[Jul 24, 2024 Free CompTIA Server+ SK0-005 Official Cert Guide PDF Download [Q189-Q203

[Jul 24, 2024] Free CompTIA Server+ SK0-005 Official Cert Guide PDF Download
CompTIA SK0-005 Official Cert Guide PDF

Q189. A company is running an application on a file server. A security scan reports the application has a known vulnerability. Which of the following would be the company’s BEST course of action?
* Upgrade the application package
* Tighten the rules on the firewall
* Install antivirus software
* Patch the server OS

The best course of action for the company is to upgrade the application package to fix the known vulnerability.

A vulnerability is a weakness or flaw in an application that can be exploited by an attacker to compromise the security or functionality of the system. Upgrading the application package means installing a newer version of the application that has patched or resolved the vulnerability. This way, the company can prevent potential attacks that may exploit the vulnerability and cause damage or loss.

Q190. Which of the following BEST describes the concept of right to downgrade?

* It allows for the return of a new OS license if the newer OS is not compatible with the currently installed software and is returning to the previously used OS
* It allows a server to run on fewer resources than what is outlined in the minimum requirements document without purchasing a license
* It allows for a previous version of an OS to be deployed in a test environment for each current license that is purchased
* It allows a previous version of an OS to be installed and covered by the same license as the newer version

The concept of right to downgrade allows a previous version of an OS to be installed and covered by the same license as the newer version. For example, if a customer has a license for Windows 10 Pro, they can choose to install Windows 8.1 Pro or Windows 7 Professional instead and still be compliant with the license terms. Downgrade rights are granted by Microsoft for certain products and programs, such as Windows and Windows Server software acquired through Commercial Licensing, OEM, or retail channels. Downgrade rights are intended to provide customers with flexibility and compatibility when using Microsoft software.

Q191. A server administrator is swapping out the GPU card inside a server. Which of the following actions should the administrator take FIRST?
* Inspect the GPU that is being installed.
* Ensure the GPU meets HCL guidelines.
* Shut down the server.
* Disconnect the power from the rack.

Q192. A server administrator is exporting Windows system files before patching and saving them to the following location:

server1ITDept

Which of the following is a storage protocol that the administrator is MOST likely using to save this data?
* eSATA
* FCoE
* CIFS
* SAS

Explanation

The storage protocol that the administrator is most likely using to save data to the location server1ITDept is CIFS. CIFS (Common Internet File System) is a protocol that allows file sharing and remote access over a network. CIFS is based on SMB (Server Message Block), which is a protocol that enables communication between devices on a network. CIFS uses UNC (Universal Naming Convention) paths to identify network resources, such as files or folders. A UNC path has the format servernamesharenamepathfilename. In this case, server1 is the name of the server, ITDept is the name of the shared folder, and is the path within the shared folder.

Q193. A hardware technician is installing 19 1U servers in a 42 the following unit sizes should be allocated per server?
* 1U
* 2U
* 3U
* 4U

1U stands for one unit and it is a standard unit of measurement for rack-mounted servers. It is equal to 1.75 inches (4.45 cm) in height. A 42U rack can accommodate 42 1U servers or a combination of servers with different unit sizes. Therefore, the unit size per server should be 1U if there are 19 1U servers in a 42U rack. Reference:
https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 1.2)

Q194. Which of the following tools will analyze network logs in real time to report on suspicious log events?
* Syslog
* DLP

* SIEM
* HIPS

Explanation

SIEM is the tool that will analyze network logs in real time to report on suspicious log events. SIEM stands for Security Information and Event Management, which is a software solution that collects, analyzes, and correlates log data from various sources, such as servers, firewalls, routers, antivirus software, etc. SIEM can detect anomalies, patterns, trends, and threats in the log data and generate alerts or reports for security monitoring and incident response. SIEM can also provide historical analysis and compliance reporting for audit purposes.

Q195. Which of the following BEST measures now much downtime an organization can tolerate Curing an unplanned outage?

* SLA
* BIA
* RTO
* MTTR

RTO (Recovery Time Objective) is a measure of how much downtime an organization can tolerate during an unplanned outage. It is the maximum time allowed for restoring normal operations after a disaster. RTO is one of the key metrics for disaster recovery planning and testing. SLA (Service Level Agreement) is a contract that defines the expected level of service and performance between a provider and a customer. BIA (Business Impact Analysis) is a process that identifies and evaluates the potential effects of a disaster on critical business functions and processes. MTTR (Mean Time To Repair) is a measure of how long it takes to fix a failed component or system. Reference: https://parachute.cloud/rto-vs-rpo/
https://www.techopedia.com/definition/13622/service-level-agreement-sla
https://www.techopedia.com/definition/1032/business-impact-analysis-bia
https://www.techopedia.com/definition/8239/mean-time-to-repair-mttr

Q196. A server technician is deploying a server with eight hard drives. The server specifications call for a RAID configuration that can handle up to two drive failures but also allow for the least amount of drive space lost to RAID overhead. Which of the following RAID levels should the technician configure for this drive array?

