon Direct Connect service partner

25.What is Amazon Cognito?

- a. **A service that can manage authentication and authorization for your public-facing applications → Amazon Cognito can manage authentication and authorization for your public-facing applications. See Chapter 13.**
- b. A service that automates the administration of authentication secrets used by your AWS resources
- c. A service that permits processing and analyzing of real-time video and data streams
- d. A relational database engine

## Review Questions – The Cloud

1. Which of the following does not contribute significantly to the operational value of a large cloud provider like AWS?
  - a. Multiregional presence
  - b. Highly experienced teams of security engineers
  - c. **Deep experience in the retail sphere** → **Having globally distributed infrastructure and experienced security engineers makes a provider's infrastructure more reliable. Metered pricing makes a wider range of workloads possible.**
  - d. Metered, pay-per-use pricing
2. Which of the following are signs of a highly available application? (Select TWO.)
  - a. **A failure in one geographic region will trigger an automatic failover to resources in a different region.** → **Security and virtualization are both important characteristics of successful cloud workloads, but neither will directly impact availability.**
  - b. Applications are protected behind multiple layers of security.
  - c. Virtualized hypervisor-driven systems are deployed as mandated by company policy.
  - d. **Spikes in user demand are met through automatically increasing resources.** → **Security and virtualization are both important characteristics of successful cloud workloads, but neither will directly impact availability.**
3. How does the metered payment model make many benefits of cloud computing possible? (Select TWO.)
  - a. Greater application security is now possible.
  - b. **Experiments with multiple configuration options are now cost-effective.** → **Security and scalability are important cloud elements but are not related to metered pricing.**
  - c. Applications are now highly scalable.
  - d. **Full-stack applications are possible without the need to invest in capital expenses.** → **Security and scalability are important cloud elements but are not related to metered pricing.**
4. Which of the following are direct benefits of server virtualization? (Select TWO.)
  - a. **Fast resource provisioning and launching** → **Security and elasticity are important but are not directly related to server virtualization.**
  - b. **Efficient (high-density) use of resources** → **Security and elasticity are important but are not directly related to server virtualization.**
  - c. Greater application security
  - d. Elastic application designs

5. What is a hypervisor?

- a. Hardware device used to provide an interface between storage and compute modules
- b. Hardware device used to provide an interface between networking and compute modules
- c. Software used to log and monitor virtualized operations
- d. Software used to administrate virtualized resources run on physical infrastructure → A hypervisor is software (not hardware) that administrates virtualized operations.**

6. Which of the following best describes server virtualization?

- a. “Sharding” data from multiple sources into a single virtual data store
- b. Logically partitioning physical compute and storage devices into multiple smaller virtual devices → Sharding, aggregating remote resources, and abstracting complex infrastructure can all be accomplished using virtualization techniques, but they aren’t, of themselves, virtualization.**
- c. Aggregating physical resources spread over multiple physical devices into a single virtual device
- d. Abstracting the complexity of physical infrastructure behind a simple web interface

7. Which of the following best describes Infrastructure as a Service products?

- a. Services that hide infrastructure complexity behind a simple interface
- b. Services that provide a service to end users through a public network
- c. Services that give you direct control over underlying compute and storage resources → PaaS products mask complexity, SaaS products provide end-user services, and serverless architectures (like AWS Lambda) let developers run code on cloud servers.**
- d. Platforms that allow developers to run their code over short periods on cloud servers

8. Which of the following best describes Platform as a Service products?

- a. Services that hide infrastructure complexity behind a simple interface → 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.**
- b. Platforms that allow developers to run their code over short periods on cloud servers
- c. Services that give you direct control over underlying compute and storage resources
- d. Services that provide a service to end users through a public network

9. Which of the following best describes Software as a Service products?

- a. Services that give you direct control over underlying compute and storage resources
- b. Services that provide a service to end users through a public network → IaaS products provide full infrastructure access, PaaS products mask complexity, and serverless architectures (like AWS Lambda) let developers run code on cloud servers.**



- c. Services that hide infrastructure complexity behind a simple interface
- d. Platforms that allow developers to run their code over short periods on cloud servers

10. Which of the following best describes scalability?

- a. **The ability of an application to automatically add preconfigured compute resources to meet increasing demand → Increasing or decreasing compute resources better describes elasticity. Efficient use of virtualized resources and billing models aren't related directly to scalability.**
- b. The ability of an application to increase or decrease compute resources to match changing demand
- c. The ability to more densely pack virtualized resources onto a single physical server
- d. The ability to bill resource usage using a pay-per-user model

11. Which of the following best describes elasticity?

- a. The ability to more densely pack virtualized resources onto a single physical server
- b. The ability to bill resource usage using a pay-per-user model
- c. **The ability of an application to increase or decrease compute resources to match changing demand → 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.**
- d. The ability of an application to automatically add preconfigured compute resources to meet increasing demand

12. Which of the following characteristics most help AWS provide such scalable services? (Select TWO.)

- a. **The enormous number of servers it operates → Capitalized assets and geographic reach are important but don't have a direct impact on operational scalability.**
- b. The value of its capitalized assets
- c. Its geographic reach
- d. **Its highly automated infrastructure administration systems → Capitalized assets and geographic reach are important but don't have a direct impact on operational scalability.**

## Review Questions – Understanding Your AWS Account

1. Which of the following EC2 services can be used without charge under the Free Tier?
  - a. Any single EC2 instance type as long as it runs for less than one hour per day
  - b. Any single EC2 instance type as long as it runs for less than 75 hours per month
  - c. A single t2.micro EC2 instance type instance for 750 hours per month
  - d. **t2.micro EC2 instance type instances for a total of 750 hours per month → 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. You want to experiment with deploying a web server on an EC2 instance. Which two of the following resources can you include to make that work while remaining within the Free Tier? (Select TWO.)
  - a. A 5 GB bucket on S3
  - b. **A t2.micro instance type EC2 instance → 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.**
  - c. **A 30 GB solid-state Elastic Block Store (EBS) drive → 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.**
  - d. Two 20 GB solid-state Elastic Block Store (EBS) drives
3. Which of the following usage will always be cost-free even after your account's Free Tier has expired? (Select TWO.)
  - a. One million API calls/month on Amazon API Gateway
  - b. **10 GB of data retrievals from Amazon Glacier per month → The API calls/month and ECR free storage are available only under the Free Tier.**
  - c. 500 MB/month of free storage on the Amazon Elastic Container Registry (ECR)
  - d. **10 custom monitoring metrics and 10 alarms on Amazon CloudWatch → The API calls/month and ECR free storage are available only under the Free Tier.**
4. Which of the following tools are available to ensure you won't accidentally run past your Free Tier limit and incur unwanted costs? (Select TWO.)
  - a. **Automated email alerts when activity approaches the Free Tier limits → There is no Top Free Tier Services Dashboard or, for that matter, a Billing Preferences Dashboard.**
  - b. **The Top Free Tier Services by Usage section on the Billing & Cost Management Dashboard → There is no Top Free Tier Services Dashboard or, for that matter, a Billing Preferences Dashboard.**
  - c. Billing & Cost Management section on the Top Free Tier Services Dashboard
  - d. The Billing Preferences Dashboard

5. Which of the following is likely to be an accurate source of AWS pricing information?
- a. Wikipedia pages relating to a particular service
  - b. The AWS Command Line Interface (AWS CLI)
  - c. **AWS online documentation relating to a particular service** → **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.**
  - d. The AWS Total Cost of Ownership Calculator
6. Which of the following will probably not affect the pricing for an AWS service?
- a. **Requests for raising the available service limit** → **Pricing will normally change based on the volume of service units you consume and, often, between AWS Regions.**
  - b. AWS Region
  - c. The volume of data saved to an S3 bucket
  - d. The volume of data egress from an Amazon Glacier vault
7. Which of the following is a limitation of the AWS Simple Monthly Calculator?
- a. You can calculate resource use for only one service at a time.
  - b. **Not all AWS services are included.** → **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.**
  - c. The pricing is seldom updated and doesn't accurately reflect current pricing.
  - d. You're not able to specify specific configuration parameters.
8. Which of the following Simple Monthly Calculator selections will likely have an impact on most other configuration choices on the page? (Select TWO.)
- a. Calculate By Month Or Year
  - b. Include Multiple Organizations
  - c. **Free Usage Tier** → **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.**
  - d. **Choose Region** → **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. Which of the following is not an included parameter in the AWS Total Cost of Ownership Calculator?
- a. **The tax implications of a cloud deployment** → **The calculator covers all significant costs associated with an on-premises deployment but doesn't include local or national tax implications.**
  - b. Labor costs of an on-premises deployment
  - c. Networking costs of an on-premises deployment

d. Electricity costs of an on-premises deployment

10. Which of the following AWS Total Cost of Ownership Calculator parameters is likely to have the greatest impact on cost?

- a. Currency
- b. AWS Region
- c. Guest OS
- d. **Number of servers** → **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. Which of the following AWS documentation URLs points to the page containing an up-to-date list of service limits?

