1. 1. Question

A company is seeking to deploy an existing .NET application onto AWS as quickly as possible. Which AWS Service should the customer use to achieve this goal?

* 1. AWS Amplify
  2. AWS Systems Manager
  3. AWS Trusted Advisor
  4. **AWS Elastic Beanstalk**

**Unattempted**

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.  
The other options are incorrect:  
“AWS Amplify“ is incorrect. AWS Amplify is used for building secure and scalable web and mobile applications. AWS Amplify consists of a set of tools (open source framework, visual development environment, console) and services (web app and static website hosting) to accelerate the development of mobile and web applications on AWS.  
Note: The AWS Amplify‘s web hosting feature can only be used to deploy static web apps or server-side rendered (SSR) web apps created using Next.js only. AWS Amplify cannot be used to deploy .NET applications.  
“AWS Trusted Advisor“ is incorrect. AWS Trusted Advisor analyzes AWS environments and provides best practice recommendations in five categories: cost optimization, security, fault tolerance, performance and service limits.  
“AWS Systems Manager“ is incorrect. AWS Systems Manager allows customers to centralize operational data from multiple AWS services and automate tasks across their AWS resources.  
References:  
<https://aws.amazon.com/elasticbeanstalk/>

1. 2. Question

​ What is the AWS Support feature that allows customers to manage support cases programmatically?

* 1. **AWS Support API**
  2. AWS Trusted Advisor
  3. AWS Health Dashboard
  4. AWS Operations Support

**Unattempted**

The AWS Support API provides programmatic access to AWS Support Center features to create, manage, and close support cases, and operationally manage Trusted Advisor check requests and status. AWS Support API is available only for AWS  customers who have a Business, Enterprise On-Ramp, or Enterprise support plan.  
The service currently provides two different groups of operations:  
1- Support Case Management operations to manage the entire life cycle of AWS support cases, from creating a case to resolving it.  
2- Trusted Advisor operations to access the checks provided by AWS Trusted Advisor.  
The other options are incorrect:  
“AWS Trusted Advisor“ is incorrect. AWS Trusted Advisor analyzes AWS environments and provides best practice recommendations in five categories: cost optimization, security, fault tolerance, performance and service limits (also referred to as Service quotas).  
“AWS Health Dashboard“ is incorrect. The AWS Health Dashboard is the single place to learn about the availability and operations of AWS services. You can view the overall status of all AWS services, and you can sign in to access a personalized view of the health of the specific services that are powering your workloads and applications. AWS Health Dashboard proactively notifies you when AWS experiences any events that may affect you, helping provide quick visibility and guidance to minimize the impact of events in progress, and plan for any scheduled changes, such as AWS hardware maintenance.  
“AWS Operations Support“ is incorrect. Included with the Enterprise support plan, Operations Support provides consultative reviews of your AWS operations and advice for optimization.  
References:  
<https://docs.aws.amazon.com/awssupport/latest/user/Welcome.html>

1. 3. Question

When granting permissions to applications running on Amazon EC2 instances, which of the following is considered best practice?

* 1. Store the required AWS credentials directly within the application code
  2. Generate new IAM access keys every time you delegate permissions
  3. **Use temporary security credentials (IAM roles) instead of long-term access keys**
  4. Do nothing; Applications that run on Amazon EC2 instances do not need permission to interact with other AWS services or resources

**Unattempted**

AWS recommends using an IAM role to manage temporary credentials for applications that run on Amazon EC2 instances. When you use a role, you don‘t have to distribute long-term credentials (such as a user name and password or access keys) to an EC2 instance. Instead, the role supplies temporary permissions that applications can use when they interact with other AWS resources. For example, if you have a photo-editing application running on an Amazon EC2 instance, and you want to grant the application permission to save user‘s photo uploads to an Amazon S3 bucket, it is best to use an IAM role to delegate the required permissions because role credentials are temporary and rotated automatically.  
IAM roles with temporary credentials are useful in the following situations:  
Applications running on Amazon EC2: You can use an IAM role to manage temporary credentials for applications running on an EC2 instance and make AWS CLI or AWS API requests. This is more secure than storing access keys within the EC2 instance.  
Federated user access: Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as federated users. AWS assigns a role to a federated user when access is requested through an identity provider.  
AWS service access: A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM.  
The other options are incorrect:  
“Store the required AWS credentials directly within the application code“ is incorrect. It is not secure to store AWS credentials (such as a username and password or access keys) within the application code. Storing credentials directly in application code often results in long-lived credentials being saved in source control, which increases the attack surface of your application.  
“Do nothing; Applications that run on Amazon EC2 instances do not need permission to interact with other AWS services or resources“ is incorrect. Amazon EC2 and all other AWS services start with no permissions. Applications running on Amazon EC2 or any other compute service cannot interact with other AWS resources without permission.  
“Generate new IAM access keys every time you delegate permissions“ is incorrect. It is not secure to use long-term credentials (such as a username and password or access keys) to delegate permissions to applications running on Amazon EC2 instances. Using IAM roles is more secure because role credentials are temporary and rotated automatically.  
References:  
<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html>

1. 4. Question

A company is using EC2 Instances to run their e-commerce site on the AWS platform. If the site becomes unavailable, the company will lose a significant amount of money for each minute the site is unavailable. Which design principle should the company use to minimize the risk of an outage?

* 1. **Fault Tolerance**
  2. Pilot Light
  3. Multi-threading
  4. Least Privilege

**Unattempted**

A system that is designed to be fault tolerant can recover gracefully from EC2 instance failures. Amazon Web Services gives customers access to a vast amount of IT infrastructure–compute, storage, and communications–that they can allocate automatically (or nearly automatically) to account for almost any kind of failure.  
The other options are incorrect:  
“Least Privilege” is incorrect. Principle of least privilege is a security concept related to access management, not fault tolerance. The principle of least privilege means granting users the required permissions to perform the tasks entrusted to them and nothing more.  
“Pilot Light” is incorrect. A pilot light scenario is a disaster recover / business continuity scenario wherein a minimal amount of services are kept running in a failover location to enable the business to meet their Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in the event of a disaster. By nature, a pilot light scenario will take some time to spin up and promote to production (as opposed to an active-active DR scenario) and will therefore not mitigate the per-minute losses that will be experienced by the company in the event of an outage.  
Additional information: Recovery time objective (RTO) and recovery point objective (RPO) are two key metrics to consider when developing a disaster recover (DR) plan. RTO represents how many hours it takes customers to return to a working state after a disaster. RPO, which is also expressed in hours, represents how much data customers could lose when a disaster happens. For example, an RPO of 1 hour means that customers could lose up to 1 hour’s worth of data when a disaster occurs.  
Read more about disaster recovery scenarios here:  
<https://aws.amazon.com/blogs/publicsector/rapidly-recover-mission-critical-systems-in-a-disaster/>  
“Multi-threading” is incorrect. Multi-threading is the ability of a central processing unit (CPU) to provide multiple threads of execution concurrently, which may lead to faster overall execution. Amazon EC2 instances support multi-threading, For example, an m5.xlarge instance type has two CPU cores and two threads per core by default—four threads in total. While multi-threading leads to maximum utilization of the CPU and improves the overall perfomance of EC2 instances, multi-threading has nothing to do with recovering EC2 instances from failures.  
References:  
<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/wellarchitected-reliability-pillar.pdf#design-your-workload-to-withstand-component-failures>

1. 5. Question

​Which AWS Service helps enterprises extend their on-premises storage to AWS in a cost-effective manner?

* 1. Amazon EFS
  2. Amazon Aurora
  3. AWS Data Pipeline
  4. **AWS Storage Gateway**

**Unattempted**

Enterprises can extend their on-premises storage to AWS Cloud for long-term backup retention and archiving, optimizing costs and increasing resilience and availability. AWS Storage Gateway is a hybrid storage service that enables on-premises applications to seamlessly use AWS cloud storage. Enterprises can use the service for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration. The storage gateway connects to AWS storage services, such as Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Amazon EBS, and AWS Backup, providing storage for files, volumes, snapshots, and virtual tapes in AWS.  
The other options are incorrect:  
“Amazon Aurora“ is incorrect. Amazon Aurora is a MySQL and PostgreSQL-compatible relational database service.  
“Amazon EFS“ is incorrect. Amazon Elastic File System (Amazon EFS) provides fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth. Although EFS can be used in hybrid environments, it is not as cost-effective as Storage Gateway.  
“AWS Data Pipeline“ is incorrect. AWS Data Pipeline is a web service that helps customers reliably process and move data between different AWS compute and storage services, as well as on-premises data sources. AWS Data Pipeline is not a storage service.  
References:  
<https://aws.amazon.com/storagegateway/>

1. 6. Question

A company wants to grant a new employee long-term access to manage Amazon DynamoDB databases. Which of the following is a recommended best-practice when granting these permissions?

* 1. Create an IAM role and attach a policy with Amazon DynamoDB access permissions
  2. Create an IAM user and attach a policy with Administrator access permissions
  3. **Create an IAM user and attach a policy with Amazon DynamoDB access permissions**
  4. Create an IAM role and attach a policy with Administrator access permissions

**Unattempted**

IAM user is the recommended IAM entity when granting a person long-term access permission. After you create an IAM user, you attach a policy that defines what he or she can and cannot do in AWS. When creating this policy, you should follow the principle of least privilege. The principle of least privilege ensures only the required permissions are granted, nothing more.  
The new employee only needs permission to access and manage Amazon DynamoDB databases. Therefore, the option that says “Create an IAM user and attach a policy with Amazon DynamoDB access permissions” is the correct answer.  
The other options are incorrect:  
“Create an IAM user and attach a policy with Administrator Access permissions” and “Create an IAM role and attach a policy with Administrator access permissions” are incorrect. Administrator Access provides full access to AWS services and resources. This option contradicts the principle of least privilege. The principle of least privileges means granting users the required permissions to perform the tasks entrusted to them and nothing more.  
“Create an IAM role and attach a policy with Amazon DynamoDB access permissions” is incorrect. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone (or any service, application, …etc) who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session.  
You can use roles to delegate access to users, applications, or services that don‘t normally have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don‘t usually have, or grant users in one AWS account access to resources in another account.  
References:  
[https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html%C2%A0)

1. 7. Question

Which methods can be used by customers to interact with AWS Identity and Access Management (IAM)? (Choose TWO)

* 1. AWS CodeCommit
  2. **AWS SDKs**
  3. **AWS CLI**
  4. AWS Security Groups
  5. AWS Network Access Control Lists

**Unattempted**

Customers can work with AWS Identity and Access Management in any of the following ways:   
1- AWS Management Console: The console is a browser-based interface that can be used to manage IAM and AWS resources.   
2- AWS Command Line Tools:  Customers can use the AWS command line tools to issue commands at your system‘s command line to perform IAM and AWS tasks. Using the command line can be faster and more convenient than the console. The command line tools are also useful if you want to build scripts that perform AWS tasks.  AWS provides two sets of command line tools: the AWS Command Line Interface (AWS CLI) and the AWS Tools for Windows PowerShell.   
3- AWS SDKs:  AWS provides SDKs (software development kits) that consist of libraries and sample code for various programming languages and platforms (Java, Python, Ruby, .NET, iOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to IAM and AWS. For example, the SDKs take care of tasks such as cryptographically signing requests, managing errors, and retrying requests automatically.   
The other options are incorrect:  
                 
“AWS Security Groups“ is incorrect. You can use security groups to control the inbound and outbound traffic for your instances.  
“AWS Network Access Control Lists“ is incorrect. Network Access Control Lists (NACLs) are used to provide fine-grained control of network traffic into and out of a subnet.  
“AWS CodeCommit“ is incorrect. AWS CodeCommit is a source code control service that hosts secure Git-based repositories. AWS CodeCommit is designed for software developers who need a secure, reliable, and scalable source control system to store and version their code.  
References:  
<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html#intro-accessing>

1. 8. Question

The TCO gap between AWS infrastructure and traditional infrastructure has widened over the recent years. Which of the following could be the reason for that?

