AWS Certified Cloud Practitioner
(Aligned to AWS CLF-C01 and AWS-CLF-C02)

Cloud Value Proposition

Question 1

A company is considering migrating its public-facing web applications to the AWS cloud. Which of the following is an advantage of hosting such applications on AWS instead of on-premises?

A. variable costs
B. Higher variable costs
C. Relocate on-premises infrastructure to AWS.
D. IT Staff can visit AWS data centers to provision infrastructure.

Correct Answer – A

One of the primary benefits of hosting applications on AWS is that there is no capital expenditure required to provide the necessary infrastructure to host your web applications.

AWS allows you to pay for resources on a consumption model since they own the infrastructure you lease. This will enable you to **trade capital expense for variable expense,** and you are charged depending on what you consume and for how long.

Given the sheer size and the vast array of services and technologies, AWS can also enjoy economies of scale by sharing physical infrastructure with millions of clients across the globe. While ensuring high levels of security, AWS can thus pass on the lower costs to its customers and ensure that variable costs are kept quiet.

In addition, costs associated with managing facilities to host necessary on-premises infrastructures such as power, cooling and security are reduced by moving to AWS.

The answer 'Higher variable costs' is incorrect because AWS can lower its costs due to economies of scale.

The answer 'Relocate on-premises infrastructure to AWS' is incorrect because you cannot host your infrastructure at AWS data centres.

The answer 'IT Staff can visit AWS data centres to provision infrastructure' is incorrect because this is not required. Using APIs, you can connect to the various services on AWS to provision resources as your business needs.

Question 2

Which feature of cloud computing enables you to automatically scale out resources based on demand, adding additional nodes when required and only paying for when those resources are consumed?

A. Scalability
B. Elasticity
C. Agility
D. High-Availability

Correct Answer – B

Elasticity refers to the ability to provision resources when required and terminate those resources when not needed. The cost of those resources is incurred only when consumed. Because resources are usually provisioned through an automated process to meet demand, there is no need to guess capacity and over-provision in anticipation of increasing demand. This reduces waste and saves on cost.

The answer, 'Scalability', is incorrect. Scalability refers to the ability to adjust demand by adding resources (for example, increasing the amount of CPU/memory etc.) or adding additional nodes (scale out).

The answer, 'Agility' is incorrect. Agility in cloud computing refers to the concept of making changes quickly and inexpensively. So an example of cloud agility on AWS is the ability to provision infrastructure in minutes instead of months, and de-provision or change the configuration of those infrastructure components just as quickly.

The answer 'High-Availability' is incorrect. High-Availability refers to the ability to function even if some components fail This is usually achieved when you have multiple copies of a resource being deployed. As an example, by deploying multiple virtual servers in the cloud serving the same application, you can ensure high availability and accessibility to that application even if some of those virtual servers fail. Furthermore, utilizing the AWS Global Infrastructure and spreading your resources across regions and availability zones can ensure high availability if a particular region or availability zone is offline.

Question 3

Which operations will help reduce cost by moving to the cloud?

A. Being able to use managed services such as Amazon RDS, ECS and DynamoDB will reduce operation costs because AWS manages the core underlying infrastructure for its customers.

B. Being able to send your IT engineers to the AWS Datacenter for racking and stacking servers.
C. Hosting your own databases on-premises and replicating that data to AWS
D. Getting technical support to configure your third-party on-premises servers.

Correct Answer – A

AWS offers several services as a managed offering, which means AWS is responsible for managing underlying infrastructure, including patching and upgrading as and when required. For example, with Amazon RDS, you are provided with a complete database solution without the operational overhead of maintaining the underlying servers, patching database software or managing backups.

The answer 'Being able to send your IT engineers to the AWS datacenter for racking and stacking servers' is incorrect. As a customer, you cannot physically access the AWS data centres.

The answer 'Hosting your own databases on-premises and replicating that data to AWS' is incorrect. While it is possible to replicate your data to AWS, this does not reduce cost. Ideally you would want to consider migrating your AWS to an AWS managed service such as Amazon RDS.

The answer 'Getting technical support to configure your third-party on-premises servers' is incorrect. AWS will only support their products and services and can offer additional guidance but not necessary support any third-part servers you run on-premises.

Cloud Computing Models

Question 4

Which cloud service model enables you to consume applications hosted by vendors in the cloud that do not require you to host any infrastructure or platform and which is generally accessible over the public Internet?

A. SaaS
B. PaaS
C. IaaS
D. BaaS

Correct Answer – A

Explanation

SaaS or Software as a Service is a model that gives quick access to cloud-based web applications. The vendor controls the entire computing stack, which you can access using a

web browser. These applications run on the cloud, and you can use them via a paid licensed subscription or for free with limited access.

The answer ‘PaaS’ stands for Platform as a Service and is incorrect. PaaS is a cloud-based platform where you can develop, test, and organize different applications for your business. Implementing PaaS simplifies the process of enterprise software development and deployment. PaaS enables you to provide an available run-time environment to deploy your application on, while in many cases also offering the flexibility to adjust the underlying hardware resources to support your application. Typical examples on AWS include the Amazon Elastic Beanstalk Service.

The answer ‘IaaS, stands for Infrastructure as a Service and is incorrect. IaaS is a virtual provision of computing resources over the cloud. An IaaS cloud provider can give you a range of computing infrastructures, including storage, servers, and networking hardware, alongside maintenance and support. With IaaS, you can build a virtual datacentre in the cloud using AWS services.

The answer ‘BaaS’ stands for Backup as a Service and is incorrect. Backup as a service (BaaS) is an approach to backing up data that involves purchasing backup and recovery services from an online data backup provider. You do not need to manage your on-premises IT backup software or hardware, and BaaS connects systems to a private, public, or hybrid cloud managed by an external provider.

Question 5

You wish to deploy a Line of Business application using your on-premises identity and access management system (Active Directory) for login authentication. This will involve setting up network connectivity between your AWS architecture and your on-premises datacentre. What is this type of cloud deployment model known as?

A. Public Cloud
B. Private Cloud
C. Hybrid Cloud
D. Multi-Region Cloud

Correct Answer – C

Explanation

Enterprise environments often mix cloud, on-premises data centers, and edge locations. Hybrid cloud architectures help organizations integrate their on-premises and cloud operations to support a broad spectrum of use cases using a standard set of cloud services, tools, and APIs across on-premises and cloud environments.

Several approaches and technology solutions can be used to build a hybrid cloud solution which includes network connectivity components such as:

- VPN and Direct Access Services

- DNS and Route53 tools
- Hybrid Storage Solutions involves hosting AWS appliances such as Storage Gateways on-premises to connect with Amazon S3 seamlessly.
- AWS Outpost and AWS RDS on VMware on-premises
- Identity Services
- Directory Services – enabling AWS resources to connect with an existing on-premises Microsoft Active Directory and manage policies with existing tools.
- Federated access from on-premises Active Directory to access the AWS Management Console and AWS service APIs.

The answer "Public Cloud" is incorrect as this cloud deployment model involves hosting all your services with a 3rd party cloud vendor such as AWS.

The answer "Private Cloud" is incorrect as this cloud deployment model involves hosting all IT resources and services on-premises with added management software.

The answer Multi-Region Cloud does not apply to this question and is a distractor.

Ref: https://aws.amazon.com/hybrid/

Question 6

Which service of the AWS Global Infrastructure enables you to distribute your content (videos, images, documents) such that they are cached locally for low latency access when your users try to download them?

A. Regions
B. Edge Locations
C. ElastiCache
D. Route53

Correct Answer – B

Explanation

Amazon hosts many Points of Presence locations that comprise Edge Locations and Regional Edge Caches. Together they enable Amazon CloudFront to offer a content delivery network allowing the distribution of content across the globe quickly and efficiently and to cache content locally for a minimum duration, reducing latency.

In addition to standard Edge Locations, Regional Edge Caches have larger cache widths than any individual edge location, so your objects remain in the cache longer at these locations. This helps keep more of your content closer to your viewers, reducing the need for CloudFront to return to your origin web server and improving overall performance for viewers. For instance, Amazon's edge locations in Europe now go to the regional edge cache in Frankfurt to fetch an object before returning to your origin web server.

The answer ‘Regions’ is incorrect because Regions are geographical areas hosting Availability Zones comprising datacentres where you build, design, and deploy your applications. Regions do not cache any data unless you configure any caching services available in each region.

Route53 needs to be corrected because Route53 is a DNS and Traffic Routing service that performs no caching.

Question 7

Which of the following features offered by cloud providers like AWS enable you to launch resources quickly in minutes?

A. AWS grants programmatic access to its environment, enabling you to configure and launch resources.
B. AWS offers dedicated racks at its data centres enabling your IT team to visit a local data centre and install your servers.
C. When you set up an AWS account, you are assigned an engineer who performs all ‘remote hands’ tasks on AWS infrastructure to provide resources dedicated to your AWS account.
D. AWS uses local third-party vendors to work with you who set up and configure your resources at its data centre.

Correct Answer – A

Explanation

Cloud Computing is the on-demand delivery of computing power, database, storage, applications, and other IT resources through a cloud services platform via the Internet with pay-as-you-go pricing.

Cloud providers like AWS offer their customers programmatic access to their platform via the Internet, using a web management console, command-line interface (CLI) and API access using SDKs. You can access the vast array of AWS services directly from your office and home network over the Internet and provision resources required to host your applications. Unlike a co-location setup, you do not need to provision and transport any hardware and spend a lot of time managing that hardware. With Cloud Computing, you use the provider's hardware to set up and configure your own virtual resources and access to those resources is strictly determined by the policies and permissions you configure.

The answer, **‘AWS offers dedicated racks at its data centers enabling your IT team to visit a local data center and install your own servers’** is incorrect. AWS does not grant customers access to its data centers, for security reasons. Furthermore, there is no requirement to visit the data centres given the fact that resources can be configured programmatically over the Internet.

The answer, **'When you set up an AWS account, you are assigned an engineer who performs all 'remote hands' tasks on AWS infrastructure to provide resources dedicated to your AWS account'** is incorrect. AWS gives you access to a wide range of programmatic tools and API access enabling you to provision and configure resources. As part of the IaaS offering, you can access core services such as compute, network and storage and provision resources as required. As a customer, you have far greater control on how those services are deployed, including deciding on sizing and configuration options such as security options and connectivity. AWS offers managed products and services, so these take the bulk of the configuration task away from the customer.

The answer, **'AWS uses local third-party vendors to work with you who setup and configure your resources at its data center'** is incorrect. AWS does not hire any third-party providers to provision your resources. As a customer, you have programmatic access to vast array of tools to perform self-service provisioning and configuration. You may choose to outsource these tasks to your managed service provider (MSP) however.

Question 8

Which of the following services are considered zonal services on AWS? (Select two answers)

A. Elastic Block Store (EBS)
B. Elastic Compute Cloud (EC2) Instances
C. Identity and Access Management (IAM)
D. Amazon CloudFront
E. Amazon Route53

Correct answer – A&B

AWS offers over 200 services from its global distribution of data center. Most of these services are regionally based, meaning that the resources deployed from those services are tied to a specific region. For example, if you wish to deploy an Amazon RDS database, you need to first select the region in which to deploy it.

Certain services are global meaning that resources created from those services are unique and accessible across all regions. For example, if you create an IAM user, that user account is unique to all regions within your AWS account. You cannot create an IAM user account called **bob** in the London region and another account with the same username in another region. Provided that the user **bob** has the right set of permissions, he will be able to access services and resources across all regions.

Finally, some services are tied to the Availability Zone in which they are deployed. These resources are tied to the underlying hardware hosted in the given Availability Zone and thus

considered zonal services. Both **EC2** instances and **EBS** volumes are tied to the Availability Zone in which you deploy them and so the correct answer for this question is EC2 and EBS.

The answer, 'Identity and Access Management (IAM)' is incorrect because it is a global service as previously explained.

The answer, 'Amazon CloudFront' and 'Amazon Route53' are also incorrect as they are considered global services. Amazon CloudFront is a content distribution solution that caches content locally at edge locations where users attempt to access such content. Amazon CloudFront enables the worldwide caching of requested content. Amazon Route53 is AWS's global DNS service and offers traffic shaping and routing services.

Finally, a quick point to note. While EBS volumes are considered zonal services, EBS snapshots are regional. This is because EBS snapshots are stored in Amazon S3 buckets which are managed by AWS.

Ref: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resources.html

AWS Service Dashboard

Question 9

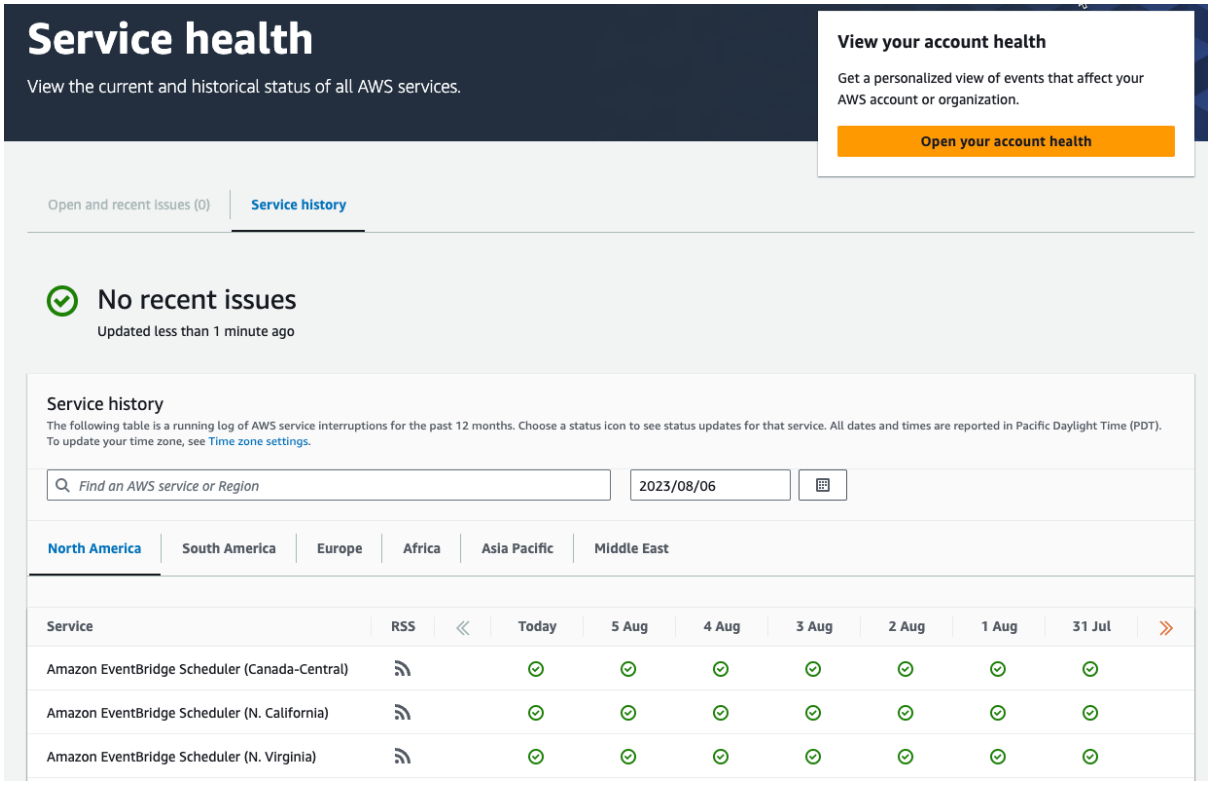
Which of the following AWS services offers up-to-the-minute information on service availability, and is any service is experiencing outages?

A. AWS Service Health Dashboard
B. AWS Personal Health Dashboard
C. AWS Config
D. AWS CloudWatch

Correct Answer – A

Explanation

The AWS Service Health Dashboard provides up-to-the-minute information on service availability across all regions and availability zones. You can also subscribe to an RSS feed to be notified of interruptions to each service.



The AWS Service Health Dashboard keeps a running log of all service interruptions for one year.
The answer, 'Personal Health Dashboard' is incorrect. While this service also provides information on service availability, it is a personalized view of the performance and availability of services that you are using and provides proactive and transparent notifications about your specific AWS environment.

The answer, 'AWS Config,' is incorrect. This service enables you to assess, audit, and evaluate the configurations of your AWS resources. However, it does not provide information about AWS service availability.

The answer, 'AWS CloudWatch,' is incorrect. This monitoring service collects performance and operational data in the form of logs, metrics, and events associated with the AWS resources you deploy in your AWS account.

Ref: https://status.aws.amazon.com/

Personal Health Dashboard

Question 10

Which AWS service provides notifications and alerts of any AWS service events or outages that may impact your workloads?

A. AWS Service Health Dashboard
B. AWS Personal Health Dashboard
C. AWS CloudWatch
D. AWS CloudTrail

Correct Answer – B

Explanation

The AWS Personal Health Dashboard (PHD) offers notifications and alerts of AWS events that might affect your environment. You can also use the PHD to create alerts for specific events that might affect your account. For example, if a maintenance event is scheduled for one of your Amazon EC2 instances, you can receive an alert with information to help you plan for, and proactively address any issues for the upcoming change.

The AWS PHD service also offers troubleshooting guidance for any events that may impact your workloads and steps to remediate. For example, if a hardware issue affects one of your Amazon Elastic Block Store (EBS) volumes, AWS will offer a list of affected resources and recommendations and help links to restore your volume from a snapshot.

The answer, 'AWS Service Health Dashboard' is incorrect. This service shows the general status of AWS services, not a personal view of impacted services that may affect your environment.
The answer, 'AWS CloudWatch' is incorrect. This is a monitoring service that collects performance and operational data in the form of logs, metrics, and events associated with the AWS resources you deploy in your AWS account.

The answer, 'AWS CloudTrail' is incorrect. This service helps you enable governance, compliance, and operational and risk auditing of your AWS account. The service records all API activity in your AWS account and captures actions made directly by the user or on behalf of the user by an AWS service.

Amazon Marketplace

Question 11

Which AWS service enables customers to find a catalogue of third-party digital software solutions that can be easily purchased and provisioned in their AWS accounts?

A. AWS Marketplace
B. AWS Service Catalog
C. AWS Config
D. Amazon SNS

Correct Answer – A

Explanation

The AWS Marketplace is an online service that makes it easy for customers to discover, procure and deploy software solutions from thousands of listings from popular categories such as security, data analytics, and business applications across various industries such as healthcare, banking, and the public sector.

The answer 'AWS Service Catalog' is incorrect. This may be confusing, but the AWS Service Catalog is an AWS service designed to help customers manage their catalogs of IT services that are approved for use within their AWS account. This could include third-party marketplace products, but generally also includes approved virtual machine images (AMIs), databases, and other tools to help architect and centrally managed multi-tier applications. The primary goal of the AWS Service Catalo is to offer a central repository of approved services to enforce compliance requirements and governance.

The answer 'AWS Config' is incorrect. AWS Config allows customers to assess, audit, and evaluate the configurations of their AWS resources, ensuring that they have been deployed in alignment with approved and desired configurations. AWS Config will help you identify deviations from such desired configurations and can be configured to send out alerts when changes occur and take any action where necessary. With AWS Config, you can track the relationships among resources and review resource dependencies before making changes.

The answer 'Amazon SNS' is incorrect. Amazon SNS (Simple Notification Service) is a pushed-based messaging service designed to facilitate application-to-application (A2A) and application-to-person (A2P) communication. With SNS, you can send out alerts to administrators when events occur in your AWS account and ultimately use it to build serverless architectures and microservices solutions. In addition, with SNS, you can send A2A messaging to various endpoints, including Amazon SQS queues, AWS Lambda functions, HTTPS endpoints, and Amazon Kinesis Data Firehose.

Ref: https://aws.amazon.com/mp/marketplace-service/overview/

AWS Global Infrastructure

Question 12

Which of the following services offered by AWS are considered global services? (Choose two answers)

A. Identity and Access Management (IAM)
B. Elastic Compute Cloud (EC2)
C. Route53
D. Express Route
E. Amazon RDS

Correct Answer – A & C

Explanations

Amazon Identity and Access Management (IAM) is a global identity service. You do not need to select a specific region to create IAM Users, Groups, or Roles as these entities are defined globally in your AWS Account and thus are unique throughout the globe.

Similarly, Route53 is a global DNS and Routing service enabling you to define global DNS records for your application and help you build highly available, fault-tolerant, and business-specific traffic routing solutions for your applications.

EC2 and Amazon RDS are both regional services, and you need to define the region in which you want to deploy these services, so these are incorrect answers.

Express Route is an incorrect answer because this is a Microsoft product and has nothing to do with AWS.

Question 13

Which AWS service enables you to experience a genuinely hybrid solution by extending AWS Infrastructure such as EC2 and EBS services to be hosted in your own on-premises datacentre?

A. AWS RDS
B. AWS Direct Connect
C. AWS Outpost
D. AWS Route53

Correct Answer – C

Explanation

With AWS Outposts, you can run Amazon EC2, Amazon EBS, container-based services such as Amazon EKS, database services such as Amazon RDS on AWS Outposts and analytics services such as Amazon EMR on-premises. This enables you to extend your Amazon Virtual Private Cloud on-premises and run some AWS services locally on Outposts hosted on your own Datacentre.