- a. <https://docs.aws.amazon.com/general/latest/gr/limits.html>
- b. [https://docs.aws.amazon.com/general/latest/gr/aws\\_service\\_limits.html](https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html) → **The correct URL is [https://docs.aws.amazon.com/general/latest/gr/aws\\_service\\_limits.html](https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html).**
- c. [https://aws.amazon.com/general/latest/gr/aws\\_service\\_limits.html](https://aws.amazon.com/general/latest/gr/aws_service_limits.html)
- d. [https://docs.aws.amazon.com/latest/gr/aws\\_service\\_limits.html](https://docs.aws.amazon.com/latest/gr/aws_service_limits.html)

12. Which of the following best describes one possible reason for AWS service limits?

- a. **To prevent individual customers from accidentally launching a crippling level of resource consumption** → **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.**
- b. To more equally distribute available resources between customers from different regions
- c. To allow customers to more gradually increase their deployments
- d. Because there are logical limits to the ability of AWS resources to scale upward

13. Is it always possible to request service limit increases from AWS?

- a. Yes. All service limits can be increased.
- b. No. A limit can never be increased.
- c. Service limits are defaults. They can be increased or decreased on demand.
- d. **No. Some service limits are hard.** → **While most service limits are soft and can be raised on request, there are some service limits that are absolute.**

14. Which is the best place to get a quick summary of this month's spend for your account?

- a. Budgets
- b. Cost Explorer
- c. Cost and usage reports

- d. Billing & Cost Management Dashboard** → **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. What is the main goal for creating a Usage budget type (in AWS Budgets)?

- a. To correlate usage per unit cost to understand your account cost efficiency
- b. To track the status of any active reserved instances on your account
- c. To track particular categories of resource consumption** → **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.**
- d. To monitor costs being incurred against your account

16. Which of the following is not a setting you can configure in a Cost budget?

- a. Period (monthly, quarterly, etc.)
- b. Instance type
- c. Start and stop dates
- d. Owner (username of resource owner)** → **You can configure the period, instance type, and start/stop dates for a budget, but you can't filter by resource owner.**

17. What is the main difference between the goals of Cost Explorer and of cost and usage reports?

- a. Cost Explorer displays visualizations of high-level historical and current account costs, while cost and usage reports generate granular usage reports in CSV format.** → **Billing events aren't triggers for alerts. Nothing in this chapter discusses intrusion events.**
- b. Cost and usage reports display visualizations of high-level historical and current account costs, while Cost Explorer generates granular usage reports in CSV format.
- c. Cost Explorer lets you set alerts that are triggered by billing events, while cost and usage reports help you visualize system events.
- d. Cost and usage reports are meant to alert you to malicious intrusions, while Cost Explorer displays visualizations of high-level historical and current account costs.

18. What is the purpose of cost allocation tags?

- a. To associate spend limits to automatically trigger resource shutdowns when necessary
- b. To help you identify the purpose and owner of a particular running resource to better understand and control deployments
- c. To help you identify resources for the purpose of tracking your account spending** → **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.**
- d. To visually associate account events with billing periods

19. Which of the following scenarios would be a good use case for AWS Organizations? (Select TWO.)

- a. **A single company with multiple AWS accounts that wants a single place to administrate everything** → 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.
- b. An organization that provides AWS access to large teams of its developers and admins
- c. **A company that's integrated some operations with an upstream vendor** → 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.
- d. A company with two distinct operational units, each with its own accounting system and AWS account

20. Which of these tools lets you design graphs within the browser interface to track your account spending?

- a. Budgets
- b. **Cost Explorer** → 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.
- c. Reports
- d. Consolidating Billing

## Review Questions – Getting Support on AWS

1. Your company is planning a major deployment on AWS. While the design and testing stages are still in progress, which of the following plans will provide the best blend of support and cost savings?
  - a. Basic
  - b. Developer
  - c. **Business** → **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.**
  - d. Enterprise
2. Your web development team is actively gearing up for a deployment of an ecommerce site. During these early stages of the process, individual developers are running into frustrating conflicts and configuration problems that are highly specific to your situation. Which of the following plans will provide the best blend of support and cost savings?
  - a. Basic
  - b. **Developer** → **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.**
  - c. Business
  - d. Enterprise
3. Your corporate website was offline last week for more than two hours—which caused serious consequences, including the early retirement of your CTO. Your engineers have been having a lot of trouble tracking down the source of the outage and admit that they need outside help. Which of the following will most likely meet that need?
  - a. Basic
  - b. Developer
  - c. Business
  - d. **Enterprise** → **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. For which of the following will AWS provide direct 24/7 support to all users—even those on the Basic Support plan?
  - a. Help with infrastructure under a massive denial-of-service (DoS) attack
  - b. Help with failed and unavailable infrastructure
  - c. **Help with making a bill payment to AWS** → **Basic plan customers are given customer support access only for account management issues and not for technical support or security breaches.**

- d. Help with accessing your infrastructure via the AWS CLI
5. The primary purpose of an AWS technical account manager is to:
- a. Provide 24/7 customer service for your AWS account
  - b. Provide deployment guidance and advocacy for Enterprise Support customers**  
→ **The TAM is available only for Enterprise Support customers. The primary function is one of guidance and advocacy.**
  - c. Provide deployment guidance and advocacy for Business Support customers
  - d. Provide strategic cost estimates for Enterprise Support customers
6. Your Linux-based EC2 instance requires a patch to a Linux kernel module. The problem is that patching the module will, for some reason, break the connection between your instance and data in an S3 bucket. Your team doesn't know if it's possible to work around this problem. Which is the most cost-effective AWS plan through which support professionals will try to help you?
- a. Developer.
  - b. Business.** → **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.**
  - c. Enterprise.
  - d. No plan covers this kind of support.
7. Your company enrolled in the Developer Support plan and, through the course of one month, consumed \$4,000 USD of AWS services. How much will the support plan cost the company for the month?
- a. \$120** → **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.**
  - b. \$29
  - c. \$100
  - d. \$480
8. Your company enrolled in the Business Support plan and, through the course of three months, consumed \$33,000 of AWS services (the consumption was equally divided across the months). How much will the support plan cost the company for the full three months?
- a. \$4,000
  - b. \$100
  - c. \$1,100
  - d. \$2,310** → **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. Which of the following AWS support services does not offer free documentation of some sort?
- a. AWS Professional Services
  - b. The Basic Support plan
  - c. **AWS Partner Network** → **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.**
  - d. The Knowledge Center
10. What is the key difference between the roles of AWS Professional Services and a technical account manager (TAM)?
- a. **The Professional Services product helps AWS Partner Network cloud professionals work alongside your own team to help you administrate your cloud infrastructure. The TAM is a cloud professional employed by AWS to guide you through the planning and execution of your infrastructure. → 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.**
  - b. The TAM is a cloud professional employed by AWS to guide you through the planning and execution of your infrastructure. The Professional Services product provides cloud professionals to work alongside your own team to help you administrate your cloud infrastructure.
  - c. The TAM is a member of your team designated as the point person for all AWS projects. The Professional Services product provides consultants to work alongside your own team to help you administrate your cloud infrastructure.
  - d. The Professional Services product is a network appliance that AWS installs in your data center to test cloud-bound workloads for compliance with best practices. The TAM is a cloud professional employed by AWS to guide you through the planning and execution of your infrastructure.
11. AWS documentation is available in a number of formats, including which of the following? (Select TWO.)
- a. Microsoft Word (DOC)
  - b. **Kindle** → **Although DOC and DocBook are both popular and useful formats, neither is used by AWS for its documentation.**
  - c. **HTML** → **Although DOC and DocBook are both popular and useful formats, neither is used by AWS for its documentation.**
  - d. DocBook
12. Which of the following documentation sites are most likely to contain code snippets for you to cut and (after making sure you understand exactly what they'll do) paste into your AWS operations? (Select TWO.)
- a. **<https://aws.amazon.com/premiumsupport/knowledge-center>** → **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.**

- b. <https://aws.amazon.com/premiumsupport/compare-plans>
- c. <https://docs.aws.amazon.com> → **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.**
- d. <https://aws.amazon.com/professional-services>

13. What is the primary function of the content linked from the Knowledge Center?

- a. To introduce new users to the functionality of the core AWS services
- b. To explain how AWS deployments can be more efficient and secure than on-premises
- c. To provide a public forum where AWS users can ask their technical questions
- d. **To present solutions to commonly encountered technical problems using AWS infrastructure → 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. On which of the following sites are you most likely to find information about encrypting your AWS resources?

- a. <https://aws.amazon.com/premiumsupport/knowledge-center>
- b. <https://aws.amazon.com/security/security-resources> → **The Knowledge Center is a general FAQ for technical problems and their solutions. The [docs.aws.amazon.com](https://docs.aws.amazon.com) site is for general documentation. There is no <https://aws.amazon.com/security/encryption> page.**
- c. <https://docs.aws.amazon.com>
- d. <https://aws.amazon.com/security/encryption>

15. When using AWS documentation pages, what is the best way to be sure the information you're reading is up-to-date?

- a. **The page URL will include the word *latest*. → Version numbers are not publicly available, and the word *Current* isn't used in this context.**
- b. The page URL will include the version number (i.e., 3.2).
- c. The page will have the word *Current* at the top right.
- d. There is no easy way to tell.

