EMC

Exam E10-001

Information Storage and Management Exam Version 2

Version: 18.0

[Total Questions: 344]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	144

Topic 1, Volume A

**Question No : 1 - (Topic 1)**

What describes a hybrid cloud?

A. Composed of distinct clouds that are bound together by standardized or proprietary technology
B. Composed of two or more distinct data centers that enable data and application portability
C. Combination of two distinct cloud infrastructures (on-premise and externally-hosted) that are managed together
D. Combination of a private cloud and a public cloud that are owned, managed, and operated by a single organization

Answer: A

Explanation:

Hybrid Cloud
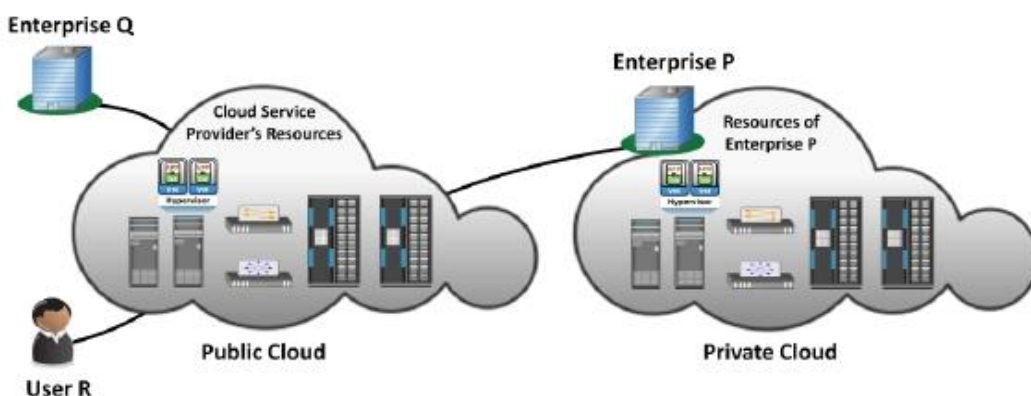
In a hybrid cloud model, the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (example, cloud bursting for load balancing between clouds).

The hybrid model allows an organization to deploy less critical applications and data to the public cloud, leveraging the scalability and cost-effectiveness of the public cloud. The organization's mission-critical applications and data remain on the private cloud that provides greater security.
EMC E10-001 Student Resource Guide. Module 13: Cloud Computing

---

Question No : 2 - (Topic 1)

Which data center requirement refers to applying mechanisms that ensure data is stored and retrieved as it was received?

A. Integrity
B. Availability
C. Security
D. Performance

Answer: A

Explanation:

Information Security Framework

The basic information security framework is built to achieve four security goals, confidentiality, integrity, and availability (CIA) along with accountability. This framework incorporates all security standards, procedures and controls, required to mitigate threats in the storage infrastructure environment.

Confidentiality: Provides the required secrecy of information and ensures that only authorized users have access to data. This requires authentication of users who need to access information. Data in transit (data transmitted over cables) and data at rest (data residing on a primary storage, backup media, or in the archives) can be encrypted to maintain its confidentiality. In addition to restricting unauthorized users from accessing information, confidentiality also requires to implement traffic flow protection measures as part of the security protocol. These protection measures generally include hiding source and destination addresses, frequency of data being sent, and amount of data sent.

Integrity: Ensures that the information is unaltered . Ensuring integrity requires detection and protection against unauthorized alteration or deletion of information. Ensuring integrity stipulate measures such as error detection and correction for both data and systems.

Availability: This ensures that authorized users have reliable and timely access to systems, data and applications residing on these systems. Availability requires protection against unauthorized deletion of data and denial of service. Availability also implies that sufficient resources are available to provide a service.

Accountability: Refers to accounting for all the events and operations that take place in the data center infrastructure. The accountability service maintains a log of events that can be

---

audited or traced later for the purpose of security.

EMC E10-001 Student Resource Guide. Module 14: Securing the Storage Infrastructure

---

Question No : 3 - (Topic 1)

In an FC SAN environment, what is a benefit of zoning?

A. Restricts RSCN traffic
B. Isolates fabric services
C. Enables online volume expansion
D. Provides non-disruptive data migration

Answer: A

Explanation:

Zoning

Zoning is an FC switch function that enables node ports within the fabric to be logically segmented into groups and communicate with each other within the group.