* 1. AWS secures AWS resources at no additional charge
  2. AWS automates all infrastructure operations, so customers save more on human resources costs
  3. AWS helps customers invest more in capital expenditures
  4. **AWS continues to lower the cost of cloud computing for its customers**

**Unattempted**

AWS continues to lower the cost of cloud computing for its customers, making everything from web apps to big data on AWS even more cost-effective and widening the TCO (Total Cost of Ownership) gap with traditional infrastructure. Since 2014, AWS has reduced the cost of compute by an average of 30%, storage by an average of 51% and relational databases by an average of 28%.  
The other options are incorrect:  
“AWS automates all infrastructure operations, so customers save more on human resources costs“ is incorrect. AWS does not automate all infrastructure operations. While certain AWS Services, such as RDS, are fully managed services, other aspects of infrastructure management, such as Amazon EC2 remain the responsibility of the customer.  
“AWS helps customers invest more in capital expenditures“ is incorrect. AWS reduces the need to invest in large capital expenditures and provides a pay-as-you-go model that empowers its customers to invest in the capacity they need and use it only when the business requires it.  
“AWS secures AWS resources at no additional charge“ is incorrect. Securing AWS resources is a shared responsibility between AWS and its customers. Additionally, some AWS security services and features have an associated cost.  
References:  
<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html>  
<https://aws.amazon.com/economics/>

1. 9. Question

​ Which features are included in the AWS Business Support Plan? (Choose TWO)

* 1. Partial access to the core Trusted Advisor checks
  2. 24x7 access to the TAM feature
  3. Access to Cloud Support Engineers via email only during business hours
  4. **Access to the Infrastructure Event Management (IEM) feature for additional fee**
  5. **24x7 access to customer service**

**Unattempted**

All AWS support plans (including the Business plan) provide 24×7 access to AWS Customer Service.  
The Business support plan provides access to Infrastructure Event Management for additional fee. AWS Infrastructure Event Management is a structured program available to Enterprise Support customers (and Business Support customers for an additional fee) that helps customers plan for large-scale events such as product or application launches, infrastructure migrations, and marketing events.  
The other options are incorrect:  
“24×7 access to the TAM feature“ is incorrect. The Technical Account Manager (TAM) feature is available only for AWS customers who have an Enterprise On-Ramp or Enterprise support plan.  
“Access to Cloud Support Engineers via email only during business hours“ is incorrect. The Business support plan provides 24×7 access to Cloud Support Engineers via phone, email, and chat.  
“Partial access to the core Trusted Advisor checks“ is incorrect. AWS Business, Enterprise On-Ramp, and Enterprise Support customers get access to all Trusted Advisor checks.  
AWS Basic Support and AWS Developer Support customers get access to 6 security checks (S3 Bucket Permissions, Security Groups – Specific Ports Unrestricted, IAM Use, MFA on Root Account, EBS Public Snapshots, RDS Public Snapshots) and 50 service limit checks.  
AWS Business, Enterprise On-Ramp, and Enterprise Support customers get access to all 115 Trusted Advisor checks (14 cost optimization, 17 security, 24 fault tolerance, 10 performance, and 50 service limits) and recommendations.  
References:  
<https://aws.amazon.com/premiumsupport/compare-plans/>

1. 10. Question

A customer is seeking to store objects in their AWS environment and to make those objects downloadable over the internet. Which AWS Service can be used to accomplish this?

* 1. Amazon EBS
  2. Amazon Instance Store
  3. **Amazon S3**
  4. Amazon EFS

**Unattempted**

Amazon S3 provides a simple web service interface that you can use to store and retrieve any amount of data, any time, from anywhere on the internet. Amazon S3 assigns a URL for each object you upload. URLs are used to download the objects you want at any time. Amazon S3 is the only AWS service that provides object level storage.  
The other options are incorrect:  
“Amazon EFS“ is incorrect. Amazon Elastic File System (Amazon EFS) is not an object store. Amazon EFS is a shared NFS file storage system that scales automatically with use.  
“Amazon Elastic Block Store (EBS)“ is incorrect. Amazon Elastic Block Store (Amazon EBS) is not an object store. Amazon EBS is a block storage service that is used to create volumes for use with Amazon EC2 and Amazon RDS.  
“Amazon Instance Store“ is incorrect. Amazon EC2 Instance Store is not an object store. Amazon EC2 Instance Store provides ephemeral block-level storage that is physically attached to Amazon EC2 instances.  
References:  
<https://aws.amazon.com/s3/faqs/>

1. 11. Question

Which of the following are examples of the customer’s responsibility to implement “security IN the cloud”? (Choose TWO)

* 1. Replacing physical hardware
  2. Creating a new hypervisor
  3. **​ File system encryption**
  4. Patch management of the underlying infrastructure
  5. **Building a schema for an application**

**Unattempted**

“Security IN the Cloud” refers to the Customer’s responsibility in the Shared Responsibility Model. Customers are responsible for items such as building application schema, monitoring server and application performance, configuring security groups and network ACLs, and encrypting their data.  
  “Security OF the Cloud” refers to the AWS’ responsibility in the Shared Responsibility Model. AWS is responsible for items such as the physical security of the DC (data center), creating hypervisors, replacement of old disk drives, and patch management of the infrastructure.  
NOTE:  
For “Patch Management“,  AWS is responsible for patching the underlying hosts and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.  
References:  
<https://aws.amazon.com/compliance/shared-responsibility-model/>

1. 12. Question

A company uses AWS Organizations to manage all of its AWS accounts. Which of the following allows the company to restrict what services and actions are allowed in each individual account?

* 1. AWS Fargate
  2. IAM Principals
  3. IAM policies
  4. **AWS Service Control Policies (SCPs)**

**Unattempted**

AWS Organizations provides central governance and management across multiple AWS accounts. AWS Service Control Policies (or AWS Organizations Policies) are a type of organization policy that you can use to manage permissions for all accounts in your organization. SCPs offer central control over the maximum available permissions for all member accounts in your organization. SCPs help you to ensure member accounts stay within your organization‘s access control guidelines. In SCPs, you can restrict which AWS services, resources, and individual API actions the users and roles in each member account can access. When AWS Organizations blocks access to a service, resource, or API action for a member account, a user or role in that account cannot access it. This block remains in effect even if an administrator of a member account explicitly grants such permissions in an IAM policy.  
Additional information:  
What is the difference between an AWS Organizations service control policy (SCP) and an IAM policy?  
      An IAM policy provides granular control over what users and roles in individual accounts can do. AWS Organizations expands that control to the account level by giving you control over what users and roles in an account or a group of accounts can do. The resulting permissions are the logical intersection of what is allowed by AWS Organizations at the account level and the permissions that are explicitly granted by IAM at the user or role level within that account. In other words, the user can access only what is allowed by both the AWS Organizations policies and IAM policies. If either blocks an operation, the user can‘t access that operation. For example, if an SCP applied to an account states that the only actions allowed are Amazon EC2 actions, and the permissions on a principal (IAM user or role) in the same AWS account allow both EC2 actions and Amazon S3 actions, the principal is able to access only the EC2 actions.  
The other options are incorrect:  
“IAM Policies” is incorrect. IAM Policies cannot be used to manage access across multiple AWS accounts. An IAM Policy provides granular control over what users and roles in an individual account can do.  
“IAM Principals” is incorrect. IAM Principals cannot be used to manage access across multiple AWS accounts. A principal is a person or application that can make a request for an action or operation on an AWS resource. The principal is authenticated as the AWS account root user or an IAM entity (users and roles) to make requests to AWS. Permissions in the IAM policies determine whether the request is allowed or denied.  
“AWS Fargate” is incorrect. AWS Fargate is a serverless compute engine for containers that works with both Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS). AWS Fargate allows customers to run containers without having to manage servers or clusters.  
References:  
<https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html>

1. 13. Question

Which of the following is NOT a characteristic of Amazon Elastic Compute Cloud (Amazon EC2)?

* 1. Amazon EC2 offers scalable computing
  2. Amazon EC2 eliminates the need to invest in hardware upfront
  3. **Amazon EC2 is considered a Serverless Web Service**
  4. Amazon EC2 can launch as many or as few virtual servers as needed

**Unattempted**

  “Amazon EC2 is considered a Serverless Web Service“  is not a characteristic of Amazon EC2 and thus is the correct choice. Serverless allows customers to shift more operational responsibilities to AWS. Serverless allows customers to build and run applications and services without thinking about servers. Serverless eliminates infrastructure management tasks such as server or cluster provisioning, patching, operating system maintenance, and capacity provisioning.  
Amazon EC2 is not a serverless service. EC2 instances are virtual servers in the cloud. Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware upfront, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.  
References:  
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html>

1. 14. Question

Which of the following AWS services scale automatically without your intervention? (Choose TWO)

* 1. Amazon EC2
  2. Amazon EBS
  3. Amazon EMR
  4. **Amazon S3**
  5. **AWS Lambda**

**Unattempted**

Amazon S3 and Amazon EFS are storage services that scale automatically in storage capacity without any intervention to meet increased demand.  
Also, AWS Lambda dynamically scales function execution in response to increased traffic.  
The other options are incorrect:  
Amazon EMR is incorrect. Amazon EMR doesn’t scale on its own. You have to configure the AWS Auto Scaling feature to scale EMR automatically.  
Amazon EC2 is incorrect. Amazon EC2 does scale automatically, but first you have to create an Auto Scaling system by creating a launch configuration, an auto scaling group, and determine the desired, minimum and maximum number of instances to provision.  
Amazon EBS is incorrect. Amazon Elastic Block Store (Amazon EBS) provides persistent block level storage volumes for use with Amazon EC2 instances in the AWS Cloud.  
References:  
<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

1. 15. Question

How do ELBs improve the reliability of your application?