16. Which of the following is not a Trusted Advisor category?

- a. Performance
- b. Service Limits
- c. **Replication → Replication is, effectively, a subset of Fault Tolerance and therefore would not require its own category.**
- d. Fault Tolerance

17. “Data volumes that aren’t properly backed up” is an example of which of these Trusted Advisor categories?

- a. **Fault Tolerance** → 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.
- b. Performance
- c. Security
- d. Cost Optimization

18. Instances that are running (mostly) idle should be identified by which of these Trusted Advisor categories?

- a. Performance
- b. **Cost Optimization** → 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.
- c. Service Limits
- d. Replication

19. Within the context of Trusted Advisor, what is a false positive?

- a. **An alert for a service state that was actually intentional** → 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.
- b. A green OK icon for a service state that is failed or failing
- c. A single status icon indicating that your account is completely compliant
- d. Textual indication of a failed state

20. Which of the following Trusted Advisor alerts is available only for accounts on the Business or Enterprise Support plan? (Select TWO.)

- a. MFA on Root Account
- b. **Load Balancer Optimization** → Both the MFA and Service Limits checks are available for all accounts.
- c. Service Limits
- d. **IAM Access Rotation** → Both the MFA and Service Limits checks are available for all accounts.

## Review Questions – Understanding The AWS Environment

1. Which of the following designations would refer to the AWS US West (Oregon) region?
  - a. us-east-1
  - b. us-west-2 → 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.**
  - c. us-west-2a
  - d. us-west-2b
2. Which of the following is an AWS Region for which customer access is restricted?
  - a. AWS Admin
  - b. US-DOD
  - c. Asia Pacific (Tokyo)
  - d. AWS GovCloud → 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. When you request a new virtual machine instance in EC2, your instance will automatically launch into the currently selected value of which of the following?
  - a. Service
  - b. Subnet
  - c. Availability Zone
  - d. Region → 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. Which of the following are *not* globally based AWS services? (Select TWO.)
  - a. RDS
  - b. Route 53 → 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.**
  - c. EC2
  - d. CloudFront → 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. Which of the following would be a valid endpoint your developers could use to access a particular Relational Database Service instance you're running in the Northern Virginia region?
  - a. us-east-1.amazonaws.com.rds
  - b. ecs.eu-west-3.amazonaws.com

- c. **rds.us-east-1.amazonaws.com** → **The correct syntax for an endpoint is <service-designation>.<region-designation>.amazonaws.com—meaning, in this case, rds.us-east-1.amazonaws.com.**
  - d. **rds.amazonaws.com.us-east-1**
6. What are the most significant architectural benefits of the way AWS designed its regions? (Select TWO.)
- a. It can make infrastructure more fault tolerant.
  - b. **It can make applications available to end users with lower latency.** → **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.**
  - c. **It can make applications more compliant with local regulations.** → **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.**
  - d. It can bring down the price of running.
7. Why is it that most AWS resources are tied to a single region?
- a. **Because those resources are run on a physical device, and that device must live somewhere** → **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.**
  - b. Because security considerations are best served by restricting access to a single physical location
  - c. Because access to any one digital resource must always occur through a single physical gateway
  - d. Because spreading them too far afield would introduce latency issues
8. You want to improve the resilience of your EC2 web server. Which of the following is the most effective and efficient approach?
- a. Launch parallel, load-balanced instances in multiple AWS Regions.
  - b. **Launch parallel, load-balanced instances in multiple Availability Zones within a single AWS Region.** → **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.**
  - c. Launch parallel, autoscaled instances in multiple AWS Regions.
  - d. Launch parallel, autoscaled instances in multiple Availability Zones within a single AWS Region.

9. Which of the following is the most accurate description of an AWS Availability Zone?

- a. **One or more independently powered data centers running a wide range of hardware host types** → “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.
- b. One or more independently powered data centers running a uniform hardware host type
- c. All the data centers located within a broad geographic area
- d. The infrastructure running within a single physical data center

10. Which of the following most accurately describes a subnet within the AWS ecosystem?

- a. The virtual limits imposed on the network access permitted to a resource instance
- b. The block of IP addresses assigned for use within a single region
- c. **The block of IP addresses assigned for use within a single Availability Zone** → 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.
- d. The networking hardware used within a single Availability Zone

11. What determines the order by which subnets/AZ options are displayed in EC2 configuration dialogs?

- a. Alphabetical order
- b. **They (appear) to be displayed in random order.** → AWS displays AZs in (apparently) random order to prevent too many resources from being launched in too few zones.
- c. Numerical order
- d. By order of capacity, with largest capacity first

12. What is the primary goal of autoscaling?

- a. To ensure the long-term reliability of a particular physical resource
- b. To ensure the long-term reliability of a particular virtual resource
- c. To orchestrate the use of multiple parallel resources to direct incoming user requests
- d. **To ensure that a predefined service level is maintained regardless of external demand or instance failures** → 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. Which of the following design strategies is *most* effective for maintaining the reliability of a cloud application?

- a. Resource isolation
- b. Resource automation
- c. **Resource redundancy** → **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.**
- d. Resource geolocation

14. Which of the following AWS services are *not likely* to benefit from Amazon edge locations? (Select TWO.)

- a. **RDS** → **RDS database instances and Lambda functions are not qualified CloudFront origins. EC2 load balancers can be used as CloudFront origins.**
- b. EC2 load balancers
- c. **Elastic Block Store (EBS)** → **RDS database instances and Lambda functions are not qualified CloudFront origins. EC2 load balancers can be used as CloudFront origins.**
- d. CloudFront

15. Which of the following is the primary benefit of using CloudFront distributions?

- a. Automated protection from mass email campaigns
- b. Greater availability through redundancy
- c. Greater security through data encryption
- d. **Reduced latency access to your content no matter where your end users live** → **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. What is the main purpose of Amazon Route 53?

- a. Countering the threat of distributed denial-of-service (DDoS) attacks
- b. **Managing domain name registration and traffic routing** → **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.**
- c. Protecting web applications from web-based threats
- d. Using the serverless power of Lambda to customize CloudFront behavior

17. According to the AWS Shared Responsibility Model, which of the following are responsibilities of AWS? (Select TWO.)

- a. **The security of the cloud** → **What's *in* the cloud is your responsibility—it includes the administration of EC2-based operating systems.**

- b. **Patching underlying virtualization software running in AWS data centers → What's *in the cloud* is your responsibility—it includes the administration of EC2-based operating systems.**
- c. Security of what's in the cloud
- d. Patching OSs running on EC2 instances

18. According to the AWS Shared Responsibility Model, what's the best way to define the status of the software driving an AWS managed service?

- a. Everything associated with an AWS managed service is the responsibility of AWS.
- b. Whatever is added by the customer (like application code) is the customer's responsibility.
- c. **Whatever the customer can control (application code and/or configuration settings) is the customer's responsibility. → 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."**
- d. Everything associated with an AWS managed service is the responsibility of the customer.

19. Which of the following is one of the first places you should look when troubleshooting a failing application?

- a. AWS Acceptable Use Monitor
- b. Service Status Dashboard
- c. AWS Billing Dashboard
- d. **Service Health Dashboard → 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. Where will you find information on the limits AWS imposes on the ways you can use your account resources?

- a. AWS User Agreement Policy
- b. **AWS Acceptable Use Policy → The correct document (and web page <https://aws.amazon.com/aup/>) for this information is the AWS Acceptable Use Policy.**
- c. AWS Acceptable Use Monitor
- d. AWS Acceptable Use Dashboard



## Review Questions – Securing AWS Resources

1. What is the primary function of the AWS IAM service?
  - a. **Identity and access management** → **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.**
  - b. Access key management
  - c. SSH key pair management
  - d. Federated access management
2. Which of the following are requirements you can include in an IAM password policy? (Select THREE.)
  - a. **Require at least one uppercase letter.** → **Including a space or null character is not a password policy option.**
  - b. **Require at least one number.** → **Including a space or null character is not a password policy option.**
  - c. Require at least one space or null character.
  - d. **Require at least one nonalphanumeric character.** → **Including a space or null character is not a password policy option.**
3. Which of the following should you do to secure your AWS root user? (Select TWO.)
  - a. Assign the root user to the “admins” IAM group.
  - b. Use the root user for day-to-day administration tasks.
  - c. **Enable MFA.** → **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.**
  - d. **Create a strong password.** → **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. How does multi-factor authentication work?
  - a. Instead of an access password, users authenticate via a physical MFA device.
  - b. In addition to an access password, users also authenticate via a physical MFA device.
  - c. Users authenticate using tokens sent to at least two MFA devices.
  - d. **Users authenticate using a password and also either a physical or virtual MFA device.** → **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. Which of the following SSH commands will successfully connect to an EC2 Amazon Linux instance with an IP address of 54.7.35.103 using a key named mykey.pem?
  - a. `echo "mykey.pem ubuntu@54.7.35.103" | ssh -i`

