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.leads4pass.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

A company wants to migrate mission-critical applications to the cloud. In order for technicians to build, decommission, and perform other routine functions, which of the following cloud characteristics would BEST satisfy this business requirement?

A. Self-service

B. Elasticity

C. Broad network access

D. Availability

Correct Answer: A

Explanation: Self-service is one of the five essential characteristics of cloud computing, along with broad network access, resource pooling, rapid elasticity, and measured service1. Self-service enables cloud customers to provision and

manage cloud resources without requiring human interaction from the cloud service provider2. Self-service allows cloud customers to have more control, flexibility, and agility over their cloud environment, and to perform various tasks such as

building, decommissioning, scaling, monitoring, and configuring cloud resources according to their business needs and preferences3. Self- service is the best cloud characteristic to satisfy the business requirement of migrating mission-critical

applications to the cloud, as it would enable technicians to perform routine functions more efficiently and effectively, and to respond to changing demands and situations more quickly and dynamically.

Broad network access is another essential characteristic of cloud computing, which means that cloud resources are available over the network and can be accessed by diverse customer platforms, such as laptops, mobile phones, tablets,

etc1. Broad network access is an important feature of cloud computing, as it enables cloud customers to access their cloud resources anytime and anywhere, and to use different devices and methods to interact with the cloud. However,

broad network access is not the best cloud characteristic to satisfy the business requirement of migrating mission-critical applications to the cloud, as it does not directly relate to the ability of technicians to build, decommission, and perform

other routine functions on the cloud resources.

Elasticity is another essential characteristic of cloud computing, which means that cloud resources can be rapidly and dynamically scaled up or down according to the customer\\'s demand1. Elasticity is a key benefit of cloud computing, as it

enables cloud customers to optimize the utilization and performance of their cloud resources, and to pay only for what they use. However, elasticity is not the best cloud characteristic to satisfy the business requirement of migrating mission-

critical applications to the cloud, as it does not directly relate to the ability of technicians to build, decommission, and perform other routine functions on the cloud resources.

Availability is not one of the five essential characteristics of cloud computing, but rather a quality attribute or a non-

functional requirement of cloud computing. Availability refers to the degree to which a system or service is operational and

accessible when required4. Availability is a critical factor for cloud computing, especially for mission-critical applications, as it affects the reliability and continuity of the cloud service. However, availability is not the best cloud characteristic to

satisfy the business requirement of migrating mission-critical applications to the cloud, as it does not directly relate to the ability of technicians to build, decommission, and perform other routine functions on the cloud resources. References:

CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 1:

Cloud Computing Concepts, pages 11-15.

QUESTION 2

The legal team is required to share legal proceedings with an outside council. The team uses SaaS fileshares. Which of the following policies will BEST state the requirements for sharing information with external parties?

A. Information security policy

B. Communication policy

C. Resource management policy

D. Identity control policy

Correct Answer: A

Explanation: An information security policy is a document that defines the rules and guidelines for protecting the confidentiality, integrity, and availability of data and systems in an organization. It covers topics such as data classification, access control, encryption, backup, incident response, and compliance. An information security policy is essential for ensuring that data is shared securely with external parties, especially when using SaaS fileshares that may have different security standards and features than the organization\\'s own systems. A communication policy, a resource management policy, and an identity control policy are all related to information security, but they are not as comprehensive and specific as an information security policy. References: CompTIA Cloud Essentials+ CLO- 002 Study Guide, Chapter 4: Security in the Cloud, page 149.

QUESTION 3

Which of the following security concerns is BEST addressed by moving systems to the cloud?