* 1. By replicating data to multiple availability zones
  2. By creating database Read Replicas
  3. **By ensuring that only healthy targets receive traffic**
  4. By distributing traffic across multiple S3 buckets

**Unattempted**

The reliability term encompasses the ability of a system to recover from infrastructure or service disruptions, and dynamically acquire computing resources to meet demand. ELBs continuously perform health checks on the registered targets (such as Amazon EC2 instances) and only routes traffic to the healthy ones. This increases the fault tolerance of your application and makes it more reliable.  
The other options are incorrect:  
“By replicating data to multiple availability zones“ is incorrect. ELBs are not responsible for replicating data.  
“By creating database Read Replicas“ is incorrect. Read Replicas are special types of database instances that are part of Amazon RDS NOT ELB. The purpose of Read Replicas on Amazon RDS is to enhance database performance and increase database availability.  
“By distributing traffic across multiple S3 buckets“ is incorrect. There is no need to create multiple S3 buckets and distribute traffic between them; One S3 bucket can handle any amount of traffic without any intervention. Amazon S3 was designed from the ground up to handle traffic for any Internet application. Amazon S3’s massive scale allows to spread load evenly, so that no individual application is affected by traffic spikes.  
References:  
<https://aws.amazon.com/elasticloadbalancing/>

1. 16. Question

Which of the following AWS services can help you perform security analysis and regulatory compliance auditing? (Choose TWO)

* 1. Amazon ECS
  2. AWS Batch
  3. **AWS Config**
  4. AWS Virtual Private Gateway
  5. **Amazon Inspector**

**Unattempted**

With AWS Config, you can discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.  
Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. This allows you to make security testing a more regular occurrence as part of development and IT operations.  
Additional information:  
One of the most important services that performs security analysis and compliance auditing is AWS CloudTrail. AWS CloudTrail simplifies your compliance audits by automatically recording and storing event logs for actions made within your AWS account. With AWS CloudTrail, you can discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in your AWS account within a specified period of time.  
The other options are incorrect:  
“AWS Virtual Private Gateway“ is incorrect. AWS Virtual Private Gateway allows creating hybrid cloud architecture by connecting your data center (or network) to your Amazon virtual private cloud (VPC).  
“Amazon ECS“ is incorrect. Amazon Elastic Container Service (Amazon ECS) is a compute service that allows you to run and scale containerized applications on AWS.  
“AWS Batch“ is incorrect. AWS Batch is a compute service that allows you to run hundreds of thousands of batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted.  
References:  
<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

1. 17. Question

​ Which design principles relate to performance efficiency in AWS? (Choose TWO)

* 1. ​ Enable audit logging
  2. Apply security at all layers
  3. **Use serverless architectures**
  4. **Build multi-region architectures to better serve global customers**
  5. ​ Implement strong Identity and Access controls

**Unattempted**

There are five design principles for performance efficiency in the cloud:  
1- Democratize advanced technologies: Technologies that are difficult to implement can become easier to consume by pushing that knowledge and complexity into the cloud vendor‘s domain. Rather than having your IT team learns how to host and run a new technology, they can simply consume it as a service. For example, NoSQL databases, media transcoding, and machine learning are all technologies that require expertise that is not evenly dispersed across the technical community. In the cloud, these technologies become services that your team can consume while focusing on product development rather than resource provisioning and management.  
2- Go global in minutes: Easily deploy your system in multiple Regions around the world with just a few clicks. This allows you to provide lower latency and a better experience for your customers at minimal cost.  
3- Use serverless architectures: In the cloud, serverless architectures remove the need for you to run and maintain servers to carry out traditional compute activities. For example, storage services can act as static websites, removing the need for web servers, and event services can host your code for you. This not only removes the operational burden of managing these servers, but also can lower transactional costs because these managed services operate at cloud scale.  
4- Experiment more often: With virtual and automatable resources, you can quickly carry out comparative testing using different types of instances, storage, or configurations.  
5- Mechanical sympathy: Use the technology approach that aligns best to what you are trying to achieve. For example, consider data access patterns when selecting database or storage approaches.  
Other options presented are related to security not performance.  
References:  
<https://docs.aws.amazon.com/wellarchitected/latest/framework/wellarchitected-framework.pdf>

1. 18. Question

Which support plan includes AWS Support Concierge Service?

* 1. Business Support
  2. Standard Support
  3. Premium Support
  4. **Enterprise Support**

**Unattempted**

Support Concierge is only available for the AWS Enterprise or Enterprise On-Ramp support plan. The Concierge Team are AWS billing and account experts that specialize in working with enterprise accounts. They will quickly and efficiently assist you with your billing and account inquiries, and work with you to implement billing and account best practices so that you can focus on what matters: running your business.  
References:  
<https://aws.amazon.com/premiumsupport/features/>

1. 19. Question

Both AWS and traditional IT distributors provide a wide range of virtual servers to meet their customers’ requirements. What is the name of these virtual servers in AWS?

* 1. AWS Managed Servers
  2. Amazon EBS Snapshots
  3. **Amazon EC2 Instances**
  4. Amazon Virtual Private Cloud

**Unattempted**

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2’s simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon’s proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate them from common failure scenarios.  
The other options are incorrect:  
“Amazon Virtual Private Cloud“ is incorrect. Amazon Virtual Private Cloud (Amazon VPC) is used to create virtual networks in the AWS cloud.  
“AWS Managed Servers“ is incorrect. Amazon EC2 instances are not managed by AWS. It is the responsibility of the customer to manage almost everything related to their instances.  
“Amazon EBS Snapshots“ is incorrect. Amazon EBS Snapshots are copies (backups) of EBS volumes.  
References:  
<https://aws.amazon.com/ec2/>

1. 20. Question

​ What is the benefit of using an API to access AWS Services?

* 1. **It allows for programmatic management of AWS resources**
  2. It improves the performance of AWS resources
  3. ​ It reduces the number of developers necessary
  4. It reduces the time needed to provision AWS resources

**Unattempted**

The AWS Application Programming Interface (API) allows customers to work with various AWS services programmatically.  
The other options are incorrect:  
“It improves the performance of AWS resources“ is incorrect. There is no difference in performance when you provision resources using the console or using the AWS API. In fact, if you access AWS through the AWS Management Console or through the command line tools, you are actually using tools that make calls to the AWS API.  
“It reduces the time needed to provision AWS resources“ is incorrect. Since AWS Console and AWS CLI both provision resources by making AWS API calls, then there will be no difference in the time needed to provision these resources using either of them.  
“​It reduces the number of developers necessary“ is incorrect. Depending on the use case, using the AWS API may actually require more developers to manage AWS resources programmatically.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/APIReference/making-api-requests.html>

1. 21. Question

Which statement best describes the concept of an AWS region?

* 1. An AWS Region is a virtual network dedicated only to a single AWS customer
  2. **An AWS Region is a geographical location with a collection of Availability Zones**
  3. An AWS Region is a geographical location with a collection of Edge locations
  4. An AWS Region represents the country where the AWS infrastructure exist

**Unattempted**

An AWS Region is a physical location in the world. Each region has multiple, isolated locations known as Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity. These Availability Zones offer you the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible to operate out of a single data center. Also, each AWS Region is designed to be completely isolated from the other AWS Regions. This achieves the greatest possible fault tolerance and stability.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

1. 22. Question

As part of the AWS Migration Acceleration Program (MAP), what does AWS provide to accelerate Enterprise adoption of AWS? (Choose TWO)

* 1. Amazon Athena
  2. **AWS Partners**
  3. Amazon PinPoint
  4. **AWS Professional Services**
  5. AWS Artifact

**Unattempted**

AWS has helped thousands of organizations, including enterprises such as GE, the Coca-Cola Company, BP, Enel, Samsung, NewsCorp, and Twenty-First Century Fox, migrate to the cloud and free-up resources by lowering IT costs while improving productivity, operational resiliency, and business agility. The AWS Migration Acceleration Program (MAP) is designed to help enterprises that are committed to a migration journey achieve a range of these business benefits by migrating existing workloads to Amazon Web Services. MAP has been created to provide consulting support, training and services credits to reduce the risk of migrating to the cloud, build a strong operational foundation and help offset the initial cost of migrations. It includes a migration methodology for executing legacy migrations in a methodical way as well as robust set of tools to automate and accelerate common migration scenarios.  
By migrating to AWS, enterprises will be able to focus on business innovation instead of dedicating time and attention to maintaining their existing systems and technical debt. Sacrifices and painful trade-offs no longer have to be made to get something to market quickly. Instead, enterprises can focus on differentiating their business in the marketplace and taking advantage of new capabilities. By building the foundation to operate mission critical workloads on AWS, you will build capabilities that can be leveraged across a variety of projects. AWS have a number of resources to support and sustain your migration efforts including an experienced partner ecosystem to execute migrations, AWS Professional Services team to provide best practices and prescriptive advice and a training program to help IT professionals understand and carry out migrations successfully.  
The other options are incorrect:  
“Amazon Athena“ is incorrect. Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. AWS customers can also use an Amazon S3 feature called S3 Select to query data on S3 using SQL commands; however, S3 Select can only be used to perform simple SQL queries on a single S3 Object.  
“Amazon PinPoint“ is incorrect. Amazon PinPoint is used to engage your customers by sending them targeted and transactional email, SMS, push notifications, and voice messages.  
“AWS Artifact“ is incorrect. AWS Artifact is a no cost, self-service portal for on-demand access to AWS’ compliance reports.  
References:  
<https://aws.amazon.com/migration-acceleration-program/>

1. 23. Question

What is the most cost-effective purchasing option for running a set of EC2 instances that must always be available for a period of two months?