- b. `ssh -i mykey.pem ec2-user@54.7.35.103` → **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.**
  - c. `ssh -i mykey.pem@54.7.35.103`
  - d. `ssh ec2-user@mykey.pem:54.7.35.103 -i`
6. What's the most efficient method for managing permissions for multiple IAM users?
- a. Assign users requiring similar permissions to IAM roles.
  - b. **Assign users requiring similar permissions to IAM groups.** → **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.**
  - c. Assign IAM users permissions common to others with similar administration responsibilities.
  - d. Create roles based on IAM policies, and assign them to IAM users.
7. What is an IAM role?
- a. A set of permissions allowing access to specified AWS resources
  - b. A set of IAM users given permission to access specified AWS resources
  - c. **Permissions granted a trusted entity over specified AWS resources** → **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.**
  - d. Permissions granted an IAM user over specified AWS resources
8. How can federated identities be incorporated into AWS workflows? (Select TWO.)
- a. **You can provide users authenticated through a third-party identity provider access to backend resources used by your mobile app.** → **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.**
  - b. You can use identities to guide your infrastructure design decisions.
  - c. You can use authenticated identities to import external data (like email records from Gmail) into AWS databases.
  - d. **You can provide admins authenticated through AWS Microsoft AD with access to a Microsoft SharePoint farm running on AWS.** → **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. Which of the following are valid third-party federated identity standards? (Select TWO.)

- a. Secure Shell
- b. SSO
- c. **SAML 2.0** → **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.**
- d. **Active Directory** → **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. What information does the IAM credential report provide?

- a. A record of API requests against your account resources
- b. A record of failed password account login attempts
- c. The current state of your account security settings
- d. **The current state of security of your IAM users' access credentials** → **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. What text format does the credential report use?

- a. JSON
- b. **CSV** → **The credential report is saved to the comma-separated values (spreadsheet) format.**
- c. ASCII
- d. XML

12. Which of the following IAM policies is the best choice for the admin user you create in order to replace the root user for day-to-day administration tasks?

- a. **AdministratorAccess** → **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.**
- b. AmazonS3FullAccess
- c. AmazonEC2FullAccess
- d. AdminAccess

13. What will you need to provide for a new IAM user you're creating who will use "programmatic access" to AWS resources?

- a. A password
- b. A password and MFA
- c. An access key ID
- d. **An access key ID and secret access key** → **"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. What will IAM users with AWS Management Console access need to successfully log in?
- a. Their username, account\_number, and a password
  - b. **Their username and password** → **When the correct login page (such as <https://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.**
  - c. Their account number and secret access key
  - d. Their username, password, and secret access key
15. Which of the following will encrypt your data while in transit between your office and Amazon S3?
- a. DynamoDB
  - b. SSE-S3
  - c. **A client-side master key** → **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.**
  - d. SSE-KMS
16. Which of the following AWS resources *cannot* be encrypted using KMS?
- a. **Existing AWS Elastic Block Store volumes** → **You can only encrypt an EBS volume at creation, not later.**
  - b. RDS databases
  - c. S3 buckets
  - d. DynamoDB databases
17. What does KMS use to encrypt objects stored on your AWS account?
- a. SSH master key
  - b. KMS master key
  - c. Client-side master key
  - d. **Customer master key** → **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. Which of the following standards governs AWS-based applications processing credit card transactions?
- a. SSE-KMS
  - b. FedRAMP
  - c. **PCI DSS** → **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.**

d. ARPA

19. What is the purpose of the Service Organization Controls (SOC) reports found on AWS Artifact?

- a. They can be used to help you design secure and reliable credit card transaction applications.
- b. They attest to AWS infrastructure compliance with data accountability standards like Sarbanes–Oxley. → 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**
- c. They guarantee that all AWS-based applications are, by default, compliant with Sarbanes–Oxley standards.
- d. They're an official, ongoing risk-assessment profiler for AWS-based deployments.

20. What role can the documents provided by AWS Artifact play in your application planning? (Select TWO.)

- a. They can help you confirm that your deployment infrastructure is compliant with regulatory standards. → 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.**
- b. They can provide insight into various regulatory and industry standards that represent best practices. → 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.**
- c. They can provide insight into the networking and storage design patterns your AWS applications use.
- d. They represent AWS infrastructure design policy.

## Review Questions – Working with AWS Resources

1. Which of the following credentials can you use to log into the AWS Management Console?
  - a. Access key ID
  - b. Account alias
  - c. Account ID
  - d. Identity and Access Management (IAM) username → 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. How long will your session with the AWS Management Console remain active?
  - a. 6 hours
  - b. 12 hours → 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.**
  - c. 8 hours
  - d. 24 hours
  - e. 15 minutes
3. While looking at the EC2 service console in the AWS Management Console while logged in as the root user, you notice all of your instances are missing. What could be the reason?
  - a. You've selected the wrong region in the navigation bar. → 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.**
  - b. You don't have view access.
  - c. You've selected the wrong Availability Zone in the navigation bar.
  - d. You don't have an access key.
4. Which of the following is true regarding a resource tag?
  - a. It must be unique within an account.
  - b. It's case insensitive.
  - c. It must have a key. → 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.**
  - d. It must have a value.
5. Which of the following is required to use the AWS Command Line Interface (CLI)?
  - a. A secret key → 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.**

- b. An IAM user
  - c. Outbound network access to TCP port 80
  - d. Linux
6. Which of the following are options for installing the AWS CLI on Windows 10? (Select TWO.)
- a. **The MSI installer** → **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.**
  - b. An AWS software development kit (SDK)
  - c. The Yum or Aptitude package manager
  - d. **Using Python and pip** → **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. After installing the AWS Command Line Interface, what should you do before using it to securely manage your AWS resources?
- a. Issue the `aws --version` command.
  - b. **Issue the `aws configure` command.** → **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.**
  - c. Reboot.
  - d. Generate a new access key ID and secret access key for the root user.
8. Which output format does the AWS CLI support?
- a. Tab-separated values (TSV)
  - b. Comma-separated values (CSV)
  - c. **JavaScript object notation (JSON)** → **The AWS CLI can display output in JSON, text, or table formats. It doesn't support CSV or TSV.**
  - d. None of these

9. Which of the following programming languages are AWS software development kits available for? (Select THREE.)

- a. Fortran
- b. **JavaScript** → 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.
- c. JSON
- d. **Java** → 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.
- e. **PHP** → 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. Which of the following software development kits (SDKs) enable developers to write mobile applications that run on both Apple and Android devices? (Select TWO.)

- a. **AWS Mobile SDK for Unity** → 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.
- b. **AWS Mobile SDK for .NET and Xamarin** → 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.
- c. AWS SDK for Go
- d. AWS Mobile SDK for iOS

11. Which of the following programming languages are AWS Internet of Things (IoT) device software development kits available for? (Select TWO.)

- a. **JavaScript** → AWS IoT device SDKs are available for C++, Python, Java, JavaScript, and Embedded C. There isn't one available for Ruby or Swift.
- b. **C++** → AWS IoT device SDKs are available for C++, Python, Java, JavaScript, and Embedded C. There isn't one available for Ruby or Swift.
- c. Swift
- d. Ruby

12. What's the difference between the AWS Command Line Interface (CLI) and the AWS software development kits (SDK)? (Select TWO.)

- a. **The AWS SDKs allow you to use popular programming languages to write applications that interact with AWS services.** → 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.

- b. **The AWS CLI allows you to interact with AWS services from a terminal.** → **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.**
- c. The AWS SDKs allow you to interact with AWS services from a terminal.
- d. The AWS CLI allows you to use popular programming languages to write applications that interact with AWS services.

13. Which of the following CloudWatch features store performance data from AWS services?

- a. Logs
- b. **Metrics** → **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.**
- c. Events
- d. Metric filters
- e. Alarms

14. For which of the following scenarios can you create a CloudWatch alarm to send a notification?

- a. A metric that doesn't change for 24 hours
- b. Termination of an EC2 instance
- c. The presence of a specific IP address in a web server log
- d. **A metric that exceeds a given threshold** → **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. Which of the following Simple Notification Service (SNS) protocols can you use to send a notification? (Select TWO.)

- a. **Short Message Service (SMS) text message** → **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.**
- b. CloudWatch Events
- c. **Simple Queue Service (SQS)** → **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.**

- d. Mobile pull notification

16. Which of the following are true regarding CloudWatch Events? (Select TWO.)

- a. It can reboot an EC2 instance when an error appears in a log file.
- b. It can send an SNS notification when an EC2 instance's CPU utilization exceeds 90%.
- c. **It can send an SNS notification when an IAM user logs in to the AWS Management Console. → 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.**
- d. **It can shut down an EC2 instance at a specific time. → 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. Which of the following trigger an API action? (Select TWO.)