The answer, ‘AWS RDS’ is incorrect as this is a database service. Although you can also now run RDS on VMware, which is an on-premises solution

The answer, ‘AWS Direct Connect’ is incorrect as although it enables you to connect your data centre to your VPC in the cloud over AWS private links, you cannot use it to host EC2 or EBS services on-premise.

The answer, ‘AWS Route53’ is incorrect as Route53 is a DNS and traffic routing service offered by AWS.

Ref: https://aws.amazon.com/outposts/

Six Advantages of Cloud Computing

Question 13

Which of the following six advantages of cloud computing enables you to achieve massive savings by avoiding hidden costs compared to an on-premises infrastructure design?

A. Stop spending money running and maintaining data centers.
B. Increase speed and agility.
C. Trade capital expense for variable expense
D. Stop guessing capacity.

Correct Answer – A

Explanation

The advantage 'Stop spending money running and maintaining data centers' is that it enables you to focus on deploying your applications in the cloud without the heavy lifting of racking servers, building network services, or implementing storage solutions. More importantly, you do not incur hidden costs for running and maintaining datacentres, including power, cooling, and security.

The answer, 'Increase speed and agility', is incorrect for this question. This advantage refers to the ability to provision new IT resources with ease and minimum deployment times, which means you reduce the time to make those resources available to your developers from weeks to just minutes.

The answer, 'Stop guessing capacity', is incorrect for this question. The advantage refers to the ability to scale out your infrastructure when you experience increased demand and then scale back in when demand drops.

The answer, 'Trade capital expense for variable expense', is incorrect. This advantage refers to the concept of avoiding large amounts of capital accruing expenses for hardware. Instead, following a consumption model, you pay for IT services and resources on a pay-as-you-go model. Prices are charged per second, minute, or hour of usage or a per gigabyte of storage and network throughput.

Ref: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html

Question 14

One of the six advantages of cloud computing suggests you can ***stop guessing capacity*** when hosting your workloads and applications in the cloud. Which of the following statements represents the meaning of the advantage?

A. The lower variable costs result from aggregating thousands of customers who consume AWS services.
B. Provision of new resources in minutes with just a few mouse clicks.
C. Access to AWS regions and availability zones across the globe
D. The ability to provision cloud resources and capacity when you need it within minutes, instead of having expensive idle resources or dealing with limited capacity.

Correct Answer – D

With traditional on-premises IT, you often must over-provision your resources to cope with unexpected demands. This meant that you would have to invest vast amounts of capital in procuring necessary hardware and software and have expensive idle resources simply going to waste. If you were on a budget, you might end up under-provisioning resources, resulting in a poor customer experience.

With AWS, you can provision resources just in time for when you need them within a moment's notice. AWS offers several services, such as Auto Scaling, that, along with CloudWatch, can monitor your usage pattern and perform real-time demand monitoring. If the load on your resources increases, AWS can automatically provision new resources to fulfil demand. Similarly, AWS will terminate unwanted resources and thus enable you to achieve cost optimization.

The statement**, 'The lower variable costs resulting from the aggregation of thousands of customers who consume AWS services,'** is incorrect because this refers to the advantage of *benefiting from massive economies of scale*

The statement, **'The ability to provision new resources in a matter of minutes with just a few mouse clicks'** is incorrect because this refers to the advantage of being able to *Increase speed and agility.*

The statement, **'Access to AWS regions and availability zones across the globe'** is incorrect because this refers to the advantage of going *global in minutes.*

Ref: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html

Question 15

Which of the six advantages of cloud computing refers to the benefit of being able to deploy applications across different countries globally and thereby reduce latency?

A. Trade capital expense for variable expense
B. Increase speed and agility.
C. Stop spending money running and maintaining data centres

D. Go global in minutes.

Correct Answer – D

When you create an AWS account, you have access to its entire Global Infrastructure, enabling you to access its services across several countries globally. If you have customers across different continents, you can host your applications in regions closer to them to reduce latency and minimize costs. In addition, deploying your applications in different regions can help you address any compliance or regulatory requirements associated with data residency laws.

The answer **'Trade capital expense for variable expense'** is incorrect because this advantage refers to avoiding huge capital expenditure procuring infrastructure often associated with on-premises IT architectures.

The answer **'Increase speed and agility** is incorrect because this advantage refers to the concept of being able to rapidly design and deploy application solutions given the fact that resources can be provisioned within a matter of minutes and you have access to some of the latest cutting-edge services and best practice approaches.

The answer **'Stop spending money running and maintaining data centres'** is incorrect because this advantage refers to the fact that customers can focus on projects that impact the business rather than infrastructure set-up, management, and maintenance.

Ref: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html

Analytics

Question 16

Which AWS services can load massive amounts of streaming data into a service like Splunk, which can be used to perform search, analysis and visualization of machine-generated data?

A. Amazon Kinesis Firehose
B. Amazon SQS
C. Amazon Athena
D. Amazon Kinesis Analytics

Correct Answer – A

Explanation

Amazon Kinesis Firehose is designed to help deliver real-time streaming data to destinations such as Amazon S3, Amazon Redshift, Amazon Elasticsearch and Splunk, among others.

Amazon Kinesis. It is easy to set up, and to start using Amazon Kinesis Firehose, you need to set up a delivery stream and then send data to it. The data is then delivered to a destination of choice.
Amazon Kinesis Firehose can send data directly to Splunk and that data can also be optionally backed up to an Amazon S3 bucket. A key point to note is that there is some latency when using Firehose.

The answer 'Amazon SQS' is incorrect. Amazon SQS is a messaging queuing solution designed to decouple application components to facilitate microservices architectures. Amazon SQS holds messages in a queue for a particular time to live. Application components that need to process those messages can then retrieve them and process them in accordance with business logic.

The answer 'Amazon Athena' is incorrect. Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. This is particularly useful when you need to run ad-hoc queries against raw data held in Amazon S3 which may be stored in various formats such as .csv etc. You pay for the service based on the queries that you run. You can also use Amazon Glue which is integrated with Amazon Athena to crawl your raw data and discover its schema.

The answer, 'Amazon Kinesis Analytics' is incorrect. Amazon Kinesis Analytics enables you to analyze streaming data in real-time, using standard SQL language. You can quickly and easily build queries and stream real-time applications. You can use Amazon Kinesis Analytics to perform time-series analytics, feed real-time dashboards, and create real-time metrics. Amazon Kinesis Analytics is serverless and you only pay for the resources used to run your streaming applications.

Ref: https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html

Question 17

Which AWS service enables you to perform ad-hoc analysis against data held in Amazon S3 using standard SQL statements?

A. Amazon Kinesis Data Analytics
B. Amazon RDS
C. Amazon Athena
D. Amazon Macie

Correct Answer – C

Explanation

Amazon Athena is a serverless solution offered by AWS which can be used to analyze unstructured, semi-structured and structured held in Amazon S3 using ANSI SQL. Data can

be stored in various formats such as CSV, JSON, and columnar formats such as Apache Parquet and Apache ORC. Ideal for running ad-hoc queries against your raw data rather than ingesting it in a database solution such as Amazon RDS. Typical use cases for Amazon Athena include processing logs, performing ad-hoc analysis, and running interactive queries. Amazon Athena is serverless, so you do need to invest in provisioning any infrastructure components. With Amazon Athena, you only pay for the queries you run and are charged based on the amount of data scanned by each query.

The answer, 'Amazon Kinesis Data Analytics' is incorrect. This service can process and analyze **streaming data** using standard SQL. run robust SQL code against streaming sources to perform time-series analytics, feed real-time dashboards, and create real-time metrics. However, you do not use it to load data from Amazon S3 to run queries against.

The answer, 'Amazon RDS' is incorrect. While Amazon RDS is AWS's relational database service used to run queries and analyze data, it requires you first to provision an RDS Database instance of a specific engine such as MySQL or PostgreSQL and then load your entire dataset into the database.

The answer, 'Amazon Macie' is incorrect. Amazon Macie is a security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. This includes data such as personally identifiable information (PII).

Ref: https://aws.amazon.com/athena/

Question 18

Which AWS service can Amazon Athena use to automatically infer database and table schema from your data in Amazon S3, making it easier to find, read, and process the data you want to query?

A. Amazon Glue
B. Amazon Kinesis Data Stream
C. Amazon QuickSight
D. Amazon RDS

Correct Answer – A

Explanation

Amazon Glue is a fully managed ETL (extract, transform, and load) service that makes it easy to discover, prepare, and combine data for analytics. AWS Glue crawlers can automatically find database and table schema from your data in Amazon S3 and store this information in AWS Glue Data Catalog. Amazon Athena can then use this database and table schema you created to query the data quickly and easily using standard SQL.

The answer, 'Amazon Kinesis Data Stream' is incorrect. This service can collect and process large streams of data records in real time. Example of such streaming data includes IT infrastructure log data, application logs, social media, market data feeds, and web clickstream data.

The answer, 'QuickSight' is incorrect. Amazon QuickSight is a business intelligence (BI) service that you can use to deliver easy-to-understand insights on your data. You can access data and prepare it for use in reporting as well as create interactive dashboards that can be accessed from browsers, and mobile devices and embedded into applications.

The answer, 'Amazon RDS' is incorrect. While Amazon RDS is AWS's relational database service used to run queries and analyze data, it requires you first to provision an RDS Database instance of a specific engine such as MySQL or PostgreSQL and then load your entire dataset into the database.

Ref: https://docs.aws.amazon.com/athena/latest/ug/glue-athena.html

Question 19

You are required to automate a daily archival task which involves copying web server log files to Amazon S3 and then run a weekly analysis of that data to generate some traffic reports. Which AWS service can you use to orchestrate the regular movement and transformation of data at specified intervals?

A. Amazon Athena
B. Amazon Data Pipeline
C. Amazon RDS
D. Amazon S3

Correct Answer – B

Explanation

Amazon Data Pipeline is a service that can automate the movement and transformation of data between AWS compute and storage services (including on-premises sources) at specified intervals. In the above use case, you can create a pipeline to create a daily task of copying the log files and then a weekly EMR task to analyze the logs and generate the traffic reports. The weekly task will launch the Amazon EMR cluster. With Data Pipeline, you can schedule, track and handle error conditions for your pipeline. Data Pipeline also integrates with Amazon SNS to send notifications of successful runs, delays, and failures.

The answer, 'Amazon Athena' is incorrect. Amazon Athena is a serverless solution offered by AWS which can be used to analyze unstructured, semi-structured and structured held in Amazon S3 using ANSI SQL.

The answer, 'Amazon RDS' is incorrect. While Amazon RDS is AWS's relational database service used to run queries and analyze data, it requires you first to provision an RDS

Database instance of a specific engine such as MySQL or PostgreSQL and then load your entire dataset into the database.

The answer, 'Amazon S3' is incorrect. Amazon S3 is an object storage service offering. Amazon S3 allows you to store and protect data for virtually any use case, such as data lakes, cloud-native applications, and mobile apps.

Question 20

Which AWS business intelligence service can combine data from multiple sources and help you deliver easy-to-understand insights via reporting services and interactive dashboards?

A. Amazon Glue
B. Amazon Athena
C. Amazon Redshift
D. Amazon QuickSight

Correct Answer – D

Explanation

Amazon QuickSight is a cloud-powered business intelligence that can provide insights into data from various sources. With Amazon QuickSight, you can create interactive dashboards that can be accessed via browsers and mobile devices and embed those dashboards into applications enabling you to explore and interpret information in an interactive visual environment.

The answer, 'Amazon Glue' is incorrect. Amazon Glue is a fully managed ETL (extract, transform, and load) service that makes it easy to discover, prepare, and combine data for analytics. AWS Glue crawlers can automatically discover database and table schema from your data in Amazon S3 and store this information in AWS Glue Data Catalog. Amazon Athena can then use this database and table schema you created to query the data quickly and easily using standard SQL.

The answer, 'Amazon Athena' is incorrect. Amazon Athena is a serverless solution offered by AWS which can be used to analyze unstructured, semi-structured and structured held in Amazon S3 using ANSI SQL.

The answer, 'Amazon Redshift' is incorrect. Amazon Redshift is a petabyte-scale data warehouse service in the AWS Cloud. Also known as an Online Analytical Processing database (OLAP), Amazon Redshift uses columnar storage and massively parallel query execution to help you analyze queries against terabytes to petabytes of structured and semi-structured data.

Ref: https://youtu.be/2V1bHRLRG-w

Security, Identity and Compliance

Question 19

Which AWS Service enables you to test a new IAM Policy to ensure it only allows access from a specific IP Address before deploying the policy?

A. IAM Policy Simulator
B. CloudWatch
C. CloudTrail
D. IAM Policy Manager

Correct Answer – A

Explanation

With the IAM Policy Simulator, you can test and troubleshoot IAM and resource-based policies to resolve any conflicting permissions and ensure that the correct policy will be deployed.

Amazon CloudWatch is an incorrect answer. This service is a monitoring tool that offers a wide range of metrics to monitor various AWS services. Action can then be taken automatically to remediate issues or send alerts.

Amazon CloudTrail needs to be corrected. This service enables governance, compliance, operational auditing, and risk auditing of your AWS account. It offers the event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services, recording all API activity.

IAM Policy Manager is an incorrect answer as there is no such service.

Ref: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_testing-policies.html

Question 20

Your company plans to host application workloads on AWS, and you wish to deploy a test environment. You wish to ensure your developers can access your AWS account using a highly secure authentication process and follow best practices. Which of the following two configuration options will help ensure enhanced security? (Choose two answers)

A. Configure your IAM Accounts with MFA
B. Configure your IAM Password Policy with Complexity Rules
C. Ensure you encrypt your EBS Volumes
D. Create RDS Databases with Multi-AZ
E. Provide the root account credential details to your developers.

Correct Answer – A & B

Explanation

You can enhance login security by enforcing the use of Multi-Factor Authentication, which involves configuring a 2-Factor authentication process. Users will need to know their IAM User Credentials and have access to a multi-Factor device (physical or virtual) to provide a one-time pin code at the time of login.

Configuring your Password Policy for complexity rules will ensure that your users create complex and challenging-to-guess passwords, further enhancing security.

While encrypting your EBS volumes will protect data held on those disks, they do not specifically ensure highly secure login access for your developers; hence, this answer must be corrected.

The answer to creating RDS Database with Multi-AZ must be corrected because it does not enhance user login security.

Providing root account credential details to your developers must be corrected because this will increase the risk of security breaches. The root account has full administrative rights for your AWS Account and should rarely be used by only a few trusted administrators.

Question 21

Which IAM service enables you to effectively manage users by creating a collection of them based on their job function and assigning them permissions according to their roles to the entire collective?

A. IAM Groups
B. IAM Policies
C. Security Groups
D. Group Policy Objects (GPOs)

Correct Answer – A

Explanations –

An IAM group is a collection of IAM users. Groups let you specify permissions for multiple users, making it easier to manage the permissions for those users. For example, you could have a group called *Admins* and give that group the permissions that administrators typically need. Any user in that group automatically has the permissions assigned to the group. If a new user joins your organization and needs administrator privileges, you can set the appropriate permissions by adding the user to that group. Similarly, if a person changes jobs in your organization, instead of editing that user's permissions, you can remove him or her from the old groups and add to the appropriate new groups.

The answer, “IAM Policies” is incorrect as these are the permissions you can apply to users or groups. IAM Policies do not let you create a collection of users.

The answer, “Security Groups,” is incorrect regarding EC2 Instance and the ability to open inbound and outbound traffic on specific ports to those instances. They have nothing to do with IAM users.

The answer, “Group Policy Objects (GPOs)”, is incorrect as there is no such service in AWS. This Microsoft term assigns permissions to Active Directory users and groups.

Question 22

Which action is the customer's responsibility under the AWS Shared Responsibility Model?

A. Upgrading the compute hypervisors that are used to provision EC2 Instances
B. Ensuring that the underlying RDS instances are routinely patched.
C. Installing anti-virus software on your EC2 instances running Microsoft Windows Server 2019
D. Maintaining multiple copies of your S3 data across various devices within a given region to offer 99.999999999% (11 9s) of durability)

Correct Answer: C

Explanation

Amazon EC2 Instances form part of AWS's Infrastructure as a Service (IaaS) offering. You have full control of the instances you deploy from the OS layer. This means you are responsible for all the applications, utilities, and security features you install and configure on those servers. This includes ensuring adequate anti-virus protection is installed and configured on those EC2 instances.

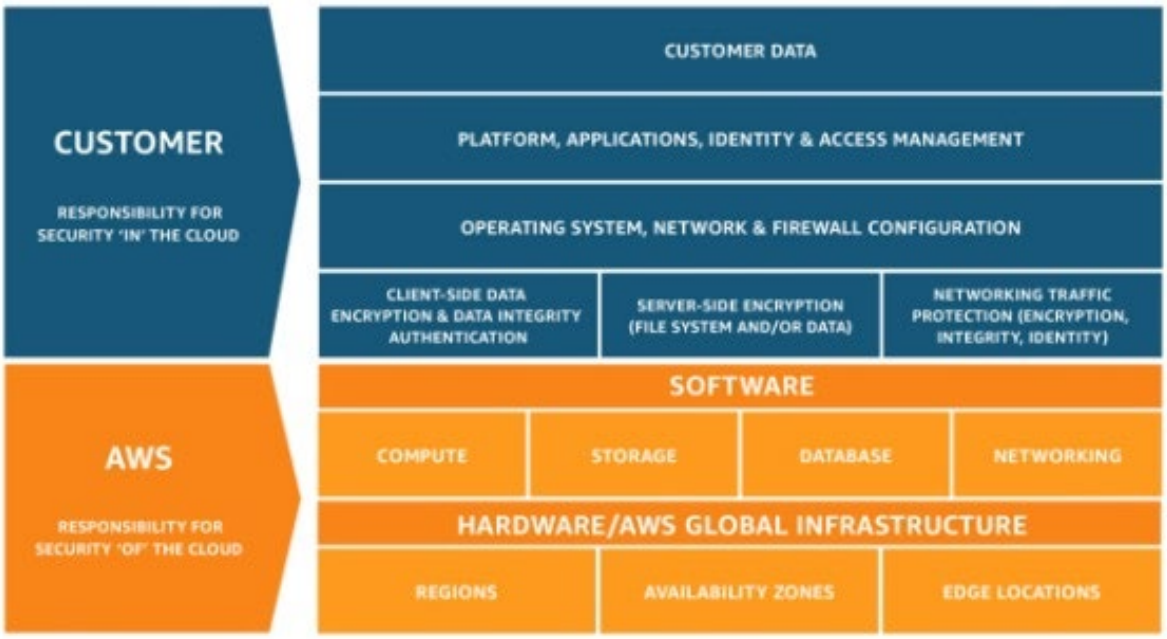
The answer ‘Upgrading the compute hypervisors used to provision EC2 Instances’ is incorrect because AWS is responsible for the underlying infrastructure and the hypervisor layer.

The answer ‘Ensuring that the underlying RDS instances are routinely patched’ is incorrect. Amazon RDS is a managed service, and AWS manages all the patching, upgrades and updates of the database software solution. Amazon recommends using managed services where possible, as AWS will manage all maintenance tasks on tho.

The answer ‘Maintaining multiple copies of your S3 data across multiple devices within a given region to offer 99.999999999% (11 9s) of durability)’ is incorrect. AWS maintains multiple copies of your data within the same region in which you upload that data. These copies ensure that AWS can offer higher levels of durability as well as availability even in situations where there might be an availability zone outage within a given region.

To decide whether a particular action is your responsibility of that of AWS, you need to determine if you have access to configure that resource is any specific way. If you have access to configure that resource, then how you configure it and what security measures you take falls within your responsibility.

The diagram below showcases the differences between AWS and customers' responsibilities.



Ref: https://aws.amazon.com/compliance/shared-responsibility-model/

Question 23

Which of the following compliance standards does AWS offer to allow customers to build and host applications that can be used to manage medical records in the United States of America?

A. PCI DSS
B. HIPAA
C. SOC 1
D. SOC 2

Correct Answer – B

Explanation

AWS is a public cloud provider and operates on a Shared Responsibility Model. AWS is responding for 'Security of the Cloud' to ensure that its underlying infrastructure is secured and adheres to various compliance and regulatory requirements. The customer is

responsible for 'Security in the Cloud', meaning that the resources they configure should align to security best practices. This includes ensuring that data held in the cloud is secured and the architecture of the applications it hosts in the cloud.

Several industries need to adhere to compliance laws. In the medical industry, one such requirement is HIPAA (Health Insurance Portability and Accountability Act of 1996) compliance. HIPAA is United States legislation that provides data privacy and security provisions for safeguarding medical information.

In terms of 'Security of the Cloud', AWS has designed and built infrastructure services as well as managed products that fulfil HIPAA compliance. As a customer, you to inherit the benefits of this compliance. However, you still need to ensure that any resources you create or applications you host also adhere to the same requirements.

The answer 'PCI DSS' is incorrect. This compliance requirement refers to payment card protection and relates to how you should accept, process, store, or transmit credit card information in a secure environment.

The answer 'SOC 1' and 'SCO 2' are also incorrect as they do not relate to the management and storage of medical data.
Ref: https://aws.amazon.com/compliance/
Ref: https://aws.amazon.com/compliance/hipaa-compliance/

Question 24

Your company is building an application which requires it to store credit card information. Your internal auditing team needs to review any documents related Payment Card Industry (PCI) that AWS offers as you plan to host the application in the cloud. Which AWS service can you use to download relevant material?