* 1. Reserved Instances - No Upfront
  2. Spot Instances
  3. **On-Demand Instances**
  4. Reserved Instances - All Upfront

**Unattempted**

The most cost-effective option for this scenario is to use On-Demand Instances.  
The other options are incorrect:  
“Spot Instances“ is incorrect. AWS Spot instances can be interrupted at any time by AWS. You should only choose Spot instances if the question clearly stated that the application can handle interruptions or if continuous processing is not required. Usually Spot instances are used for batch processing jobs or for non-production applications, such as development and test servers, where occasional downtime is acceptable.  
“Reserved Instances – All Upfront“ and “Reserved Instances – No Upfront“are incorrect. Since the duration is just for two months, we should use On-demand instances. Reserved instances require a purchase term of at least one year.  
References:  
<https://aws.amazon.com/ec2/pricing/on-demand/>

1. 24. Question

App development companies move their business to AWS to reduce time-to-market and improve customer satisfaction, what are the AWS automation tools that help them deploy their applications faster? (Choose TWO)

* 1. AWS IAM
  2. Amazon Macie
  3. AWS Migration Hub
  4. **AWS Elastic Beanstalk**
  5. **AWS Cloud​Formation**

**Unattempted**

      AWS Elastic Beanstalk makes it easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.  
      AWS CloudFormation automates and simplifies the task of repeatedly and predictably creating groups of related resources that power your applications. Creating and interconnecting all resources your application needs to run is now as simple as creating a single EC2 or RDS instance.  
The other options are incorrect.  
“Amazon Macie“ is incorrect. Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved.  
“AWS IAM“ is incorrect. AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and user groups, and use permissions to allow and deny their access to AWS resources.  
“AWS Migration Hub“ is incorrect. AWS Migration Hub is used to track the progress of application migrations to AWS.  
References:  
<https://aws.amazon.com/elasticbeanstalk/>  
<https://aws.amazon.com/cloudformation/>

1. 25. Question

According to the AWS Well-Architected Framework, which of the following are design principles for operational excellence in the AWS cloud? (Choose TWO)

* 1. Go global in minutes
  2. Implement a strong identity foundation
  3. Automatically recover from failure
  4. **Make frequent, small, reversible changes**
  5. **Anticipate failure**

**Unattempted**

     The Operational Excellence pillar includes the ability to run workloads effectively, gain insight into their operations, and to continuously improve supporting processes and procedures to deliver business value.  
There are five design principles for operational excellence in the cloud:  
1- Perform operations as code: In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events. By performing operations as code, you limit human error and enable consistent responses to events.  
2- Make frequent, small, reversible changes: Design workloads to allow components to be updated regularly. Make changes in small increments that can be reversed if they fail (without affecting customers when possible).  
3- Refine operations procedures frequently: As you use operations procedures, look for opportunities to improve them. As you evolve your workload, evolve your procedures appropriately. Set up regular game days to review and validate that all procedures are effective and that teams are familiar with them.  
4- Anticipate failure: Perform “pre-mortem“ exercises to identify potential sources of failure so that they can be removed or mitigated. Test your failure scenarios and validate your understanding of their impact. Test your response procedures to ensure that they are effective, and that teams are familiar with their execution. Set up regular game days to test workloads and team responses to simulated events.  
5- Learn from all operational failures: Drive improvement through lessons learned from all operational events and failures. Share what is learned across teams and through the entire organization.  
The other options are incorrect:  
“Automatically recover from failure“ is incorrect. One of the most important AWS Well-Architected Framework design principles is to design systems that can automatically recover from failure. Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significant events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. For example, AWS Elastic Load Balancing offers health-checking capabilities that can validate the health of compute components using a variety of network protocols (i.e., TCP, HTTP, HTTPS, and SSL). When integrated with Amazon CloudWatch, these capabilities provide operational alerting and can trigger automated remediation of failures. “Automatically recover from failure“ is a design principle of the Reliability pillar of the AWS Well-Architected Framework.  
“Go global in minutes“ is incorrect. Deploying your workload in multiple AWS Regions around the world allows you to provide lower latency and a better experience for your worldwide customers. “Go global in minutes“ is a design principle of the Performance Efficiency pillar.  
“Implement a strong identity foundation“ is incorrect. AWS recommends you implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources. AWS also suggests you centralize identity management and reduce or eliminate reliance on long-term static credentials. “Implement a strong identity foundation“ is a design principle of the Security pillar.  
References:  
<https://docs.aws.amazon.com/wellarchitected/latest/operational-excellence-pillar/design-principles.html>  
<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/design-principles.html>  
<https://docs.aws.amazon.com/wellarchitected/latest/performance-efficiency-pillar/design-principles.html>  
<https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/security.html>

1. 26. Question

A company is planning to migrate a database with high read/write activity to AWS. What is the best storage option to use?

* 1. Amazon ECR
  2. **Amazon EBS**
  3. Amazon S3
  4. AWS Storage Gateway

**Unattempted**

Databases require high read \ write performance and as such Amazon EBS is the correct answer. Amazon EBS volumes offer consistent and low-latency performance compared to other storage options. You can use EBS volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application.  
The other options are incorrect:  
“Amazon ECR“ is incorrect. Amazon Elastic Container Registry (Amazon ECR) is a Docker container registry that allows developers to store, manage, and deploy container images and artifacts.  
“AWS Storage Gateway“ is incorrect. AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage. You can use the service for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration.  
“Amazon S3“ is incorrect. Amazon S3 is an object-level storage, not block-level storage. Object storage is not suited for use in a high read/write scenarios because of performance limitations. In contrast, Amazon EBS is a block-level storage that provides an extremely high performance compared to Amazon S3. Amazon S3 is well suited for storing static assets such as photos and videos, backups, and log files.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html>

1. 27. Question

Which of the following are use cases for Amazon S3? (Choose TWO)

* 1. Hosting websites that require sustained high CPU utilization
  2. **A media store for the CloudFront service**
  3. Processing data streams at any scale
  4. **Hosting static websites**
  5. Cost-effective database and log storage

**Unattempted**

              You can host a static website on Amazon Simple Storage Service (Amazon S3). On a static website, individual webpages include static content. They might also contain client-side scripts. To host a static website, you configure an Amazon S3 bucket for website hosting, allow public read access, and then upload your website content to the bucket. By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting. Amazon Web Services (AWS) also has resources for hosting dynamic websites such as Amazon EC2.  
             Amazon S3 is an excellent storage facility for your media assets. It is infinitely scalable, has built-in redundancy, and is available to you on a pay-as-you-go basis. For example, if you want to deliver or stream video files to your global users, all you need to do is to put your content in an S3 bucket and create a CloudFront distribution that points to the bucket. Your user’s video player will use CloudFront URLs to request the video file. The request will be directed to the best edge location, based on the user’s location. The Amazon Cloudfront Content Delivery Network (CDN) will serve the video from its cache, fetching it from the S3 bucket if it has not already been cached. The CDN caches content at the edge locations for consistent, low-latency, high-throughput video delivery.  
The other options are incorrect:  
“Cost-effective database and log storage“ is incorrect. Amazon S3 can be used to store log files, images, videos (or any static content), but not databases. Databases and dynamic websites require block-level storage (such as EBS). S3 is an object-level storage, not Block-level storage. Object-level storage has limited I/O and is therefore ill-suited for use as a database store.  
“Hosting websites that require sustained high CPU utilization“ is incorrect. S3 can only be used to host static websites.  
“Processing data streams at any scale“ is incorrect. S3 is not a compute service.  
References:  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>  
<https://aws.amazon.com/cloudfront/streaming/>

1. 28. Question

A company wants to keep a secondary backup copy of its databases to meet regulatory requirements. Compliance policies require that the data be retrievable immediately when requested. What is the most cost-effective storage option that will meet these requirements?

* 1. Amazon S3 Standard (S3 Standard)
  2. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)
  3. Amazon S3 Glacier Flexible Retrieval
  4. **Amazon S3 Standard-Infrequent Access (S3 Standard-IA)**

**Unattempted**

The most cost-effective storage option that meets the requirements of immediate data retrieval for regulatory compliance is **Amazon S3 Standard-Infrequent Access (S3 Standard-IA)**.

Here’s why:

* + **Amazon S3 Standard-IA:**
    - **Designed for data that is accessed less frequently but requires rapid access when needed.**
    - **Offers the same high durability and availability as S3 Standard but at a lower storage cost.**
    - Retrieval times are in milliseconds, meeting the “retrievable immediately” requirement.

Here’s why the other options are not ideal:

* + **Amazon S3 Standard (S3 Standard):**
    - While it offers immediate retrieval, it is more expensive than S3 Standard-IA, making it less cost-effective for infrequently accessed data.
  + **Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA):**
    - This option stores data in a single Availability Zone, which makes it less durable than S3 Standard-IA. If that AZ goes down, the data is lost. This conflicts with regulatory requirements for data availability.
  + **Amazon S3 Glacier Flexible Retrieval (formerly Glacier):**
    - **Glacier Flexible Retrieval is designed for archival data with retrieval times ranging from minutes to hours.**

This does not meet the “retrievable immediately” requirement.

1. 29. Question

​ When running a workload in AWS, the customer is NOT responsible for: (Select TWO)

* 1. **Data center operations**
  2. Auditing and regulatory compliance
  3. Running penetration tests
  4. Reserving capacity
  5. **Infrastructure security**

**Unattempted**

         AWS is responsible for the infrastructure security and all data center operations such as racking, stacking, and powering servers, so customers can focus on revenue generating activities rather than on IT infrastructure.  
The other options are incorrect:  
“Reserving capacity“ is incorrect. Amazon does not perform reservations for a customer; capacity reservation is a customer action.  
“Running penetration tests“ is incorrect. Penetration testing is the practice of testing a network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing is the responsibility of the customer.  
“Auditing and regulatory compliance“ is incorrect. There are many services on AWS to use for auditing and compliance such as AWS CloudTrail, AWS Config  and Amazon Inspector. However, these services must be configured by the customer, not by AWS.  
References:  
<https://aws.amazon.com/compliance/shared-responsibility-model/>

1. 30. Question

​ What are AWS shared controls?

* 1. Controls that the customer and AWS collaborate together upon to secure the infrastructure
  2. **Controls that apply to both the infrastructure layer and customer layers**
  3. Controls that are solely the responsibility of the customer based on the application they are deploying within AWS services
  4. Controls that a customer inherits from AWS

**Unattempted**

 Shared Controls are controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:  
– Patch Management – AWS is responsible for patching the underlying hosts and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.  
– Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.  
– Awareness & Training – AWS trains AWS employees, but a customer must train their own employees.  
The other options are incorrect:  
“Controls that are solely the responsibility of the customer based on the application they are deploying within AWS services“ is incorrect because it refers to “Customer-Specific” controls.  
“Controls that a customer inherits from AWS“ is incorrect because it refers to “Inherited Controls”.  
“Controls that the customer and AWS collaborate together upon to secure the infrastructure“ is incorrect. Securing the infrastructure is the responsibility of AWS, not the customer.   
References:  
<https://aws.amazon.com/compliance/shared-responsibility-model/>

1. 31. Question

Data security is one of the top priorities of AWS. How does AWS deal with old storage devices that have reached the end of their useful life?