- a. Configuring the AWS Command Line Interface (CLI)
- b. **Viewing an S3 bucket from the AWS Management Console → 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.**
- c. Logging into the AWS Management Console
- d. **Listing IAM users from the AWS Command Line Interface (CLI) → 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. What's the most cost-effective way to view and search only the last 60 days of management API events on your AWS account?

- a. **Use CloudTrail event history. → 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.**
- b. Create a trail.
- c. Stream CloudTrail logs to CloudWatch.
- d. Use CloudWatch Events.

19. You want to log every object downloaded from an S3 bucket in a specific region. You want to retain these logs indefinitely and search them easily. What's the most cost-effective way to do this? (Select TWO.)

- a. **Stream CloudTrail logs to CloudWatch Logs.** → **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.**
- b. Use CloudTrail event history.
- c. Enable CloudTrail logging of global service events.
- d. **Create a trail to log S3 data events.** → **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. What is a benefit of using CloudTrail log file integrity validation?

- a. It lets you assert that no CloudTrail log files have been deleted from CloudWatch.
- b. **It lets you assert that no CloudTrail log files have been deleted from S3.** → **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.**
- c. It prevents unauthorized users from deleting CloudTrail log files.
- d. It tells you how a CloudTrail log file has been tampered with.

21. Which of the following Cost Explorer report types can show you the monthly costs for your reserved EC2 instances?

- a. Reserved instance recommendations
- b. Reserved Instances (RI) Coverage reports
- c. Reserved Instances (RI) Utilization reports
- d. **Costs and usage reports** → **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. Which of the following services allow you to purchase reserved instances to save money?

- a. **Amazon Relational Database Service (RDS)** → **RDS lets you purchase reserved instances to save money. Lambda, S3, and Fargate don't use instances.**
- b. Lambda
- c. S3
- d. AWS Fargate

23. Which Cost Explorer report shows the amount of money you've saved using reserved instances?

- a. Daily costs
- b. Reservation Utilization → 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.**
- c. Reservation Coverage
- d. Monthly EC2 running hours costs and usage

24. You've been running several Elasticsearch instances continuously for the past three months. You check the reserved instance recommendations in Cost Explorer but see no recommendations. What could be a reason for this?

- a. The recommendation parameters are based on the past seven days.
- b. You haven't selected the Elastic Compute Cloud (EC2) service.
- c. Cost Explorer doesn't make reservation recommendations for Elasticsearch.
- d. Your instances are already covered by reservations. → 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.**
- e. You haven't selected the ElastiCache service.

# Review Questions – The Core Compute Service

1. What is the function of an EC2 AMI?
  - a. To define the hardware profile used by an EC2 instance
  - b. To serve as an instance storage volume for high-volume data processing operations
  - c. **To serve as a source image from which an instance's primary storage volume is built** → **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).**
  - d. To define the way data streams are managed by EC2 instances
2. Where can you find a wide range of verified AMIs from both AWS and third-party vendors?
  - a. **AWS Marketplace** → **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.**
  - b. Quick Start
  - c. Community AMIs
  - d. My AMIs
3. Which of the following could be included in an EC2 AMI? (Select TWO.)
  - a. A networking configuration
  - b. **A software application stack** → **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.**
  - c. **An operating system** → **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.**
  - d. An instance type definition
4. Which of the following are EC2 instance type families? (Select TWO.)
  - a. c5d.18xlarge
  - b. **Compute optimized** → **c5d.18xlarge and t2.micro are the names of EC2 instance types, not instance type families.**
  - c. t2.micro
  - d. **Accelerated computing** → **c5d.18xlarge and t2.micro are the names of EC2 instance types, not instance type families.**

5. When describing EC2 instance types, what is the role played by the vCPU metric?
- a. vCPUs represent an instance's potential resilience against external network demands.
  - b. vCPUs represent an instance type's system memory compared to the class of memory modules on a physical machine.
  - c. vCPUs represent an AMI's processing power compared to the number of processors on a physical machine.
  - d. **vCPUs represent an instance type's compute power compared to the number of processors on a physical machine. → 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. Which of the following describes an EC2 dedicated instance?
- a. **An EC2 instance running on a physical host reserved for the exclusive use of a single AWS account → 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.**
  - b. An EC2 instance running on a physical host reserved for and controlled by a single AWS account
  - c. An EC2 AMI that can be launched only on an instance within a single AWS account
  - d. An EC2 instance optimized for a particular compute role
7. Which of the following describes an EBS volume?
- a. A software stack archive packaged to make it easy to copy and deploy to an EC2 instance
  - b. A virtualized partition of a physical storage drive that's directly connected to the EC2 instance it's associated with
  - c. **A virtualized partition of a physical storage drive that's not directly connected to the EC2 instance it's associated with → 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.**
  - d. A storage volume that's encrypted for greater security
8. Why might you want to use an instance store volume with your EC2 instance rather than a volume from the more common EBS service? (Select TWO.)
- a. Instance store volumes can be encrypted.
  - b. Instance store volumes, data will survive an instance shutdown.
  - c. **Instance store volumes provide faster data read/write performance. → Instance store volumes cannot be encrypted, nor will their data survive an instance shutdown. Those are features of EBS volumes.**

**d. Instance store volumes are connected directly to your EC2 instance. → Instance store volumes cannot be encrypted, nor will their data survive an instance shutdown. Those are features of EBS volumes.**

9. Your web application experiences periodic spikes in demand that require the provisioning of extra instances. Which of the following pricing models would make the most sense for those extra instances?

a. Spot

**b. On-demand → 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.**

c. Reserved

d. Dedicated

10. Your web application experiences periodic spikes in demand that require the provisioning of extra instances. Which of the following pricing models would make the most sense for the "base" instances that will run constantly?

a. Spot

b. On-demand

c. Spot fleet

**d. Reserved → 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. Which of the following best describes what happens when you purchase an EC2 reserved instance?

**a. Charges for any instances you run matching the reserved instance type will be covered by the reservation. → 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.**

b. Capacity matching the reserved definition will be guaranteed to be available whenever you request it.

c. Your account will immediately and automatically be billed for the full reservation amount.

d. An EC2 instance matching your reservation will automatically be launched in the selected AWS Region.

12. Which of the following use cases are good candidates for spot instances? (Select TWO.)

- a. **Big data processing workloads** → **Because spot instances can be shut down, they're not recommended for applications that provide any kind of always-on service.**
- b. **Ecommerce websites**
- c. **Continuous integration development environments** → **Because spot instances can be shut down, they're not recommended for applications that provide any kind of always-on service.**
- d. Long-term, highly available, content-rich websites

13. Which AWS services simplify the process of bringing web applications to deployment? (Select TWO.)

- a. Elastic Block Store
- b. Elastic Compute Cloud
- c. **Elastic Beanstalk** → **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.**
- d. **Lightsail** → **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. Which of the following services bills at a flat rate regardless of how it's consumed?

- a. **Lightsail** → **Beanstalk, EC2 (non-reserved instances), and RDS all bill according to actual usage.**
- b. Elastic Beanstalk
- c. Elastic Compute Cloud
- d. Relational Database Service

15. Which of these stacks are available from Lightsail blueprints? (Select TWO.)

- a. Ubuntu
- b. **Gitlab** → **Ubuntu is an OS, not a stack. WordPress is an application, not an OS.**
- c. WordPress
- d. **LAMP** → **Ubuntu is an OS, not a stack. WordPress is an application, not an OS.**

16. Which of these AWS services use primarily EC2 resources under the hood? (Select TWO.)

- a. Elastic Block Store
- b. **Lightsail** → **Elastic Block Store is, for practical purposes, an EC2 resource. RDS is largely built on its own infrastructure.**
- c. **Elastic Beanstalk** → **Elastic Block Store is, for practical purposes, an EC2 resource. RDS is largely built on its own infrastructure.**
- d. Relational Database Service



17. Which of the following AWS services are designed to let you deploy Docker containers? (Select TWO.)

- a. **Elastic Container Service** → While you could, in theory at least, manually install Docker Engine on either a Lightsail or EC2 instance, that's not their primary function.
- b. Lightsail
- c. **Elastic Beanstalk** → While you could, in theory at least, manually install Docker Engine on either a Lightsail or EC2 instance, that's not their primary function.
- d. Elastic Compute Cloud

18. Which of the following use container technologies? (Select TWO.)

- a. **Docker** → Both Lambda and Lightsail are compute services that—while they might possibly make use of containers under the hood—are not themselves container technologies.
- b. **Kubernetes** → Both Lambda and Lightsail are compute services that—while they might possibly make use of containers under the hood—are not themselves container technologies.
- c. Lambda
- d. Lightsail

19. What role can the Python programming language play in AWS Lambda?

- a. Python cannot be used for Lambda.
- b. It is the primary language for API calls to administrate Lambda remotely.
- c. **It is used as the underlying code driving the service.** → Python is, indeed, a valid choice for a function's runtime environment. There is no one "primary" language for Lambda API calls.
- d. It can be set as the runtime environment for a function.

