CLO-002 Q&As

CompTIA Cloud Essentials+

Pass CompTIA CLO-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/clo-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Which of the following is a scientific study of algorithms and statistical models that a computer system integrates to improve performance of a specific task effectively based on information?

A. IoT

B. Big Data

C. Machine learning

D. Blockchain

Correct Answer: C

Explanation: Machine learning Comprehensive Explanation: Machine learning is a scientific study of algorithms and statistical models that a computer system integrates to improve performance of a specific task effectively based on information1. Machine learning is a subfield of artificial intelligence that uses data and algorithms to imitate the way that humans learn, gradually improving its accuracy2. Machine learning enables machines to perform tasks that would otherwise only be possible for humans, such as categorizing images, analyzing data, or predicting price fluctuations2. Machine learning algorithms are typically created using frameworks that accelerate solution development, such as TensorFlow and PyTorch2. IoT, or Internet of Things, is a network of physical devices, vehicles, appliances, and other items embedded with sensors, software, and connectivity that enable these objects to exchange data and interact with each other3. IoT is not a scientific study of algorithms and statistical models, but a technological paradigm that connects various devices and systems to the internet. Big Data is a term that refers to the large, complex, and diverse sets of data that are generated at high speed from various sources, such as social media, sensors, web logs, or transactions4. Big Data is not a scientific study of algorithms and statistical models, but a data phenomenon that poses challenges and opportunities for analysis and processing. Blockchain is a system of storing and transferring information in a distributed, decentralized, and secure way using cryptographic principles and peer-to-peer networks5. Blockchain is not a scientific study of algorithms and statistical models, but a data structure and protocol that enables trustless and transparent transactions and records. References : Machine learning -Wikipedia; What Is Machine Learning? Definition, Types, and Examples; What is the Internet of Things (IoT)? | IBM; What is big data? | IBM; What is blockchain? | IBM.

QUESTION 2

Which of the following cloud migration methods would take full advantage of the cloud computing model?

A. Rip and replace

B. Lift and shift

C. Phased

D. Hybrid

Correct Answer: A

Explanation: Rip and replace is a cloud migration method that involves discarding the existing legacy system and building a new one from scratch on the cloud platform. This method allows the organization to take full advantage of the cloud computing model, such as scalability, elasticity, performance, and cost-efficiency. Rip and replace also enables the organization to leverage the cloud-native features and services, such as serverless computing, microservices, and containers. However, rip and replace is also the most complex and risky migration method, as it requires a complete redesign and redevelopment of the system, which can be time-consuming, expensive, and prone to errors. Therefore,

rip and replace is only suitable for systems that are outdated, incompatible, or unsuitable for the cloud environment, and that have a clear business case and return on investment for the migration. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 5: Cloud Migration, page 1971

QUESTION 3

A systems administrator needs to transfer 300GB of data to the cloud every month. Given the information below:

Connection type	Connectivity costs	Transfer limits
VPN (100MB)	Free	$5 per GB after 10GB
Direct Connect (500MB)	$200 per month	Free up to 250GB; $10 per GB after
Enhanced VPN (200MB)	Free	$10 per GB after 10GB
Enhanced Direct Connect (1GB)	$500 per month	Unlimited

Which of the following connection methods would be the MOST cost-effective and satisfy the monthly transfer requirements?

A. VPN (100MB)

B. Direct Connect (500MB)

C. Enhanced VPN (200MB)

D. Enhanced Direct Connect (1GB)

Correct Answer: B

According to the CompTIA Cloud Essentials objectives and documents, the most cost- effective and satisfying monthly transfer requirements connection method would be Direct Connect (500MB). This is because it has a fixed cost of $200 per month and a transfer limit of up to 250GB, which is enough to satisfy the 300GB monthly transfer requirement. Additionally, it has a lower cost per GB after the transfer limit is reached compared to the other options. The other connection methods are either more expensive or insufficient for the monthly transfer requirement. VPN (100MB) has a fixed cost of $50 per month and a transfer limit of up to 50GB, which is not enough for the 300GB monthly transfer requirement. Enhanced VPN (200MB) has a fixed cost of $100 per month and a transfer limit of up to 100GB, which is also not enough for the 300GB monthly transfer requirement. Enhanced Direct Connect (1GB) has a fixed cost of $400 per month and a transfer limit of up to 500GB, which is more than enough for the 300GB monthly transfer requirement, but also more expensive than Direct Connect (500MB). References: 1, 2, 3

QUESTION 4

A business analyst is drafting a risk assessment.