A. AWS Artifact
B. Amazon Macie
C. Amazon AUP
D. Amazon Concierge

Correct Answer – A

AWS Artifact is an online repository offered by Amazon from which you can access a vast array of compliance reports and select online agreements. These include Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports and various Non-Disclosure Agreements (NDAs).

With AWS Artifact, you can review, accept, and manage your agreements with AWS and apply them to your current and future accounts.

The answer 'Amazon Macie' is incorrect. Amazon Macie is a data security and data privacy service that uses machine learning (ML) to discover and protect your sensitive data. These include Personal Identifiable Information (PII) data.

The answer 'Amazon AUP' is incorrect. Amazon AUP stands for Acceptable Use Policy which describes what activities (technical and non-technical) you can or cannot perform on AWS. The answer 'Amazon Concierge' is incorrect. This feature is offered as part of the AWS Enterprise Support Plan, which focuses on helping you achieve your outcomes and succeed in the cloud via a concierge team from AWS.

Ref: https://aws.amazon.com/artifact/

Question 25

Your CEO recently heard that a competitor who migrated to AWS suffered from an attack. The competitors' AWS Account was used to mine cryptocurrency for an illegal concern. Which AWS security services offer threat detection capabilities using machine learning and behaviour models to help detect such malicious activity?

A. AWS QLBD Database
B. AWS GuardDuty
C. Security Groups
D. NACLs

Correct Answer – B

Explanation

GuardDuty identifies threats by continuously monitoring the network activity and account behaviour within the AWS environment. GuardDuty uses machine learning and behaviour models to help you detect activities such as cryptocurrency mining, credential compromise behaviour, communication with known command-and-control servers, or API calls from known malicious IPs.

GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs. GuardDuty can also be integrated with Amazon CloudWatch Events and Lambda to trigger automatic responses to various threats.

The answer, 'AWS OLDB' is incorrect. Amazon QLDB is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log owned by a central trusted authority. Amazon QLDB tracks each application data change and maintains a complete and verifiable history.

The answer, 'AWS Security Group' is incorrect. A security group acts as a virtual firewall to control inbound and outbound traffic for your instance. When you launch an instance in a VPC

The answer, 'AWS NACLs' is incorrect. Network Access Control Lists (NACLs) act as a firewall for controlling traffic in and out of one or more subnets within your VPC.

Ref: https://youtu.be/ocZjGirQT9A

Question 26

Which service in AWS protects your virtual network and resources from common Distributed Denial of Service (DDoS) attacks?

A. AWS Shield
B. AWS WAF
C. AWS CloudFront
D. Amazon Macie

Correct Answer – A

Explanation

AWS Shield offers DDoS protection that helps to safeguard your applications running on AWS. AWS offers two tiers of the service – AWS Shield Standard and AWS Shield Advanced.

AWS Shield Standard is offered free of charge and helps you to defend against the most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications. AWS Shield Advance protects against attacks that target your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53 resources.

The answer, 'AWS WAF' is incorrect. AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits such as SQL injection or cross-site scripting.

The answer, 'AWS CloudFront' is incorrect. Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

The answer, 'Amazon Macie' is incorrect. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property and provides dashboards and alerts that give visibility into how this data is being accessed or moved.

Ref: https://aws.amazon.com/shield/

Question 27

Which AWS service uses machine learning to help identify the root cause of suspicious activities and API calls against resources in your AWS account?

A. Amazon CloudWatch
B. Amazon Detective
C. AWS CloudTrail
D. AWS Systems Manager

Correct Answer – B

Amazon Detective extracts, analyses, and identifies suspicious activities from sources such as login attempts, API calls and network traffic such as those from VPC flow logs, to identify the root cause of such security findings. The service uses machine learning and visualizations to build interactive views of your resources' behaviour over time. This can then identify activities that may fall outside what is considered normal and patterns that may suggest security issues.

The answer 'Amazon CloudWatch' is incorrect. Amazon CloudWatch is a service that monitors resource metrics and utilization. Amazon CloudWatch can help you define alarms when specific metric values cross certain thresholds for a period can be used to ingest log data from other resources for analysis.

The answer 'AWS CloudTrail' is incorrect. AWS CloudTrail is an always-on auditing service that can help you record all user activities in your AWS accounts across multiple regions. It's ideal for storing audit records for all API calls made in your AWS, which can be used for auditing purposes.

The answer 'AWS Systems Manager' is incorrect. AWS Systems Manager is a suite of tools designed to help you manage your resources, such as EC2 instances and even on-premises servers. With features such as patch management, run command and session manager, and parameter store, it is designed to help you centrally manage, detect and resolve operational issues and maintain resource compliance against your patching and security updates.

Question 28

Which AWS services enable you to perform security assessment against your EC2 instance using pre-defined rules mapped to security best practices, thus enabling to perform standard checks such as access to your EC2 instances from the internet, remote root login being enabled, or vulnerable software versions installed?

A. AWS Inspector
B. AWS Macie
C. AWS Glue
D. AWS WAF

Correct answer – A

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector security assessments help you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities in those EC2 instances, as well as Lambda functions and ECS containers.

Amazon Inspector uses the AWS Systems Manager Agent (SSM Agent) to collect the software inventory and configurations from your Amazon EC2 instances.

The answer, 'AWS Macie' is incorrect. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property (such as your corporate application source codes) and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved.

The answer, 'AWS Glue' is incorrect. AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics.

The answer, 'AWS WAF' is incorrect. AWS WAF can be used to control how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you configure.

Ref: https://aws.amazon.com/inspector/

Question 29

A public sector organization plans to host data on AWS and needs to encrypt that data using its single-tenant hardware security module. This ensures the organization has complete control over how the keys are created and used. Which AWS service would you recommend for the organization?

A. AWS CloudHSM
B. AWS KMS
C. Amazon Macie
D. AWS GuardDuty

Correct Answer – A

AWS CloudHSM is a fully managed encryption service that allows you to generate and use cryptographic keys on dedicated FIPS 140-2 Level 3 single-tenant HSM instances. These HSM instances are dedicated to your AWS account only and not shared with other customers as is the case with AWS Key Management Service (KMS). The single-tenant HSM instances are placed in your VPC and not accessible by other customers. AWS will still take care of your time-consuming administrative tasks, such as hardware provisioning, software patching, high availability, and backups. However, you have exclusive control over your keys' use via an authentication mechanism independent from AWS.

You can use AWS CloudHSM to support a variety of use cases, such as Digital Rights Management (DRM), Public Key Infrastructure (PKI), document signing, and cryptographic functions using PKCS#11, Java JCE, or Microsoft CNG interfaces.

The answer 'AWS KMS' is incorrect. AWS KMS is a fully managed encryption solution that lets you create, manage, and control cryptographic keys across your applications. However, unlike CloudHSM, AWS KMS uses multi-tenanted, FIPS-validated hardware service modules (HSMs) that AWS manages. As such the HSMs are shared with other customers too and therefore does not fulfil the requirements of the questions.

The answer 'Amazon Macie' is incorrect. This service uses machine learning and pattern matching to discover and protect your sensitive data such as Personally Identifiable Information (PII).

The answer 'AWS GuardDuty' is incorrect. Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

Ref: https://aws.amazon.com/cloudhsm/

Video Ref: https://youtu.be/BLnuUtjJNLE

Question 30

Your company is planning on hosting vast quantities of sensitive data on AWS. To ensure higher levels of security, data stored in Amazon S3 will be encrypted. Which encryption option provides an audit trail showing when your key was used and by whom?

A. Server-Side Encryption with KMS (SSE-KMS)
B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
D. Server-Side Encryption with Amazon GuardDuty

Correct Answer – A

Server-Side Encryption with KMS (SSE-KMS) enables you to encrypt each object in an S3 bucket with a unique key. With KMS, you create Customer Master Keys (CMKs) which can then used to encrypt data up to 4 KB in size. CMKs are used to encrypt data keys that are ultimately used to encrypt and decrypt the actual data.

In addition, separate permissions for the use of a KMS key provides additional protection against unauthorized access of your objects in Amazon S3. SSE-KMS integrates with Amazon CloudTrail and provides an audit trail showing when your KMS key was used and by whom.

The answer 'Server-Side Encryption with Customer-Provided Keys (SSE-C)' is incorrect. With SS3-C, you manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption, when you access your objects.

The answer 'Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)' is incorrect. SSE-S3 uses 256-bit Advanced Encryption Standard (AES-256) GCM, to encrypt your data. It is a fully managed service where AWS will create and manage your keys as well as the encryption service. Amazon S3 encrypts each object with a unique key. It also encrypts the key itself with a key that rotates regularly.

The answer 'Server-Side Encryption with Amazon GuardDuty' is incorrect. Amazon GuardDuty is not an encryption service. It is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

Question 31

Which AWS service collects log data from sources such as Virtual Private Cloud (VPC) Flow Logs, AWS CloudTrail, and Amazon GuardDuty that is then used to identify the root cause of potential security issues in your AWS account?

A. AWS CloudTrail
B. AWS CloudWatch
C. AWS Trusted Advisor
D. Amazon Detective

Correct Answer – D

Explanation

Amazon Detective collects log data from various sources such as s Virtual Private Cloud (VPC) Flow Logs, AWS CloudTrail, and Amazon GuardDuty to help identify the root cause of security issues or suspicious activities.

Services like Amazon GuardDuty and Amazon Macie are excellent in alerting you to various security issues as they happen. However, Amazon Detective goes one step further by helping

you isolate the root cause of those potential security issues. The service uses machine learning, statistical analysis, and graph theory to help you perform efficient security investigations.

The answer 'AWS CloudTrail' is incorrect. AWS CloudTrail is a service that allows you to monitor your account from an operational and risk auditing perspective. AWS CloudTrail can audit all actions you take in your account, whether in the web console, CLI or API calls. However, it is not designed to perform root cause analysis on security issues within your AWS account.

The answer 'AWS Trusted Advisor' is incorrect. AWS Trusted Advisor is a web service that can analyze how your resources are used and configured. The service uses a traffic light system to help you easily identify issues and potential security threats. However, it does not perform root cause analysis on those security issues. AWS Trusted Advisor can evaluate the total spend on your resources and identify if there are any cost savings you can benefit from through its cost optimization category.

The answer 'Amazon CloudWatch' is incorrect. Amazon CloudWatch records your AWS resources, applications' performance, and health metric information. You can then create dashboards and alarms for those metrics.

Ref: https://aws.amazon.com/detective/

Video Ref: https://youtu.be/84BhFGIxIqg

Question 32

A software development company has designed a new application for your business. To deploy the application in your AWS account, you need to grant them temporary credentials necessary to create resources such as EC2 Instances and S3 buckets that will host the application. Which of the following would you recommend they use to access your AWS account?

A. IAM user account with restrictive policies
B. IAM role
C. IAM group
D. Web Application Firewall (WAF)

Correct Answer – B

An IAM role is an identity that does not require storing long-term credentials in the form of a username and password or a set of access keys. IAM roles are created independent of any specific user and can be assumed by both internal and external entities (such as the software development company) when needed. IAM roles require you to specify a trust policy, identifying the external software development company as the entity that can assume the role. Furthermore, the role itself will have a policy attached to it which can be used to

determine exactly what action the software development company can or cannot do in your AWS account.

IAM roles enable you to grant temporary credentials to entities that need access to your AWS account to create resources. By using IAM roles, you avoid having to create long-term credentials which would be required if you provided an IAM user account instead. While the latter is also an also option, it requires you to ensure that those long-term credentials are secured and rotated on a regular basis.

The answer, 'IAM user account with restrictive policies' is incorrect. IAM user accounts can only be configured with long-term credentials in the form of a username and password for console access. For programmatic access, you would need to create a set of access keys (access key ID and secret access key) which are also long-term credentials

The answer, 'IAM group' is incorrect. IAM groups are designed to apply common policies to a group of IAM users that share a common job function. IAM users can be configured as members of an IAM group and permissions applied to the group are inherited by the IAM users that are members of the group.

The answer, 'Web Application Firewall (WAF)' is incorrect. AWS WAF is designed to protect applications hosted on AWS from common web exploits such as cross-site scripting and SQL injections.

Ref: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

Question 33

Which AWS service can you use to centrally configure and manage firewall rules that can be applied across all accounts in your AWS Organization?

A. AWS Firewall Manager
B. AWS Certificate Manager
C. AWS WAF
D. AWS Shield

Correct Answer – A

Explanation

AWS Firewall Manager allows you to provision and centrally manage all your firewall rules across your networks and applications within AWS accounts hosted in an AWS Organization. This allows you to better manage your various rules across VPCs, AWS WAF and AWS Shield from a central console.

You can use AWS Firewall Manager to to build firewall rules, create security policies, and enforce them in a consistent, hierarchical manner across all resources such as load balancers

and CloudFront distributions. In addition, AWS Firewall Manager makes it easy to track for compliance and reporting.

The answer ‘AWS Certificate Manager’ is incorrect. Amazon Certificate Manager (ACM) enables you to provision, manage, and deploy public and private SSL/TSL certificates for use with AWS services.

The answer ‘AWS WAF’ is incorrect. AWS Web Application Firewall (AWS WAF) is a firewall security service that enables you to define security rules to protect your application from common web exploits such as SQL injections and cross-site scripting. You can use AWS Firewall Manager to configure and manage all your AWS WAF rules centrally.

The answer ‘AWS Shield’ is incorrect. AWS Shield is a managed security service that protects customers' resources and applications from Distributed Denial of Service (DDoS) attacks. You can use AWS Firewall Manager to configure and manage all your AWS Shield configurations centrally.

Ref: https://aws.amazon.com/firewall-manager/

Question 34

You plan to host a web application on AWS and would like to ensure protection against common web exploits such as SQL injections. Which AWS service can you use that offers firewall protection at the application layer?

A. AWS WAF
B. Amazon Shield
C. AWS GuardDuty
D. Amazon Macie

Correct Answer – A

Explanation

AWS Web Application Firewall (AWS WAF) is a firewall security service that enables you to define security rules to protect your application from common web exploits such as SQL injections and cross-site scripting.

With AWS WAF you can filter web requests based on conditions such as IP addresses, HTTP headers and body, or custom URIs. AWS WAF also offers protection against attacks from bot traffic that can consume excess resources.

The answer ‘AWS Shield’ is incorrect. AWS Shield protects your resources and applications from layer 3 & 4 attacks defending your services from distributed denial of service (DDoS) attacks.

The answer ‘Amazon Macie’ is incorrect. Amazon Macie is a data security and privacy service that can be configured to discover and protect sensitive data held in your Amazon S3 buckets.

The answer ‘Amazon GuardDuty’ is incorrect. Amazon GuardDuty is a threat detection service that continuously monitors and analyses activity within your AWS account. The service analyses tens of billions of events from Amazon S3 logs, CloudTrail logs, DNS logs, Kubernetes audit logs, and Amazon VPC flow logs. It then uses threat intelligence feeds, such as lists of malicious IP addresses and domains, to help identify any malicious activity within your AWS environment.

Ref: https://aws.amazon.com/waf/

Video ref: https://youtu.be/nUI7G9UzyN8

Question 35

Which AWS storage service does Amazon Macie monitor and analyze to discover sensitive data such as personally identifiable information (PII)?

A. Amazon EBS
B. Amazon EFS
C. Amazon S3
D. Amazon DynamoDB

Correct Answer – C

Explanation

Amazon Macie is a data security and data privacy service that can be configured to discover and protect your sensitive data held in your Amazon S3 buckets. Once configured, the service continuously monitors your Amazon S3 environment to search, filter, and sort buckets by metadata variables, such as bucket names, tags, and security controls like encryption status or public accessibility. You can use Amazon Macie to send out alerts if it discovers unencrypted, publicly accessible data as well as if you have any buckets being shared with AWS accounts outside of your AWS Organization.

Amazon Macie can be used to help fulfil your regulatory and compliance requirements by identifying and protecting data that such as personally identifiable information (PII) and other sensitive data types such as GDPR, PCI-DSS, and HIPAA.

The answer ‘Amazon EFS’ is incorrect. Amazon Elastic File Storage (EFS) is file system that lets you share file data without provisioning or managing storage and primarily used to share data between Linux EC2 instances. Amazon Macie currently does not analyze data held in Amazon EFS.

The answer ‘Amazon EBS’ is incorrect. Amazon Elastic Block Store (EBS) is a block storage service that allows you to attach block volumes to EC2 Instances to be used as virtual hard drives. Amazon Macie currently does not analyze data held in Amazon EBS

The answer ‘Amazon DynamoDB’ is incorrect. Amazon DynamoDB is a NoSQL database solution offered by AWS. Currently Amazon Macie cannot be used to analyze data held in DynamoDB tables.

Ref: https://aws.amazon.com/macie/

Video Link: https://youtu.be/CenD1dq3xj8

Question

Which best practice relates to the concept that IAM users should be provided with only the necessary permissions required for their job role or function?

A. The Principle of Least Privilege
B. The Shared Responsibility Model
C. The Well-Architected Framework
D. Use IAM roles instead of long-term credentials.

Correct Answer – A

Explanation

The Principle of Least Privilege is a best practice security concept in which users should be granted minimum levels of access or permissions to ensure they can perform their job functions. Often for the sake of easy administration, elevated permissions are granted which goes against this best practice recommendation.

The answer ‘The Shared Responsibility Model’ is incorrect. This model refers to security as a shared responsibility between the customer and AWS. AWS is responsible for ‘Security of the Cloud’ whereas the customer is responsible for ‘Security in the Cloud’. More details can be found here - https://aws.amazon.com/compliance/shared-responsibility-model/

The answer ‘The Well Architected Framework’ is incorrect. The Well Architected Framework is based is a set of best practices and methodologies that is designed to help customers build secure, high-performing, resilient, and efficient infrastructure to support their applications. The frameworks are based on six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. More details can be found here -

https://aws.amazon.com/architecture/well-architected/

The answer ‘ Use IAM roles instead of long-term credentials’ is incorrect. This recommendation is a best practice that relates to using temporary credentials in favour or long-term ones.

Ref: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Question 36

If you accidentally give your access key ID and secret access key to an unauthorized person, what can you do to protect your account?

A. Raise a support request with Amazon to block the keys
B. Make Inactive using the IAM console or CLI
C. Re-create your IAM Account
D. Reset your IAM User password

Correct Answer – B

Explanation

You can choose 'Make Inactive' to disable your Access Key ID and Secret Access Key if you feel the keys may have been compromised.

Question 37

As part of your yearly auditing requirements, you are required to produce a list of all users in your AWS account, the status of their passwords, access keys, and whether they have MFA enabled. How can you create such as list?

A. Generate and download the credentials report.
B. Generate and download the MFA report.
C. Generate and download the Access Key List.
D. Generate and download the Key Pairs List.

Correct Answer – A

Explanation

The Credentials report enables you to produce a list of all users in your AWS Account and the status of their various credentials such as when they last used their passwords to access the account. The report will also highlight whether their accounts have enabled and activated MFA. The report can assist with auditing and compliance requirements, and you can generate the report every four hours to review updates.

The answer, 'Generate and download the MFA report,' is incorrect as there is no such option.

The answer, 'Generate and download the Access Key List' is incorrect as there is no such option.

The answer, 'Generate and download the Key Pairs List' is incorrect. Key Pairs are public/private key combinations used to remotely access Linux and Windows EC2 Instances

In the IAM dashboard, you can generate and download the Credentials Report on the left-hand menu.

Ref: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html#getting-credential-reports-console

Ref: https://console.aws.amazon.com/iam

Question 38

Which AWS feature can you use to enable two-factor authentication for your AWS root user?

A. Access Keys
B. MFA
C. Username and Passwords
D. Certificates

Correct Answer – B

MFA or Multi-Factor Authentication is a feature that enables you to add a layer of security by requiring the user to provide two forms of authentication. The first is the username and password combination. The second form is a one-time password (or pin) from an associated multi-factor authentication device (which can be a virtual device such as an authentication mobile app).

In addition to enforcing two-factor authentication for your root user, it is highly recommended that IAM users are also configured with MFA.

Ref: https://www.youtube.com/watch?v=cP_IbgnK8yk&t=94s

Application Integration

Question 39

Which Amazon SQS queue type offers maximum throughput, best-effort ordering, and at least once delivery?

A. SQS Standard Queue
B. SQS Power Queue
C. SQS FIFO Queue

D. SQS LIFO Queue

Correct Answer – A

Explanation

Amazon SQS offers standard as the default queue type. Standard queues support nearly unlimited transactions per second (TPS) per API action. Standard queues support at-least-once message delivery. However, occasionally (because of the highly distributed architecture that allows nearly unlimited throughput), more than one copy of a message might be delivered out of order. Standard queues provide best-effort ordering, ensuring that messages are generally delivered in the same order they're sent.

The answer, 'SQS Power Queue' is incorrect as there is no such queue type

The answer, 'SQS FIFO Queue' is incorrect. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent

The answer, 'SQS LIFO Queue' is incorrect as there is no such queue type

Ref: https://aws.amazon.com/sqs/

Question 40

You are required to configure an Amazon S3 event alert such that your legal team gets a notification if someone tries to delete an object from a sensitive S3 Bucket. Which AWS Service is used by Amazon S3 to send notifications to your legal team?