20. What is the maximum time a Lambda function may run before timing out?

- a. **15 minutes** → While the maximum time was, at one point, 5 minutes, that's been changed to 15.
- b. 5 minutes
- c. 1 minute
- d. 1 hour

## Review Questions – The Core Storage Service

1. When trying to create an S3 bucket named documents, AWS informs you that the bucket name is already in use. What should you do in order to create a bucket?
  - a. Use a different region.
  - b. **Use a globally unique bucket name.** → **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.**
  - c. Use a different storage class.
  - d. Use a longer name.
  - e. Use a shorter name.
  
2. Which S3 storage classes are most cost-effective for infrequently accessed data that can't be easily replaced? (Select TWO.)
  - a. **STANDARD\_IA** → **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.**
  - b. ONEZONE\_IA
  - c. **GLACIER** → **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.**
  - d. STANDARD
  - e. INTELLIGENT\_TIERING
  
3. What are the major differences between Simple Storage Service (S3) and Elastic Block Store (EBS)? (Select TWO.)
  - a. **EBS stores volumes.** → **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.**
  - b. EBS stores snapshots.
  - c. S3 stores volumes.
  - d. **S3 stores objects.** → **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.**

- e. EBS stores objects.
4. Which tasks can S3 object life cycle configurations perform automatically? (Select THREE.)
- a. **Deleting old object versions** → 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.
  - b. **Moving objects to Glacier** → 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.
  - c. Deleting old buckets
  - d. **Deleting old objects** → 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.
  - e. Moving objects to an EBS volume
5. What methods can be used to grant anonymous access to an object in S3? (Select TWO.)
- a. **Bucket policies** → 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.
  - b. **Access control lists** → 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.
  - c. User policies
  - d. Security groups
6. Your budget-conscious organization has a 5 TB database file it needs to retain off-site for at least 5 years. In the event the organization needs to access the database, it must be accessible within 8 hours. Which cloud storage option should you recommend, and why? (Select TWO.)
- a. S3 has the most durable storage.
  - b. S3.
  - c. **S3 Glacier.** → 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.

- d. **Glacier is the most cost effective.** → 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.
  - e. S3 has the fastest retrieval times.
  - f. S3 doesn't support object sizes greater than 4 TB.
7. Which of the following actions can you perform from the S3 Glacier service console?
- a. Delete an archive
  - b. **Create a vault** → 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.
  - c. Create an archive
  - d. Delete a bucket
  - e. Retrieve an archive
8. Which Glacier retrieval option generally takes 3 to 5 hours to complete?
- a. Provisioned
  - b. Expedited
  - c. Bulk
  - d. **Standard** → 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. What's the minimum size for a Glacier archive?
- a. **1 byte** → A Glacier archive can be as small as 1 byte and as large as 40 TB. You can't have a zero-byte archive.
  - b. 40 TB
  - c. 5 TB
  - d. 0 bytes

10. Which types of AWS Storage Gateway let you connect your servers to block storage using the iSCSI protocol? (Select TWO.)
- a. Cached gateway
  - b. **Tape gateway** → **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.**
  - c. File gateway
  - d. **Volume gateway** → **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. Where does AWS Storage Gateway primarily store data?
- a. Glacier vaults
  - b. **S3 buckets** → **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.**
  - c. EBS volumes
  - d. EBS snapshots
12. You need an easy way to transfer files from a server in your data center to S3 without having to install any third-party software. Which of the following services and storage protocols could you use? (Select FOUR.)
- a. **AWS Storage Gateway—file gateway** → **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.**
  - b. **iSCSI** → **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.**
  - c. AWS Snowball
  - d. **SMB** → **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.**
  - e. **AWS Storage Gateway—volume gateway** → **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.

f. The AWS CLI

13. Which of the following are true regarding the AWS Storage Gateway—volume gateway configuration? (Select THREE.)

- a. **Stored volumes asynchronously back up data to S3 as EBS snapshots.** → 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.
- b. Stored volumes can be up to 32 TB in size.
- c. **Cached volumes locally store only a frequently used subset of data.** → 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.
- d. Cached volumes asynchronously back up data to S3 as EBS snapshots.
- e. **Cached volumes can be up to 32 TB in size.** → 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. What's the most data you can store on a single Snowball device?

- a. 42 TB
- b. 50 TB
- c. **72 TB** → 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.
- d. 80 TB

15. Which of the following are security features of AWS Snowball? (Select TWO.)

- a. **It enforces encryption at rest.** → 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.
- b. **It uses a Trusted Platform Module (TPM) chip.** → 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.**

- c. It enforces NFS encryption.
- d. It has tamper-resistant network ports.

16. Which of the following might AWS do after receiving a damaged Snowball device from a customer?

- a. Copy the customer's data to Glacier
- b. Replace the Trusted Platform Module (TPM) chip
- c. **Securely erase the customer's data from the device → 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.**
- d. Copy the customer's data to S3

17. Which of the following can you use to transfer data to AWS Snowball from a Windows machine without writing any code?

- a. NFS
- b. **The Snowball Client → 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.**
- c. iSCSI
- d. SMB
- e. The S3 SDK Adapter for Snowball

18. How do the AWS Snowball and Snowball Edge devices differ? (Select TWO.)

- a. **Snowball Edge supports copying files using NFS. → 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.**
- b. Snowball devices can be clustered together for storage.
- c. Snowball's QSFP+ network interface supports speeds up to 40 Gbps.
- d. **Snowball Edge can run EC2 instances. → 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. Which of the following Snowball Edge device options is the best for running machine learning applications?

- a. Compute Optimized
- b. **Compute Optimized with GPU → 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.**

- c. Storage Optimized
- d. Network Optimized

20. Which of the following hardware devices offers a network interface speed that supports up to 100 Gbps?

- a. Snowball Edge with the Storage Optimized configuration
- b. Snowball Edge with the Compute Optimized configuration → 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.**
- c. Storage Gateway
- d. 80 TB Snowball



## Review Questions – The Core Database Service

1. Which type of database stores data in columns and rows?
  - a. Nonrelational
  - b. Relational** → **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.**
  - c. Key-value store
  - d. Document
2. Which of the following Structured Query Language (SQL) statements can you use to write data to a relational database table?
  - a. CREATE
  - b. INSERT** → **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.**
  - c. QUERY
  - d. WRITE
3. Which of the following statements is true regarding nonrelational databases?
  - a. You can create only one table.
  - b. No primary key is required.
  - c. You can't store data with a fixed structure.
  - d. You don't have to define all the types of data that a table can store before adding data to it.** → **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. What is a no-SQL database?
  - a. A nonrelational database without primary keys
  - b. A schemaless relational database
  - c. A schemaless nonrelational database** → **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.**
  - d. A relational database with primary keys
5. What do new Relational Database Service (RDS) instances use for database storage?
  - a. Instance volumes
  - b. Elastic Block Store (EBS) volumes** → **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.

- c. Snapshots
  - d. Magnetic storage
6. Which of the following are database engine options for Amazon Relational Database Service (RDS)? (Select TWO.)
- a. IBM dBase
  - b. PostgreSQL → 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.**
  - c. DynamoDB
  - d. Amazon Aurora → 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.**
  - e. Redis
7. What two databases is Amazon Aurora compatible with? (Select TWO.)
- a. MySQL → 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.**
  - b. PostgreSQL → 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.**
  - c. MariaDB
  - d. Oracle
  - e. Microsoft SQL Server
8. Which of the following features of Relational Database Service (RDS) can prevent data loss in the event of an Availability Zone failure? (Select TWO.)
- a. Read replicas
  - b. Multi-AZ → 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.**
  - c. Snapshots → 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.**
  - d. IOPS
  - e. Vertical scaling

9. Which RDS database engine offers automatically expanding database storage up to 64 TB?

- a. Microsoft SQL Server
- b. Amazon Aurora → 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.**
- c. Oracle
- d. Amazon Athena

10. Which of the following Relational Database Service (RDS) features can help you achieve a monthly availability of 99.95 percent?

- a. Multi-AZ → 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.**
- b. Read replicas
- c. Point-in-time recovery
- d. Horizontal scaling

11. What is true regarding a DynamoDB partition? (Select TWO.)

- a. It's stored within a table.
- b. It's backed by solid-state drives. → 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.**
- c. It's a way to uniquely identify an item in a table.
- d. It's replicated across multiple Availability Zones. → 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. What is the minimum monthly availability for DynamoDB in a single region?

- a. 99.99 percent → 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.**
- b. 99.95 percent
- c. 99.9 percent
- d. 99.0 percent

13. Which of the following statements is true regarding a DynamoDB table?

- a. It can store only one data type.
- b. When you create a table, you must define the maximum number of items that it can store.

- c. Items in a table can have duplicate values for the primary key.
- d. **Items in a table don't have to have all the same attributes. → 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. Which configuration parameters can you adjust to improve write performance against a DynamoDB table? (Select TWO.)