Which of the following components should be included in the draft? (Choose two.)

A. Asset management

B. Database type

C. Encryption algorithms

D. Certificate name

E. Asset inventory

F. Data classification

Correct Answer: EF

Explanation: A risk assessment is a process of identifying, analyzing, and controlling hazards and risks within a situation or a place1. According to the CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), a risk assessment should include the following steps2: Identify the assets that are relevant to the scope of the assessment. Assets can be physical, such as hardware and software, or non-physical, such as data and information. Identify the threats and vulnerabilities that could affect the assets. Threats are sources of potential harm, such as natural disasters, cyberattacks, or human errors. Vulnerabilities are weaknesses or gaps in the security or protection of the assets, such as outdated software, misconfigured settings, or lack of encryption. Analyze the likelihood and impact of each threat-vulnerability pair. Likelihood is the probability of a threat exploiting a vulnerability, and impact is the severity of the consequences if that happens. The combination of likelihood and impact determines the level of risk for each pair. Evaluate the risks and prioritize them based on their level. Risks can be categorized as low, medium, high, or critical, depending on the organization\\'s risk appetite and tolerance. Risk appetite is the amount of risk that the organization is willing to accept, and risk tolerance is the degree of variation from the risk appetite that the organization can endure. Implement appropriate controls to mitigate or reduce the risks. Controls are measures or actions that can prevent, detect, or correct the occurrence or impact of a risk. Controls can be administrative, technical, or physical, and they can have different functions, such as preventive, detective, corrective, deterrent, or compensating. Based on these steps, two components that should be included in the draft of a risk assessment are asset inventory and data classification. Asset inventory is the process of identifying and documenting the assets that are within the scope of the assessment1. Data classification is the process of categorizing data based on its sensitivity, value, and criticality to the organization3. These components are essential for determining the potential risks and impacts that could affect the assets and data, and for applying the appropriate controls and protection levels.

https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide
https://books.google.com/books/about/CompTIA_Cloud_Essentials+_Certification.html?id= S2TNDwAAQBAJ

QUESTION 5

Which of the following are true about the use of machine learning in a cloud environment? (Choose two).

A. Specialized machine learning algorithms can be deployed to optimize results for specific scenarios.

B. Machine learning can just be hosted in the cloud for managed services.

C. Just one type of cloud storage is available in the cloud for machine learning workloads.

D. Machine learning can leverage processes in a cloud environment through the use of cloud storage and auto-scaling.

E. Machine learning requires a specialized IT team to create the machine learning models from scratch.

F. Using machine learning solutions in the cloud removes the data-gathering step from the learning process.

Correct Answer: AD

Explanation: Machine learning is a subset of artificial intelligence that enables a system to autonomously learn and improve using neural networks and deep learning, without being explicitly programmed, by feeding it large amounts of data1. Machine learning can be used in a cloud environment to leverage the benefits of cloud computing, such as scalability, flexibility, and cost-effectiveness. Some of the ways that machine learning can use cloud processes are: Specialized machine learning algorithms can be deployed to optimize results for specific scenarios. Depending on the