A. Amazon SNS
B. Amazon Email
C. Amazon CloudWatch
D. Amazon Trusted Advisor

Correct Answer – A

Explanation

You can configure Amazon S3 Events to send notifications to an Amazon SNS topic for various actions on a given S3 Bucket. For example, you can send out a notification message to an SNS topic when someone deletes an object. Subscribers to the SNS Topic will then receive that notification.

The answer, 'Amazon Email' is incorrect as no such service exists.

The answer, 'Amazon CloudWatch,' is incorrect. Amazon CloudWatch can help you visualize key metrics, like CPU utilization and memory, and compare them to capacity. You can also correlate the log pattern of a specific metric and set alarms to be proactively alerted about performance and operational issues.

The answer, 'Amazon Trusted Advisor,' is incorrect. AWS Trusted Advisor offers recommendations that can save money by highlighting unused resources and opportunities to reduce your bill.

Ref: https://aws.amazon.com/sns/

Compute Services

Question 41

Which AWS EC2 pricing option enables you to take advantage of unused EC2 capacity in the AWS cloud and can offer up to a 90% discount compared to On-Demand prices?

A. Spot Instances
B. Reserved Instances
C. On-Demand Instance
D. Dedicated Hosts

Correct Answer – A

Explanation

Amazon EC2 Spot Instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices. You can use Spot Instances for various stateless, fault-tolerant, or flexible applications such as big data, containerized workloads, CI/CD, web servers, high-performance computing (HPC), and other test & development workloads.

However, you should remember that Spot Instances are subject to potential interruptions if the Spot Price exceeds your Bid Price or if there is no available spare capacity.

The answer, Reserved Instances is incorrect as the purchase of this pricing option requires a commitment to a 1- or 3-year contract and while it is available at a discount when compared to On-Demand instances, it does not offer the same level of flexibility as Spot Instances

On-Demand Instances is incorrect as this is available at standard pay-as-you-go rates and does not offer the discounts you can get on Spot Instances. However, the On-Demand pricing option is not subject to interruptions that could happen with Spot Instances.

Dedicated Hosts is incorrect as it is designed for workloads running on dedicated instances to meet compliance or licensing requirements.

Ref: https://aws.amazon.com/ec2/pricing/

Question 42

Which feature of the AWS EC2 Services helps to prevent the accidental termination of an EC2 Instance by preventing the user from issuing a termination command either from the console or CLI?

A. Enable 'Termination Protection'
B. Enable 'Termination Protect'
C. Enable 'Prevent Termination'
D. Enable 'Protect EC2'

Correct Answer – A

Explanation

To help protect against data loss caused by the accidental termination of an Amazon EC2 instance, you can enable the 'Termination Protection' feature, which prevents an instance from being accidentally terminated by requiring you to disable the protection before deleting the instance.

The other options listed are distractors and do not exist on the platform.

Question 43

Which storage solution enables you to share a standard file storage system across multiple Linux-based EC2 Instances that can be used to support applications requiring data access with low latency connectivity?

A. Elastic File System (EFS)
B. Elastic Block Store (EBS)
C. Amazon Simple Storage Service (Amazon S3)
D. NT File System (NTFS)

Correct Answer – A

Explanation

Amazon EFS is a fully managed service providing shared file system storage for Linux workloads. It provides a simple interface allowing you to quickly create and configure file systems. It controls the file storage infrastructure for you, removing the complexity of deploying, patching, and maintaining the underpinnings of a file system. You can use to provide your application that runs on multiple EC2 instances to share a standard file system that offers low latency connectivity.

The answer, “EBS”, is incorrect because although you can configure a file system on EBS Volumes, you cannot share an EBS volume across multiple EC2 Instances.

The answer, “S3” is incorrect because it is not a file system. Also, EFS would offer much lower latency. Amazon S3 is object storage and is ideally used to host assets such as documents, images, and videos, which web applications can reference.

The answer, “NTFS” is incorrect because this is a file system, specifically a Windows File System and not the actual storage option.

Ref: https://aws.amazon.com/efs/

Question 44

Which type of EBS volume would you recommend for a high-performance application that is particularly sensitive to high latency?

A. EBS General Purpose SSD (gp2)
B. EBS Throughput Optimized HDD (st1)
C. Cold HDD (sc1)
D. EBS Provisioned IOPS SSD (io1)

Correct Answer – D

Explanation

IO1 is backed by solid-state drives (SSDs). It is the highest-performance EBS storage option designed for critical, I/O-intensive database and application workloads and throughput-intensive database and data warehouse workloads, such as HBase, Vertica, and Cassandra. These volumes are ideal for IOPS-intensive and throughput-intensive workloads requiring extremely low latency.

The answer “EBS General Purpose SSD (gp2) is incorrect and ideally suited to non-intensive workloads.

The answer “EBS Throughput Optimized HSS (st1) is incorrect as there is no such.

Question 45

Which of the following types of EBS volumes can be used as boot volumes for your EC2 Instances? (Select two answers)

A. General Purposes SSD (gp2)
B. Provisioned IOPS SSD (io1)
C. Throughput Optimized HDD (st1)
D. Cold HDD (sc1)
E. FSx for Windows

Correct Answer – A&B

Explanation

AWS Offers Elastic Block Storage for creating and attaching volumes to your EC2 Instances. Only the General Purpose SSD (gp2) and Provisioned IOPS SSD (io1) can be used as boot volumes.

Throughput Optimized HDD and Cold HDD cannot be used for boot volumes. Amazon FSx for Windows is a file system for Windows shares and not a standard block storage solution that you can attach to ECS Instances.

Question 46

Which AWS service enables you to quickly launch a web server with a pre-configured WordPress installation pack, offer predictable monthly pricing with integrated certificate management, and provide free SSL/TLS certificates?

A. AWS LightSail
B. AWS EC2
C. AWS RDS
D. AWS Elastic Beanstalk

Correct Answer – A

Explanation

AWS LightSail offers virtual servers that are easy to set up and manage. AWS LightSail servers offer preconfigured virtual specifications for your servers with a predictable pricing strategy. You can launch your website, web application, or project in minutes and manage your instance from the intuitive LightSail console or API. Applications like WordPress can be deployed preconfigured, making it very easy to provision a website within minutes and where you do not need the complexity associated with manually configuring an EC2 server, such as storage, load balancing, and certificate management.

LightSail also offers free SSL/TLS certificates that can be provisioned and added to a load balancer in just a few clicks.

The answer, 'AWS EC2', is incorrect because EC2 offers multiple configuration options and individual components, like WordPress, must be managed separately or via scripts. Furthermore, you must configure your Elastic Load Balancers, install SSL Certs, etc.

As your requirements become more complex, you can easily upgrade your LightSail environment and move to EC2 with a simple, guided experience.

The answer, 'AWS RDS' is incorrect because AWS RDS is a managed database solution, not a virtual server solution to host websites and applications like WordPress.

The answer, 'Elastic Beanstalk,' is incorrect as it is a platform service enabling you to automatically provision an entire infrastructure environment to support application code you can upload.

Ref: https://aws.amazon.com/lightsail/features/

Question 47

You must host a website across a fleet of web servers on the Amazon platform. To build a highly cost-effective solution, you want to automatically provision additional web servers configured with the necessary application stack when demand on those servers increases over a period and then terminate web servers when there is a decrease in CPU load.

How would you configure your solution?

A. Configure an Elastic Load Balancer to distribute incoming traffic to your web servers. As part of the configuration, configure the ELB to launch additional servers when CPU Utilization goes above a threshold for a short period. Configure the Elastic Load Balancer to terminate web servers when the CPU Utilization levels drop below a certain threshold for a specified period.
B. Configure Auto Scaling to manage your web servers. As part of the configuration, configure the launch of additional servers when CPU Utilization goes above a threshold for a short period. Configure the Auto Scaling service to terminate web servers when the CPU Utilization levels drop below a certain threshold for a specified period.
C. Configure Server Manager to manage your web servers. As part of the configuration, configure the launch of additional servers when CPU Utilization goes above a threshold for a short period. Configure the Auto Scaling service to terminate web servers when the CPU Utilization levels drop below a certain threshold for a specified period.
D. Configure Route53 to manage your web servers. As part of the configuration, configure the launch of additional servers when CPU Utilization goes above a threshold for a short period. Configure the Auto Scaling service to terminate web servers when the CPU Utilization levels drop below a certain threshold for a specified period.

Correct Answer – B

Explanation

Amazon EC2 Auto Scaling is a service that can be used to ensure application availability by allowing you to automatically add or remove EC2 instances according to conditions such as CPU Utilization and Network Traffic. You can use the fleet management features of Amazon EC2 Auto Scaling to maintain the health and availability of your fleet. You can also use the dynamic and predictive scaling features of Amazon EC2 Auto Scaling to add or remove EC2 instances.

The answer, ‘Elastic Load Balancer,’ is incorrect because ELBs are primarily used to distribute traffic to healthy EC2 Instances evenly. They do not launch or terminate EC2 Instances.

The answer, ‘Server Manager’ is incorrect as no such service exists.

The answer,’Reoute53,’ is incorrect because Route53 is a DNS and Routing service that can direct traffic to your feel of EC2 Instances across the globe based on the routing policy configured. While Route53 can perform health checks and redirect traffic, they cannot be used to increase or decrease your fleet size.

Ref: https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html

Question 48

Which AWS service automatically provisions the necessary infrastructure (e.g. load balancing, auto-scaling, and health monitoring) and enables developers to automatically deploy applications built-in supported languages such as node.js, PHP and python?

A. AWS CloudFormation
B. AWS Lambda
C. AWS Elastic Beanstalk
D. AWS Deployer

Correct Answer – C

Explanation

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.

You can upload your code, and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, and auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.

The answer, ‘AWS Lambda’ is incorrect. AWS Lambda enables you to execute code you upload in response to various triggers such as events. However, it does not build out an infrastructure stack that can be used to support a full-end to the end application stack

The answer, ‘AWS CloudFormation’ is incorrect. AWS CloudFormation is an Infrastructure as a Code (IoC) service that allows you to design and deploy infrastructure in the cloud based on templates you built. However, it is application-agnostic and is designed to focus more on creating an underlying architecture you design in code rather than provisioning infrastructure for a specific application you wish to deploy.

The answer, ‘AWS Deployer’ is incorrect as no such service exists.

Ref: https://www.youtube.com/watch?v=sAyCmAryjU4

Question 49

Which AWS service can execute code in response to events and triggers as part of your application workflow and help companies design and architect serverless applications on AWS?

A. AWS Lambda
B. AWS Simple Notification Service (Amazon SNS)
C. Amazon Relational Database Services (Amazon RDS)
D. Amazon Snowball

Correct Answer – A

Explanation

AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. Amazon S3 and API gateway can invoke your code when responding to an event or application workflow trigger.

The answer, 'AWS SNS' is incorrect as it is a messaging service designed to send notifications to subscribers in response to an action or event.

The answer, 'AWS RDS' is incorrect as RDS is Amazon's relational database service which helps you launch managed database engines such as MySQL and Oracle.

The answer, 'AWS Snowball' is incorrect as Amazon Snowball is used to migrate large amounts of data from on-premises to Amazon S3 using securely enclosed disks and is an offline data migration and transfer process.

Ref: https://www.youtube.com/watch?v=VD_rF_tIBOY&t=256s

Question 50

Which AWS Elastic Container Service (ECS) types will enable you to focus on the application packaging rather than worry about provisioning, patching, and scaling servers?

A. AWS EC2 Launch Type
B. Fargate
C. AWS Hybrid
D. AWS Elastic Beanstalk

Correct Answer – B

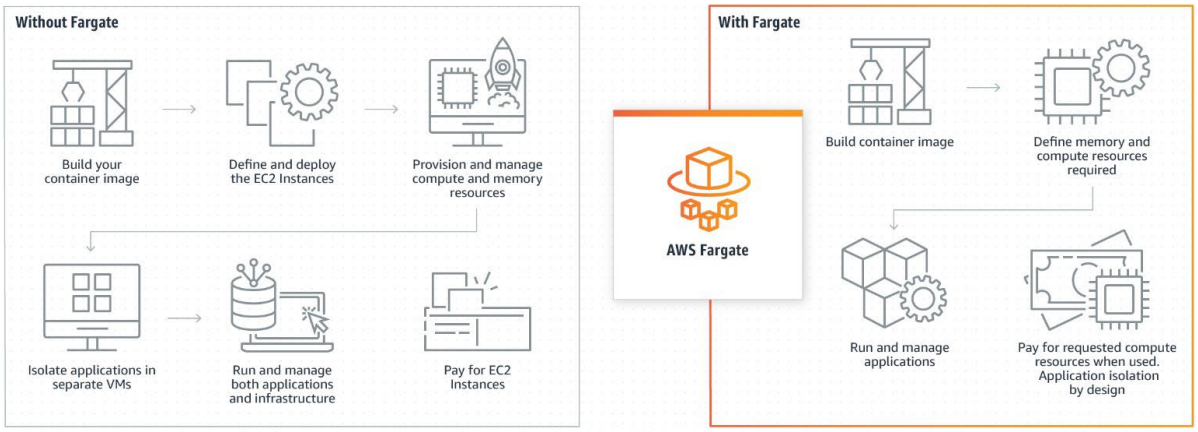
Explanation

With the Fargate launch type, you must package your application in containers, specify the CPU and memory requirements, define networking and IAM policies, and launch the application. You do not need to provision, manage, or patch clusters of EC2 Instances. Fargate lets you specify and pay for resources per application and improves security through application isolation by design.

The answer, 'EC2 Launch Type' is incorrect because, with this ECS type, you do have to manage your cluster of servers. It means you have more granular control over the infrastructure that runs your container applications.

The answer, 'AWS Hybrid' is incorrect as there is no such ECS mode

The answer, 'Elastic Beanstalk' is incorrect as Elastic Beanstalk is a platform solution designed to provide complete environments to support standard application deployment.



Ref: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/AWS_Fargate.html

Question 51

You have a project that will require 120 hours of computing time. The application is stateless and can be interrupted and restarted without adverse effects. Which of the following computing options offers the most cost-effective solution?

A. Spot
B. On-Demand
C. Reserved
D. Spark

Correct Answer – A

Explanation

Spot Instances can help when an application is stateless and unaffected by interruptions.

Question 52

Which AWS service makes it easy to deploy, manage, and scale containerized applications using Kubernetes on AWS

A. Amazon EKS
B. Amazon ECS
C. Amazon EC2
D. Amazon EMR

Correct Answer – A

Explanation

Amazon Elastic Kubernetes Service (Amazon EKS) is a fully managed Kubernetes service. Amazon EKS runs the Kubernetes management infrastructure for you across multiple AWS availability zones to eliminate a single point of failure. Amazon EKS is a certified Kubernetes conformant so you can use existing tooling and plugins from partners and the Kubernetes community. Applications running on any standard Kubernetes environment are fully compatible and can be easily migrated to Amazon EKS

The answer to Amazon ECS is incorrect. Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers and allows you to easily run and scale containerized applications on AWS. Amazon ECS eliminates the need for you to install and operate your own container orchestration software, manage and scale a cluster of virtual machines, or schedule containers on those virtual machines.

The answer to Amazon EC2 is incorrect. Amazon EC2 offers you virtual servers that run on the AWS platform in your own VPC. You can host both Linux and Windows-based servers in the cloud.

The answer to Amazon EMR is incorrect. Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. With EMR you can run Petabyte-scale analysis at less than half of the cost of traditional on-premises solutions and over 3x faster than standard Apache Spark.

Databases on AWS

Question 53

Which is the primary benefit of using an Amazon RDS Database instead of installing a MySQL-compatible database on your EC2 Instance?

A. Amazon takes care of managing the database, including patching and backup.
B. Managing the database, including patching and backup, is handled by the customer.
C. You can install older-style databases like FoxPro with Amazon RDS
D. You can choose which drive and partition to install the RDS database on

Correct Answer – A

Explanation

One of the most significant advantages of using Amazon RDS is that you offload all management functions to AWS. This includes batching and backups as well as ensuring the underlying servers are secured.

By contrast, if you were installing a MySQL relational database on an EC2 Instance, you would need to take care of all management functions as well as ensure that the underlying EC2 Instances were patched with the latest security and system updates.

Ref: https://youtu.be/eMzCI7S1P9M

Question 54

Which AWS Database service is suitable for your company's new Smart IoT product ranges that can be used to manage trillions of events per day and be used to store a time series of events from those devices?

A. AWS RDS
B. AWS DynamoDB
C. AWS Timestream
D. AWS IoTDB2

Correct Answer - C

Explanation

Amazon Timestream is a fast, scalable, fully managed time-series database service for IoT and operational applications that makes it easy to store and analyze trillions of events per day at 1/10th the cost of relational databases.

Amazon DynamoDB is an incorrect answer as this is Amazon's NoSQL solution designed to support modern web and mobile application solutions.

Amazon RDS is an incorrect answer, as it is far more costly when managing such a large volume of daily transactions is inefficient.

The answer, 'AWS IoTDB2' is incorrect as no such service exists.

Ref: https://youtu.be/oTPpIyXoE3k

Question 55

Which of the following Database engines are available on Amazon RDS? (Choose 2 answers)

A. MySQL
B. DB2
C. Microsoft Access
D. Oracle
E. FoxPro

Correct Answer – A & D

Explanation

Amazon RDS offers six different database engines. These are

- MySQL
- Microsoft SQL Server
- Oracle
- PostgreSQL
- MariaDB
- Aurora

Ref: https://aws.amazon.com/rds/

Question 56

You are planning a MySQL database deployment to host all customer's profile data. Customers can update their profiles as and when required. You wish to implement disaster recovery using a managed solution from AWS, such that if the primary database fails, you have a standby database to failover to. How should you configure your RDS database?

A. Configure Multi-AZ
B. Configure Read Replicas
C. Configure EFS Mount Points
D. Configure an EC2 Cluster

Correct Answer – A

Explanation

Multi-AZ offers disaster recovery such that if the primary DB Instance fails, you can start using a standby instance by promoting it as the primary.

Amazon RDS read replicas is an incorrect answer. This feature allows you to create additional read copies of your RDS database to facilitate scaling read queries away from the primary master copy of the database. This eases the burden on the master copy of your database and improves read performance for your applications. In addition, you can have read replicas configured across AWS regions which can help bring data closer to your end users and reduce read query latency.

EFS mount points and EC2 clusters are not required in this scenario as you wish to use a managed solution from AWS for your database requirements.

Question 57

Which Amazon Database platform is most suited for Data Warehousing solutions

A. Amazon DynamoDB
B. Amazon RDS using the MySQL engine.
C. Amazon Redshift
D. Amazon Aurora

Correct – C

Explanation

Amazon Redshift is designed explicitly for Data Warehousing and Business Intelligence (BI) applications. It offers a petabyte-scale data warehouse service that makes it simple and cost-effective to analyze all your data using your existing business intelligence tools. The database uses SQL to analyze structured and semi-structured data across data warehouses.

The answer 'Amazon RDS using the MySQL engine' is incorrect. Amazon RDS is better suited to traditional relational databases for transactional processing of data rather than analytical processing with BI solutions.

The answer 'Amazon DynamoDB' is incorrect. Amazon DynamoDB is a NoSQL (Non-Relational) database service. This service offers a serverless, key-value data store capable of handling more than 10 trillion daily requests and is designed to run internet-scale applications. It provides features like DynamoDB Accelerator (DAX), an in-memory caching engine, and the ability to host global multi-master tables using Global Tables.

The answer Amazon Aurora is incorrect. Amazon Aurora is a relational database service designed for online transactional processing (OLTP), whereas Amazon Redshift is a data warehousing solution designed for online analytical processing (OLAP)

Ref: https://youtu.be/lWwFJV_9PoE

Question 58

As a cloud practitioner, you have been tasked with recommending an appropriate database solution for a web-gaming application requiring key-value data storage and handling more than 10 million daily requests. Which of the following database solution would you recommend?

A. Amazon DynamoDB
B. Amazon RDS
C. Quantum Ledger Database (QLDB)
D. MySQL hosted on EC2.

Correct Answer – A

Explanation

Amazon DynamoDB is AWS's NoSQL database solution that can handle key-value and document data formats. The database is highly scalable and offers single-digit millisecond performance, capable of handling 10 trillion daily requests.

It provides features like DynamoDB Accelerator (DAX), an in-memory caching engine, and the ability to host global multi-master tables using Global Tables.

The answer 'Amazon RDS using the MySQL engine' is incorrect. Amazon RDS is better suited to traditional relational databases for transactional processing of data rather than analytical processing with BI solutions.

The answer 'Quantum Ledger Database (QLDB)' is incorrect. Amazon QLDB is a ledger-style database that offers transparent, immutable, and cryptographically verifiable transaction logs owned by a central trusted authority. This database is ideal for ledger-style solutions often used by banks and similar organizations. QLDB offers an immutable change history, meaning that it cannot be altered or deleted. QLDB offers a transactional log, known as a journal, that tracks each application data change and maintains a complete and verifiable history of changes over time.

The answer 'MySQL hosted on EC2' is incorrect. MySQL is a relational database engine that does not offer key-value or document-style data format storage.

Question 59

You are looking to host a production-grade enterprise relational database solution that offers high-end features such as self-healing storage systems capable of scaling up to 128TB per database instance. Which of the following AWS database solutions fulfils the requirement?