A. Availability

B. Authentication

C. Confidentiality

D. Integrity

Correct Answer: A

Explanation: Availability is the security concern that is best addressed by moving systems to the cloud. Availability refers

to the ability of a system or service to be accessible and functional when needed by authorized users. Availability is one of the key benefits of cloud computing, as it provides high reliability, scalability, and performance for the cloud systems and services. Cloud providers use various techniques and technologies to ensure availability, such as: Redundancy: Cloud providers replicate the data and resources across multiple locations, such as regions, zones, or data centers, to prevent single points of failure and provide backup and failover capabilities in case of disasters or disruptions. Load balancing: Cloud providers distribute the workload and traffic among multiple servers or instances to optimize the resource utilization and performance of the cloud systems and services. Auto-scaling: Cloud providers automatically adjust the amount of resources allocated to the cloud systems and services based on the demand or usage, to prevent overloading or underutilizing the resources and ensure consistent availability. Monitoring and recovery: Cloud providers continuously monitor the health and status of the cloud systems and services, and provide alerts and notifications in case of any issues or incidents. Cloud providers also provide tools and methods to recover the cloud systems and services from failures or errors, such as snapshots, backups, or restore points. Availability is different from other security concerns, such as authentication, confidentiality, or integrity. Authentication is the process of verifying the identity and credentials of a user or system before granting access to the cloud systems and services. Confidentiality is the process of protecting the data and information from unauthorized access or disclosure, such as by using encryption, access control, or data masking. Integrity is the process of ensuring the data and information are accurate, complete, and consistent, and have not been modified or corrupted by unauthorized or malicious parties, such as by using hashing, digital signatures, or checksums. References: Cloud Computing Availability - CompTIA Cloud Essentials+ (CLO-002) Cert Guide, Cloud Security ?Amazon Web Services (AWS), Azure infrastructure availability - Azure security | Microsoft Learn, What is Cloud Security? Cloud Security Defined | IBM

QUESTION 4

A cloud systems administrator needs to migrate several corporate applications to a public cloud provider and decommission the internal hosting environment. This migration must be completed by the end of the month. Because these applications are internally developed to meet specific business accounting needs, the administrator cannot use an alternative application.

Which of the following BEST describes the approach the administrator should use?

A. Hybrid deployment

B. Phased migration

C. Lift and shift

D. Rip and replace

Correct Answer: C

Explanation: Lift and shift is a cloud migration strategy that involves moving an application or workload from one environment to another without making significant changes to its architecture, configuration, or code. This approach is suitable for applications that are not cloud-native, have complex dependencies, or have tight deadlines for migration. Lift and shift can help reduce the cost and risk of maintaining legacy infrastructure, improve scalability and availability, and leverage cloud services and features12. Hybrid deployment is a cloud deployment model that involves using both public and private cloud resources to deliver services and applications. This approach is suitable for applications that have varying performance, security, or compliance requirements, or that need to integrate with existing on-premises systems. Hybrid deployment can help optimize the use of resources, increase flexibility and agility, and balance trade-offs between cost and control34. Phased migration is a cloud migration strategy that involves moving an application or workload from one environment to another in stages or increments. This approach is suitable for applications that have modular components, low interdependencies, or high complexity. Phased migration can help reduce the impact of migration on business operations, test the functionality and performance of each component, and address any issues or challenges along the way . Rip and replace is a cloud migration strategy that involves discarding an application or workload from one environment and replacing it with a new one in another environment. This approach is suitable for applications that are outdated, incompatible, or inefficient, or that have high maintenance costs. Rip and replace can