- a. Decrease read capacity units (RCU)
- b. Increase read capacity units
- c. **Increase write capacity units (WCU) → 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.**
- d. Decrease write capacity units
- e. **Enable DynamoDB Auto Scaling → 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. Which DynamoDB operation is the most read-intensive?

- a. Write
- b. Query
- c. **Scan → 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.**
- d. Update

16. Which of the following would be appropriate to use for a primary key in a DynamoDB table that stores a customer list?

- a. The customer's full name
- b. The customer's phone number
- c. The customer's city
- d. **A randomly generated customer ID number → 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. Which type of Redshift node uses magnetic storage?

- a. Cost-optimized
- b. **Dense compute → Dense compute nodes use magnetic disks. Dense storage nodes use SSDs. There are no such nodes as dense memory or cost-optimized.**

- c. Dense storage
- d. Dense memory

18. Which Redshift feature can analyze structured data stored in S3?

- a. **Redshift Spectrum** → **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.**
- b. Redshift S3
- c. Amazon Athena
- d. Amazon RDS

19. What is the term for a relational database that stores large amounts of structured data from a variety of sources for reporting and analysis?

- a. Data storehouse
- b. **Data warehouse** → **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.**
- c. Report cluster
- d. Dense storage node

20. What's the maximum amount of data you can store in a Redshift cluster when using dense storage nodes?

- a. **2 PB** → **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.**
- b. 326 TB
- c. 2 TB
- d. 326 PB
- e. 236 TB

## Review Questions – The Core Networking Services

1. Which of the following are true of a default VPC? (Select TWO.)
  - a. A default VPC spans multiple regions.
  - b. **AWS creates a default VPC in each region. → 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.**
  - c. AWS creates a default VPC in each Availability Zone.
  - d. **By default, each default VPC is available to one AWS account. → 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. Which of the following is a valid CIDR for a VPC or subnet?
  - a. **10.0.0.0/28 → 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.**
  - b. 10.0.0.0/29
  - c. 10.0.0.0/8
  - d. 10.0.0.0/15
3. Which of the following are true regarding subnets? (Select TWO.)
  - a. A VPC must have at least two subnets.
  - b. **A subnet must have a CIDR that's a subset of the CIDR of the VPC in which it resides. → 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.**
  - c. **A subnet spans one Availability Zone. → 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.**
  - d. A subnet spans multiple Availability Zones.
4. Which of the following is true of a new security group?
  - a. It contains an inbound rule denying access from public IP addresses.
  - b. It contains an outbound rule denying access to public IP addresses.
  - c. **It contains an outbound rule allowing access to any IP address. → 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.**
  - d. It contains an inbound rule allowing access from any IP address.
  - e. It contains an inbound rule denying access from any IP address.

5. What's the difference between a security group and a network access control list (NACL)? (Select TWO.)
- a. A network access control list operates at the instance level.
  - b. A security group operates at the instance level. → 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.**
  - c. A security group operates at the subnet level.
  - d. A network access control list operates at the subnet level. → 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. Which of the following is true of a VPC peering connection?
- a. It's a private connection that connects more than three VPCs.
  - b. It's a private connection between two VPCs. → 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.**
  - c. It's a public connection between two VPCs.
  - d. It's a virtual private network (VPN) connection between two VPCs.
7. What are two differences between a virtual private network (VPN) connection and a Direct Connect connection? (Select TWO.)
- a. A Direct Connect connection offers predictable latency because it doesn't traverse the internet. → 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.**
  - b. A VPN connection uses the internet for transport. → 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.**
  - c. A Direct Connect connection uses AES 128- or 256-bit encryption.
  - d. A VPN connection requires proprietary hardware.
8. Which of the following are true about registering a domain name with Route 53? (Select TWO.)
- a. The registrar you use to register a domain name determines who will host DNS for that domain.
  - b. You can register a domain name for a term of up to 10 years. → 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.**

- c. Route 53 creates a private hosted zone for the domain.
- d. **Route 53 creates a public hosted zone for the domain. → 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. Which of the following Route 53 routing policies can return set of randomly ordered values?

- a. Simple
- b. **Multivalue Answer → 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.**
- c. Failover
- d. Latency

10. Which of the following Route 53 routing policies doesn't use health checks?

- a. Latency
- b. Multivalue Answer
- c. **Simple → All Route 53 routing policies except for Simple can use health checks.**
- d. Geolocation

11. Which of the following types of Route 53 health checks works by making a test connection to a TCP port?

- a. Simple
- b. CloudWatch alarm
- c. **Endpoint → 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.**
- d. Calculated

12. You have two EC2 instances hosting a web application. You want to distribute 20 percent of traffic to one instance and 80 percent to the other. Which of the following Route 53 routing policies should you use?

- a. **Weighted → 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.**
- b. Failover



- c. Multivalue Answer
- d. Simple

13. Resources in a VPC need to be able to resolve internal IP addresses for other resources in the VPC. No one outside of the VPC should be able to resolve these addresses. Which of the following Route 53 resources can help you achieve this?

- a. A public hosted zone
- b. A private hosted zone → 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.**
- c. Domain name registration
- d. Health checks

14. You want to provide private name resolution for two VPCs using the domain name company.pri. How many private hosted zones do you need to create?

- a. 1 → 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.**
- b. 2
- c. 3
- d. 4

15. On how many continents are CloudFront edge locations distributed?

- a. 7
- b. 6 → CloudFront has edge locations on six continents (Antarctica is a hard place to get to).**
- c. 5
- d. 4

16. From where does CloudFront retrieve content to store for caching?

- a. Regions
- b. Origins → 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.**
- c. Distributions
- d. Edge locations

17. Which CloudFront distribution type requires you to provide a media player?

- a. Streaming
- b. RTMP → 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.**

- c. Web
- d. Edge

18. You need to deliver content to users in the United States and Canada. Which of the following edge location options will be the most cost effective for your CloudFront distribution?

- a. United States, Canada, and Europe → 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.**
- b. United States, Canada, Europe, and Asia
- c. United States, Canada, Europe, Asia, and Africa
- d. All edge locations

19. Approximately how many different CloudFront edge locations are there?

- a. About 50
- b. More than 150 → There are more than 150 edge locations throughout the world.**
- c. More than 300
- d. More than 500

20. Which of the following are valid origins for a CloudFront distribution? (Select TWO.)

- a. EC2 instance → An origin can be an EC2 instance or a public S3 bucket. You can't use a private S3 bucket as an origin.**
- b. A public S3 bucket → An origin can be an EC2 instance or a public S3 bucket. You can't use a private S3 bucket as an origin.**
- c. A private S3 bucket that you don't have access to
- d. A private S3 bucket that you own

## Review Questions – Automating Your AWS Workloads

1. Which of the following is an advantage of using CloudFormation?
  - a. It uses the popular Python programming language.
  - b. It prevents unauthorized manual changes to resources.
  - c. **It lets you create multiple separate AWS environments using a single template.**  
→ **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.**
  - d. It can create resources outside of AWS.
2. What formats do CloudFormation templates support? (Select TWO.)
  - a. XML
  - b. **YAML → CloudFormation templates are written in the YAML or JSON format.**
  - c. HTML
  - d. **JSON → CloudFormation templates are written in the YAML or JSON format.**
3. What's an advantage of using parameters in a CloudFormation template?
  - a. **Allow customizing a stack without changing the template.** → **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.**
  - b. Prevent unauthorized users from using a template.
  - c. Prevent stack updates.
  - d. Allow multiple stacks to be created from the same template.
4. Why would you use CloudFormation to automatically create resources for a development environment instead of creating them using AWS CLI commands? (Select TWO.)
  - a. **Resources CloudFormation creates are organized into stacks and can be managed as a single unit.** → **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.**
  - b. **CloudFormation stack updates help ensure that changes to one resource won't break another.** → **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.**

- c. Resources created by CloudFormation always work as expected.
  - d. CloudFormation can provision resources faster than the AWS CLI.
5. What are two features of CodeCommit? (Select TWO.)
- a. **Versioning** → **CodeCommit is a private Git repository that offers versioning and differencing. It does not perform deployments.**
  - b. Automatic deployment
  - c. **Differencing** → **CodeCommit is a private Git repository that offers versioning and differencing. It does not perform deployments.**
  - d. Manual deployment
6. In the context of CodeCommit, what can differencing accomplish?
- a. Allowing reverting to an older version of a file
  - b. **Understanding what code change introduced a bug** → **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.**
  - c. Deleting duplicate lines of code
  - d. Seeing when an application was last deployed
7. What software development practice regularly tests new code for bugs but doesn't do anything else?
- a. Differencing
  - b. Continuous deployment
  - c. Continuous delivery
  - d. **Continuous integration** → **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. Which CodeBuild build environment compute types support Windows operating systems? (Select TWO.)
- a. build.general2.large
  - b. **build.general1.medium** → **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.**
  - c. build.general1.small
  - d. **build.general1.large** → **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.**
  - e. build.windows1.small

9. What does a CodeBuild environment always contain? (Select TWO.)

- a. **An operating system** → **A CodeBuild build environment always contains an operating system and a Docker image. It may contain the other components but doesn't have to.**
- b. **A Docker image** → **A CodeBuild build environment always contains an operating system and a Docker image. It may contain the other components but doesn't have to.**
- c. The Python programming language
- d. .NET Core
- e. The PHP programming language

10. Which of the following can CodeDeploy do? (Select THREE.)

- a. **Deploy an application to an on-premises Windows instance.** → **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.**
- b. **Deploy a Docker container to the Elastic Container Service.** → **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.**
- c. **Upgrade an application on an EC2 instance running Red Hat Enterprise Linux.** → **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.**
- d. Deploy an application to an Android smartphone.
- e. Deploy a website to an S3 bucket.