* 1. AWS sells the old devices to other hosting providers
  2. **AWS destroys the old devices in accordance with industry-standard practices**
  3. AWS stores the old devices in a secure place
  4. AWS sends the old devices for remanufacturing

**Unattempted**

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses specific techniques to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.  
References:  
<https://aws.amazon.com/compliance/data-center/controls/>

1. 32. Question

Which of the following activities supports the Operational Excellence pillar of the AWS Well-Architected Framework?

* 1. **Using AWS CloudFormation to manage infrastructure as code**
  2. Using AWS Trusted Advisor to find underutilized resources
  3. Using AWS CloudTrail to record user activities
  4. Deploying an application in multiple Availability Zones

**Unattempted**

      The AWS Well-Architected Framework helps you understand the pros and cons of decisions you make while building systems on AWS. By using the Framework, you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement.  
The AWS Well-Architected Framework is based on six pillars:  
• Operational Excellence  
• Security  
• Reliability  
• Performance Efficiency  
• Cost Optimization  
• Sustainability  
     The operational excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.  
     AWS CloudFormation can help you define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events. This will help you build a more consistent operating model and continually improve over time.  
The other options are incorrect:  
“Deploying an application in multiple Availability Zones” is incorrect. This statement is much more related to the Reliability pillar. The reliability pillar focuses on ensuring a workload performs its intended function correctly and consistently when it’s expected to. A resilient workload quickly recovers from failures to meet business and customer demand. Deploying the application resources across multiple availability zones will guarantee that even if one availability zone goes down, there will still be other availability zones to run the application efficiently.  
“Using AWS CloudTrail to record user activities” is incorrect. This statement is much more related to the Security pillar. The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events. AWS CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.  
“Using AWS Trusted Advisor to find underutilized resources” is incorrect. . This statement is much more related to the Cost Optimization pillar. The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding and controlling where money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending. AWS Trusted Advisor inspects your AWS environment and makes recommendations that can potentially save you money by highlighting unused resources and opportunities to reduce your bill.  
References:  
<https://docs.aws.amazon.com/wellarchitected/latest/operational-excellence-pillar/wellarchitected-operational-excellence-pillar.pdf>  
<https://aws.amazon.com/architecture/well-architected/>

1. 33. Question

What are the benefits of using the Amazon Relational Database Service? (Choose TWO)

* 1. Supports the document and key-value data structure
  2. Complete control over the underlying host
  3. **Resizable compute capacity**
  4. Scales automatically to larger or smaller instance types
  5. **Lower administrative burden**

**Unattempted**

          Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable Compute (and\or Storage) capacity while automating time-consuming administration tasks such as hardware provisioning, operating system maintenance, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.  
The other options are incorrect:  
“Complete control over the underlying host“ is incorrect. The user doesn’t have access to the underlying host. For managed services like this, AWS is responsible for performing all the operations needed to keep the service running.  
“Supports the document and key-value data structure“ is incorrect. RDS doesn’t support document and key-value data structures. The AWS service that support them is DynamoDB.  
“Scales automatically to larger or smaller instance types“ is incorrect. Amazon RDS provides you with six widely-used database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server. The only RDS database that can scale instances automatically is Amazon Aurora.  
Additional information:  
For RDS databases other than Aurora, RDS only supports storage auto-scaling, NOT instance auto-scaling. If you want to scale Amazon RDS instances (other than Aurora), you have two options:  
1- Manual horizontal scaling (by adding read replicas)  
2- Manual vertical scaling (by upgrading/downgrading an existing instance).  
References:  
<https://aws.amazon.com/nosql/>  
<https://aws.amazon.com/rds/>  
<https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally/>

1. 34. Question

Why do many startup companies prefer AWS over traditional on-premises solutions? (Choose TWO)

* 1. AWS allows them to pay later when their business succeed
  2. AWS removes the need to invest in operational expenditure
  3. AWS can build complete data centers faster than any other Cloud provider
  4. **Using AWS, they can reduce time-to-market by focusing on business activities rather than on building and managing data centers**
  5. **Using AWS allows companies to replace large capital expenditure with low variable costs**

**Unattempted**

         Instead of building and managing data centers, AWS provides startups, enterprises, and government agencies all the services they need to quickly build their business and grow faster. AWS has significantly more services, and more features within those services, than any other cloud provider – from infrastructure technologies like compute, storage, and databases –to emerging technologies, such as machine learning and artificial intelligence, data lakes and analytics, and Internet of Things. This makes it faster, easier, and more cost effective to build nearly anything they can imagine.  
        Capital expenditures (CapEx) are a company‘s major, long-term expenses. Examples of CAPEX include physical assets such as buildings, equipment, and machinery.  
         Instead of having to invest heavily in these Capital expenditures (e.g. physical data centers and servers) before it is known they will be used, companies can pay only when consuming AWS resources, and pay only for how much they consume. In brief, AWS replaces their investments in large capital expenditures (CAPEX) with low variable “pay-as-you-go“ costs.  
The other options are incorrect:  
“AWS can build complete data centers faster than any other Cloud provider“ is incorrect. AWS does not build out physical data centers for customers, only for itself. AWS is a Cloud Computing provider.  
“AWS removes the need to invest in operational expenditure“ is incorrect. Operating expenses (OpEx) are a company‘s day-to-day expenses. Examples of OPEX include employee salaries, rent, utilities, and property taxes. With AWS, Startups can reduce (not remove) their day to day operating expense (OpEx) costs.  
“AWS allows them to pay later when their business succeed“ is incorrect. AWS does not offer a “pay later“ option for its customers. AWS provides three payment models: “Pay-as-you-go“, “Save when you commit“ and “Pay less by using more“.  
References:  
<https://aws.amazon.com/what-is-aws/>  
<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html>  
<https://aws.amazon.com/pricing/>

1. 35. Question

​ For managed services like Amazon DynamoDB, which of the below is AWS responsible for? (Choose TWO)

* 1. **Patching the database software**
  2. Logging access activity
  3. **Operating system maintenance**
  4. Protecting credentials
  5. Creating access policies

**Unattempted**

AWS has increased responsibilities for its managed services. Examples of managed services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, and Amazon Elastic MapReduce. These services provide the scalability and flexibility of cloud-based resources with less operational overhead because AWS handle basic security tasks like guest operating system (OS) and database patching, installing antivirus software, backup, and disaster recovery. For most managed services, you only configure logical access controls and protect account credentials, while maintaining control and responsibility of any personal data.  
Note:  
If you are using Amazon EC2 instead of the AWS managed services to run your databases and applications, you will be responsible for performing all of the necessary security configuration and management tasks.  
The other options are incorrect:  
“Creating access policies“ is incorrect. The customer is responsible for creating the required access policies for all users using the Identity and Access Management service.  
“Protecting credentials“ is incorrect. The customer (or anyone in their team) is responsible for protecting their credentials.  
“Logging access activity“ is incorrect. Logging user access activities is the responsibility of the customer, whether they are using a managed service or any other services. The AWS customer can use AWS CloudTrail to record and monitor all API calls made in their AWS account.  
References:  
<https://aws.amazon.com/dynamodb/faqs/>  
<https://aws.amazon.com/compliance/shared-responsibility-model/>

1. 36. Question

TYMO Cloud Corp is looking forward to migrating their entire on-premises data center to AWS. What tool can they use to build a Business Case for moving to the AWS Cloud?

* 1. AWS Migration Hub
  2. AWS DMS
  3. AWS Snowball Migration Service
  4. **AWS Migration Evaluator**

**Unattempted**

      A business case is the first step in your migration journey. Creating business cases on your own can be time-consuming and does not always identify the least expensive deployment and purchasing options. AWS Migration Evaluator is a migration assessment service that helps you create a directional business case for AWS cloud planning and migration.  
      Migration Evaluator analyzes your on-premises compute footprint, including server configuration, utilization, annual costs to operate, eligibility for bring-your-own-license, and hundreds of other parameters. Following data collection, you will quickly receive an assessment including a projected cost estimate and savings of running your on-premises workloads in the AWS Cloud. After receiving your initial assessment, your organization can work with the Migration Evaluator team to create a directional business case that best fits your organization‘s requirements.  
The other options are incorrect:  
“AWS Migration Hub“ is incorrect. AWS Migration Hub provides a single location to track the progress of application migrations across multiple AWS and partner solutions.  
“AWS Snowball Migration Service“ is incorrect. Snowball is a petabyte-scale data transport solution that uses secure devices to transfer large amounts of data into and out of the AWS Cloud.  
“AWS DMS“ is incorrect. AWS Database Migration Service (AWS DMS) is used to migrate your data to and from most widely used commercial and open-source databases. AWS DMS supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle or Microsoft SQL Server to Amazon Aurora.  
References:  
<https://aws.amazon.com/migration-evaluator/>

1. 37. Question

Which AWS service can be used to send promotional text messages (SMS) to more than 200 countries worldwide?

* 1. Amazon Simple Queue Service (Amazon SQS)
  2. Amazon Simple Storage Service (Amazon S3)
  3. **Amazon Simple Notification Service (Amazon SNS)**
  4. Amazon Simple Email Service (Amazon SES)

**Unattempted**

     Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication. The A2P functionality enables you to send messages to users at scale via SMS, mobile push, and email.  
     Amazon SNS enables you to send messages or notifications directly to users with SMS text messages to over 200 countries. Additionally, you can mark your SMS messages as Transactional to optimize for reliable delivery, or you can mark them as Promotional to optimize for cost savings. SMS messages that carry marketing messaging should be marked Promotional. Amazon SNS ensures that promotional messages are sent over routes that have reasonable delivery reliability but are substantially cheaper than the most reliable routes.  
The other options are incorrect:  
“Amazon Simple Email Service (Amazon SES)” is incorrect. Amazon SES can only be used to send emails, not text (SMS) messages. Amazon SES is a cloud-based email sending service designed to help digital marketers and application developers send marketing, notification, and transactional emails.  
“Amazon Simple Queue Service (Amazon SQS)“ is incorrect. Amazon SQS is a highly reliable message queuing service that enables asynchronous message-based communication between distributed components of an application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.  
“Amazon Simple Storage Service“ is incorrect. Amazon Simple Storage Service (Amazon S3) is an object storage service.  
References:  
<https://aws.amazon.com/sns/>

1. 38. Question

A company needs to track resource changes using the API call history. Which AWS service can help the company achieve this goal?