use case, an organization may choose different cloud services to support their machine learning projects, such as artificial intelligence as a service (AIaaS) or GPU as a service (GPUaaS)2. AIaaS provides pre-trained models for common tasks, such as image recognition, natural language processing, or sentiment analysis, while GPUaaS provides access to high-performance computing resources for training custom models. These services can help organizations achieve better results faster and more efficiently. Machine learning can leverage processes in a cloud environment through the use of cloud storage and auto-scaling. Cloud storage provides a scalable and secure way to store and access large amounts of data, which is essential for machine learning. Cloud storage also enables data integration and collaboration across different sources and platforms3. Auto-scaling is a feature of cloud computing that automatically adjusts the amount of resources allocated to a machine learning application based on the demand and workload. This helps optimize the performance and cost of machine learning in the cloud4. The other options are false because: Machine learning can just be hosted in the cloud for managed services. This is not true because machine learning can also be used in a hybrid or multi-cloud environment, where some components of the machine learning project are hosted on-premises or on different cloud providers. This can provide more flexibility and control over the machine learning process, as well as address security and compliance issues2. Just one type of cloud storage is available in the cloud for machine learning workloads. This is not true because there are different types of cloud storage available for machine learning workloads, such as object storage, block storage, or file storage. Each type of storage has its own advantages and disadvantages, depending on the data format, size, and access frequency. For example, object storage is suitable for storing unstructured data, such as images or videos, while block storage is suitable for storing structured data, such as databases or files3. Machine learning requires a specialized IT team to create the machine learning models from scratch. This is not true because machine learning does not always require a specialized IT team to create the models from scratch. There are many tools and services available in the cloud that can help simplify and automate the machine learning process, such as data preparation, model building, testing, deployment, and monitoring. For example, Google Cloud AutoML is a service that allows users to create custom machine learning models with minimal coding and expertise4. Using machine learning solutions in the cloud removes the data-gathering step from the learning process. This is not true because using machine learning solutions in the cloud does not remove the data-gathering step from the learning process. Data-gathering is a crucial step in machine learning, as it provides the input for the machine learning models to learn from. Data-gathering involves collecting, cleaning, labeling, and transforming data from various sources, such as sensors, databases, or web pages. Using machine learning solutions in the cloud can help with data-gathering, but it does not eliminate it3. References:

1: What is Machine Learning? Types and Uses | Google Cloud

2: Machine Learning in the Cloud: Complete Guide [2023] - Run

3: Role: Artificial Intelligence and Machine Learning in Cloud Environment

4: Data science and machine learning on Cloud AI Platform

QUESTION 6

Which of the following types of risk is MOST likely to be associated with moving all data to one cloud provider?

A. Vendor lock-in

B. Data portability

C. Network connectivity

D. Data sovereignty

Correct Answer: A

Explanation: Vendor lock-in is the type of risk that is most likely to be associated with moving all data to one cloud provider. Vendor lock-in refers to the situation where a customer is dependent on a particular vendor\\'s products and services to such an extent that switching to another vendor becomes difficult, time-consuming, or expensive. Vendor

lock-in can limit the customer\\'s flexibility, choice, and control over their cloud environment, and expose them to potential issues such as price increases, service degradation, security breaches, or compliance violations. Vendor lock-in can also prevent the customer from taking advantage of new technologies, innovations, or opportunities offered by other vendors. Vendor lock-in can be caused by various factors, such as proprietary formats, standards, or protocols, lack of interoperability or compatibility, contractual obligations or penalties, or high switching costs12 References: CompTIA Cloud Essentials+ Certification Exam Objectives3, CompTIA Cloud Essentials+ Study Guide, Chapter 2: Business Principles of Cloud Environments2, Moving All Data to One Cloud Provider: Understanding Risks1

QUESTION 7

A company is moving to the cloud and wants to enhance the provisioning of compute, storage, security, and networking. Which of the following will be leveraged?