11. What is the minimum number of actions in a CodePipeline pipeline?

- a. 1
- b. **2** → **At the very least, a CodePipeline must consist of a source stage and a deploy stage.**
- c. 3
- d. 4
- e. 0

12. You want to predefine the configuration of EC2 instances that you plan to launch manually and using Auto Scaling. What resource must you use?

- a. CloudFormation template
- b. Instance role
- c. Launch configuration
- d. **Launch template** → **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. What Auto Scaling group parameters set the limit for the number of instances that Auto Scaling creates? (Select TWO.)

- a. **Maximum** → **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.**
- b. Group size
- c. Desired capacity
- d. **Minimum** → **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. An Auto Scaling group has a desired capacity of 7 and a maximum size of 7. What will Auto Scaling do if someone manually terminates one of these instances?

- a. It will not launch any new instances.
- b. **It will launch one new instance.** → **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.**
- c. It will terminate one instance.
- d. It will change the desired capacity to 6.

15. What Auto Scaling feature creates a scaling schedule based on past usage patterns?

- a. **Predictive scaling** → **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.**
- b. Scheduled scaling
- c. Dynamic scaling
- d. Pattern scaling

16. What type of AWS Systems Manager document can run Bash or PowerShell scripts on an EC2 instance?

- a. Run document
- b. **Command document** → **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.**
- c. Automation document

d. Script document

17. What type of AWS Systems Manager document can take a snapshot of an EC2 instance?

a. Command document

b. Run document

c. Script document

**d. Automation document** → **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. Which of the following OpsWorks services uses Chef recipes?

a. AWS OpsWorks for Puppet Enterprise

**b. AWS OpsWorks Stacks** → **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.**

c. AWS OpsWorks Layers

d. AWS OpsWorks for Automation

19. What configuration management platforms does OpsWorks support? (Select TWO.)

a. SaltStack

**b. Puppet Enterprise** → **OpsWorks supports the Puppet Enterprise and Chef configuration management platforms. It doesn't support SaltStack, Ansible, or CFEngine.**

c. CFEngine

**d. Chef** → **OpsWorks supports the Puppet Enterprise and Chef configuration management platforms. It doesn't support SaltStack, Ansible, or CFEngine.**

e. Ansible

20. Which of the following OpsWorks Stacks layers contains at least one EC2 instance?

a. EC2 Auto Scaling layer

b. Elastic Container Service (ECS) cluster layer

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

d. Relational Database Service (RDS) layer

e. Elastic Load Balancing (ELB) layer

## Review Questions – Common Use Case Scenarios

1. Which of the following is *not* one of the pillars of the Well-Architected Framework?
  - a. Performance efficiency
  - b. Reliability
  - c. **Resiliency** → **The five pillars of the Well-Architected Framework are reliability, performance efficiency, security, cost optimization, and operational excellence. Resiliency is not one of them.**
  - d. Security
  - e. Cost optimization
  
2. Which of the following are examples of applying the principles of the security pillar of the Well-Architected Framework? (Select TWO.)
  - a. **Granting each AWS user their own IAM username and password** → **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.**
  - b. Creating a security group rule to deny access to unused ports
  - c. Deleting an empty S3 bucket
  - d. **Enabling S3 versioning** → **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. You're hosting a web application on two EC2 instances in an Auto Scaling group. The performance of the application is consistently acceptable. Which of the following can help maintain or improve performance efficiency? (Select TWO.)
  - a. Monitoring for unauthorized access
  - b. Doubling the number of instances in the Auto Scaling group
  - c. **Implementing policies to prevent the accidental termination of EC2 instances in the same Auto Scaling group** → **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.**



**d. Using CloudFront** → 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. Which of the following can help achieve cost optimization? (Select TWO.)

- a. Deleting unused S3 objects** → 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.
- b. Deleting empty S3 buckets
- c. Deleting unused application load balancers** → 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.
- d. Deleting unused VPCs

5. Which of the following is a key component of operational excellence?

- a. Adding more security personnel
- b. Automating manual processes** → 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.
- c. Making minor improvements to bad processes
- d. Making people work longer hours

6. Your default VPC in the us-west-1 Region has three default subnets. How many Availability Zones are in this Region?

- a. 2
- b. 3** → 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.
- c. 4
- d. 5

7. Your organization is building a database-backed web application that will sit behind an application load balancer. You add an inbound security group rule to allow HTTP traffic on TCP port 80. Where should you apply this security group to allow users to access the application?
- a. **The application load balancer listener** → **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.**
  - b. The database instance
  - c. The subnets where the instances reside
  - d. None of these
8. How does an application load balancer enable reliability?
- a. **By routing traffic away from failed instances** → **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.**
  - b. By replacing failed instances
  - c. By routing traffic to the least busy instances
  - d. By caching frequently accessed content
9. Which of the following contains the configuration information for instances in an Auto Scaling group?
- a. Launch directive
  - b. Dynamic scaling policy
  - c. CloudFormation template
  - d. **Launch template** → **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. You've created a target tracking policy for an Auto Scaling group. You want to ensure that the number of instances in the group never exceeds 5. How can you accomplish this?
- a. Set the group size to 5.
  - b. **Set the maximum group size to 5.** → **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.

- c. Set the minimum group size to 5.
- d. Delete the target tracking policy.

11. Which of the following is an example of a static website?

- a. A WordPress blog
- b. A website hosted on S3 → 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.**
- c. A popular social media website
- d. A web-based email application

12. Which of the following features of S3 improve the security of data you store in an S3 bucket? (Select TWO.)

- a. Objects in S3 are not public by default. → 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.**
- b. All objects are readable by all AWS users by default.
- c. By default, S3 removes ACLs that allow public read access to objects. → 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.**
- d. S3 removes public objects by default.

13. Which of the following is required to enable S3 static website hosting on a bucket?

- a. Enable bucket hosting in the S3 service console. → 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.**
- b. Disable default encryption.
- c. Disable object versioning.
- d. Enable object versioning.
- e. Make all objects in the bucket public.

14. You've created a static website hosted on S3 and given potential customers the URL that consists of words and numbers. They're complaining that it's too hard to type in. How can you come up with a friendlier URL?
- a. Re-create the bucket using only words in the name.
  - b. **Use a custom domain name.** → **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.**
  - c. Re-create the bucket in a different Region.
  - d. Re-create the bucket using only numbers in the name.
15. Which of the following is true regarding static websites hosted in S3?
- a. **The content served is not encrypted in transit.** → **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.**
  - b. Anyone can modify the content.
  - c. You must use a custom domain name.
  - d. A website hosted on S3 is stored in multiple Regions.
16. Which of the following can impact the reliability of a web application running on EC2 instances?
- a. Taking EBS snapshots of the instances.
  - b. The user interface is too difficult to use.
  - c. **Not replacing a misconfigured resource that the application depends on.** → **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.**
  - d. Provisioning too many instances.
17. You have a public web application running on EC2 instances. Which of the following factors affecting the performance of your application might be out of your control?
- a. Storage
  - b. Compute
  - c. **Network** → **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.**
  - d. Database

18. An Auto Scaling group can use an EC2 system health check to determine whether an instance is healthy. What other type of health check can it use?

- a. S3
- b. SNS
- c. VPC
- d. **ELB** → **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. You're hosting a static website on S3. Your web assets are stored under the Standard storage class. Which of the following is true regarding your site?

- a. Someone may modify the content of your site without authorization.
- b. **You're responsible for S3 charges.** → **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.**
- c. You're charged for any compute power used to host the site.
- d. An Availability Zone outage may bring down the site.

20. You're hosting a static website on S3. Your web assets are stored in the US East 1 Region in the bucket named mygreatwebsite. What is the URL of the website?

- a. <http://mygreatwebsite.s3-website-us-east-1.amazonaws.com> → **The format of the URL is the bucket name, followed by s3-website-, the Region identifier, and then amazonaws.com.**
- b. <http://mygreatwebsite.s3.amazonaws.com>
- c. <http://mygreatwebsite.s3-website-us-east.amazonaws.com>
- d. <http://mygreatwebsite.s3-us-east-1.amazonaws.com>