CV0-003 Q&As

CompTIA Cloud+ Certification

QUESTION 1

The administrator of virtual infrastructure needs to provision block storage for a virtual machine on which a business critical application will be installed. Considering performance, which of the following describes how the administrator should attach the storage to the VM?

A. Using NFS

B. Using CIFS

C. Using IPv6

D. Using iSCSI

Correct Answer: D

http://www.techrepublic.com/blog/the-enterprise-cloud/block-level-storage-vs-file-level-storage-a-comparison/

QUESTION 2

A security audit related to confidentiality controls found the following transactions occurring in the system:

GET http://gateway.securetransaction.com/privileged/api/v1/changeResource?id=123anduser=277

Which of the following solutions will solve the audit finding?

A. Using a TLS-protected API endpoint

B. Implementing a software firewall

C. Deploying a HIDS on each system

D. Implementing a Layer 4 load balancer

Correct Answer: A

Reference: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet .html

QUESTION 3

A system administrator has provisioned a new web server. Which of the following, in combination, form the best practice to secure the server\\'s OS? (Choose three.)

A. Install TLS certificates on the server.

B. Forward port 80 traffic to port 443.

C. Disable TLS 1.0/1.1 and SSL.

D. Disable password authentication.

E. Enable SSH key access only.

F. Provision the server in a separate VPC.

G. Disable the superuser/administrator account.

H. Restrict access on port 22 to the IP address of the administrator\\'s workstation.

Correct Answer: ADE

These are the best practices to secure the OS of a new web server that has been provisioned in a cloud environment: Install TLS certificates on the server: TLS (Transport Layer Security) certificates are digital documents that contain information such as identity, public key, expiration date, etc., that can be used to prove one\\'s identity and establish secure communication over a network. Installing TLS certificates on the web server can encrypt and secure web traffic between the server and the clients, as well as prevent spoofing or impersonation attacks. Disable password authentication: Password authentication is a method of verifying and authenticating users or devices based on passwords or other credentials. Password authentication can be insecure or vulnerable to attacks such as brute force, dictionary, phishing, etc., especially if passwords are weak, reused, or compromised. Disabling password authentication can enhance security by preventing unauthorized or malicious access to the web server using passwords. Enable SSH key access only: SSH key access is a method of verifying and authenticating users or devices based on digital keys issued by a trusted authority. SSH key access can provide more security and convenience than password authentication, as it does not require users or devices to remember or enter passwords every time they access the web server. Enabling SSH key access only can ensure that only authorized or trusted users or devices can access the web server using keys.

QUESTION 4

A systems administrator is securing a new email system for a large corporation. The administrator wants to ensure private corporate information is not emailed to external users. Which of the following would be MOST useful to accomplish this task?

A. DLP

B. EDR

C. DNSSEC

D. SPF

Correct Answer: A

The most useful tool to prevent private corporate information from being emailed to external users is data loss prevention (DLP). DLP is a type of security solution that monitors and controls the flow of data in and out of a system or network. It can detect and prevent unauthorized access, transmission, or leakage of sensitive data, such as personal information, financial records, or intellectual property. DLP can also enforce encryption, masking, or deletion of sensitive data to protect its confidentiality. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 2.0 Security, Objective 2.5 Given a scenario, apply data security techniques in the cloud.

QUESTION 5

A company has two identical environments (X and Y) running its core business application. As part of an upgrade, the X environment is patched/upgraded and tested while the Y environment is still serving the consumer workloads. Upon successful testing of the X environment, all workload is sent to this environment, and the Y environment is then upgraded before both environments start to manage the workloads. Which of the following upgrade methods is being used?

A. Active-passive

B. Canary

C. Development/production

D. Blue-green

Correct Answer: D

Reference: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.managing.bgdeploy.html