A. Infrastructure as code

B. Infrastructure templates

C. Infrastructure orchestration

D. Infrastructure automation

Correct Answer: A

Explanation: Infrastructure as code (IaC) is a DevOps practice that uses code to define and deploy infrastructure, such as networks, virtual machines, load balancers, and connection topologies1. IaC ensures consistency, repeatability, and scalability of the infrastructure, as well as enables automation and orchestration of the provisioning process2. IaC is different from infrastructure templates, which are predefined configurations that can be reused for multiple deployments3. Infrastructure orchestration is the process of coordinating multiple automation tasks to achieve a desired state of the infrastructure4. Infrastructure automation is the broader term for any technique that uses technology to perform infrastructure tasks without human intervention5. References: CompTIA Cloud Essentials CLO-002 Certification Study Guide, Chapter 4: Operating in the Cloud, page 137 What is infrastructure as code (IaC)?, Azure DevOps | Microsoft Learn CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 4: Operating in the Cloud, page 137 Infrastructure Automation: 7 DevOps Tools for Orchestration, Secrets Management, and More, Apriorit Blog Infrastructure As Code Vs Configuration Management, DevOpsCube Blog

QUESTION 8

Which of the following allows for the management of network policies from a central portal while maintaining a hardware-agnostic approach?

A. Virtual private network

B. Software-defined network

C. Load balancing

D. Direct Connect

Correct Answer: B

Explanation: A software-defined network (SDN) is a network architecture that allows for the management of network policies from a central portal while maintaining a hardware- agnostic approach. SDN separates the control plane, which is responsible for making decisions about how to route traffic, from the data plane, which is responsible for forwarding

traffic based on the control plane\\'s instructions. SDN enables network administrators to configure, monitor, and manage network devices and services using a software application, regardless of the vendor or type of hardware. SDN also provides automation, programmability, scalability, and flexibility for network operations. A virtual private network (VPN) is a network technology that creates a secure and encrypted connection over a public network, such as the Internet. A VPN allows remote users to access a private network and its resources securely. A VPN is not related to the management of network policies from a central portal or the hardware-agnostic approach of SDN. Load balancing is a network technique that distributes traffic across multiple servers or devices to optimize performance, reliability, and availability. Load balancing can be implemented using hardware or software, but it does not provide the same level of centralized management and control as SDN. Direct Connect is a service offered by some cloud providers that allows customers to establish a dedicated network connection between their on-premises network and the cloud provider\\'s network. Direct Connect bypasses the public Internet and provides lower latency, higher bandwidth, and more consistent network performance. However, Direct Connect is not a generic network architecture that supports a hardware-agnostic approach, and it does not offer the same degree of network programmability and automation as SDN. References: CompTIA Cloud Essentials+ CLO- 002 Study Guide, Chapter 4: Cloud Design Principles, Section 4.2: Cloud Network Concepts, Page 1051 and What is software-defined networking (SDN)? | Cloudflare

QUESTION 9

Which of the following are considered secure access types of hosts in the cloud? (Choose two.)

A. HTTPS

B. HTTP

C. SSH

D. Telnet

E. RDP

F. FTP

Correct Answer: AC

Explanation: HTTPS and SSH are considered secure access types of hosts in the cloud because they use encryption and authentication to protect the data and the identity of the users. HTTPS is a protocol that uses SSL or TLS to encrypt the

communication between a web browser and a web server. SSH is a protocol that allows secure remote login and file transfer over a network. Both HTTPS and SSH prevent unauthorized access, eavesdropping, and tampering of the data in

transit. References: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 3:

Security in the Cloud, pages 83-84.

QUESTION 10

Which of the following stores transactions in a distributed ledger of which all users have a copy?