A. Amazon DynamoDB
B. Amazon Aurora
C. Amazon Redshift
D. Amazon Neptune

Correct Answer – B

Explanation

Amazon Aurora is an enterprise-grade relational database service offered as part of the managed AWS RDS solution. Amazon Aurora is a fully managed database service that is five times faster than standard MySQL and three times faster than PostgreSQL databases. It offers up to 15 low-latency Read Replicas, point-in-time recovery, and replicates data across three Availability Zones (AZs).

With regards to database storage, your database volume size automatically grows as your storage needs grow. Amazon Aurora will allocate increments of 10 GB storage up to a maximum of 128TB. Furthermore, to offer higher levels of fault tolerance, each 10GB chunk is replicated six ways, across three Availability Zones (two copies in each of the three Availability Zones).

Amazon Aurora storage also offers self-healing capabilities – the data blocks and disks are continuously scanned for errors and replaced automatically as part of the overall management service.

The answer, 'Amazon DynamoDB' is incorrect as DynamoDB is a **non-relational (NoSQL)** database.

The answer, 'Amazon Redshift' is incorrect. Amazon Redshift is a data warehousing solution and is not self-healing.

The answer, 'Neptune' is incorrect as it is designed for a different use case. Specifically, Amazon Neptune is a graph database solution.

Developer Tools

Question 60

You plan to deploy a web application on AWS that must be updated regularly. You wish to rapidly release new features as and when they are approved and thus require a tool to seamlessly manage your application source code using a private Git repository. Which AWS service can you use to help you fulfil this requirement?

A. AWS CodePipeline
B. Amazon RDS
C. Amazon EFS
D. AWS CodeCommit

Correct answer – D

AWS CodeCommit is a highly secure source control service that enables you to host private Git repositories on AWS. The service makes it easy to collaborate on your application code among your development team and offers all the essential features and functionality of Git. You can use your existing Git-based tools as well.

The service also encrypts your files in transit and at rest and can be configured with user-based access controls using AWS IAM.

The answer 'AWS CodePipeline' is incorrect. AWS CodePipeline is a fully managed continuous delivery service enabling you to automatically release the of code as soon as it's committed to update your application stacks. You can use CodePipeline with external tools like GitHub too.

The answer 'Amazon RDS' is incorrect. Amazon RDS is a managed relational database service on AWS offering six database engines: Amazon Aurora, MySQL, PostgreSQL, Microsoft SQL, Oracle and MariaDB.

The answer 'Amazon EFS' is incorrect. Amazon EFS is file-based storage solution that can be used to build shared file systems for your Linux-based EC2 Instances and on-premises servers.

Ref: https://aws.amazon.com/codecommit/

Question 61

Which AWS development tool allows you to compile source code, runs tests, and produce software packages that are ready to deploy?

A. AWS CodeCommit
B. AWS CodeDeploy
C. AWS CodeBuild
D. AWS CodePipeline

Correct Answer – C

AWS CodeBuild is a software build service that enables you to compile source code, run tests and then deploy your applications. You do not need to provision your own build servers or software, which would add to the overall costs and increase the administrative burden.

AWS CodeBuild integrates with AWS CodeCommit and AWS CodeDeploy to help you efficiently design and full software lifecycle process.

The answer 'AWS CodeCommit' is incorrect. AWS CodeCommit is a managed source control service that can be used to host source code in private and scalable Git repositories.

The answer ‘AWS CodeDeploy’ is incorrect. AWS CodeDeploy is a service that automates code deployments to any instance, including EC2 instances and servers running on-premises.

The answer ‘AWS CodePipeline’ is incorrect. AWS CodePipeline is a fully managed continuous delivery service enabling you to automate the code release as soon as its committed and update your application stacks. You can use CodePipeline with external tools like GitHub too.

Ref: https://aws.amazon.com/codebuild/

Question 62

Which AWS service can you use to automate software deployments to your on-premises servers and facilitate the rapid release of new features as part of your overall DevOps process?

A. AWS CodeDeploy
B. AWS Lambda
C. AWS CloudFormation
D. Amazon Outpost

Correct Answer – A

AWS CodeDeploy is part of a suite of development services offered by AWS that enables the automatic release and deployment of application code to Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers.

The service is fully managed, so you do not need to set up any underlying infrastructure and it allows you to track the status of your application deployments through the AWS Management Console or the AWS CLI.

The answer ‘AWS Lambda’ is incorrect. AWS Lambda is a serverless compute solution that allows you to run functions in response to events that occur in your environment. You can use AWS Lambda to help build event-driven serverless application solutions on AWS

The answer ‘AWS CloudFormation’ is incorrect. AWS CloudFormation is an Infrastructure as Code (IaC) solution offered by AWS which can be used to build templates that describe how a set of underlying infrastructure resources need to be provisioned and deployed. These templates are written in either JSON or YAML open-source declarative languages, that can help automate provisioning and updating your infrastructure in a safe and controlled manner.

The answer Amazon Outpost’ is incorrect. Amazon Outposts comprises physical hardware comprising of a 42U rack that can scale from 1 rack to 96 racks to create pools of compute

and storage capacity. You can deploy Amazon RDS on Outposts to set up, operate, and scale Microsoft SQL Server, MySQL, and PostgreSQL relational databases on-premises.

Ref: https://aws.amazon.com/codedeploy/

Question 63

Which AWS service can you use to automate your application releases' build, test, and deploy phases whenever a code changes?

A. AWS CodePipeline
B. AWS CloudFormation
C. AWS CodeDeploy
D. AWS CodeBuild

Correct Answer – A

AWS CodePipeline is a continuous delivery service that enables you to automate the build, test, and deploy phases of your application releases. AWS CodePipeline can process your application code updates and trigger a pipeline to complete the build, test and release of those updates. The service can also integrate with third-party services such as GitHub or with your own custom plugin.

The answer 'AWS CloudFormation' is incorrect. AWS CloudFormation is an Infrastructure as Code (IaC) solution offered by AWS which can be used to build templates that describe how a set of underlying infrastructure resources need to be provisioned and deployed. These templates are written in either JSON and YAML open-source declarative languages, that can help automate provisioning and updating your infrastructure in a safe and controlled manner.

The answer 'AWS CodeDeploy' is incorrect. AWS CodeDeploy can be used part of a CodePipeline deployment in that it enables the automatic release and deploy application code to Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers.

The answer 'CodeBuild' is incorrect. AWS CodeBuild is a fully managed and scalable software build solution that enables you to compile source code, run tests and then deploy your applications. You do not need to provision your own build servers or software, which would add to the overall costs and increase administrative burden.

Ref: https://aws.amazon.com/codepipeline/

Question 64

Which AWS service can be used to quickly set up and implement a development and continuous delivery environment to help you code, build, test and deploy your application?

A. AWS CodePipeline
B. AWS CodeStar
C. AWS Cloud 9
D. AWS CloudShell

Correct Answer – B

AWS CodeStar is a DevOps toolkit that lets you quickly set up a development and continuous delivery environment. To use CodeStart, you set up a project management dashboard to easily track progress across your entire software development process. It also integrates with an issue-tracking feature powered by Atlassian JIRA Software.

The answer 'AWS CodePipeline' is incorrect. AWS CodePipeline is a continuous delivery service enabling you to automate your application releases' build, test, and deploy phases. AWS CodePipeline can process your application code updates and trigger a pipeline to complete the build, test and release of those updates. The service can also integrate with third-party services such as GitHub or with your own custom plugin.

Although CodePipeline is like CodeStar, the latter is an umbrella tool that helps you manage AWS development tools, offers dashboard services, and incorporates the AWS Code 9 IDE environment.

The answer 'AWS Cloud 9' is incorrect. AWS Cloud 9. AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser. It includes a code editor, debugger, and terminal.

The answer 'AWS CloudShell' is incorrect. AWS CloudShell is a browser-based shell offered by AWS to help interact with AWS services and resources. Rather than use your local computer configured with the AWS CLI tools, you can use CloudShell instead. The service has all necessary tools installed and updated on a pre-configured Amazon Linux 2 environment.

Ref: https://aws.amazon.com/codestar/

Question 65

You have an active, highly mobile development team that helps build client applications. Which AWS service can you use to provide your development team with a cloud-based integrated development environment (IDE) that would allow them to work on projects from your office, home, or anywhere using an internet-connected machine?

A. AWS CodeCommit
B. AWS CodeDeploy
C. AWS CodePipeline
D. AWS Cloud 9

Correct Answer – D

AWS Cloud9 is a cloud-based integrated development environment (IDE) that includes a code editor, debugger, and terminal. Development teams can use AWS Cloud9 IDE, including support for JavaScript, Python, PHP, and more programming languages.

Your development teams can write, run, and debug applications using a browser and thus avoid the need to install or maintain a local IDE. Cloud9 also offers collaboration capabilities which allows your team members can see each other type in real-time, and chat with one another from within the IDE.

The answer 'AWS CodeCommit' is incorrect. AWS CodeCommit is a managed source control service that can be used to host source code in private and scalable Git repositories.

The answer 'AWS CodeDeploy' is incorrect. AWS CodeDeploy is a service that automates code deployments to any instance, including EC2 instances and servers running on-premises.

The answer 'AWS CodePipeline' is incorrect. AWS CodePipeline is a fully managed continuous delivery service enabling you to automatically release code as soon as it is committed to update your application stacks. You can use CodePipeline with external tools like GitHub too.

Ref: https://aws.amazon.com/cloud9/

Question 66

Which AWS Service enables developers to analyze and debug applications, identifying the root cause of performance issues and errors?

A. AWS X-Ray
B. AWS CloudTrail
C. AWS Trusted Advisor
D. Access Analyzer

Correct Answer – A

Explanation

AWS X-Ray helps developers analyze and debug production, and distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors.

The answer, 'AWS CloudTrail' is incorrect. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With

CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

The answer, 'AWS Trusted Advisor' is incorrect. AWS Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices. To help you maximize utilization of Reserved Instances, AWS Trusted Advisor checks your Amazon EC2 computing consumption history and calculates an optimal number of Partial Upfront Reserved Instances. Recommendations are based on the previous calendar month's hour-by-hour usage aggregated across all consolidated billing accounts.

Machine Learning

Question 67

You have been tasked with developing a solution that can analyze customer emails to extract sentiments such as negative reviews or positive feedback. Which AWS services use natural language processing (NLP) to help identify insights and relationships in the text?

A. Amazon Polly
B. Amazon Comprehend
C. Amazon Rekognition
D. Amazon RDS

Correct Answer – B

Explanation - Amazon Comprehend uses machine learning to help understand the text and ascertain the context in which it is written. With natural language processing (NLP), Amazon Comprehend can be used to analyze the language of the text; identify key phrases, places, people, brands, or events and extract data on how positive or negative the text is.

Another subset of this offering is Amazon Comprehend Medical, which can identify medical information, such as medical conditions, medications, dosages, strengths, and frequencies from sources like doctor's notes.

The answer 'Amazon Polly' is incorrect. Amazon Polly synthesizes natural-sounding human speech, so you can convert text to speech and playback using a range of lifelike voices across a broad set of languages.

The answer 'Amazon Rekognition' is incorrect. Amazon Rekognition uses machine learning to analyze images and videos, detect objects, scenes, and faces, extract text, recognize celebrities, and identify inappropriate content.

The answer 'Amazon RDS' is incorrect. Amazon RDS is a managed relational database service for MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server.

Ref: https://aws.amazon.com/comprehend/

Question 68

You are building a blog website hosting hundreds of articles about a vegan diet and offering various vegan recipes. You wish to add a feature that automatically converts the articles to podcasts so that users who find it hard to read and listen to the articles instead. Which AWS service enables you to convert text into lifelike speech, using an Amazon artificial intelligence (AI) service that uses advanced deep learning technologies to synthesize speech that sounds like a human voice?

A. Amazon Rekognition
B. Amazon Polly
C. Amazon Translate
D. Amazon Talk Talk

Correct Answer – B

Explanation

Amazon Polly is a service that turns text into lifelike speech. Polly lets you create applications that talk, enabling you to build entirely new categories of speech-enabled products. Polly is an Amazon artificial intelligence (AI) service that uses advanced deep learning technologies to synthesize speech that sounds like a human voice. Polly includes 47 lifelike voices spread across 24 languages, so you can select the ideal voice and build speech-enabled applications that work in many different countries.

The answer, 'Amazon Rekognition' is incorrect. Amazon Rekognition is a service that makes adding image analysis to your applications easy. With Rekognition, you can detect objects, scenes, and faces in images. You can also search and compare faces.

The answer, 'Amazon Translate' is incorrect. Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation. Neural machine translation is a form of language translation automation that uses deep learning models to deliver more accurate and more natural-sounding translation than traditional statistical and rule-based translation algorithms.

The answer, 'Amazon TalkTalk' is incorrect as there is no such service

Ref: https://youtu.be/jXPN12ReUJg

Question 69

Which AWS Service enables you to develop computer vision applications based on a deep learning model and AI?

A. AWS Snowball
B. AWS DeepLens
C. AWS Video
D. AWS Robo

Correct Answer – B

Explanation

AWS DeepLens is a wireless-enabled video camera and development platform integrated with the AWS Cloud. It lets you use the latest Artificial Intelligence (AI) tools and technology to develop computer vision applications based on a deep learning model.

Question 70

You work for a legal company and your attorneys must record all client conversations. Which AWS service can help you convert speech to text against the vast array of mp3 files stored in your S3 buckets?

A. AWS Transcribe
B. Amazon Polly
C. AWS Digital Convert
D. AWS Translate

Correct Answer – A

Explanation

AWS offers AWS Transcribe, which is a fully managed service. The service can transcribe audio files stored in common formats, like WAV and MP3, with timestamps for every word so that you can easily locate the audio in the source by searching for the text.

The answer, 'AWS Polly', is incorrect. Amazon Polly is a service that turns text into lifelike speech. Polly lets you create applications that talk, enabling you to build entirely new categories of speech-enabled products. Polly is an Amazon artificial intelligence (AI) service that uses advanced deep learning technologies to synthesize speech that sounds like a human voice. Polly includes 47 lifelike voices spread across 24 languages, so you can select the ideal voice and build speech-enabled applications that work in many different countries.

The answer, 'AWS Digital Convert' is incorrect as no such service exists.

The answer, 'AWS Translate' is incorrect. Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation. It uses deep

learning models to deliver more accurate and natural-sounding translations than traditional statistical and rule-based translation algorithms.

Question 71

A pharmaceutical company is conducting extensive research into a new project called "Prevent Future Pandemics" and has sent out a survey form by post to every individual across the country. Which AWS Service offers Artificial Intelligence to "read" the completed forms and extract all data contained with its context intact?

A. AWS Transcribe
B. AWS Textract
C. AWS Forms
D. Amazon CloudWatch

Correct Answer – B

Explanation

Amazon Textract is a fully managed machine learning service that automatically extracts printed text, handwriting, and other data from scanned documents. The service uses artificial intelligence to understand the data relationships in any embedded forms or tables and extracts everything with its context intact.

The answer, 'AWS Transcribe' is incorrect. Amazon Transcribe is an automatic speech recognition (ASR) that enables you to convert speech to text quickly and accurately. The service can be used to transcribe customer service calls, podcasts, and other audio recordings. The service also offers automatic subtitling. An alternative version of the product, Amazon Transcribe Medical can be used to add medical speech-to-text capabilities to clinical documentation applications.

The answer, 'AWS Forms' is incorrect. This is a distractor answer and there is no such service.

The answer, 'AWS CloudWatch' is incorrect. AWS CloudWatch enables you to collect, access, and correlate performance and health metric information of the various AWS resources you deploy. You can then create alarms to alert you of any resource which may be experiencing performance issues and take appropriate action.

Ref: https://youtu.be/5Cs4_e2CJRo

Management and Governance

Question 72

Which AWS Service enables you to centrally manage multiple AWS Accounts with service control policies (SCPs) to determine which services can be used in those individual AWS member Accounts?

A. AWS Organizations
B. AWS System Manager
C. AWS Config
D. AWS CloudTrail

Correct Answer – A

Explanation

Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance.

You can use Service Control Policies (SCPs) to apply permission boundaries on AWS Identity and Access Management (IAM) users and roles. For example, you can apply an SCP that restricts users in accounts in your organization from launching any resources in regions that you do not explicitly allow.

The answer, 'AWS System Manager' is incorrect. While you can use System Manager to manage resources **within an** account, AWS Organization lets you manage multiple AWS Accounts centrally and apply account-wide SCPs that enforce which services can be accessed and configured within an Account.

The answer, 'AWS Config' is incorrect. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. You can think of AWS Config as a centralized configuration management database (CMDB) tool with rules to ensure any service you configure is in alignment with corporate policies that you define.

The answer, 'AWS CloudTrail' is incorrect. With CloudTrail, you can log, continuously monitor and retain account activity related to actions across your AWS infrastructure. 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.

Ref: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html

Ref: https://www.youtube.com/watch?v=Tuaf3AfjKz4&t=15s

Question 73

You have been asked to design an infrastructure solution that can be repeatedly created using scripted templates to create individual sandbox environments for your developers. Some infrastructure components will include the setup and configuration of a VPC, EC2 Instances, S3 buckets etc. Which AWS service enables you to design an infrastructure template that can be deployed to create repeatable infrastructure for your developers to use as a sandbox environment?

A. AWS CloudFormation
B. AWS Systems Manager
C. FSX for Lustre
D. AWS Config

Correct Answer – A

Explanation

AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them orderly and predictable. You can use AWS CloudFormation's sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application. You don't need to figure out the order for provisioning AWS services or the subtleties of making those dependencies work. CloudFormation takes care of this for you. After the AWS resources are deployed, you can modify and update them in a controlled and predictable way, applying version control to your AWS infrastructure the same way you do with your software.

The answer, 'AWS System Manager', is incorrect. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and act on your groups of resources.

The answer, 'AWS Config', is incorrect. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of documented configurations against desired designs.

The answer, 'AWS FSx for Lustre', is incorrect. Amazon FSx for Lustre makes launching and running a high-performance file storage system easy and cost-effective. Use it for workloads where speed matters, such as machine learning, high-performance computing (HPC), video processing, and financial modelling.

Ref: https://youtu.be/Omppm_YUG2g

Question 74

As part of implementing change management, which AWS service can be used to assess, audit, and evaluate change configurations of your AWS resources, enabling you to identify if a change was the cause of an incident?

A. AWS Config
B. AWS CloudWatch
C. AWS Outpost
D. AWS CloudTrail

Correct Answer – A

Explanation

With AWS Config, you can track the relationships among resources and review resource dependencies before making changes. Once a change occurs, you can quickly review the history of the resource's configuration and determine what the resource's configuration looked like at any point in the past. Config provides information to assess how a change to a resource configuration would affect your other resources, minimising the impact of change-related incidents.

The answer, 'AWS CloudTrail' is incorrect. You can use CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.

The answer, 'AWS CloudWatch' is incorrect. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing a unified view of AWS resources, applications, and services that run on AWS and on-premises servers.

The answer, 'AWS Outpost' is incorrect. AWS Outposts is a fully managed service that extends AWS infrastructure, AWS services, APIs, and tools to virtually any data center, co-location space, or on-premises facility for a consistent hybrid experience.

Ref: https://youtu.be/MJDuAvNEv64

Ref: https://aws.amazon.com/config/

Question 75

Which AWS service can help you monitor performance metrics of your EC2 instances such as CPU utilization, and then configure alarms to send out notifications if thresholds are breached?

A. Amazon CloudWatch

B. AWS Config
C. AWS CloudTrail
D. AWS Lambda

Correct Answer – A

Amazon CloudWatch is a fully managed monitoring service in the form of logs, metrics, and events. With Amazon CloudWatch. You can also create custom dashboards to display metrics about your custom applications and resources.

You can also create alarms to monitor metrics and take action such as send out a email notification when those metrics cross a specified threshold. You also trigger other actions automatically when alarms are triggered such as stop your E2 Instances or perform an Auto Scaling action.

Following is a screenshot of Amazon CloudWatch showing the CPU utilization of a webserver:

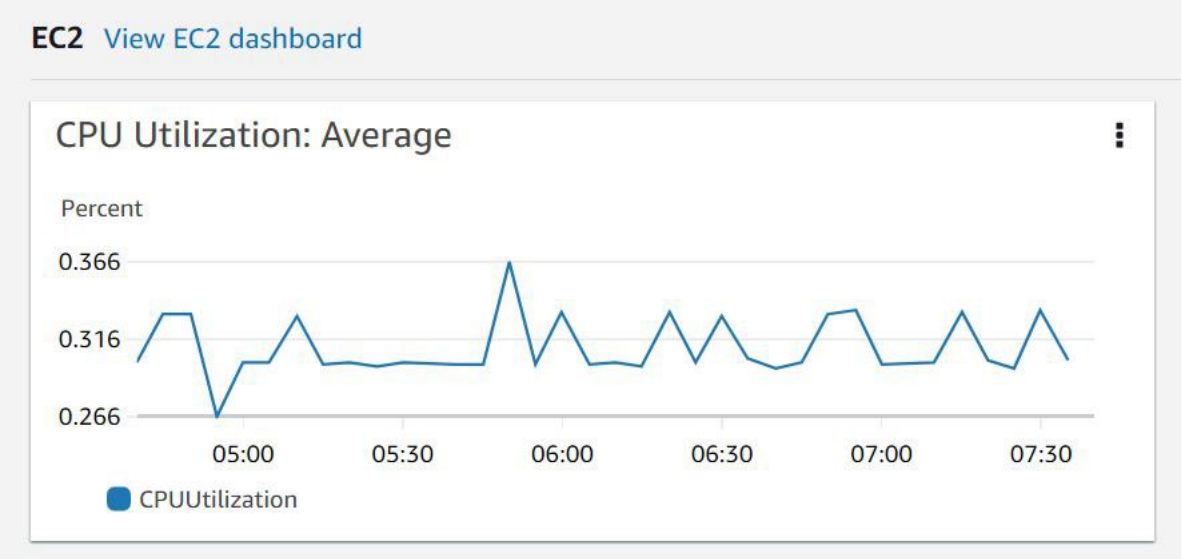


Figure: CPU Utilization for EC2 Instance in Amazon CloudWatch

The 'AWS Config' is incorrect. AWS Config allows you to define configuration settings and rules for any set of resources you wish to create in your AWS account. It does not monitor resource metrics.