* 1. AWS Config
  2. Amazon CloudWatch
  3. **AWS CloudTrail**
  4. AWS CloudFormation

**Unattempted**

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.  With CloudTrail, you can get a history of AWS API calls for your account, including API calls made using the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.  
The other options are incorrect:  
“AWS Config“ is incorrect.  
              Both AWS Config and AWS CloudTrail can be used to track resource changes, and it is very important to distinguish between them. AWS Config is used to monitor and audit changes in AWS resources and allow you to automate the evaluation of recorded configurations of a specific resource against desired configurations. AWS CloudTrail records user API activity on your account and allows you to access information about this activity. You get full details about API actions, such as identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS service.  
             AWS Config records point-in-time configuration details for your AWS resources as Configuration Items (CIs). You can use a CI to answer “What did my AWS resource look like?” at a point in time. You can use AWS CloudTrail to answer “Who made an API call to modify this resource?” For example, you can use the AWS Management Console for AWS Config to detect security group “Production-DB” was incorrectly configured in the past. Using the integrated AWS CloudTrail information, you can pinpoint which user misconfigured “Production-DB” security group. In brief, AWS Config provides information about the changes made to a resource, and AWS CloudTrail provides information about who made those changes.  
“AWS CloudFormation“ is incorrect. AWS CloudFormation is a service that allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts.  
“Amazon CloudWatch“ is incorrect. Amazon CloudWatch is used to monitor and collect custom and granular metrics about your AWS resources.  
References:  
<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

1. 39. Question

A company has hundreds of VPCs in multiple AWS Regions worldwide. What service does AWS offer to simplify the connection management among the VPCs?

* 1. **AWS Transit Gateway**
  2. AWS PrivateLink
  3. Amazon Connect
  4. VPC Peering

**Unattempted**

      AWS Transit Gateway is a network transit hub that simplifies how customers interconnect all of their VPCs, across thousands of AWS accounts and into their on-premises networks. Customers can easily and quickly connect into a single centrally-managed gateway, and rapidly growing the size of their network. Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes. This hub and spoke model significantly simplifies management and reduces operational costs because each network only has to connect to the Transit Gateway and not to every other network. Any new VPC is simply connected to the Transit Gateway and is then automatically available to every other network that is connected to the Transit Gateway. This ease of connectivity makes it easy to scale networks as business grow.  
The other options are incorrect:  
“VPC Peering” is incorrect. A VPC peering connection is a networking connection between two VPCs that enables customers to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. Using VPC peering to connect hundreds of VPCs is very complex and time consuming because customers need to peer each Amazon VPC to each other manually.  
With AWS Transit Gateway, each VPC only has to connect to the Transit Gateway and not to every other VPC. Customers simply connect each Amazon VPC to the AWS Transit Gateway, and the Gateway will route traffic to and from each VPC.  
“Amazon Connect“ is incorrect. Amazon Connect is a cloud-based contact center service that makes it easy for businesses to deliver customer service at low cost.  
“AWS PrivateLink“ is incorrect. AWS PrivateLink enables you to securely connect your VPCs to supported AWS services: to your own services on AWS, to services hosted by other AWS accounts, and to third-party services on AWS Marketplace. With AWS PrivateLink, traffic between AWS resources, VPCs, and third-party services stays on the global AWS backbone and never traverses the public internet, reducing exposure to brute force and distributed denial-of-service attacks, along with other threats.  
For example, customers who want to use a SaaS application offered by an independent software vendor in the AWS Marketplace have to choose between allowing Internet access from their VPC, which puts the VPC resources at risk, and not using these applications at all. With AWS PrivateLink, customers can connect to AWS services and SaaS applications from their VPC in a private, secure, and scalable manner and without traversing the public internet.  
References:  
<https://aws.amazon.com/transit-gateway/>

1. 40. Question

A company is planning to migrate an application from Amazon EC2 to AWS Lambda to use a serverless architecture. Which of the following will be the responsibility of AWS after migration? (Choose TWO)

* 1. Access control
  2. Application management
  3. **Capacity management**
  4. Data management
  5. **Operating system maintenance**

**Unattempted**

      For AWS Lambda, AWS manages the underlying infrastructure and foundation services, the operating system, the runtime environment, and the application platform. AWS Lambda performs all the operational and administrative activities on the customer‘s behalf, including operating system maintenance, provisioning and scaling compute capacity to maintain consistent performance, monitoring fleet health, applying security patches to the underlying compute resources, encrypting code, deploying code, and running a web service front end.  
      AWS Lambda enables customers to run their applications without provisioning or managing servers. AWS customers are only responsible for building and managing their applications, managing their data, and controlling access to the Lambda service and within their Lambda Functions.  
The other options are incorrect:  
“Data management” is incorrect. Data management is a customer responsibility.  
“Application management” is incorrect. Application management is a customer responsibility.  
“Access control” is incorrect. Access control is a customer responsibility.  
References:  
<https://docs.aws.amazon.com/whitepapers/latest/security-overview-aws-lambda/the-shared-responsibility-model.html>

1. 41. Question

A company needs to migrate their website from on-premises to AWS. Security is a major concern for them, so they need to host their website on hardware that is NOT shared with other AWS customers. Which of the following EC2 instance options meets this requirement?

* 1. On-demand instances
  2. Reserved instances
  3. Spot instances
  4. **Dedicated instances**

**Unattempted**

Dedicated Instances are Amazon EC2 instances that run in a virtual private cloud (VPC) on hardware that‘s dedicated to a single customer. Dedicated Instances that belong to different AWS accounts are physically isolated at the hardware level. In addition, Dedicated Instances that belong to AWS accounts that are linked to a single payer account are also physically isolated at the hardware level. However, Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances.  
The other options are incorrect:  
“Reserved instances“ and “Spot instances“ and “On-demand instances“ are incorrect. Reserved, Spot and On-demand instances all share hardware with other customers.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-instance.html>

1. 42. Question

Which of the following allows you to create new RDS instances? (Choose TWO)

* 1. **AWS Management Console**
  2. AWS DMS
  3. **AWS CloudFormation**
  4. AWS Fargate
  5. AWS Partner Solutions

**Unattempted**

The AWS Management Console lets you create new RDS instances through a web-based user interface.  
You can also use AWS CloudFormation to create new RDS instances using the CloudFormation template language.  
The other options are incorrect:  
“AWS DMS“ is incorrect. AWS DMS is used to migrate databases to AWS.  
“AWS Partner Solutions“ is incorrect. AWS Partner Solutions (formerly AWS Quick Starts) are built by AWS solutions architects and partners to help you deploy popular technologies on AWS, based on AWS best practices for security and high availability. These accelerators reduce hundreds of manual procedures into just a few steps, so you can build your production environment quickly and start using it immediately.  
“AWS Fargate” is incorrect. AWS Fargate is a serverless compute engine for containers that works with both Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS). AWS Fargate allows customers to run containers without having to manage servers or clusters.  
References:  
<https://docs.aws.amazon.com/awsconsolehelpdocs/index.html>  
<https://aws.amazon.com/cloudformation/>

1. 43. Question

What is the framework created by AWS Professional Services that helps organizations design a road map to successful cloud adoption?

* 1. AWS WAF
  2. **AWS CAF**
  3. Amazon EFS
  4. AWS Secrets Manager

**Unattempted**

        AWS Professional Services created the AWS Cloud Adoption Framework (AWS CAF) to help organizations design and travel an accelerated path to successful cloud adoption. The guidance and best practices provided by the framework help you build a comprehensive approach to cloud computing across your organization, and throughout your IT lifecycle. Using the AWS CAF helps you realize measurable business benefits from cloud adoption faster and with less risk.  
The other options are incorrect:  
“AWS Secrets Manager“ is incorrect. AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily store, rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.  
“Amaozn EFS“ is incorrect. Amazon Elastic File System (Amazon EFS) Amazon EFS is a fully-managed service that makes it easy to set up, scale, and cost-optimize file storage in the Amazon Cloud. Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance.  
“AWS WAF“ is incorrect. AWS WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor (count) web requests based on conditions that you define.  
References:  
<https://aws.amazon.com/professional-services/CAF/>

1. 44. Question

What is the minimum level of AWS support that provides 24×7 access to technical support engineers via phone and chat?

* 1. Enterprise Support
  2. Developer Support
  3. **Business Support**
  4. Basic Support

**Unattempted**

Each of the Business, Enterprise On-Ramp, and Enterprise support plans provide 24×7 access to technical support engineers via phone, email, and chat. The Business Support Plan is the least expensive. Therefore, the correct answer is Business.  
The other options are incorrect:  
“Basic Support“ is incorrect. The technical support is not available for the Basic support plan.  
“Developer Support“ is incorrect. Developer support plan provides business hours access to technical support associates via email only.  
References:  
<https://aws.amazon.com/premiumsupport/plans/>

1. 45. Question

What is the AWS Compute service that executes code only when triggered by events?

* 1. AWS Transit Gateway
  2. Amazon CloudWatch
  3. Amazon EC2
  4. **AWS Lambda**

**Unattempted**

AWS Lambda is a serverless compute service that runs code in response to events. For example, you can create a Lambda function that creates thumbnail images when users upload images to Amazon S3. The Lambda event, in this case, will be the user’s uploads. Once a user uploads an image to Amazon S3, AWS Lambda will automatically run the application and creates a thumbnail for that image.  
The other options are incorrect:  
“AWS Transit Gateway“ is incorrect. AWS Transit Gateway is a network transit hub that customers can use to interconnect their virtual private clouds (VPCs) and their on-premises networks. AWS transit gateway simplifies how customers interconnect all of their VPCs, across thousands of AWS accounts and into their on-premises networks.  
“Amazon EC2“ is incorrect. After provisioning an EC2 instance, it continues to run all the time until being stopped or terminated. But with Lambda, the application code will run only when triggered.  
“Amazon CloudWatch“ is incorrect. Amazon CloudWatch is a monitoring service, not a compute service.  
References:  
<https://aws.amazon.com/lambda/>

1. 46. Question

What is the connectivity option that uses Internet Protocol Security (IPSec) to establish encrypted connectivity between an on-premises network and the AWS Cloud?