help modernize the application architecture, design, and code, improve the user experience and functionality, and take advantage of cloud-native features and services . References: [CompTIA Cloud Essentials+ CLO-002 Study Guide], Chapter 3: Management and Technical Operations, Section 3.3: Cloud Migration, p. 123-125 [CompTIA Cloud+ CV0-003 Study Guide], Chapter 5: Deploying a Cloud Solution, Section 5.2: Cloud Migration, p. 241-244 [CompTIA Cloud Essentials+ CLO-002 Study Guide], Chapter 1: Cloud Concepts, Section 1.3: Cloud Deployment Models, p. 25-28 [CompTIA Cloud+ CV0-003 Study Guide], Chapter 1: Cloud Architecture and Design, Section 1.2: Cloud Deployment Models, p. 19-22 [CompTIA Cloud Essentials+ CLO-002 Study Guide], Chapter 3: Management and Technical Operations, Section 3.3: Cloud Migration, p. 125-126 [CompTIA Cloud+ CV0-003 Study Guide], Chapter 5: Deploying a Cloud Solution, Section 5.2: Cloud Migration, p. 244-245 [CompTIA Cloud Essentials+ CLO-002 Study Guide], Chapter 3: Management and Technical Operations, Section 3.3: Cloud Migration, p. 126-127 [CompTIA Cloud+ CV0-003 Study Guide], Chapter 5: Deploying a Cloud Solution, Section 5.2: Cloud Migration, p. 245-246 [CompTIA Cloud Essentials+ CLO-002 Study Guide], ISBN: 978-1-119-64768-9, Publisher: Wiley [CompTIA Cloud+ CV0-003 Study Guide], ISBN: 978-1-119-64767-2, Publisher: Wiley

QUESTION 5

A company recently launched the first version of an application. Based on customer feedback, the company identified the features that need to be incorporated in the next release. Which of the following will help the company understand the extra effort required to meet the customer requirements?

A. Statement of work

B. Baseline

C. Benchmark

D. Gap analysis

Correct Answer: D

Explanation: A gap analysis is the best option for helping the company understand the extra effort required to meet the customer requirements. A gap analysis is a step-by-step process for examining the current state of a system or process

and comparing it with the desired future state, and then identifying the gaps or differences between them1. A gap analysis can help to determine the scope, feasibility, and priority of the changes or improvements needed to bridge the gap and

achieve the desired outcomes2. A gap analysis can also help to estimate the resources, time, and cost involved in implementing the changes or improvements3.

A gap analysis is different from the other options listed in the question, which are not directly related to understanding the extra effort required to meet the customer requirements. A statement of work is a document that describes the scope,

objectives, deliverables, and terms and conditions of a project or contract4. A statement of work can help to define the expectations and responsibilities of the parties involved in the project or contract, but it does not provide a detailed analysis

of the current and future states of the system or process. A baseline is a reference point or standard that is used to measure the performance or progress of a project or process. A baseline can help to track the changes or deviations from the

original plan or goal, but it does not provide a comprehensive comparison of the current and future states of the system or process. A benchmark is a point of reference or criterion that is used to evaluate the quality or performance of a

system or process against a best practice or industry standard. A benchmark can help to identify the strengths and weaknesses of the system or process, but it does not provide a specific assessment of the gaps or differences between the

current and future states of the system or process.

References: What is Gap Analysis? Definition, Methodology and Examples, What is Gap Analysis? Gap Analysis: A How-To Guide with Examples | The Blueprint, What is Gap Analysis? Gap Analysis: Definition, Benefits, and How to Do It,

What is Gap Analysis? Statement of Work (SOW) - Project Management Docs, Statement of Work Definition. [What is a Baseline? - Definition from Techopedia], Baseline Definition. [What is Benchmarking? - Definition from Techopedia],

Benchmarking Definition.

QUESTION 6

A cloud administrator for an ISP identified a vulnerability in the software that controls all the firewall rules for a geographic area. To ensure the software upgrade is properly tested, approved, and applied, which of the following processes should the administrator follow?

A. Configuration management

B. Incident management

C. Resource management

D. Change management

Correct Answer: D

Explanation: Change management is an IT practice that aims to minimize disruptions to IT services while making changes to critical systems and services5. Change management involves planning, testing, approving, and implementing changes in a controlled and systematic manner6. A change is defined as adding, modifying, or removing anything that could have a direct or indirect effect on services5. In this case, the cloud administrator should follow the change management process to ensure that the software upgrade is properly tested, approved, and applied. References: Change management types, Atlassian Change management vs Configuration management, Virima

---

QUESTION 7

A business analyst is reviewing a software upgrade plan. The plan mentions the term "hash" value. Which of the following BEST represents what this term implies?