Whenever a change takes place in the name server database, the fabric controller sends a Registered State Change Notification (RSCN) to all the nodes impacted by the change. If zoning is not configured, the fabric controller sends an RSCN to all the nodes in the fabric. Involving the nodes that are not impacted by the change results in increased fabric-management traffic. For a large fabric, the amount of FC traffic generated due to this process can be significant and might impact the host-to-storage data traffic. Zoning helps to limit the number of RSCNs in a fabric. In the presence of zoning, a fabric sends the RSCN to only those nodes in a zone where the change has occurred.

EMC E10-001 Student Resource Guide. Module 5: Fibre Channel Storage Area Network (FC SAN)
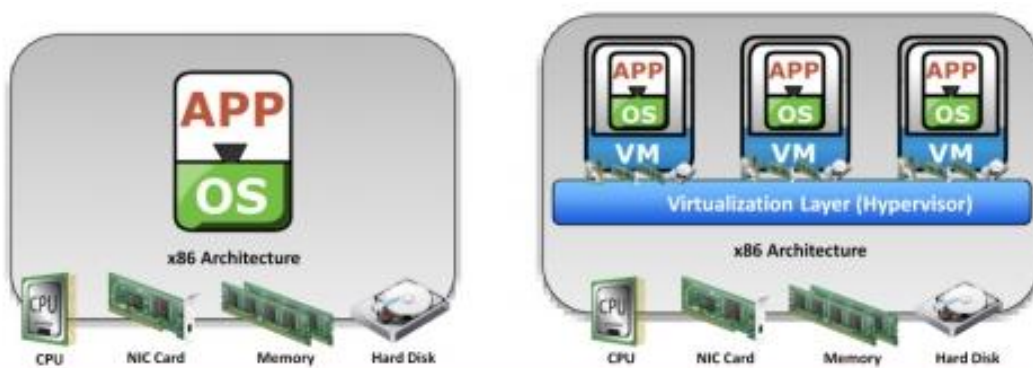

Question No : 4 - (Topic 1)

5

What is a key benefit of virtualization?

A. Improved resource utilization
B. Improved performance
C. Enhanced interoperability
D. Unlimited resource scaling

Answer: A

Explanation:

Need for Compute Virtualization

Before Virtualization	After Virtualization
• Runs single operating system (OS) per machine at a time	• Runs multiple operating systems (OSs) per physical machine concurrently
• Couples s/w and h/w tightly	• Makes OS and applications h/w independent
• May create conflicts when multiple applications run on the same machine	• Isolates VM from each other, hence, no conflict
• Underutilizes resources	• Improves resource utilization
• Is inflexible and expensive	• Offers flexible infrastructure at low cost

EMC E10-001 Student Resource Guide. Module 2: Data Center Environment

Question No : 5 - (Topic 1)

Which NAS implementation consolidates file-based and block-based access on a single storage platform?

A. Unified
B. Scale-out
C. Gateway

D. Integrated

Answer: A

Explanation:

NAS Implementation - Unified NAS

The unified NAS consolidates NAS-based and SAN-based data access within a unified storage platform and provides a unified management interface for managing both the environments.

Unified NAS performs file serving and storing of file data, along with providing access to block-level data. It supports both CIFS and NFS protocols for file access and iSCSI and FC protocols for block level access. Due to consolidation of NAS-based and SAN-based access on a single storage platform, unified NAS reduces an organization's infrastructure and management costs.

A unified NAS contains one or more NAS heads and storage in a single system. NAS heads are connected to the storage controllers (SCs), which provide access to the storage. These storage controllers also provide connectivity to iSCSI and FC hosts. The storage may consist of different drive types, such as SAS, ATA, FC, and flash drives, to meet different workload requirements.

EMC E10-001 Student Resource Guide. Module 7: Network-Attached Storage (NAS)

Question No : 6 - (Topic 1)

What are the key components of an intelligent storage system?

A. Front-end, cache, back-end, and physical disks
B. Host, connectivity, back-end, and storage array
C. Switch, ports, back-end, and physical disks
D. Host, LUNs, cache, and physical disks

Answer: A

Question No : 7 - (Topic 1)

What is a characteristic of an FC-AL implementation?