A. Big Data

B. Block chain

C. Machine learning

D. Artificial intelligence

Correct Answer: B

Explanation: A block chain is a type of distributed ledger that stores transactions in a public or private peer-to-peer network. Distributed ledgers use independent computers (referred to as nodes) to record, share, and synchronize transactions in their respective electronic ledgers instead of keeping data centralized as in a traditional ledger. A block chain organizes data into blocks, which are chained together in an append-only mode. Each block contains a timestamp and a cryptographic hash of the previous block, thus making the block chain an auditable, immutable history of all transactions in the network. All users have a copy of the block chain, which they can verify and validate by consensus. A block chain is different from other options, such as big data, machine learning, and artificial intelligence. Big data is a term that refers to the large volume, variety, and velocity of data that is generated, collected, and analyzed by various sources and applications. Machine learning is a branch of artificial intelligence that uses algorithms and data to learn from experience and improve performance without explicit programming. Artificial intelligence is a field of computer science that aims to create machines and systems that can perform tasks that normally require human intelligence, such as reasoning, learning, and decision making. References: Blockchain basics: Introduction to distributed ledgers, Blockchain and Distributed Ledger Technology (DLT) - World Bank Group, Blockchain and Distributed Ledger Technology (DLT), Blockchain Vs. Distributed Ledger Technology

QUESTION 11

Which of the following are the appropriate responses to risks?

A. Mitigate, accept, avoid, validate

B. Migrate, accept, avoid, transfer

C. Mitigate, accept, avoid, transfer

D. Migrate, accept, avoid, validate

Correct Answer: C

Explanation: According to the CompTIA Cloud Essentials+ CLO-002 Study Guide, there are four common risk response types: avoid, share or transfer, mitigate, and accept1. These are the appropriate responses to risks, depending on the risk type, assessment, and attitude. The other options are incorrect because they include terms that are not valid risk responses. For example, migrate is not a risk response, but a cloud deployment strategy. Validate is not a risk response, but a quality assurance technique. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 4: Cloud Security, Section 4.2: Cloud Security Concepts, Page 153.

QUESTION 12

A company\\'s finance team is reporting increased cloud costs against the allocated cloud budget. Which of the following is the BEST approach to match some of the cloud operating costs with the appropriate departments?

A. Right-sizing

B. Scaling

C. Chargeback

D. Showback

Correct Answer: C

Explanation: Chargeback is the best approach to match some of the cloud operating costs with the appropriate departments. Chargeback is a process where the IT department bills each department for the amount of cloud resources they use, such as compute, storage, network, or software. Chargeback can help the company to allocate the cloud costs more accurately and fairly, as well as to encourage the departments to optimize their cloud consumption and reduce waste. Chargeback can also provide the company with more visibility and accountability of the cloud usage and spending across the organization12 Chargeback is different from showback, which is a process where the IT department shows each department the amount of cloud resources they use, but does not charge them for it. Showback can also help the company to increase the awareness and transparency of the cloud costs, but it may not have the same impact on the behavior and efficiency of the departments as chargeback12 Right-sizing and scaling are not approaches to match the cloud costs with the departments, but rather techniques to adjust the cloud resources to the actual demand and performance of the applications or services. Right-sizing and scaling can help the company to save money and improve the cloud utilization, but they do not address the issue of cost allocation or attribution34 References: CompTIA Cloud Essentials+ Certification Exam Objectives, CompTIA Cloud Essentials+ Study Guide, Chapter 2: Business Principles of Cloud Environments, IT Chargeback vs Showback: What\\'s The Difference?2, Cloud Essentials+ Certification Training

QUESTION 13

A company decommissioned its testing environment. Which of the following should the company do FIRST to avoid charges?