A. Non-repudiation of data

B. Integrity of data

C. Confidentiality of data

D. Availability of data

Correct Answer: B

Explanation: A hash value is a unique code that is generated by applying a mathematical algorithm to a piece of data. Hash values are used to ensure the integrity of data, which means that the data has not been altered or corrupted in any way. By comparing the hash value of the original data with the hash value of the received or stored data, one can verify that the data is identical and has not been tampered with. Hash values can also be used for digital signatures, which provide non-repudiation of data, meaning that the sender or owner of the data cannot deny its authenticity or origin. However, hash values alone do not provide confidentiality or availability of data, which are other aspects of data security. Confidentiality means that the data is protected from unauthorized access or disclosure, and availability means that the data is accessible and usable when needed. Hash values do not encrypt or hide the data, nor do they prevent data loss or downtime. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 5: Cloud Security Principles, Section 5.2: Data Security Concepts, Page 1471 and Ensuring Data Integrity with Hash Codes - .NET | Microsoft Learn

QUESTION 8

A human resources department is considering a SaaS-based human resources portal and requires a risk analysis.

Which of the following are requirements to consider? (Choose two.)

A. Support

B. Threats

C. Chargebacks

D. Vulnerabilities

E. Maintenance

F. Gap analysis

Correct Answer: BD

Explanation: A risk analysis is a process of identifying and assessing the potential threats and vulnerabilities that could affect the confidentiality, integrity, and availability of data and systems. A SaaS-based human resources portal is a cloud

service that provides access to human resources applications and data over the internet. The human resources department should consider the following requirements when conducting a risk analysis for this service:

Threats: These are the sources or events that could exploit the vulnerabilities of the service and cause harm to the data or systems. For example, malicious actors, natural disasters, power outages, network failures, etc. The human resources

department should identify the possible threats that could affect the SaaS service and evaluate their likelihood and impact.

Vulnerabilities: These are the weaknesses or gaps in the security of the service that could be exploited by the threats. For example, misconfigurations, outdated software, lack of encryption, insufficient authentication, etc. The human

resources department should identify the existing and potential vulnerabilities of the SaaS service and evaluate their severity and exposure. The other options are not relevant for a risk analysis:

Support: This is the assistance or guidance provided by the SaaS provider or a third party to the customers of the service. Support is not a requirement for a risk analysis, but rather a factor to consider when selecting or evaluating a SaaS

provider.

Chargebacks: These are the fees or penalties imposed by the SaaS provider to the customers for exceeding the agreed-upon service levels or usage limits. Chargebacks are not a requirement for a risk analysis, but rather a factor to consider

when negotiating or reviewing the service level agreement (SLA) with the SaaS provider.

Maintenance: This is the process of updating, repairing, or improving the service to ensure its functionality and performance. Maintenance is not a requirement for a risk analysis, but rather a responsibility of the SaaS provider that should be

specified in the SLA.

Gap analysis: This is a process of comparing the current state and the desired state of a system or a process and identifying the gaps or differences between them. Gap analysis is not a requirement for a risk analysis, but rather a tool to use

for planning or implementing improvements or changes.

References:

CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 2: Cloud Concepts and Models, Section 2.3: Cloud Security Concepts, p. 54-55 CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 4: Cloud Business Principles, Section

4.1: Cloud Service Agreements, p. 116-117

QUESTION 9

A company is deploying a new application and must decide whether to build an infrastructure to host the application on premises or in the cloud. Which of the following BEST describes the financial impact of hosting the application in the cloud?