* 1. Internet Gateway
  2. **AWS Site-to-Site VPN**
  3. AWS PrivateLink
  4. AWS Direct Connect

**Unattempted**

AWS Virtual Private Network (AWS VPN) is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to AWS. AWS Client VPN enables you to securely connect users (from any location) to AWS or on-premises networks.  
AWS Site-to-Site VPN utilizes Internet Protocol Security (IPSec) to establish encrypted connectivity between your on-premises network and AWS over the Internet. With AWS Client VPN, your users can access AWS or on-premises resources from any location using a secure TLS connection.  
What is IPsec?  
IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.  
The other options are incorrect:  
“AWS Direct Connect” is incorrect. AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your on-premises network or branch office site and the AWS Cloud. AWS Direct Connect is a network service that provides an alternative to using the Internet to connect customer‘s on-premise sites to AWS. Using AWS Direct Connect, data that would have previously been transported over the Internet can now be delivered through a private network connection between AWS and your datacenter or corporate network. Companies of all sizes use AWS Direct Connect to establish private connectivity between AWS and datacenters, offices, or colocation environments.  
“Internet Gateway“ is incorrect. An internet gateway is a VPC component that allows communication between your VPC and the internet.  
“AWS PrivateLink“ is incorrect. AWS PrivateLink enables you to securely connect your VPCs to supported AWS services: to your own services on AWS, to services hosted by other AWS accounts, and to third-party services on AWS Marketplace. With AWS PrivateLink, traffic between AWS resources, VPCs, and third-party services stays on the global AWS backbone and never traverses the public internet, reducing exposure to brute force and distributed denial-of-service attacks, along with other threats.  
For example, customers who want to use a SaaS application offered by an independent software vendor in the AWS Marketplace have to choose between allowing Internet access from their VPC, which puts the VPC resources at risk, and not using these applications at all. With AWS PrivateLink, customers can connect to AWS services and SaaS applications from their VPC in a private, secure, and scalable manner and without traversing the public internet.  
References:  
<https://aws.amazon.com/vpn/>

1. 47. Question

What are the benefits of implementing a tagging strategy for AWS resources? (Choose TWO)

* 1. **Track AWS spending across multiple resources**
  2. **Quickly identify resources that belong to a specific project**
  3. Quickly identify deleted resources and their metadata
  4. Track API calls in your AWS account
  5. Quickly identify software solutions on AWS

**Unattempted**

Amazon Web Services (AWS) allows customers to assign metadata to their AWS resources in the form of tags. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. Although there are no inherent types of tags, they enable customers to categorize resources by purpose, owner, environment, or other criteria. An effective tagging strategy will give you improved visibility and monitoring, help you create accurate chargeback/showback models, and get more granular and precise insights into usage and spend by applications and teams.  
The other options are incorrect:  
“Track API calls in your AWS account“ is incorrect. AWS CloudTrail is the service that can be used to track API calls in your AWS account.  
“Quickly identify deleted resources and their metadata“ is incorrect. You cannot use tags to find deleted resources. Also, once you delete a resource, all its metadata will be deleted with it.  
“Quickly identify software solutions on AWS“ is incorrect. The AWS marketplace is the service that allows you to search for software solutions on AWS.  
References:  
<https://docs.aws.amazon.com/aws-technical-content/latest/cost-optimization-laying-the-foundation/tagging.html>

1. 48. Question

A developer needs to set up an SSL security certificate for a client‘s eCommerce website in order to use the HTTPS protocol. Which of the following AWS services can be used to deploy the required SSL server certificates? (Choose TWO)

* 1. **AWS Identity & Access Management**
  2. AWS Directory Service
  3. Amazon Route 53
  4. **AWS ACM**
  5. AWS Data Pipeline

**Unattempted**

The two AWS services that can be used to deploy SSL server certificates for HTTPS are:

* + **AWS Identity & Access Management (IAM)**
  + **AWS ACM (AWS Certificate Manager)**

Here’s why:

* + **AWS ACM (AWS Certificate Manager):**
    - **ACM is the primary service for provisioning, managing, and deploying SSL/TLS certificates for use with AWS services.**
    - **It integrates directly with services like Elastic Load Balancing, Amazon CloudFront, and API Gateway.**
    - It is the best option for managing certificates within the AWS ecosystem.
  + **AWS Identity & Access Management (IAM):**
    - **IAM can be used to store and manage server certificates.** **You can upload your own certificates to IAM and then reference them when configuring services like Elastic Load Balancing.**
    - **It is generally used when you are importing certificates from a third party.**

Here’s why the other options are incorrect:

* + **AWS Directory Service:**
    - AWS Directory Service is used for managing directories, such as Microsoft Active Directory, and is not related to SSL certificate management.
  + **Amazon Route 53:**
    - **Amazon Route 53 is a DNS web service and is used for routing traffic to your website.** While it works with HTTPS, it does not deploy SSL certificates.
  + **AWS Data Pipeline:**
    - **AWS Data Pipeline is a data orchestration service and is not related to SSL certificate management.**

Therefore, the correct answers are AWS IAM and AWS ACM.

1. 49. Question

A company plans to migrate a large amount of archived data to AWS. The archived data must be maintained for a period of 5 years and must be retrievable within 5 hours of a request. What is the most cost-effective AWS storage service to use?

* 1. Amazon EBS Infrequent Access
  2. Amazon EFS Infrequent Access
  3. Amazon S3 Standard
  4. **Amazon S3 Glacier Flexible Retrieval**

**Unattempted**

AWS Customers can use Amazon S3 Glacier Instant Retrieval, Amazon S3 Glacier Flexible Retrieval, or Amazon S3 Glacier Deep Archive to backup large amounts of data at very low costs.  
Choosing between S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, or S3 Glacier Deep Archive depends on how quickly you must retrieve your data. S3 Glacier Instant Retrieval delivers the fastest access to archive storage, with the same throughput and milliseconds access as the S3 Standard and S3 Standard-IA storage classes. With S3 Glacier Flexible Retrieval, you can retrieve your data within a few minutes to several hours (1-5 minutes to 12 hours), whereas with S3 Glacier Deep Archive, the minimum retrieval period is 12 hours.  
For archive data that needs immediate access, such as medical images, news media assets, or genomics data, choose the S3 Glacier Instant Retrieval storage class. For archive data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, such as backup or disaster recovery use cases, choose S3 Glacier Flexible Retrieval (formerly S3 Glacier), with retrieval in minutes or free bulk retrievals in 5 – 12 hours. To save even more on long-lived archive storage such as compliance archives and digital media preservation, choose S3 Glacier Deep Archive, the lowest cost storage in the cloud with data retrieval from 12 – 48 hours.  
The other options are incorrect:  
“Amazon EFS Infrequent Access“ is incorrect. Amazon Elastic File System (Amazon EFS) is not a cost-effective solution for data archiving. Amazon EFS is a file storage service for use with Amazon compute (EC2, containers, serverless) and on-premises servers. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances.  
What is Amazon EFS Infrequent Access?  
Amazon EFS Standard-Infrequent Access (EFS Standard-IA) and Amazon EFS One Zone-Infrequent Access (EFS One Zone-IA) are storage classes that provide price/performance that is cost-optimized for files not accessed every day, with storage prices up to 92% lower compared to Amazon EFS Standard (EFS Standard) and Amazon EFS One Zone (EFS One Zone) storage classes respectively. To get started with Infrequent Access (IA) storage classes, simply enable Amazon EFS Lifecycle Management for your file system by selecting a lifecycle policy that matches your needs. Amazon EFS will automatically and transparently move your files to the lower cost regional EFS Standard-IA storage class or EFS One Zone-IA storage class based on the last time they were accessed. You don‘t have to worry about which of your files are actively used and which are infrequently accessed.  
“Amazon EBS Infrequent Access“ is incorrect. Amazon EBS is not a cost-effective solution for data archiving. Amazon EBS provides block-level storage volumes for use with Amazon EC2 and RDS instances. Amazon EBS does not offer storage tiers for less frequently accessed data. Infrequent Access storage tiers are available only for Amazon S3 and Amazon EFS.  
“Amazon S3 Standard“ is incorrect. Amazon S3 Standard is not a cost-effective solution for data archiving. Amazon S3 Standard is a general-purpose object storage for active, frequently accessed data with millisecond access. S3 Standard use cases include: cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.  
Additional information:  
In S3, we can only host static websites, or static assets of a dynamic website (such as images, audio files, video files, etc.).  
A dynamic website relies on server-side processing and it uses server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting and cannot be used to host dynamic websites. AWS has computing resources for hosting dynamic websites such as Amazon EC2 or Lambda.  
References:  
<https://aws.amazon.com/s3/storage-classes/>

1. 50. Question

Which AWS Service provides the current status of all AWS Services in all AWS Regions?

* 1. Amazon Rekognition
  2. AWS Management Console
  3. **AWS Health Dashboard**
  4. Amazon CloudWatch

**Unattempted**

AWS uses the AWS Health Dashboard to publish most up-to-the-minute information on AWS service availability. The dashboard provides access to current status and historical data about every AWS Service. You can get information about the current status and availability of any AWS service any time using the AWS Health Dashboard that is available at this link: [https://health.aws.amazon.com](https://health.aws.amazon.com/)  
The AWS Health Dashboard is the single place to learn about the availability and operations of AWS services. You can view the overall status of all AWS services, and you can sign in to access a personalized view of the health of the specific services that are powering your workloads and applications, enabling you to quickly see when AWS is experiencing issues that may impact you. For example, in the event of a lost EBS volume associated with one of your EC2 instances, you would gain quick visibility into the status of the specific service you are using, helping save precious time troubleshooting to determine the root cause.  
The other options are incorrect:  
“Amazon Rekognition“ is incorrect. Amazon Rekognition allows you to add image and video analysis to your applications. For example, you can use it detect faces in millions of images uploaded to S3.  
“Amazon CloudWatch“ is incorrect. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.  
“AWS Management Console“ is incorrect. AWS Management Console allows you to access and manage Amazon Web Services through a simple and intuitive web-based user interface.  
References:  
<https://aws.amazon.com/premiumsupport/technology/aws-health-dashboard/>

1. 51. Question

Which of the following is used to control network traffic in AWS? (Choose TWO)

* 1. IAM Policies
  2. **Security Groups**
  3. Key Pairs
  4. Access Keys
  5. **Network Access Control Lists (NACLs)**

**Unattempted**

You can control network traffic in AWS by configuring security groups, network access control lists, and route tables.  
1- Security groups: Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.  
2- Network access control lists (ACLs): Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.  
3- Route Tables: A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.  
Note:  
Controlling network traffic using any of the above methods is the responsibility of the customer.  
The other options are incorrect:  
“Access keys“ is incorrect. Access keys are long-term credentials for an IAM user or the AWS account root user. Access keys allows you to interact with AWS services programmatically using the AWS CLI or the AWS SDK.  
“IAM Policies“ is incorrect. By default, IAM users don‘t have permission to create or modify resources in AWS. IAM policies are used to grant IAM users permission to use the specific resources and API actions they‘ll need.  
“Key Pairs“ is incorrect. Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. Public-key cryptography uses a public key to encrypt a piece of data, and then the recipient uses the private key to decrypt the data. The public and private keys are known as a key pair. Public-key cryptography enables you to securely access your instances using a private key instead of a password.  
References:  
<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html>  
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>  
<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html>

1. 52. Question

What are the benefits of using an AWS-managed service? (Choose TWO)

* 1. **​ Allows customers to deliver new solutions faster**
  2. Provides complete control over the virtual infrastructure
  3. **Lowers operational complexity**
  4. Allows developers to control all patching related activities
  5. Eliminates the need to encrypt data