The answer 'AWS CloudTrail' is incorrect. AWS CloudTrail is a service that allows you to monitor your account from an operational and risk auditing perspective. AWS CloudTrail can be used to audit all actions you take in your account whether in the web console, CLI or using API calls. However, it is not designed to setup configuration rules to analyze how resources are configured.

The answer 'AWS Lambda' is incorrect. AWS Lambda is a serverless compute service that allows you to trigger compute functions in response of events or at scheduled intervals. With AWS Lambda, you don't have to host or manage any instances.

Question 76

Which Amazon CloudWatch feature enables you to monitor your resources in a single view, even if those resources are spread across different Regions?

A. CloudWatch Dashboards
B. CloudWatch Logs
C. CloudWatch Alarms
D. CloudWatch Events

Correct Answer – A

Amazon CloudWatch offers a feature to help you create custom dashboards. These dashboards can be used to display resource metric information in the form of graphs and other widget that can help you visualize the health of those resources and applications.

Metric information for resources across multiple regions can displayed in a single dashboard allowing to you have a single view for all resources that may be related to each other, for example, for a globally distributed application.

The answer 'CloudWatch logs' is incorrect. CloudWatch logs can be used to centralize the logging information from all of your resources applications, and AWS services. You can then take action on the log data, for example, troubleshoot issues with resources.

The answer 'CloudWatch Alarms' is incorrect. CloudWatch Alarms are a feature that can be used to alert you when specified metric values cross a threshold that you define for a period of time. You can also automate remediation action when alarms are triggered such as initiate an auto scaling launch of an EC2 instance if the CPU utilization of existing instances in a fleet rises above a specific level.

The answer 'CloudWatch Events' is incorrect. CloudWatch Events delivers a near real-time stream of system events that describe changes in AWS resources. You can then match events and route them to one or more target functions or streams. This allows you to trigger an action when an event occurs. You can also schedule an event using rate or cron expressions. Note, CloudWatch Events is currently being superseded by Amazon EventBridge, which offers many more features.

Ref:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html

Question 77

Which AWS service can you use to monitor user activity and API calls across AWS your AWS accounts and help to answer questions like “who did what, where, and when"?

A. AWS CloudWatch
B. AWS CloudTrail
C. AWS Config
D. AWS Trusted Advisor

Correct Answer – B
AWS CloudTrail is an always-on auditing service that can help you record all user activities in your AWS accounts across multiple regions. You can use the CloudTrail service to record two types of events:

- Management events - used to record actions such as creating or deleting resources, such as creating and deleting Amazon S3 buckets.
- Data events record actions within a resource, such as reaching and writing an Amazon S3 object.

AWS CloudTrail is enabled by default when you create an AWS account and records the 90 days of activity in the **Event History**. In addition, you can create a CloudTrail **trail** to archive, analyze, and respond to changes in your AWS resources. To setup a trail, you need to define an Amazon S3 bucket to store your data in. You can create two types of trails:

- A trail that applies to all regions – events are recorded from all regions (and any new regions that come online) and delivered to the CloudTrail event log files in an S3 bucket you specify.
- A trail that applies to one region – events are recorded from one region only. You can create additional trails later.

Here is a screenshot of how CloudTrail records events:

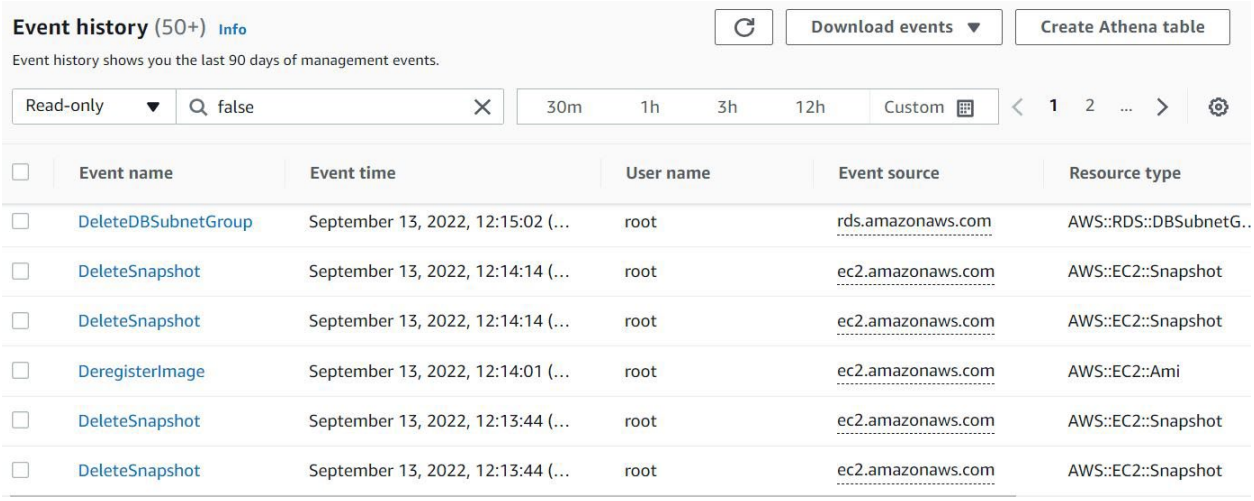


Figure: An example of delete actions performed by the root user of the AWS account.

The answer ‘Amazon CloudWatch’ is incorrect. Amazon CloudWatch records your AWS resources and applications' performance and health metric information. You can then create dashboards and alarms for those metrics.

The ‘AWS Config’ is incorrect. AWS Config allows you to define configuration settings and rules for any resources you wish to create in your AWS account. It does not monitor resource metrics.

The answer ‘AWS Trusted Advisor’ is incorrect. AWS Trusted Advisor performs a series of checks against the resources and configurations you have implemented in your AWS account. It uses this information to provide recommendations that help you follow AWS best practices to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas.

Question 78

Which AWS service can analyze your resources, usage, configuration and spending and help you reduce costs by suggesting actionable recommendations?

A. AWS Config
B. AWS CloudTrai
C. Amazon Macie
D. AWS Trusted Advisor

Correct Answer – D

AWS Trusted Advisor is a web service that can analyse how your resources are used and configured. The service uses a traffic light system to help you quickly identify issues and potential security threats. In addition, the service can evaluate the total spend on your resources and identify if there are any cost savings you can benefit from through its cost optimization category.

AWS Trusted advisor is a free service for AWS accounts that have an active Business or Enterprise support plan. For the Basic and Developer plans, you only get limited recommendations.

The ‘AWS Config’ is incorrect. AWS Config allows you to define configuration settings and rules for any set of resources you wish to create in your AWS account. It does not monitor resource metrics.

The answer ‘AWS CloudTrail’ is incorrect. AWS CloudTrail is a service that allows you to monitor your account from an operational and risk auditing perspective. AWS CloudTrail can be used to audit all actions you take in your account whether in the web console, CLI or

using API calls. However, it is not designed to setup configuration rules to analyze how resources are configured.

The answer 'Amazon Macie' is incorrect. Amazon Macie is data security and data privacy service that uses machine learning (ML) and pattern matching to discover and protect your sensitive data such as Personal Identifiable Information (PII).

Ref: https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

Video Ref: https://youtu.be/i0IkKN9NoPk

Question 79

You plan to deploy several Windows-based EC2 instances that will require monthly software updates and patching. Which AWS service can be used to deploy your regular security patches MOST efficiently?

A. Use AWS System Manager to automatically deploy security patches at regular monthly intervals.
B. Use Amazon CloudWatch to check which software patches have been deployed and install ones that are outdated.
C. Connect to each EC2 Instance and perform the installation of new security updates.
D. Use the EC2 management console and enable the automatic patch updates feature

Correct Answer – A

AWS System Manager offers a feature called Patch Manager. This service can help automate the deployment of both operating system and application patches and updates. With Patch Manager, you can also install service packs on windows instances as well as perform version upgrades on Linux ones.

Patch Manager can also be used to deploy security updates and patches to your on-premises virtual machines (VMs). The service can be used to scan your fleet of VMs for missing patches and generate reports.

Patch Manager now also offers a new feature called *patch policies* which offer a more centralized approach to diplopy patches and offers capabilities such as single setup, multi-account/multi-region support and the ability to specify different schedules for scanning and installing patches.

Note: On Windows servers, application support is limited to only those that are released by Microsoft.

The answer ‘Use Amazon CloudWatch to check which software patches have been deployed and install ones that are outdated’ is incorrect. Amazon CloudWatch is designed to monitor performance metrics and not specifically to deploy patch updates.

The answer ‘Connect to each EC2 Instance and perform the installation of new security updates’ is incorrect. This is a very manual process and more appropriate reliable services such as System Manager can be used for patch deployments.

The answer ‘Use the EC2 management console and enable automatic patch updates feature’ is incorrect as no such feature exists.

Question 80

Which of the following options will provide an easy and straightforward approach to remotely running ad-hoc shell scripts across multiple Linux EC2 instances without logging in to those instances manually?

A. Configure AWS Systems Manager to manage your instances in a fleet and deploy shell scripts using the ‘Run command’ feature.
B. Configure Amazon CloudWatch to run shell scripts at scheduled intervals.
C. Use Amazon Config to run shell scripts.
D. Configure CloudTrail with your shell scripts to be pushed out to your fleet of EC2 Instance

Correct Answer – A

AWS System Manager enables you to manage your infrastructure. A key feature is the ability to use the ‘Run command’ service to automate common administrative tasks such as remotely executing shell scripts or PowerShell commands, installing applications, and making changes to operating system.

The answer ‘Configure Amazon CloudWatch to run shell scripts at scheduled intervals’ is incorrect. While you can use CloudWatch to run events on your EC2 instances, the question refers to the ability to execute ad-hoc shell scripts which can be easily achieved using the ‘Run command' feature of System Manager

The answer ‘Use Amazon Config to issue shell scripts’ is incorrect. Amazon Config provides a detailed breakdown of the resources you have deployed on AWS and how they relate to each other. With Amazon Config, you create rules that automatically check resource configuration and ensure they are compliant by corporate policy and regulatory requirements.

The answer ‘Configure CloudTrail with your shell scripts to be pushed out to your fleet of EC2 Instance’ is incorrect. Amazon CloudTrail is an auditing service that records all API calls for your account. With CloudTrail you can get a history of all API calls made, who made them, the source IP address etc.

Question 81

To ensure application layer security, you must avoid hard-coding database connection strings, including usernames and passwords in your application code. Which of the following is services can you use to easily store and retrieve critical information by your application in a secure manner?

A. AWS System Manager Parameter Store
B. AWS System Manager Patch Manager
C. Amazon Macie
D. AWS Config

Correct Answer – A

AWS System Manager's *Parameter Store* can store sensitive information such as usernames, passwords, and database connection strings securely either in plain text or encrypted.

Applications that require access to such sensitive information can make timely calls to System Manager Parameter Store, improving the overall security posture by separating data from application code. Data can be stored in hierarchies and include multiple versions. The service also offers auditing and control at granular levels. Encryption is offered through integration with AWS Key Management Service (KMS) allowing to ensure that only authorized entities can access and decrypt the data.

The answer 'AWS System Manager Patch Manager' is incorrect. AWS System Manager Patch Manager is a service designed to help you automate patch deployment to your Linux and Windows EC2 instances.

The answer 'Amazon Macie' is incorrect. Amazon Macie uses machine learning to help discover and protect sensitive data such as Personally Identifiable Information (PII) hosted in Amazon S3 buckets.

The answer 'AWS Config' is incorrect. Amazon Config provides a detailed breakdown of the resources you have deployed on AWS and how they relate to each other. With Amazon Config, you create rules that automatically check resource configuration and ensure they are compliant in accordance with corporate policy and regulatory requirements.

Question 82

Which AWS Service enables you to centrally manage multiple AWS Accounts with service control policies (SCPs) to determine which services can be used in those individual AWS member Accounts?

A. AWS Organization
B. AWS Systems Manager

C. AWS CloudTrail
D. AWS Config

Correct Answer – A

Explanation

Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance.

You can use Service Control Policies (SCPs) to apply permission boundaries on AWS Identity and Access Management (IAM) users and roles. For example, you can apply an SCP that restricts users in accounts in your organization from launching any resources in regions that you do not explicitly allow.

The answer, 'AWS System Manager' is incorrect. While you can use System Manager to manage resources **within an** account, AWS Organization lets you manage multiple AWS Accounts centrally and apply account-wide SCPs that enforce which services can be accessed and configured within an Account.

The answer, 'AWS Config' is incorrect. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. You can think of AWS Config as a centralized configuration management database (CMDB) tool with rules to ensure any service you configure is in alignment with corporate policies that you define.

The answer, 'AWS CloudTrail' is incorrect. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides the event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services.

Ref: https://youtu.be/T4NK8fv8YdI

Question 83

Which of the following requires custom CloudWatch metrics to monitor?

A. Disk
B. CPU
C. Memory
D. Network

Correct Answer – C

Explanation

Amazon CloudWatch works on the Hypervisor level and does not monitor memory utilization. CloudWatch will monitor CPU, Disk, Networking and Status

Migration and Transfer Services

Question 84

Your company is planning on migrating to the AWS Cloud. As part of a one-time data migration effort migration, you need to transfer over 500TB of data to Amazon S3 is a couple of weeks. Which is the most cost-effective strategy to move this amount of data to the cloud?

A. Use the Amazon Direct Connect Service
B. Use the Amazon Snowball Service
C. Use the Amazon VPN to set up a site-to-site connection between your on-premises data centre and your Amazon VPC.
D. Setup VPC Peering

Correct Answer – B

Explanation

Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers, including high network costs, long transfer times, and security concerns.

The Amazon Snowball Service comes in the following formats:

· Amazon Snowball – Standard Device with a secure enclosure unit that can be used to transfer data into and out of Amazon S3

· Amazon Snowball Edge - Snowball Edge Storage Optimized provides both block storage, Amazon S3-compatible object storage, and 24 vCPUs. It is well suited for local storage and large-scale data transfer.

o Snowball Edge Compute Optimized provides 52 vCPUs, block and object storage, and an optional GPU for use cases such as advanced machine learning and full-motion video analysis in disconnected environments.

The answer ‘Amazon Direct Connect’ is incorrect. while it will enable you to gain high-speed connectivity between your on-premises datacentre and the AWS cloud, it is not the most cost-effective strategy for a one-time data migration task.

The answer ‘Amazon VPN for a site-to-site connection supports because the bandwidth limitations would not enable the transfer for 500TB of data in very short space of time.

The answer ‘VPC Peering’ is incorrect because VPC Peering is designed to connect multiple VPCs to each other over AWS private links and is not related to the question.

Ref: https://youtu.be/9uc2DSZ1wL8

Networking and Content Delivery

Question 85

Which AWS Service is used to ensure that only specific traffic on specific ports is allowed inbound to your EC2 Instances and acts as a firewall at the Instance Level?

A. Network Access Control Lists (NACLs)
B. Security Groups
C. IAM Groups
D. EC2 Policies

Correct Answer – B

Explanation

A *security group* acts as a virtual firewall to control inbound and outbound traffic for your instance. When you launch an Instance in a VPC, you can assign up to five security groups to the Instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups. If you do not specify a group at launch time, the instance is automatically assigned to the default security group for the VPC.

The answer "Network Access Control List" is incorrect because they act as firewalls at the Subnet Level rather than the individual instance level.

The answer "IAM Groups" is incorrect as IAM Groups are used to contain and assign permissions to groups of IAM Users. These do not provide any firewall protection to EC2 Instances.

The answer "EC2 Policy" is incorrect as there is no such termed service.

Question 86

Which AWS Service enables you to purchase and register new domain names that can be used to publish your website on the Internet?

A. Route53
B. VPC
C. RDS

D. Elastic Beanstalk

Correct Answer – A

Explanation

Amazon Route53 offers Domain Name Registration. You can purchase and manage domain names such as example.com and Amazon Route53 will automatically configure DNS settings for your domains.

The answer, 'Amazon VPC', is incorrect. Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including a selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

The answer, 'Amazon RDS', is incorrect. Amazon RDS is a managed relational database service which offers six database engines - MySQL, Microsoft SQL, PostgreSQL, Aurora, Oracle and MariaDB

The answer 'Amazon Elastic Beanstalk', is incorrect. 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.

Ref: https://youtu.be/RGWgfhZByAI

Question 87

Which AWS Service enables you to distribute your digital assets such that it is cached locally to users who attempt to access this content for a time to live, and thus helps to reduce network latency?

A. AWS CloudFront
B. AWS CloudWatch
C. AWS CloudTrail
D. AWS CloudScape

Correct Answer – A

Explanation

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

The answer, ‘AWS Cloudtrail’, is incorrect. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

The answer, ‘AWS CloudWatch’, is incorrect. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

The answer, ‘AWS CloudScape’, is incorrect as no such service exists.

Ref: https://youtu.be/AT-nHW3_SVI

Question 88

Which AWS Service enables developers to create, publish, maintain, monitor, and secure APIs for serverless applications that need to access data, business logic, or functionality from your backend services?

A. API Gateway
B. EC2
C. Lambda
D. Route53

Correct Answer – A

Explanation

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs are the "front door" for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

The answer, ‘Lambda Functions’, is incorrect. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

The answer, ‘EC2 Instances’, is incorrect. Amazon EC2 presents a virtual computing environment, allowing you to use web service interfaces to launch instances with various operating systems, load them with your custom application environment, manage your network’s access permissions, and run your image using as many or few Instances as you desire.

The answer, ‘Route53’, is incorrect. Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect. Amazon Route 53 is fully compliant with IPv6 as well.

Ref: https://aws.amazon.com/api-gateway/

Question 89

Which AWS Service enables you to connect your private datacenter to your Amazon VPC with up to 10Gbps network connectivity?

A. Snowball
B. Direct Connect
C. Virtual Private Network (VPN)
D. Virtual Satellite Network (VSN)

Correct Answer – B

Explanation

AWS Direct Connect provides 1 Gbps and 10 Gbps connections, and you can easily provision multiple connections if you need more capacity. You can also use AWS Direct Connect instead of establishing a VPN connection over the Internet to your Amazon VPC, avoiding the need to utilize VPN hardware that frequently can’t support data transfer rates above 4 Gbps.

Question 90

Which service provides you with static IP addresses that serve as a fixed entry point to your applications, thereby ensuring that you don’t need to make any client-facing changes or update DNS records as you modify or replace endpoints such as Application Load Balancers to connect to your application?

A. AWS Global Accelerator
B. AWS NACL
C. AWS Elastic IPs
D. AWS VPN

Correct Answer – A

Explanation

AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers, or Amazon EC2 instances.

The answer, 'AWS NACL', is incorrect. AWS NACLs are VPC firewalls that protect subnets in your VPC where you define what types of IP traffic can be allowed into the subnet

The answer, 'AWS Elastic IPs', is incorrect. Elastic IPs are designed to provide static IP Address to individual EC2 Instances and are regionally specific. So if you are changing your load balancers or even EC2 Instances across regions, this will not provide global static IP Addressing for you.

The answer, 'AWS VPN', is incorrect. AWS VPN enables you to connect your on-premises networks to your VPC in the cloud.

Reg: https://youtu.be/GAxrPQ3ycsQ

Question 91

Your organization hosts multiple AWS Accounts with multiple VPCs. You would like to connect these VPCs and centrally manage connectivity policies. Which AWS service enables you to connect multiple VPCs configured as a hub that controls traffic routed among all the connected networks which act like spokes?

A. AWS Transit Gateway
B. AWS Global Accelerator
C. AWS VPC Peering
D. AWS Virtual Private Gateway

Correct Answer – A

Explanation

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. This allows you to connect your on-premises network and all your VPCs in a hub and spoke configuration, which significantly simplifies management and reduces operational costs because each network only has to connect to the Transit Gateway and not to every other network.

The answer, 'AWS Global Accelerator', is incorrect. AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers, or Amazon EC2 instances.

The answer, 'AWS VPC Peering', is incorrect. While VPC Peering allows you to connect two VPCs, It goes not enable you to manage multiple VPCs connections centrally. You could configure all your VPCs with individual peering connections, but this becomes very difficult to manage.

The answer, 'AWS Virtual Private Gateway', is incorrect. AWS Virtual Private Gateway is a component of your Site-to-Site VPN connection that must be configured to build a VPC tunnel with your on-premise network.

Ref: https://aws.amazon.com/transit-gateway/

Question 92

NACLs traffic rules and restrictions are applied to:

A. EC2 Instances
B. Subnets
C. VPCs
D. Regions

Correct Answer – B

Explanation

Network Access Control Lists (NACLs) are stateless firewalls that are applied at the Subnet Level. Security Groups are applied at the Instance level. You do not have any AWS firewall service at the VPC level itself or at regional level.