A. The company\\'s capital expense will be less.

B. The company will be able to defer licensing costs.

C. The provider will share responsibility for the company\\'s monthly bill.

D. Monthly operating costs will remain constant despite usage.

Correct Answer: A

Explanation: Hosting the application in the cloud means that the company does not need to invest in building and maintaining an infrastructure to host the application on premises. This reduces the company\\'s capital expense, which is the money spent on acquiring or upgrading fixed assets, such as servers, storage, network, and software1. Instead, the company can pay for the cloud services that they use on a subscription or consumption basis, which is considered an operating expense, which is the money spent on the day-to-day running of the business1. Hosting the application in the cloud can also provide other financial benefits, such as lower energy costs, higher scalability, and faster time to market2. The other options are not correct, as they do not describe the financial impact of hosting the application in the cloud accurately. The company will not be able to defer licensing costs, as they will still need to pay for the software licenses that they use in the cloud, either as part of the cloud service fee or separately3. The provider will not share responsibility for the company\\'s monthly bill, as the company will be solely responsible for paying for the cloud services that they consume, based on the provider\\'s pricing model and terms of service4. Monthly operating costs will not

remain constant despite usage, as the cloud services are typically charged based on the amount of resources or features that the company uses, such as storage, bandwidth, CPU, memory, or transactions4. Therefore, the monthly operating costs will vary depending on the usage and demand of the application. References: Capital Expenditure (CapEx) Definition; Cloud Computing Benefits: 7 Key Advantages for Your Business; Cloud Computing Licensing: What You Need to Know; Cloud Computing Pricing Models: A Comprehensive Guide.

QUESTION 10

Which of the following is an example of outsourcing administration in the context of the cloud?

A. Managed services

B. Audit by a third party

C. Community support

D. Premium support

Correct Answer: A

Managed services are a type of outsourcing administration in the context of the cloud, where a third-party provider takes over the responsibility of managing and operating cloud services on behalf of the customer. Managed services can include various functions such as maintenance, monitoring, security, backup, recovery, and support. Managed services can help customers to reduce costs, improve performance, enhance security, and focus on their core business. Managed services are different from other types of support, such as audit, community, or premium support, which do not involve the transfer of control or ownership of cloud services to a third-party provider. References: CompTIA Cloud Essentials+ Certification Exam Objectives1, CompTIA Cloud Essentials+ Study Guide, Chapter 2: Business Principles of Cloud Environments2, Outsourcing Cloud Administration

QUESTION 11

Transferring all of a customer\\'s on-premises data and virtual machines to an appliance, and then shipping it to a cloud provider is a technique used in a:

A. phased migration approach.

B. replatforming migration approach.

C. rip and replace migration approach.

D. lift and shift migration approach.

Correct Answer: D

Explanation: A lift and shift migration approach, also known as rehosting, is a cloud migration strategy where applications and infrastructure are moved from one environment to another without making substantial changes to the underlying architecture123. This approach can be faster, cheaper, and less risky than other migration strategies, as it does not require extensive redesign or reconfiguration of the applications. However, it may also limit the ability to leverage the native features and benefits of the cloud platform, such as scalability, elasticity, and performance1245. One of the challenges of a lift and shift migration is transferring large amounts of data and virtual machines over the network, which can be time-consuming, costly, and prone to errors. To overcome this challenge, some cloud providers offer a technique where the customer can transfer all of their on-premises data and virtual machines to an appliance, such as a physical storage device or a server, and then ship it to the cloud provider. The cloud provider then uploads

the data and virtual machines to the cloud platform, where they can be accessed by the customer12. This technique can reduce the network bandwidth and latency issues, as well as the security risks, associated with transferring data over the internet. However, it may also introduce additional costs and delays for shipping and handling the appliance, as well as the risk of damage or loss during transit2. Therefore, transferring all of a customer\\'s on-premises data and virtual machines to an appliance, and then shipping it to a cloud provider is a technique used in a lift and shift migration approach. References:

1: Lift and Shift: An Essential Guide | IBM

2: What Is Lift and Shift? | 5 Strategies to Consider | NetApp

3: What Is Lift and Shift Migration? | Pure Storage

4: Lift and Shift: Business Benefits, Planning and Execution - NetApp

5: Lift and Shift Cloud Migration: Benefits, Disadvantages and Use Cases ...

