E10-001 Q&As

Information Storage and Management Exam Version 2

Pass EMC E10-001 Exam with 100% Guarantee

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

https://www.geekcert.com/E10-001.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An application generates 4200 small random I/Os at peak workloads with a read/write ratio of

2:1.

What is the disk load at peak activity for a RAID 5 configuration?

A.

2,800

B.

5,600

C.

8,400

D.

11,200

Correct Answer: C

QUESTION 2

Which functionality is offered by user access management software?

A. Provides a user interface to browse the service catalog and request cloud services

B. Enables a user to create VMs and allocate them to CPU, memory, and storage capacity

C. Provides a user interface to view a consolidated view of existing physical and virtual infrastructures across data centers

D. Allows a user to monitor performance, capacity, and availability of physical and virtual resources centrally

Correct Answer: A

QUESTION 3

How can an organization reduce vulnerabilities in their environment?

A. Minimize the attack surface and maximize the work factor

B. Maximize the attack surface and minimize the work factor

C. Minimize both the attack surface and work factor

D. Maximize both the attack surface and work factor

Correct Answer: A

Vulnerabilities The paths that provide access to information are vulnerable to potential attacks. Each of the paths may contain various access points, which provide different levels of access to the storage resources. It is important to implement adequate security controls at all the access points on an access path. Implementing security controls at each access point of every access path is known as defense in depth. Defense in depth recommends using multiple security measures to reduce the risk of security threats if one component of the protection is compromised. It is also known as a "layered approach to security". Because there are multiple measures for security at different levels and defense in depth gives additional time to detect and respond to an attack. This can reduce the scope or impact of a security breach.

Attack surface, attack vector, and work factor are the three factors to consider when assessing the extent to which an environment is vulnerable to security threats. Attack surface refers to the various entry points that an attacker can use to launch an attack. Each component of a storage network is a source of potential vulnerability. An attacker can use all the external interfaces supported by that component, such as the hardware and the management interfaces, to execute various attacks. These interfaces form the attack surface for the attacker. Even unused network services, if enabled, can become a part of the attack surface.

An attack vector is a step or a series of steps necessary to complete an attack. For example, an attacker might exploit a bug in the management interface to execute a snoop attack whereby the attacker can modify the configuration of the storage device to allow the traffic to be accessed from one more host. This redirected traffic can be used to snoop the data in transit. Work factor refers to the amount of time and effort required to exploit an attack vector. For example, if attackers attempt to retrieve sensitive information, they consider the time and effort that would be required for executing an attack on a database. This may include determining privileged accounts, determining the database schema, and writing SQL queries. Instead, based on the work factor, they may consider a less effort-intensive way to exploit the storage array by attaching to it directly and reading from the raw disk blocks.

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

QUESTION 4

What is prevented using RAID technology?

A. Data loss

B. Host Bus Adapter failures

C. Security breach

D. Switch failure

Correct Answer: A

Today\\'s data centers house hundreds of disk drives in their storage infrastructure. Disk drives are inherently susceptible to failures due to mechanical wear and tear and other environmental factors, which could result in data loss. The greater the number of disk drives in a storage array, the greater the probability of a disk failure in the array. For example, consider a storage array of 100 disk drives, each with an average life expectancy of 750,000 hours. The average life expectancy of this collection in the array, therefore, is 750,000/100 or 7,500 hours. This means that a disk drive in this array is likely to fail at least once in 7,500 hours. RAID is an enabling technology that leverages multiple drives as part of a set that provides data protection against drive failures. In general, RAID implementations also improve the storage system performance by serving I/Os from multiple disks simultaneously. Modern arrays with flash drives also benefit in terms of protection and performance by using RAID.

EMC E10-001 Student Resource Guide. Module 3: Data Protection - RAID

QUESTION 5

Which security feature is available in a Microsoft Windows file sharing environment using Network Attached Storage?

A. Windows Security Identifier (SID)

B. Discretionary Access Control Lists (DACL)

C. Operating System Control Lists (OSCL)

D. Global Unique Identifier (GUID)

Correct Answer: B

NAS File Sharing: Windows ACLs Windows supports two types of ACLs: discretionary access control lists (DACLs) and system access control lists (SACLs). The DACL, commonly referred to as the ACL, that determines access control. The SACL determines what accesses need to be audited if auditing is enabled.

In addition to these ACLs, Windows also supports the concept of object ownership. The owner of an object has hard-coded rights to that object, and these rights do not need to be explicitly granted in the SACL. The owner, SACL, and DACL are all statically held as attributes of each object. Windows also offers the functionality to inherit permissions, which allows the child objects existing within a parent object to automatically inherit the ACLs of the parent object.

ACLs are also applied to directory objects known as security identifiers (SIDs). These are automatically generated by a Windows server or domain when a user or group is created, and they are abstracted from the user. In this way, though a user may identify his login ID as "User1," it is simply a textual representation of the true SID, which is used by the underlying operating system. Internal processes in Windows refer to an account\\'s SID rather than the account\\'s username or group name while granting access to an object. ACLs are set by using the standard Windows Explorer GUI but can also be configured with CLI commands or other third- party tools. EMC E10-001 Student Resource Guide. Module 14: Securing the Storage Infrastructure