Question 93

You are building a multi-tier architecture with web servers placed in the public subnet and application servers in the private subnet of your VPC. You must deploy Elastic Load Balancers to distribute traffic to the web server and application server farms. Which type of load balancer would you choose to distribute traffic to your application servers?

A. Internet-facing
B. Internal load balancers
C. Dynamic load balancers
D. Static load balancers

Correct Answer – B

Explanation - When creating a load balancer, you must choose whether to make it an internal or internet-facing load balancer. In a multi-tier architecture described above, you would deploy an internal load balancer to distribute traffic from the webservers to the application servers. The nodes of an internal load balancer have only private IP addresses. The DNS name of an internal load balancer is publicly resolvable to the private IP addresses of the nodes. Therefore, internal load balancers can only route requests from clients with access to the VPC for the load balancer.

The answer “Internet-facing” is incorrect as this configuration is used to support traffic to the web-servers from users on the Internet.

The answers “Dynamic load balancers” and “Static load balancers” are incorrect as no such service exists.

Ref: https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html#load-balancer-scheme

Storage

Question 94

Which of the following is true regarding the Amazon Simple Storage Service (Amazon S3)? (Select 2 answers)

A. Amazon S3 is Object-Based Storage
B. Amazon S3 is Block-Based Storage
C. You can install non-compatible RDS database engines not available on Amazon RDS
D. Amazon S3 Standard Storage Class offers 99.999999999 Durability
E. Amazon S3 can be configured as shared mount volumes for Linux based EC2 Instances

Correct Answers – A & D

Explanation

Amazon S3 is object-based storage. Object storage takes each piece of data and designates it as an object. Data is kept in separate storehouses versus files in folders and is bundled with associated metadata and a unique identifier to form a storage pool. Also, Amazon S3 offers varying levels of durability and data availability depending on the storage class used to store data.

Block-Based Storage is an incorrect answer. Block-based storage can be treated like a normal disk. You could format it with a filesystem, store files on it, combine multiple devices into a RAID array, or configure a database to write directly to the block device.

Amazon S3 is an Object Storage solution that does not offer any of the features available on block storage, so you cannot install a database or any other application on it. Furthermore, you cannot mount volumes for Linux based EC2 Instances. For this, you need a file system solution such as Amazon Elastic File System (EFS)

Question 95

Which AWS service is more cost-effective for hosting static website content for an upcoming product launch?

A. Amazon EC2
B. Amazon S3
C. Amazon EFS
D. Express Route

Correct Answer – B

Explanation

Amazon S3 Buckets can be configured to host static websites that comprise of static HTML content, assets like images, video, and documents as well as client-side scripts that run on client browsers. Due to the scalability nature of Amazon S3, hosting static websites which may have unpredictable traffic is a much more cost-effective strategy than hosting the same website on a fleet of EC2 Instances that may need to expand to many servers rapidly based on traffic flow.

Typical use cases include product launches that need not have server-side scripting but where you anticipate traffic increasing rapidly as the launch date approaches.

Amazon EFS is an incorrect answer as it does not meet the basic requirement of this question, which is to be highly cost-effective to host static websites. Furthermore, Amazon EFS is a shared filesystem that multiple Linux based EC2 instances can connect to. While you can store website content on an EFS volume, It would be more appropriate to host dynamic websites instead.

Amazon EC2 is an incorrect answer because although you can host static websites on it, it would be more cost-effective to use Amazon S3 for this use case instead.

Express Route is an incorrect answer as it is not an AWS service. Express Route is a Microsoft Networking solution to connect your on-premise network to the Azure Cloud.

Ref: https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html

Question 96

Which Amazon S3 service can you use to automatically migrate data from one storage class to another after a set number of days to reduce your costs, especially where frequent instant access may not be required to the entire dataset?

A. Versioning
B. Lifecycle Management
C. Storage Transition
D. S3 Migration

Correct Answer – B

Explanation

You can use Lifecycle Management to automatically move objects from one storage class to another for better management of costs. Two types of actions can be performed on your S3 Objects:

· Transition Actions – Defines when to move an object from one class to another. For example, you know that after 90 days, some files will be rarely accessed and so you can move them to a cheaper storage class.

· Expiration Actions – Define when an object is to be expired, which deletes the object from S3. For example, you do not need to keep certain documents after 7 Years, so you can automatically delete these after the retention period to save on costs.

Ref: https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html

Question 97

Which feature of the Amazon S3 platform enables you to upload content to a centralized bucket from across any location, such that the data is uploaded via AWS Edge Locations, ensuring faster transfer speeds, and avoiding public Internet congestion?

A. Amazon S3 Transfer Acceleration
B. Amazon S3 Storage Gateway
C. Amazon Snowball
D. Availability Zones

Correct Answer – A

Explanation

Amazon S3 Transfer Acceleration (S3TA) improves transfer performance by routing traffic through Amazon CloudFront's globally distributed Edge Locations and over AWS backbone networks and by using network protocol optimizations.

The answer, 'Amazon S3 Storage Gateway,' is incorrect. AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to the Amazon S3 platform enabling you to transfer data to and from the S3 service.

The answer, 'Amazon Snowball,' is incorrect. Amazon Snowball is a migration service enabling you to transfer large amounts of data using offline storage devices and bypass Internet congestion issues.

The answer, 'Availability Zones,' is incorrect. An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region

Ref: https://youtu.be/J2CVnmUWSi4

Question 98

Which S3 storage class would you recommend for hosting data that is quickly accessible but infrequently accessed and can be re-created if required hence offering even cheaper storage costs?

A. S3 Standard
B. S3 Standard Infrequent Access (IA)
C. S3 One-Zone IA
D. Glacier

Correct Answer – C

Explanation

S3 One Zone-IA is intended for use cases with infrequently accessed data that is re-creatable, such as storing secondary backup copies of on-premises data or for storage that is already replicated in another AWS Region for compliance or disaster recovery purposes. With S3 One Zone-IA, customers can now store infrequently accessed data within a single Availability Zone at 20% lower cost than S3 Standard-IA.

Ref: https://aws.amazon.com/s3/storage-classes/

Question 99

Which AWS S3 service feature can be used to help prevent accidental deletion of objects?

A. Versioning
B. Lifecycle Management
C. Prevent Delete Option
D. Shadow Copy Service

Correct Answer – A

Explanation

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. When you enable versioning for a bucket, if Amazon S3 receives multiple write requests for the same object simultaneously, it stores all of the objects.

Ref: https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html

Question 100

Which AWS S3 Glacier retrieval option will enable you to restore a small subset of data (<250MB) within 5 minutes for a critically urgent requirement?

A. Standard Retrieval Option
B. Urgent Retrieval Option
C. Expedited Retrieval Option
D. Bulk Retrieval Option

Correct Answer – C

Explanation

Expedited Retrieval Option enables you to urgently access a subset of your data held in a Glacier archive, where such data can be available to download within 1 to 5 minutes. You can further procure Provisioned Capacity to ensure the retrieval capacity is available for expedited requests.

The answer, 'Urgent Retrieval Option' is incorrect as no such option exists.

The answer, 'Standard Retrieval Option' is incorrect as, under this option, retrieval requests usually take between 3 to 5 hours to complete.

The answer. 'Bulk Retrieval Option' is incorrect as under this option, retrieval requests will take within 5 to 12 hours to complete.

If cost is an issue and there is no urgency for your request, you can also consider hosting your data in Amazon Glacier Deep Archive. This storage class offers the lowest cost for storage, but retrieval requests can take between 12 to 48 hours before being able to receive the first byte.

Ref: https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html

Ref: https://youtu.be/EKaJENJqD8E

Question 101

You wish to configure a bucket that will enforce a policy enabling anonymous access to its content if they connect to the data from the Corporate and branch offices as part of your security strategy. Which S3 configuration feature will enable you to define the IP Ranges from where you will allow access to the data?

A. Security Groups
B. Bucket Policy
C. NTFS Permissions
D. Network Access Control Lists (NACLs)

Correct Answer – B

Explanation

S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to. Bucket Policies enable you to also define conditional statements to restrict access based on location, for example. Also, note that S3 supports bucket policies of up 20 kb.

Security Groups is an incorrect answer because these protect EC2 Instances by allowing you to only allow traffic inbound/outbound on specific ports.

NTFS Permissions is an incorrect answer. NTFS (NT File System) permissions are available to drives formatted with NTFS. The advantage of NTFS permissions is that they affect local and network users, and they are based on the permission granted to each user at the Windows logon, regardless of where the user is connecting.

Network Access Control Lists (NACLs) is an incorrect answer. NACL is a VPC Firewall security service that enables you to configure which inbound and outbound ports you can open at a subnet level,

Ref: https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s3-resources/

Question 102

You have a fleet of on-premises servers that require access to a centrally managed cloud storage service. The application running on your servers need to be able to store and retrieve files as durable objects on Amazon S3 over standard NFS based access with local caching. Which AWS service can help you deliver a solution to meet the above required?

A. AWS Storage Gateway
B. AWS Snowball
C. Amazon Redshift
D. EBS Volumes

Correct Answer – A

Explanation

AWS Storage Gateway's file gateway enables you to connect to the cloud to store application data files as durable objects on Amazon S3 cloud storage. The File gateway services offer SMB or NFS-based access to data in Amazon S3 with local caching. It can be used for on-premises applications and for Amazon EC2-resident applications that need file storage in S3 for object-based workloads.

The answer, 'AWS Snowball' is incorrect because it will not offer standard ongoing access over NFS mount points, which the Storage Gateway offers. Amazon Snowball is an offline data transfer/migration service that uses physical disks secured in enclosure units to transport large volumes of data between on-premises and the AWS cloud.

The answer, 'Amazon Redshift' is incorrect as it is a Data Warehousing solution rather than a file management service.

The answer, 'EBS Volumes' is incorrect as it is a virtual block storage solution that is attached to EC2 instances in the cloud, much like attaching a physical disk to your physical servers on-premises.

Ref: https://youtu.be/tP5edaxBEEI

Support Plans

Question 103

Which AWS support plans are suitable if you require telephone technical support? (Choose two Answers)

A. Basic
B. Developer
C. Business
D. Enterprise
E. Global

Correct Answer – C & D

Explanation

AWS Support offers a range of plans that provide access to tools and expertise that support your AWS solutions' success and operational health. All support plans provide 24/7 access to customer service, AWS documentation, whitepapers, and support forums. For technical support and more resources to plan, deploy, and improve your AWS environment, you can choose a support plan that best aligns with your AWS use case. Telephonic technical support plans are available on the Business and Enterprise plans.

Ref: https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html

Question 104

Which Amazon S3 Glacier storage class would be the most cost-effective for archiving data, where extended retrieval times of more than 12 hours would be acceptable?

A. Amazon S3 Glacier Instant Retrieval storage class
B. Amazon S3 Glacier Flexible Retrieval storage class
C. Amazon S3 Glacier Deep Archive storage class
D. Amazon S3 One-Zone IA storage class

Correct Answer – C

Amazon S3 Glacier Deep Archive storage class is designed to offer 75% lower cost (than S3 Glacier Flexible Retrieval. This storage class is ideal for archive data, which needs to be stored for the longer term, accessed less than once per year, and retrieved asynchronously.

The answer, 'Amazon S3 Glacier Flexible Retrieval storage class', is incorrect. This storage class is designed for archiving data that does not require immediate but needs to be flexible in that retrieval of large data sets should not incur additional costs. This storage is best for backup of disaster recovery use cases. This storage class offers a discount of up to 10% cheaper than Amazon S3 Instant Retrieval.

The answer 'Amazon S3 Glacier Instant Retrieval storage class', is incorrect. This storage class offers a discount of up to 68% lower costs than the Standard-Infrequent Access storage class. However, it is not the cheapest and is designed for data that needs to be accessed once per quarter and requires millisecond retrieval.

The answer, 'Amazon S3 One-Zone IA storage class', is incorrect. This storage class is a standard storage class that enables end users to access data immediately and more expensive that some of the Glacier storage classes. In addition, data is only stored in a single availability zone; thus, it does not offer the levels of availability that the other classes offer. The question does not specifically state that this lower level of availability is acceptable and so this answer is incorrect.

Question 105

Which AWS service offers the lowest-cost storage solution for retaining database backups generated by your custom database solution hosted on an EC2 instance?

A. Amazon S3 One-Zone IA
B. Amazon EBS
C. Amazon Fsx for Windows File Share
D. Amazon S3 Glacier

Correct Answer D

Amazon S3 Glacier is a storage class that is designed for archival storage and long-term backup solution. The service provides a cost-effective solution for storing data that spans months, years, or even decades. The service offers 99.999999999% of durability and so your data is highly secure.

Amazon S3 Glacier offers different retrieval options ideal for a vast number of use cases. These options are:

- **S3 Glacier Instant Retrieval** – This is ideal for data that is rarely accessed but requires milliseconds retrieval. The data storage costs are lower than that of the Standard-IA storage class, but only if data is accessed rarely. This is because the cost of the data access is higher than that of the Standard-IA storage class.
- **S3 Glacier Flexible Retrieval** – This is ideal for data where you may require flexible retrieval timescales depending on the amount of data and use case. For example, you can use the **expedited retrieval option** to access your data within 1 to 5 minutes. This retrieval option can also be used for free **bulk retrievals** in up to 5-12 hours. Note that the minimum storage duration of 90 days.
- **S3 Glacier Deep Archive** – This is ideal for data that rarely need to be accessed and offers the lowest option when compared to the other classes. This storage class has a minimum storage duration period of 180 days and a default retrieval time of 12 hours. You can further reduce the costs by using the bulk retrieval option which increases the retrieval time to 48 hours.

The answer 'Amazon EBS' is incorrect. While you can store database backups on an EBS volume, it is not the most cost-effective solution for archiving data. Amazon EBS offers a block storage solution, that allows you to create block volumes which can be attached to your EC2 instances. These volumes can host the operating systems for your EC2 instances, and you can install applications on them.

The answer 'Amazon FSx for Windows File Share' is incorrect. This solution is designed to help you set up a file system storage solution for your Microsoft Windows-based EC2 instances. Here again, you could store database backups on the filesystem, but it is not the most cost-effective.

The answer 'Amazon S3 One-Zone IA' is incorrect. This storage class is not ideal for hosting backup copies of your database unless they are secondary copies. This is because data

resides in a single availability zone. Furthermore, the storage class is more expensive than some Glacier options.

Ref: https://youtu.be/gMzVi7Z8zBo

Miscellaneous

Question 106

Which policy governs your use of the services offered by Amazon Web Services?

A. IAM Policy
B. Password Policy
C. Bucket Policy
D. Acceptable Usage Policy (AuP)

Correct Answer – D

The AWS Acceptable Usage Policy (AuP) governs your use of the services offered by Amazon Web Services and its affiliates. The policy defines several prohibitive use cases (such as for any illegal or fraudulent activity) which you must adhere to as a customer.

The answer, 'IAM Policy' is incorrect. IAM policies are identity-based policies that you define what a *principal* can or cannot do in your AWS account.

The answer, 'Bucket Policy' is incorrect. Bucket policies are resource-based policies that you can use to grant access permissions to your Amazon S3 buckets and the objects contained within those buckets.

The answer, 'Password Policy' is incorrect. IAM password policies enable you to set a custom password policy on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords.

Question 107

Which of the following AWS Services is a better option to securely grant necessary permissions to a web application running on an EC2 Instance that needs access to digital assets hosted on an S3 Bucket?

A. Access keys
B. IAM Roles
C. IAM Group

D. Security Group

Correct Answer – B

Explanation

An IAM role is an IAM entity that defines a set of permissions for making AWS service requests. IAM roles are not associated with a specific user or group. Instead, trusted entities, such as IAM users, applications, or AWS services, such as EC2, assume roles.

The answer "Access Keys" is incorrect because it is not a better option. You can use Access Keys to grant an application permission to access other AWS Services. However, Access Keys used in this manner carry a security risk if exposed and require management overhead with regard to ensuring key rotation regularly.

The answer "IAM Groups" is incorrect because IAM Groups are containers that can host IAM Users. You can then assign permissions to the Group. However, applications cannot be members of the group.

The answer "Security Group" is incorrect because Security Groups are firewalls you attach to EC2 instances to enable inbound and outbound traffic on specific ports. Security Groups cannot be used to provide any access permissions required for the above use case.

Question 108

Which AWS Service ensures that only specific traffic on specific ports is allowed inbound to your EC2 Instances and acts as a firewall at the Instance Level?

A. Network Access Control List
B. Security Groups
C. IAM Groups
D. EC2 Policy

Correct Answer – B

Explanation

A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups. If you do not specify a group at launch time, the instance is automatically assigned to the default security group for the VPC.

The answer "Network Access Control List" is incorrect because they act as firewalls at the Subnet Level rather than individual instance level.

The answer “IAM Groups” is incorrect as IAM Groups are used to contain and assign permissions to groups of IAM Users. These do not provide any firewall protection to EC2 Instances.

The answer “EC2 Policy” is incorrect as there is no such termed service.

Question 109

You are planning on developing a website in multiple languages such that you have one fleet of EC2 Instances serving the English version of your site and another serving the Spanish version of your site. For each language version, you will be configuring URLs with different paths such that the English version of your site will contain /en/ in the path, and the Spanish version will have/es/.

Which type of Load Balancer would you use to route traffic to ensure users connect to the site in their desired language?

A. Classic Load Balancer
B. Network Load Balancer
C. Application Load Balancer
D. Path-Based Load Balancer

Correct Answer – C

Explanation

Application Load Balancer support path-based routing. You can configure rules for your listener that forward requests based on the URL in the request.

Classic Load Balancers is the incorrect answer as you cannot configure path-based routing with this type of Load Balancer. Furthermore, Classic Load Balancers are intended only for testing purposes and should ideally not be used for production workloads.

Network Load Balancers is the incorrect answer. A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second and could be better for application-specific type load balancing as Application Load Balancers would be in this use case.

Ref: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html

Question 110

Which AWS service allows you to register any application resources, such as databases, queues, microservices, and other cloud resources, with custom names, that allow your applications to query the registry for the location of such resources easily?

A. CloudMap
B. CloudTrail
C. CloudWatch
D. CloudFront

Correct Answer – A

Explanation

AWS Cloud Map is a cloud resource discovery service. With Cloud Map, you can define custom names for your application resources, and it maintains the updated location of these dynamically changing resources. This increases your application availability because your web service always discovers the most up-to-date locations of its resources.

Amazon CloudTrail is not the right answer. You can use CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.

Amazon CloudWatch is not the right answer. CloudWatch can help you visualize key metrics, like CPU utilization and memory, and compare them to capacity. You can also correlate the log pattern of a specific metric and set alarms to be proactively alerted about performance and operational issues.

Amazon CloudFront is not the right answer. CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

AWS Well-Architected Framework

Question 111

As a Cloud Practitioner, you have been tasked to architect an application solution which will be deployed on AWS. Which of the following well-architected design principles can help you increase reliability in line with best practices? (Choose two answers)

A. The solution must automatically recover from failure
B. Any application upgrades, bug fixes or feature updates must be carried out regularly as small frequent reversible changes
C. The application architecture must incorporate security at all levels

D. Any changes in the demand for the application must be addressed by automatically adding or removing resources to maintain the optimal level required to satisfy demand without over- or under-provisioning.
E. Data to and from the application must be encrypted in transit

Correct Answer: A & D

The Reliability Pillar of the Well-Architected Framework enables you to follow best practices when architecting your application solution to ensure that it performs its intended function correctly, consistently, and as expected. The key design principles for increasing reliability are:

- Automatic recovery from failure
- Test recovery procedures
- Scale horizontally to increase aggregate workload availability
- Stop guessing capacity
- Manage change in automation

The answer, 'Any application upgrades, bug fixes or feature updates must be carried out regularly as small frequent reversible changes' is incorrect. This best practice ensures that if application components are upgraded as small frequent reversible changes, then any failures can easily be reserved. This design principle is part of the Well-Architected Framework Operations Pillar.

The answer, 'The application architecture must incorporate security at all levels' is incorrect. This best practice emphasizes the importance of designing security at all layers of the application stack comprising the network, compute, storage, operating system, and application code. This design principle is part of the Well-Architected Framework Security Pillar.

The answer, 'Data to and from the application must be encrypted in transit is incorrect. This best practice suggests classifying data into sensitive levels and applying security features such as encryption, tokenization, and access control. This design principle is part of the Well-Architected Framework Security Pillar.

Ref: https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/design-principles.html
Ref: https://docs.aws.amazon.com/wellarchitected/latest/framework/wellarchitected-framework.pdf

Question 112

A company wants to build a cloud application which will be hosted on AWS. You have been hired to architect the application solution that must be highly cost-effective. To achieve this, you have suggested that development and test compute environments should be comprised of On-Demand instances since they will only be used for eight hours a day (Monday to

Friday), and you are not charged for compute resources when those instances are in the stopped state. Which AWS Cost Optimization Pillar design principle does this suggestion related to?