A. Reserves one address for connecting an FC-SW port
B. Supports connectivity up to 15 million nodes
C. Devices can be added and removed dynamically without any impact
D. Requires at least one connectivity device

Answer: A

Question No : 8 - (Topic 1)

Click on the calculator icon in the upper left corner.

A stripe depth of 64 KB has been assigned to a five-disk RAID 0 set. What is the stripe size?

A. 64 KB
B. 128 KB
C. 256 KB
D. 320 KB

Answer: D

Question No : 9 - (Topic 1)

What describes a repudiation attack?

A. An attempt to compromise accountability goals of the security
B. Stealing a private key to decrypt the data-in-transit
C. Unauthorized access to information to compromise confidentiality
D. A series of repetitive attacks to the physical information infrastructure

Answer: A

Question No : 10 - (Topic 1)

What are the two mechanisms that can be employed to address threats of user identity

spoofing?

A. User authentication and user authorization

B. Access Control Lists (ACLs) and access control to storage objects

C. Access control to storage objects and auditing

D. User authentication and Information Rights Management (IRM)

Answer: A

Question No : 11 - (Topic 1)

What is a benefit of cloud computing over traditional computing?

A. Reduces the time to provision and deploy new applications

B. Eliminates consumer's IT operational expenditure

C. Enables the use of proprietary APIs to access IT resources

D. Lowers migration cost and prevents vendor lock-in

Answer: A

Explanation:

Benefits of Cloud Computing

Cloud computing offers the following key benefits:

- ✐ Reduced IT cost: Cloud services can be purchased based on pay-per-use or subscription pricing.
- ✐ This reduces or eliminates consumer's IT capital expenditure (CAPEX).

Business agility:

- ✐ Cloud computing provides the capability to allocate and scale computing capacity quickly.
- ✐ Cloud can reduce the time required to provision and deploy new applications and services from months to minutes.
- ✐ This enables businesses to respond more quickly to market changes and reduce time-to-market.

Flexible scaling: Cloud computing enables consumers to scale up, scale down, scale out, or scale in the demand for computing resources easily. Consumers can unilaterally and automatically scale computing resources without any interaction with cloud service providers. The flexible service provisioning capability of cloud often provides a sense of unlimited scalability to the cloud service consumers.

• High availability: Cloud computing has the ability to ensure resource availability at varying levels depending on the consumer's policy and priority. Redundant infrastructure components (servers, network paths, and storage equipment, along with clustered

software) enable fault tolerance for cloud deployments. These techniques can encompass multiple data centers located in different geographic regions, which prevents data unavailability due to regional failures.
EMC E10-001 Student Resource Guide. Module 13: Cloud Computing

Question No : 12 - (Topic 1)

What is needed to perform a non-disruptive migration of virtual machines (VMs) between hypervisors?

A. Hypervisors must have access to the same storage volume
B. Physical machines running hypervisors must have the same configuration
C. Hypervisors must be running within the same physical machine
D. Both hypervisors must have the same IP address

Answer: A

Explanation:

VM Migration: Hypervisor-to-Hypervisor
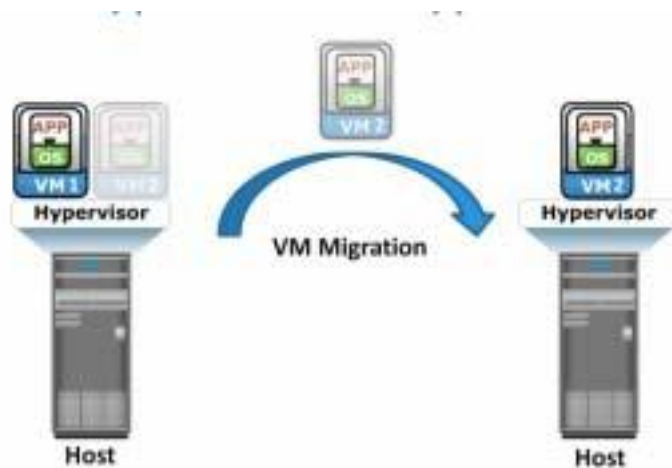
In hypervisor-to-hypervisor VM migration, the entire active state of a VM is moved from one hypervisor to another. This method involves copying the contents of virtual machine memory from the source hypervisor to the target and then transferring the control of the VM's disk files to the target hypervisor. Because the virtual disks of the VMs are not migrated, this technique requires both source and target hypervisor access to the same storage.