QUESTION 12

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 13

A report identified that several of a company\\'s SaaS applications are against corporate policy. Which of the following is the MOST likely reason for this issue?

A. Shadow IT

B. Sensitive data

C. Encryption

D. Vendor lock-in

Correct Answer: A

Explanation: Shadow IT refers to any IT resource used by employees or end users without the IT department\\'s approval or oversight. This can include SaaS applications that are not aligned with corporate policy or governance. Employees or

teams may adopt shadow IT for convenience, productivity, or innovation, but it can also pose significant security risks and compliance concerns. Therefore, it is important for IT organizations to have visibility and control over the IT devices,

software, and services used on the enterprise network. References: : CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 1, page 14 :

CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 1, page 15 : CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 1, page 16Top of Form Bottom of Form

---

QUESTION 14

A company would like to improve its current DR plan with an emphasis on high availability. Which of the following metrics should the company focus on?

A. MTTR

B. RTO

C. QoS

D. RPO

Correct Answer: B

Explanation: A company that would like to improve its current disaster recovery (DR) plan with an emphasis on high availability should focus on the metrics of recovery time objective (RTO) and recovery point objective (RPO). RTO is the maximum duration of time that a system or service can be unavailable after a disaster or disruption before the business suffers unacceptable consequences. RPO is the maximum amount of data loss that a system or service can tolerate in a disaster or disruption before the business suffers unacceptable consequences. Both RTO and RPO measure the impact of downtime on the business and help determine the appropriate recovery strategies and solutions. High availability requires low RTO and RPO values, which means that the system or service should be restored quickly and with minimal data loss in case of a disaster or disruption. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 6: Cloud Operations Principles, Section 6.2: Disaster Recovery Concepts, Page 1791 and Service Availability: Calculations and Metrics, Five 9s, and Best Practices ?BMC Software | Blogs

QUESTION 15

Which of the following aspects of cloud design enables a customer to continue doing business after a major data center incident?

A. Replication

B. Disaster recovery

C. Scalability

D. Autoscaling

Correct Answer: B

Explanation: Disaster recovery is the aspect of cloud design that enables a customer to continue doing business after a major data center incident. Disaster recovery is the process of restoring and resuming the normal operations of IT systems and services after a disaster, such as a natural calamity, a cyberattack, a power outage, or a human error1. Disaster recovery involves creating and storing backup copies of critical data and workloads in a secondary location or multiple locations, which are known as disaster recovery sites. A disaster recovery site can be a physical data center or a cloud-based platform2. Disaster recovery in cloud computing offers many advantages, such as34: Cost-effectiveness: Cloud disaster recovery eliminates the need to invest in and maintain expensive hardware, software, and facilities for the secondary site. Cloud disaster recovery also allows customers to pay only for the resources they use, and to scale up or down as needed. Reliability: Cloud disaster recovery ensures that the backup data and workloads are always available and accessible from any location and device. Cloud disaster recovery also leverages the security, performance, and redundancy features of the cloud provider to protect the data and workloads from corruption, loss, or theft. Flexibility: Cloud disaster recovery enables customers to choose from different cloud service models and deployment options, such as public, private, hybrid, or multicloud, depending on their business needs and preferences. Cloud disaster recovery also allows customers to customize and automate their recovery plans and policies, such as recovery point objective (RPO) and recovery time objective (RTO). References: What is Disaster Recovery and Why Is It Important? - Google Cloud, What is Disaster Recovery and Why Is It Important? Disaster Recovery In Cloud

Computing: What, How, And Why - NAKIVO, Cloud Disaster Recovery vs. Traditional Disaster Recovery. Benefits of Disaster Recovery in Cloud Computing - NAKIVO, Benefits of Cloud- Based Disaster Recovery. Cloud Disaster Recovery (Cloud DR): What It Is and How It Works

-phoenixNAP, Benefits of Cloud Disaster Recovery.