A. Detach and delete disposable resources.

B. Empty the logging directory.

C. Delete infrastructure as code templates.

D. Disable alerts and alarms.

Correct Answer: A

Explanation: Disposable resources are cloud resources that are not needed for the long- term operation of an application or service, and can be easily created and deleted on- demand. Examples of disposable resources include temporary storage, spot instances, and disposable virtual machines. Disposable resources can help to reduce costs and improve flexibility, but they also incur charges when they are in use or attached to other resources. Therefore, when a company decommissioned its testing environment, it should detach and delete disposable resources first to avoid charges12 Emptying the logging directory is not the best option to avoid charges, because logging directory is a folder that stores the records of events and activities that occur in an application or service. Logging directory can help to monitor and troubleshoot the performance and issues of the application or service, but it does not directly affect the charges of the cloud resources. Emptying the logging directory may also result in the loss of valuable information and insights that can be used for future improvement or analysis. Deleting infrastructure as code templates is not the best option to avoid charges, because infrastructure as code templates are files that define and configure the cloud resources using code or scripts. Infrastructure as code templates can help to automate and standardize the deployment and management of the cloud resources, but they do not directly affect the charges of the cloud resources. Deleting infrastructure as code templates may also make it harder to recreate or modify the cloud resources in the future. Disabling alerts and alarms is not the best option to avoid charges, because alerts and alarms are notifications that are triggered by certain conditions or thresholds that are set for the cloud resources. Alerts and alarms can help to notify and respond to the changes or issues of the cloud resources, but they do not directly affect the charges of the cloud resources. Disabling alerts and alarms may also make it difficult to detect and resolve any problems or anomalies that may occur in the cloud resources. References: 1: https://docs.microsoft.com/en-us/azure/virtual-machines/disposable-vm 2: https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide, page 46

QUESTION 14

A business analyst has been drafting a risk response for a vulnerability that was identified on a server. After considering the options, the analyst decides to decommission the server. Which of the following describes this approach?

A. Mitigation

B. Transference

C. Acceptance

D. Avoidance

Correct Answer: D

Explanation: Avoidance is a risk response strategy that involves eliminating the threat or uncertainty associated with a risk by removing the cause or the source of the risk. Avoidance can help to prevent the occurrence or the impact of a negative risk, but it may also result in the loss of potential opportunities or benefits. Avoidance is usually applied when the risk is too high or too costly to mitigate, transfer, or accept12 The business analyst is using the avoidance strategy by decommissioning the server that has a vulnerability. By doing so, the analyst is eliminating the possibility of the vulnerability being exploited or causing harm to the system or the data. However, the analyst is also losing the functionality or the value that the server provides, and may need to find an alternative solution or resource. Mitigation is not the correct answer, because mitigation is a risk response strategy that involves reducing the probability or the impact of a negative risk by implementing actions or controls that can minimize or counteract the risk. Mitigation can help to lower the exposure or the severity of a risk, but it does not eliminate the risk completely. Mitigation is usually applied when the risk is moderate or manageable, and the cost of mitigation is justified by the potential benefit12 Transference is not the correct answer, because transference is a risk response strategy that involves shifting the responsibility or the impact of a negative risk to a third party, such as a vendor, a partner, or an insurer. Transference can help to share or distribute the risk, but it does not reduce or remove the risk. Transference is usually applied when the risk is beyond the control or the expertise of the organization, and the cost of transference is acceptable or affordable12 Acceptance is not the correct answer, because acceptance is a risk response strategy that involves acknowledging the existence or the possibility of a negative risk, and being prepared to deal with the consequences if the risk occurs. Acceptance can be passive, which means no action is taken to address the risk, or active, which means a contingency plan or a reserve is established to handle the risk. Acceptance is usually applied when the risk is low or inevitable, and the cost of avoidance, mitigation, or transference is higher than the cost of acceptance12 References: 1: https://www.projectengineer.net/5-risk-response-strategies/ 2: https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide, page 50

QUESTION 15

An incident response team requires documentation for an email phishing campaign against a company\\'s email server. Which of the following is the BEST resource to use to start the investigation?

A. Audit and system logs

B. Change management procedures

C. Departmental policies

D. Standard operating procedures

Correct Answer: A

Explanation: Audit and system logs are the best resource to use to start the investigation of an email phishing campaign against a company\\'s email server. Audit and system logs are records of events and activities that occur on a system or a network, such as user login, file access, configuration changes, or network traffic. Audit and system logs can help an incident response team to identify the source, scope, and impact of the phishing attack, as well as to collect evidence, trace the attack steps, and determine the root cause. Audit and system logs can also help the incident response team to evaluate the security posture and controls of the email server, and to recommend remediation and mitigation actions12 References: CompTIA Cloud Essentials+ Certification Exam Objectives3, CompTIA Cloud Essentials+ Study Guide, Chapter 7: Cloud Security, Cloud Essentials+ Certification Trainin