A. Analyze and attribute expenditure
B. Adopt a consumption model
C. Experiment more often
D. Stop guessing capacity

Correct Answer: B

A key design principle for the Cost Optimization pillar discusses the importance of adopting a consumption model for provisioning resources on AWS. This means you should only pay for services when you use them and increase or decrease usage depending on business requirements. As per the example given, if you are only using On-Demand instances for eight hours a day (Monday to Friday), then you only pay for those 40 hours a week of computing capacity. Given that you are not charged for those compute resources when the instances are in the stopped state, there is a potential cost savings of 75% (40 hours versus 168 hours).

The answer 'Analyze and attribute expenditure' is incorrect. Although this design principle is part of the Cost Optimization pillar, it refers to the ability to accurately identify the cost and usage of workloads and measure return on investment (ROI) for services consumed and resources deployed.

The answer, 'Experiment more often' is incorrect. This design principle is part of Performance Pillar and allows you to compare different resource types and sizes to identify ones that enable you to design highly performant architectures.

The answer, 'Stop guessing capacity is incorrect. This design principle is part of the Reliability Pillar and allows you to provision resources when there is demand using automated scaling processes when required.

Ref: https://docs.aws.amazon.com/wellarchitected/latest/cost-optimization-pillar/design-principles.html

Question 113

Which of the following are design principles for the AWS Well-Architected Sustainability Pillar? (Choose two answers)

A. Use managed services
B. Maximize utilization
C. Prepare for security events
D. Make frequent small, reversible changes
E. Consider mechanical sympathy

Correct Answer – A & B

The AWS Well-Architected Sustainability Pillar is designed to help organizations fulfil and directly contribute to their sustainability goals. This helps companies monitor and manage the long-term environmental, economic, and societal impact of their business activities.

Using managed services rather than self-managed resources where possible can help businesses fulfil the design requirements for the sustainability pillar. For example, with container technology, you can either use the ECS 'EC2 launch type' or the 'Fargate launch type'. The latter is a serverless solution where AWS will manage scaling and the efficient operation of the underlying resources. While the EC2 launch type gives you greater control over the underlying EC2 instances, you are still required to manage those resources yourself. If there are idle resources simply waiting to be used, then this increases your indirect emissions and has a negative impact on the environment. Using managed services reduces the amount of infrastructure needed to support cloud workloads.

Another design principle for the AWS Well-Architected Sustainability Pillar refers to the importance of maximizing utilization. By right-sizing your workloads, you consume resources more efficiently and this directly impacts the environment. For example, two hosts running at 30% utilization are less efficient than one host running at 60% due to baseline power consumption per host.

The answer, 'Prepare for security events' is incorrect. This design principle relates to the Security Pillar of the AWS Well-Architected Framework. Specifically, it refers to the concept of having incident management and investigation policy and processes in place to respond to security incidents. It also suggests that you incorporate simulations and use tools that automatically increase your speed for detection, investigation, and recovery.

The answer, 'Make frequent small, reversible changes' is incorrect. This design principle relates to the Operational Excellence Pillar of the AWS Well-Architected Framework. Specifically, it refers to the concept of making frequent small, reversable changes so that if components fail, it is easier to reserve without having a massive impact on your customers. In addition, making regular small changes is better than one large change.

The answer, 'Consider mechanical sympathy' is incorrect. This design principle relates to the Performance Efficiency Pillar of the AWS Well Architected Framework. Specifically, it refers to the concept of using the right technology approach that aligns best with your workload goals. So for example, understanding your data access patterns will ensure you choose the right storage type.

Ref: https://docs.aws.amazon.com/wellarchitected/latest/sustainability-pillar/design-principles-for-sustainability-in-the-cloud.html

Question 114

Which AWS Well Architected Framework Pillar focuses on the ability to run workloads effectively, continuously improve supporting processes and procedures to deliver business value?

A. Security Pillar
B. Operational Excellence
C. Reliability Pillar
D. Sustainability Pillar

Correct Answer – B

The Operational Excellence Pillar focuses on the ability to support the development and run workloads effectively, gain insight into their operations, and improve processes and procedures to deliver business value. This pillar is all about making ongoing and iterative efforts in improving the operations of workloads. Analyze operational events and failures to improve the operations of your architecture.

To improve the operational excellence of your applications, you need to understand needs of your workloads, create, and maintain runbooks for routine activities, design playbooks to guide issue resolution, script your operations procedures and automate their execution by triggering them in response to events.

Another aspect of building for Operational Excellence is to ensure that your application components can be updated regularly as small, reversible changes. This enables rollback processes to be easily implemented if those updates fail and minimize the impact on your customers.

The answer, 'Security Pillar' is incorrect. This pillar focuses on using cloud technologies to protect data, systems, and assets in a way that can improve the overall security of your applications.

The answer, 'Reliability Pillar' is incorrect. This pillar focuses on ensuring that your workload will perform its intended function correctly and consistently when it's expected to.
The answer, 'Sustainability Pillar' is incorrect. This pillar focuses on reducing energy consumption and increasing efficiency across all components of a workload by maximizing the benefits from the provisioned resources and minimizing the total resources required.

Ref: https://docs.aws.amazon.com/wellarchitected/latest/framework/wellarchitected-framework.pdf

Question 115

Which AWS service enables you to review the state of your applications and workloads against AWS best practices by answering a set of foundational questions, with the option to create your own custom lenses?

A. AWS Trusted Advisor

B. AWS Personal Health Dashboard
C. AWS Well-Architected Tool
D. AWS Inspector

Correct Answer – C

The AWS Well-Architected Tool enables you to analyze your workloads and applications against a series of best practices. In addition to the foundation questions, you can also create your own questions and evaluate your workloads using your organization's best practices via custom lenses. This service enables you to evaluate your workloads against the six pillars of the Well-Architected Framework – Operational Excellence, Reliability, Performance Efficiency, Security, Cost Optimization, and the Sustainability Pillar.

The AWS Well-Architected Tool is available at no charge in the AWS Management Console.

The answer, 'AWS Personal Health Dashboard (PHD)' is incorrect. This service provides alerts and guidance for AWS events that might affect your environment.

The answer, 'AWS Trusted Advisor' is incorrect. This service offers recommendations that help you follow AWS best practices. The Well Architected Framework, however, describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud.

The answer, 'AWS Inspector' is incorrect. This automated vulnerability management service continually scans AWS workloads for software vulnerabilities and unintended network exposure on your EC2 Instances.

Ref: https://aws.amazon.com/well-architected-tool/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

Ref: https://youtu.be/n4BTqappip0

Question 116

Which AWS cloud architecture design principle supports the use of the technology that aligns best with your workload goals? For example, using the right storage type for the workload and operation?

A. Automatically recover from failure
B. Enable traceability
C. Consider mechanical sympathy
D. Adopt a consumption model

Correct Answer – C

Consider mechanical sympathy is part of a design principle for the Performance Efficiency pillar and focuses on the concept of understanding how different cloud services are meant to be consumed in alignment with the type of workload goals you have. There is no point in using Amazon S3 buckets when you are really require block storage that need to be accessible for your EC2 Instances on which you can install applications. Similarly, it makes more sense to use object storage and Amazon S3 for storing digital assets for your website such as images and videos.

The answer 'Automatically recover from failure' is incorrect. This design principle belongs to the Reliability pillar that discusses the importance of distributing your workloads across multiple availability zones so that if one component fails or if an entire availability zones goes offline, you application is still accessible.

The answer 'Enable traceability' is incorrect. This design principle belongs to the Security pillar and discusses the importance of monitoring and auding actions and changes to your environment in real time.

The answer 'Adopt a consumption model' is incorrect. This design principle belongs to the Cost Optimization pillar which focuses on the importance of paying only for the resources you require and increase or decrease usage depending on business requirements. The key benefit here is that you do not over-provision resources unnecessarily which results is wastage.

Ref: https://docs.aws.amazon.com/wellarchitected/latest/framework/perf-dp.html

Question 117

Which AWS design principle supports the implementation of the *principle of least privilege* by enforcing the separation of duties using appropriate permissions?

A. Implement a strong identity foundation
B. Enable traceability
C. Test recovery procedures
D. Perform operations as code

Correct Answer: A

Implementing the principle of least privilege and enforcing separation of duties is a key ingredient for implementing a strong identity foundation design principle.

By ensuring that your team members have only the necessary permissions to get the job done and separating out duties, you can ensure that accidents are reduced and malicious actions prevented.

Another key element of this design principle is to eliminate reliance on long-term credentials. Even if an individual occasionally needs elevated privileges, a break-glass

approach can be adopted as a standard. In this case, the individual has minimum permissions are granted for day-to-day operations but can assume a role for any elevated actions that may need to be performed due to certain events or schedules.

The answer 'Enable traceability' is incorrect. While this design principle is also part of the Security pillar, it refers more to the ability to monitor and audit actions that take place in a given AWS account.
The answer 'Test recovery procedures' is incorrect. This design principle relates to the Reliability Pillar. This design principle discusses the importance of regular testing to prove that workloads work in given scenarios. You can then simulate failure scenarios and identify recovery options before any failure occurs.

The answer 'Perform operations as code' is incorrect. This design principle relates to the Operational Excellence pillar. The key benefit is defining operations procedures as code and automating their execution by triggering them in response to events.

Ref: https://docs.aws.amazon.com/wellarchitected/latest/framework/sec-design.html

Question 118

Which of the following is an example of High Availability on AWS?

A. Deploying and configuring resources such that the application remains accessible even if some of the resources fail
B. Automatically provisioning more resources as demand increases
C. Procuring reserved instances for long term consistent use cases
D. Implementing AWS Organizations to facilitate multi-account management

Correct Answer – A

You can deploy multiple replicas of your resources across different availability zones and regions and configure those resources such as your application continues to serve traffic even if some of the resources in specific availability zones fail. This ensures high availability of your application and is a recommended best practice when designing your application architecture

The answer 'Automatically provision more resources as demand increases' is incorrect. This recommendation refers to the ability to automatically scale your resources where you can add additional resource nodes to facilitate increased demand

The answer 'Procuring reserved instances for long-term consistent use cases' is incorrect. This recommendation refers to designing your resource configuration for cost optimization. Purchasing reserved instances refer to the pricing option of those resources where you benefit from a large discount if you commit to a minimum contractual term for those resources

The answer ‘Implementing AWS Organizations to facilitate multi-account management’ is incorrect. This recommendation refers to managing multiple AWS accounts for different use cases such as provisioning environments for development, testing and production.

Question 119

Which of the following are design principles for the AWS Well Architected Sustainability Pillar? (Choose two answers)

A. Use managed services.
B. Maximize utilization.
C. Prepare for security events.
D. Make frequent small, reversible changes.
E. Consider mechanical sympathy.

Correct Answer – A & B

Explanation

The AWS Well Architected Sustainability Pillar is designed to help organizations fulfil and directly contribute to their sustainability goals. This helps companies monitor and manage the long-term environmental, economic, and societal impact of their business activities.

Using managed services rather than self-managed resources where possible can help businesses fulfil the design requirements for the sustainability pillar. For example, with container technology, you can either use the ECS EC2 launch type or the Fargate launch type. The latter is a serverless solution where AWS will manage scaling and the efficient operation of the underlying resources. While the EC2 launch type gives you greater control over the underlying EC2 instances, you are still required you to manage those resources yourself. If there are idle resources simply waiting to be used, then this increases your indirect emissions and have a negative impact on the environment. Using managed services reduces the amount of infrastructure needed to support cloud workloads.

Another design principle for the AWS Well Architected Sustainability Pillar refers to the importance of maximizing utilization. By right sizing your workloads, you consume resources more efficiently and this directly impacts the environment. For example, two hosts running at 30% utilization are less efficient than one host running at 60% due to baseline power consumption per host.

The answer, ‘Prepare for security events’ is incorrect. This design principle relates to the Security Pillar of the AWS Well Architected Framework. Specifically, it refers to the concept of having incident management and investigation policy and processes in place to respond to security incidents. It also suggests that you incorporate simulations and use tools that automatically increases your speed for detection, investigation, and recovery.

The answer, ‘Make frequent small, reversable changes’ is incorrect. This design principle relates to the Operational Excellence Pillar of the AWS Well Architected Framework. Specifically, it refers to the concept of making frequent small, reversable changes so that if components fail, it is easier to reserve without having a massive impact on your customers. In addition, making regular small changes is better than one large change.

The answer, ‘Consider mechanical sympathy’ is incorrect. This design principle relates to the Performance Efficiency Pillar of the AWS Well Architected Framework. Specifically, it refers to the concept of using the right technology approach that aligns best with your workload goals. So for example, understanding your data access patterns will ensure you choose the right storage type.

Ref: https://docs.aws.amazon.com/wellarchitected/latest/sustainability-pillar/design-principles-for-sustainability-in-the-cloud.html

Cost and FinOps

Question 120

To reduce costs, you have been asked to automate the shutdown of a fleet of UAT Test Servers every weekday at 7 PM and then restart the following weekday at 8 AM. Servers should remain in the shutdown state at weekends.

Which AWS service can help you achieve the above requirements?

A. Amazon SQS
B. Amazon Athena
C. Amazon SNS
D. Amazon EventBridge

Correct Answer – D

Explanation

Amazon EventBridge is a serverless Event Bus Service that allows you to stream real-time events from your applications, SaaS-based services, and AWS services to a variety of targets. For the above requirements, you can set up a scheduled EventBridge rule to run an AWS Lambda function that performs the automatic shutdown and restart of your EC2 Instances at a predefined date and time. You can use CRON expressions to define your Lambda function's schedules.

The answer, ‘Amazon Athena’ is incorrect. Amazon Athena is an interactive query service that helps you analyze raw data held in S3. You only pay for the queries you run against the data as there is no infrastructure to manage.

The answer, ‘Amazon SNS’ is incorrect. Amazon SNS is a push-based notification service that allows one application component to communicate with another application component or a person. Amazon SNS can be used to send out alerts to end-users or applications of an event that has occurred.

The answer, ‘Amazon SQS’ is incorrect. Amazon SQS is a pull-based message queuing system allowing you to build decoupled application architectures that can send, store, and receive messages between software components at any volume without losing messages or requiring other services to be available.

Question 121

Which AWS Service can be used to track costs you have incurred so far in your AWS account with a graphical visualization?

A. Cost Explorer
B. X-ray
C. Total Cost of Ownership (TCO) or Migration Evaluator
D. AWS Pricing Calculator

Correct Answer – A

Explanation

AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer helps you visualize, understand, and manage your AWS costs and usage over a daily or monthly granularity. The solution also lets you dive deeper using granular filtering and grouping dimensions such as Usage Type and Tags. You can also access your data with further granularity by enabling hourly and resource-level granularity.

The answer, ‘AWS Migration Evaluator’ can help you compare the cost of your applications in an on-premises or traditional hosting environment to AWS.

The answer, ‘AWS Pricing Calculator’ is incorrect. Previously known as the Simple Monthly Calculator, the new AWS Pricing Calculator enables you to work out cost estimate that fits your unique business or personal needs with AWS products and services. Using the calculator, you can work out your estimated monthly costs based on the workloads you configure in your AWS Account.

The answer, ‘AWS X-Ray’ is incorrect. AWS X-Ray helps developers analyze and debug production, and distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors.

Ref: https://aws.amazon.com/aws-cost-management/aws-cost-explorer/

Question 122

Which AWS service enables you to set custom cost and usage budgets to manage your AWS spending more easily?

A. AWS Migration Evaluator
B. AWS Budgets
C. Billing Alarm
D. AWS Shield

Correct Answer – B

Explanation

AWS Budgets allows you to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount.

You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. Reservation alerts are supported for Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache, and Amazon Elasticsearch reservations.

The answer, 'AWS Migration Evaluator,' is incorrect. The AWS Migration Evaluator is an online calculator to compare the cost of your applications in an on-premises or traditional hosting environment to AWS.

The answer, 'AWS Billing Alarm' is incorrect. AWS Billing Alarms can be created using Amazon CloudWatch to alert you when your account billing exceeds the threshold you specify.

The answer, 'AWS Shield' is incorrect. AWS Shield offers DDoS protection that help to safeguard your applications running on AWS. AWS offers two tiers of the service – AWS Shield Standard and AWS Shield Advanced.

Ref: https://youtu.be/pjrKDkzbas8

Question 123

Which AWS EC2 pricing option can help you reduce costs by allowing you to use your existing server-bound software licenses?

A. On-Demand Instances
B. Reserved Instances
C. Spot Instances
D. Dedicated Hosts

Correct Answer – D

Explanation

Dedicated Hosts allow you to use your existing per-socket, per-core, or per-VM software licenses, including Microsoft Windows Server, Microsoft SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, or other software licenses that are bound to VMs, sockets, or physical cores, subject to your license terms.

When you launch instances on a Dedicated Host, the instances run on a physical server that is dedicated to your use. While Dedicated instances also run on dedicated hardware, Dedicated Hosts provide further visibility and control by allowing you to place your instances on a specific, physical server. This enables you to deploy instances using configurations that help address corporate compliance and regulatory requirements.

Ref: https://aws.amazon.com/ec2/pricing/

Question 124

Which AWS Calculator can be used to work out your monthly AWS costs for services deployed in your AWS Account?

A. AWS Pricing Calculator
B. AWS Service Calculator
C. AWS Cost Calculator
D. AWS Monthly Calculator

Correct Answer – A

Explanation

The AWS Simple Monthly Calculator helps users to work out and estimate their monthly costs for AWS Workloads more efficiently.

Question 125

Which of the following components determines the cost of your RDS Database Instance? (Choose three answers)

A. Storage amount
B. Hours of use
C. Number of requests
D. Data transfer in
E. The number of buckets used.

Correct Answer – A, B & C

Explanation

Hours of use, Additional Storage and Number of Requests determine the overall cost of your RDS Instance.

Question 126

Which AWS Report enables you to view line items for each unique combination of AWS products, usage types, and operations your AWS account uses?

A. AWS Artifact
B. AWS Single Bill
C. AWS Cost and Usage Report
D. AWS Cost Management Report

Correct Answer – C

Explanation

The AWS Cost and Usage report tracks your AWS usage and provides estimated charges associated with your AWS account. The report contains line items for each unique combination of AWS products, usage types, and operations that your AWS account uses. You can customize the AWS Cost and Usage report to aggregate the information by the hour or day. Ref:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-costusage.html

Question 127

Which AWS savings plan type provides the maximum flexibility by applying discounts pricing against EC2 Instances, Lambda and Fargate compute services?

A. Compute Savings Plans
B. Serverless Savings Plans
C. SageMaker Savings Plans
D. EC2 Instance Savings Plans

Correct Answer – A

Explanation – Compute Savings Plans offer the most flexibility and can offer up to 66% discount on On-Demand rates for EC2 Instances (applicable across families, sizes, regions, operating systems, or tenancy), Fargate and Lambda usage. This means you still get

discounted rates if you migrate applications from EC2 to ECS using Fargate or build serverless compute resources using AWS Lambda.

The answer 'Serverless Savings Plans' is incorrect as there is no such plan

The answer 'SageMaker Savings Plans' is incorrect. This plan applies to your SageMaker instance usage offering up to 64 percent discount on the On-Demand rates.

The answer 'EC2 Instance Savings Plan' is incorrect. This plan only applies to EC2 instances within a specific family in a chosen AWS Region. However, it also offers a maximum discount of up to 72 percent on the On-Demand rates.

Ref: https://docs.aws.amazon.com/savingsplans/latest/userguide/what-is-savings-plans.html#plan-types

Additional Question

Question 128

Which storage solution enables you to share a common file system across multiple Linux-based EC2 Instances that can be used to support applications requiring data access with very low latency connectivity?

A. EFS
B. EBS
C. S3
D. NTFS

Correct – A

Explanation

Amazon EFS is a fully managed service providing shared file system storage for Linux workloads. It provides a simple interface allowing you to create and configure file systems quickly and manages the file storage infrastructure for you, removing the complexity of deploying, patching, and maintaining the underpinnings of a file system. You can use to provide your application that runs on multiple EC2 instances to share a common file system that offers very low latency connectivity.

The answer, "EBS", is incorrect because although you can configure a file system on EBS Volumes, you cannot share an EBS volume across multiple EC2 Instances.

The answer, "S3", is incorrect because it is not a file system. Also, EFS would offer much lower latency. Amazon S3 is object storage and is ideally used to host assets such as documents, images, and videos, which web applications can reference.

The answer, “NTFS”, is incorrect because this is a file system, specifically a Windows File System, not. the actual storage option.

Question 129

Which type of EBS volume would you recommend for a high-performance application that is particularly sensitive to high latency?

A. EBS General Purpose SSD (gp2)
B. EBS Throughput Optimized HDD (st1)
C. Cold HDD (sc1)
D. EBS Provisioned IOPS SSD (io1)

Correct Answer – D

Explanation

IO1 is backed by solid-state drives (SSDs) and is the highest performance EBS storage option designed for critical, I/O intensive database and application workloads, as well as throughput-intensive database and data warehouse workloads, such as HBase, Vertica, and Cassandra. These volumes are ideal for both IOPS-intensive and throughput-intensive workloads that require extremely low latency.

The answer “EBS General Purpose SSD (gp2) is incorrect and ideally suited to non-intensive workloads.

The answer “EBS Throughput Optimized HSS (st1) is incorrect as there is no such.

Question 130

Which tool in Amazon IAM can you use to configure company-wide password rules such as complexity level, number of passwords to remember, and length of password?

A. Password Policy
B. Password Complexity Generator
C. Password Rules
D. IAM Password Settings

Correct Answer – A

Explanation

You can set a **password policy** on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords.

Ref:https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html