CCSP^{Q&As}

Cloud Security

Pass ISC CCSP Exam with 100% Guarantee

QUESTION 1

Which cloud storage type resembles a virtual hard drive and can be utilized in the same manner and with the same type of features and capabilities?

A. Volume

B. Unstructured

C. Structured

D. Object

Correct Answer: A

Volume storage is allocated and mounted as a virtual hard drive within IaaS implementations, and it can be maintained and used the same way a traditional file system can. Object storage uses a flat structure on remote services that is accessed via opaque descriptors, structured storage resembles database storage, and unstructured storage is used to hold auxiliary files in conjunction with applications hosted within a PaaS implementation.

QUESTION 2

Which cloud storage type is typically used to house virtual machine images that are used throughout the environment?

A. Structured

B. Unstructured

C. Volume

D. Object

Correct Answer: D

Object storage is typically used to house virtual machine images because it is independent from other systems and is focused solely on storage. It is also the most appropriate for handling large individual files. Volume storage, because it is allocated to a specific host, would not be appropriate for the storing of virtual images. Structured and unstructured are storage types specific to PaaS and would not be used for storing items used throughout a cloud environment.

QUESTION 3

What controls the formatting and security settings of a volume storage system within a cloud environment?

A. Management plane

B. SAN host controller

C. Hypervisor

D. Operating system of the host

Correct Answer: D

Once a storage LUN is allocated to a virtual machine, the operating system of that virtual machine will format, manage, and control the file system and security of the data on that LUN.

QUESTION 4

Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like:

A. Ransomware

B. Syn floods

C. XSS and SQL injection

D. Password cracking

Correct Answer: C

WAFs detect how the application interacts with the environment, so they are optimal for detecting and refuting things like SQL injection and XSS. Password cracking, syn floods, and ransomware usually aren\\'t taking place in the same way as injection and XSS, and they are better addressed with controls at the router and through the use of HIDS, NIDS, and antimalware tools.

QUESTION 5

Which of the following security measures done at the network layer in a traditional data center are also applicable to a cloud environment?

A. Dedicated switches

B. Trust zones

C. Redundant network circuits

D. Direct connections

Correct Answer: B

Trust zones can be implemented to separate systems or tiers along logical lines for great security and access controls. Each zone can then have its own security controls and monitoring based on its particular needs.

QUESTION 6

Which data sanitation method is also commonly referred to as "zeroing"?

A. Overwriting

B. Nullification

C. Blanking

D. Deleting

Correct Answer: A

The zeroing of data--or the writing of null values or arbitrary data to ensure deletion has been fully completed--is officially referred to as overwriting. Nullification, deleting, and blanking are provided as distractor terms.

QUESTION 7

What is used for local, physical access to hardware within a data center?

A. SSH

B. KVM

C. VPN

D. RDP

Correct Answer: B

Local, physical access in a data center is done via KVM (keyboard, video, mouse) switches.

QUESTION 8

Which of the following terms is NOT a commonly used category of risk acceptance?

A. Moderate

B. Critical

C. Minimal

D. Accepted

Correct Answer: D

Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

QUESTION 9

What changes are necessary to application code in order to implement DNSSEC?

A. Adding encryption modules

B. Implementing certificate validations

C. Additional DNS lookups

D. No changes are needed.

Correct Answer: D

To implement DNSSEC, no additional changes are needed to applications or their code because the integrity checks are all performed at the system level.

QUESTION 10

Which of the following is NOT considered a type of data loss?

A. Data corruption

B. Stolen by hackers

C. Accidental deletion

D. Lost or destroyed encryption keys

Correct Answer: B

The exposure of data by hackers is considered a data breach. Data loss focuses on the data availability rather than security. Data loss occurs when data becomes lost, unavailable, or destroyed, when it should not have been.

QUESTION 11

Which of the following best describes a sandbox?

A. An isolated space where untested code and experimentation can safely occur separate from the production environment.

B. A space where you can safely execute malicious code to see what it does.

C. An isolated space where transactions are protected from malicious software

D. An isolated space where untested code and experimentation can safely occur within the production environment.

Correct Answer: A

Options C and B are also correct, but A is more general and incorporates them both. D is incorrect, because sandboxing does not take place in the production environment.

QUESTION 12

What are SOC 1/SOC 2/SOC 3?

A. Audit reports

B. Risk management frameworks

C. Access controls

D. Software developments

Correct Answer: A

An SOC 1 is a report on controls at a service organization that may be relevant to a user entity\\'s internal control over financial reporting. An SOC 2 report is based on the existing SysTrust and WebTrust principles. The purpose of an SOC 2 report is to evaluate an organization\\'s information systems relevant to security, availability, processing integrity, confidentiality, or privacy. An SOC 3 report is also based on the existing SysTrust and WebTrust principles, like a SOC 2 report. The difference is that the SOC 3 report does not detail the testing performed.

QUESTION 13

With an application hosted in a cloud environment, who could be the recipient of an eDiscovery order?

A. Users

B. Both the cloud provider and cloud customer

C. The cloud customer

D. The cloud provider

Correct Answer: B

Either the cloud customer or the cloud provider could receive an eDiscovery order, and in almost all circumstances they would need to work together to ensure compliance.

QUESTION 14

What strategy involves replacing sensitive data with opaque values, usually with a means of mapping it back to the original value?

A. Masking

B. Anonymization

C. Tokenization

D. Obfuscation

Correct Answer: C

Tokenization is the practice of utilizing a random and opaque "token" value in data to replace what otherwise would be a sensitive or protected data object. The token value is usually generated by the application with a means to map it back to the actual real value, and then the token value is placed in the data set with the same formatting and requirements of the actual real value so that the application can continue to function without different modifications or code changes.

QUESTION 15

With a cloud service category where the cloud customer is provided a full application framework into which to deploy their code and services, which storage types are MOST likely to be available to them?

A. Structured and unstructured

B. Structured and hierarchical

C. Volume and database

D. Volume and object

Correct Answer: A

The question is describing the Platform as a Service (PaaS) cloud offering, and as such, structured and unstructured storage types will be available to the customer. Volume and object are storage types associated with IaaS, and although the other answers present similar-sounding storage types, they are a mix of real and fake names.