**Unattempted**

 AWS services that are managed lower operational complexity by automating time-consuming administration tasks such as hardware provisioning, software setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, security and compatibility they need. Because these services are instantly available to developers, they reduce dependency on in-house specialized skills and allow organizations to deliver new solutions faster.  
The other options are incorrect:  
“Provides complete control over the virtual infrastructure“ is incorrect. When using a managed service you don’t have complete control of it. You are limited in what you can do with it. For example, Amazon RDS limits you to seven database engines to choose from. However, Amazon EC2 allows you to install and run any database.   
“Allows developers to control all patching related activities“ is incorrect. For managed services, patching activities are managed by AWS.  
“Eliminates the need to encrypt data“ is incorrect. It is always the customer’s responsibility to encrypt data.  
References:  
<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

1. 53. Question

Which of the following are factors in determining the appropriate database technology to use for a specific workload? (Choose TWO)

* 1. **The nature of the queries**
  2. Availability Zones
  3. **The number of reads and writes per second**
  4. Software bugs
  5. Data sovereignty

**Unattempted**

The following questions can help you take decisions on which solutions to include in your architecture:  
– Is this a read-heavy, write-heavy, or balanced workload? How many reads and writes per second are you going to need? How will those values change if the number of users increases?  
– How much data will you need to store and for how long? How quickly do you foresee this will grow? Is there an upper limit in the foreseeable future? What is the size of each object (average, min, max)? How are these objects going to be accessed?  
– What are the requirements in terms of durability of data? Is this data store going to be your “source of truth”?  
– What are your latency requirements? How many concurrent users do you need to support?  
– What is your data model and how are you going to query the data? Are your queries relational in nature (e.g.,JOINs between multiple tables)? Could you denormalize your schema to create flatter data structures that are easier to scale?  
– What kind of functionality do you require? Do you need strong integrity controls or are you looking for more flexibility (e.g.,schema-less data stores)? Do you require sophisticated reporting or search capabilities? Are your developers more familiar with relational databases than NoSQL?  
The other options are incorrect:  
“Data sovereignty“ is incorrect. Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Data sovereignty is a factor you should consider when choosing your AWS region NOT the database.  
“Software bugs“ is incorrect. A software bug is an error, flaw, failure, or fault in a system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways. Most bugs are due to human errors made in source code or software design, so if software has bugs, you have to search for a fix. Database technologies cannot help you with application bugs, as they provide services related only to databases.  
“Availability Zones“ is incorrect. Availability zones in a region are all relatively the same. There is no reason to prefer any Availability Zone in which to run a database.  
References:  
<https://aws.amazon.com/products/databases/>

1. 54. Question

Why would an organization decide to use AWS over an on-premises data center? (Choose TWO)

* 1. Free commercial software licenses
  2. Free technical support
  3. **Cost Savings**
  4. **Elastic resources**
  5. On-site visits for auditing

**Unattempted**

AWS continues to lower the cost of cloud computing for its customers. AWS recently lowered prices again for compute, storage, caching, and database services for all customers, making everything from web apps to big data on AWS even more cost-effective and widening the TCO gap with traditional infrastructure.  
Elasticity is a system’s ability to monitor user demand and automatically increase and decrease deployed resources accordingly. Elasticity is one of the most important advantages of AWS. The purpose of elasticity is to match the resources allocated with actual amount of resources needed at any given point in time. This ensures that you are only paying for the resources you actually need.   
The other options are incorrect:  
“Free technical support“ is incorrect. Technical support is not free in AWS. Technical Support requires subscription to an AWS Support Plan.  
“On-site visits for auditing“ is incorrect. AWS does not allow on-site visits to its datacenters under any circumstances.  
“Free commercial software licenses“ is incorrect. Neither AWS nor on-premises datacenters provide free commercial software licenses. However, AWS allows you to pay for these licenses as-you-go. For example, using license included windows instances allows you access to fully compliant Microsoft software licenses bundled with Amazon EC2 or Amazon RDS instances and pay for them as you go with no upfront costs or long-term investments.  
References:  
<https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/six-advantages-of-cloud-computing.html>

1. 55. Question

Which of the below are responsibilities of the customer when using Amazon EC2? (Choose TWO)

* 1. **Installing and configuring third-party software**
  2. Setup and operation of managed databases
  3. **Protecting sensitive data**
  4. Maintaining consistent hardware components
  5. Patching of the underlying infrastructure

**Unattempted**

Amazon EC2 requires the customer to perform all of the necessary security configuration and management tasks. When customers deploy Amazon EC2 instances, they are responsible for management of  custom Amazon Machine Images, management of the guest operating systems (including updates and security patches), securing application access and data, installing and configuring third-party applications or utilities, and the configuration of the AWS-provided firewall (called a security group) on each instance.  
The other options are incorrect:  
“Patching of the underlying infrastructure“ is incorrect. AWS is responsible for patching the underlying infrastructure. The customer is responsible for patching the operating system and any software or application run on EC2.  
“Setup and operation of managed databases“ is incorrect.  
AWS customers have two options to host their databases on AWS:  
1- Using a managed database:  
AWS Customers can use managed databases such as Amazon RDS and Amazon DynamoDB to host their databases. In this case, AWS is responsible for performing all database management tasks such as hardware provisioning, patching, setup, configuration, backups, or recovery.  
2- Installing a database software on Amazon EC2:  
Instead of using a managed database, AWS customers can install any database software they want on Amazon EC2 and host their databases. In this case, AWS customers are responsible for performing all of the necessary configuration and management tasks.  
“Maintaining consistent hardware components“ is incorrect. AWS is responsible for maintaining consistency of all hardware components.  
References:  
<https://aws.amazon.com/compliance/shared-responsibility-model/>

1. 56. Question

What is the AWS’ recommendation regarding access keys?

* 1. Delete all access keys and use passwords instead
  2. **Rotate them regularly**
  3. Save them within your application code
  4. Only share them with trusted people

**Unattempted**

AWS recommends that you change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources.  
The other options are incorrect:  
“Save them within your application code“ is incorrect. It is not secure to save any type of credentials within your application code.  
“Only share them with trusted people“ is incorrect. AWS recommends that you do not ever share your credentials with anyone.  
“Delete all access keys and use passwords instead“ is incorrect. Usernames and passwords are used to sign in to the AWS management console. They cannot be used to sign programmatic requests to the AWS CLI or AWS API like access keys.  
References:  
<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

1. 57. Question

Which of the following can be used to protect data at rest on Amazon S3? (Choose TWO)

* 1. Conversion
  2. Decryption
  3. **Versioning**
  4. Deduplication
  5. **Permissions**

**Unattempted**

Amazon S3 provides a number of security features for the protection of data at rest, which you can use or not depending on your threat profile:  
1- Permissions: Use bucket-level or object-level permissions alongside IAM policies to protect resources from unauthorized access and to prevent information disclosure, data integrity compromise or deletion.  
2- Versioning: Amazon S3 supports object versions. Versioning is disabled by default. Enable versioning to store a new version for every modified or deleted object from which you can restore compromised objects if necessary.  
3- Replication: Although Amazon S3 stores your data across multiple geographically diverse Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-region replication (CRR) allows you to replicate data between distant AWS Regions to help satisfy these requirements. CRR enables automatic, asynchronous copying of objects across buckets in different AWS Regions.  
4- Encryption – server side: Amazon S3 supports server-side encryption of user data. Server-side encryption is transparent to the end user. AWS generates a unique encryption key for each object, and then encrypts the object using AES-256.  
5- Encryption – client side: With client-side encryption you create and manage your own encryption keys. Keys you create are not exported to AWS in clear text. Your applications encrypt data before submitting it to Amazon S3, and decrypt data after receiving it from Amazon S3. Data is stored in an encrypted form, with keys and algorithms only known to you.  
Additional information: (IMPORTANT)  
           AWS also provides a fully managed security service called AWS Macie to help protect your sensitive data in Amazon S3. Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in Amazon S3. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks. Today, Amazon Macie is available to protect data stored in Amazon S3, with support for additional AWS data stores coming later this year.  
The other options are incorrect:  
“Deduplication“ is incorrect. Deduplication is the process of removing duplicate data, and will do nothing to prevent data loss of data at rest.  
“Conversion“ is incorrect. Conversion is the process of transforming data from one format to another.  
“Decryption“ is incorrect. Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form.  
References:  
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html>

1. 58. Question

Which AWS service or feature can be used to call AWS Services from different programming languages?

* 1. AWS Management Console
  2. AWS Command Line Interface
  3. AWS CodeDeploy
  4. **AWS Software Development Kit**

**Unattempted**

The AWS Software Development Kit (AWS SDK) can simplify using AWS services in your applications with an API tailored to your programming language or platform. Programming languages supported include Java, JavaScript, .NET, Node.js, PHP, Python, Ruby, Kotlin, Rust, Go, Swift, and C++.  
The other options are incorrect:  
“AWS CodeDeploy“ is incorrect. AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, serverless Lambda functions, or Amazon ECS services.  
“AWS Management Console“ is incorrect. AWS management Console allows you to manage AWS services through a web-based user interface.  
“AWS Command Line Interface“ is incorrect. AWS Command Line Interface (AWS CLI) allows you to control multiple AWS services from the command line and automate them through scripts NOT from programming languages.  
References:  
<https://aws.amazon.com/developer/tools/>  
<https://aws.amazon.com/cli/>

1. 59. Question

Why does every AWS Region contain multiple Availability Zones?

* 1. Multiple Availability Zones results in lower total cost compared to deploying in a single Availability Zone
  2. Multiple Availability Zones within a region increases the storage capacity available in that region
  3. Multiple Availability Zones allows for data replication and global reach
  4. **Multiple Availability Zones allows you to build resilient and highly available architectures**

**Unattempted**

Resilience is the ability of an architecture to continue providing the same quality of service even if some of its resources become inaccessible. Deploying your resources across multiple Availability Zones offer you the ability to operate production applications and databases that are more resilient, highly available, and scalable than would be possible from a single data center.  
The other options are incorrect:  
“Multiple Availability Zones within a region increases the storage capacity available in that region“ is incorrect. In AWS, you have virtually unlimited storage capacity regardless of Regions or Availability Zones in a region.  
“Multiple Availability Zones results in lower total cost compared to deploying in a single Availability Zone“ is incorrect. Deploying your resources across multiple availability zones has no cost benefits.  
“Multiple Availability Zones allows for data replication and global reach“ is incorrect. Multiple Availability Zones within a region allows for data replication but not global reach.  
References:  
<https://aws.amazon.com/about-aws/global-infrastructure/>