* RAID 0
* RAID 5
* RAID 6
* RAID 10

Reference:

https://www.booleanworld.com/raid-levels-explained/

Q197. A company stores extremely sensitive data on an alt-gapped system. Which of the following can Be Implemented to increase security against a potential insider threat?

* Two-person Integrity
* SSO
* SIEM
* Faraday cage
* MFA

Two-person integrity is a security measure that can be implemented to increase security against a potential insider threat on an air-gapped system. An air-gapped system is a system that is isolated from any network connection and can only be accessed physically. An insider threat is a malicious actor who has authorized access to an organization’s system or data and uses it for unauthorized or harmful purposes. Two-person integrity is a system of storage and handling that requires the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures, for accessing certain sensitive data or material. This way, no single person can compromise the security or integrity of the data or material without being noticed by another person. SSO (Single Sign-On) is a feature that allows users to access multiple applications or systems with one set of

credentials, but it does not prevent insider threats. SIEM (Security Information and Event Management) is a tool that collects and analyzes log data from various sources to detect and respond to security incidents, but it does not work on air-gapped systems. A Faraday cage is a structure that blocks electromagnetic signals from entering or leaving, but it does not prevent physical access or insider threats. MFA (Multi-Factor Authentication) is a method that requires users to provide two or more pieces of evidence to verify their identity, such as something they know, something they have, or something they are, but it does not prevent insider threats. Reference: https://www.howtogeek.com/169080/air-gap-how-to-isolate-a-computer-to-protect-it-from-hackers/ https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/ https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/ https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/

Q198. Which of the following open ports should be closed to secure the server properly? (Choose two.)
* 21
* 22
* 23
* 53
* 443
* 636

The administrator should close ports 21 and 23 to secure the server properly. Port 21 is used for FTP (File Transfer Protocol), which is an unsecure protocol that allows file transfer between a client and a server over a network connection. FTP does not encrypt the data or the credentials that are transmitted, making them vulnerable to interception or modification by attackers. Port 23 is used for Telnet, which is an unsecure protocol that allows remote login and command execution over a network connection using a CLI. Telnet does not encrypt the data or the credentials that are transmitted, making them vulnerable to interception or modification by attackers.

Q199. Corporate policy mandates that logs from all servers be available for review regardless of the state of the server. Which of the following must be configured to comply with this policy?
* Aggregation
* Subscription
* Merging
* Collection

Explanation

Aggregation is the process of collecting, standardizing, and consolidating log data from multiple sources into a central location. Aggregation makes it easier to search, analyze, and report on log data, as well as to comply with security policies and regulations. By aggregating logs from all servers, regardless of their state, the corporate policy can ensure that no log data is lost or inaccessible in case of a server failure or outage

Q200. A server administrator is testing a disaster recovery plan. The test involves creating a downtime scenario and taking the necessary steps. Which of the following testing methods is the administrator MOST likely performing?
* Backup recovery
* Simulated
* Tabletop
* Live failover

The live failover testing method is the most likely one that the server administrator is performing when creating a downtime scenario and taking the necessary steps. A live failover test involves switching from the primary system to the secondary system (or backup site) in a real environment, without any simulation or preparation. A live failover test can evaluate the effectiveness and readiness of the disaster recovery plan, but it also carries a high risk of data loss, corruption, or disruption. Reference: https://www.ibm.com/cloud/learn/disaster-recovery-testing

Q201. A server technician is installing application updates on a Linux server. When the technician tries to install a MySQL update,

the GUI displays the following error message: AVC denial. Which of the following should the technician do for the MySQL update to install?

* Download the update manually and run a checksum utility to verify file integrity.
* Issue the setenforce 0 command.
* Create a firewall rule to allow port 3306 through the firewall.
* Issue the yum -y update mysql command.

The AVC denial error message indicates that SELinux (Security-Enhanced Linux) is preventing the MySQL update from installing. SELinux is a security module that enforces mandatory access control policies on Linux systems. To install the MySQL update, the technician should issue the setenforce 0 command, which temporarily disables SELinux enforcement until the next reboot. Downloading the update manually, creating a firewall rule, or issuing the yum -y update mysql command will not resolve the error. Reference: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Server Administration, Objective 4.3: Given a scenario, troubleshoot server issues using appropriate tools.

Q202. A systems administrator deployed a new web proxy server onto the network. The proxy server has two interfaces: the first is connected to an internal corporate firewall, and the second is connected to an internet-facing firewall. Many users at the company are reporting they are unable to access the Internet since the new proxy was introduced. Analyze the network diagram and the proxy server’s host routing table to resolve the Internet connectivity issues.

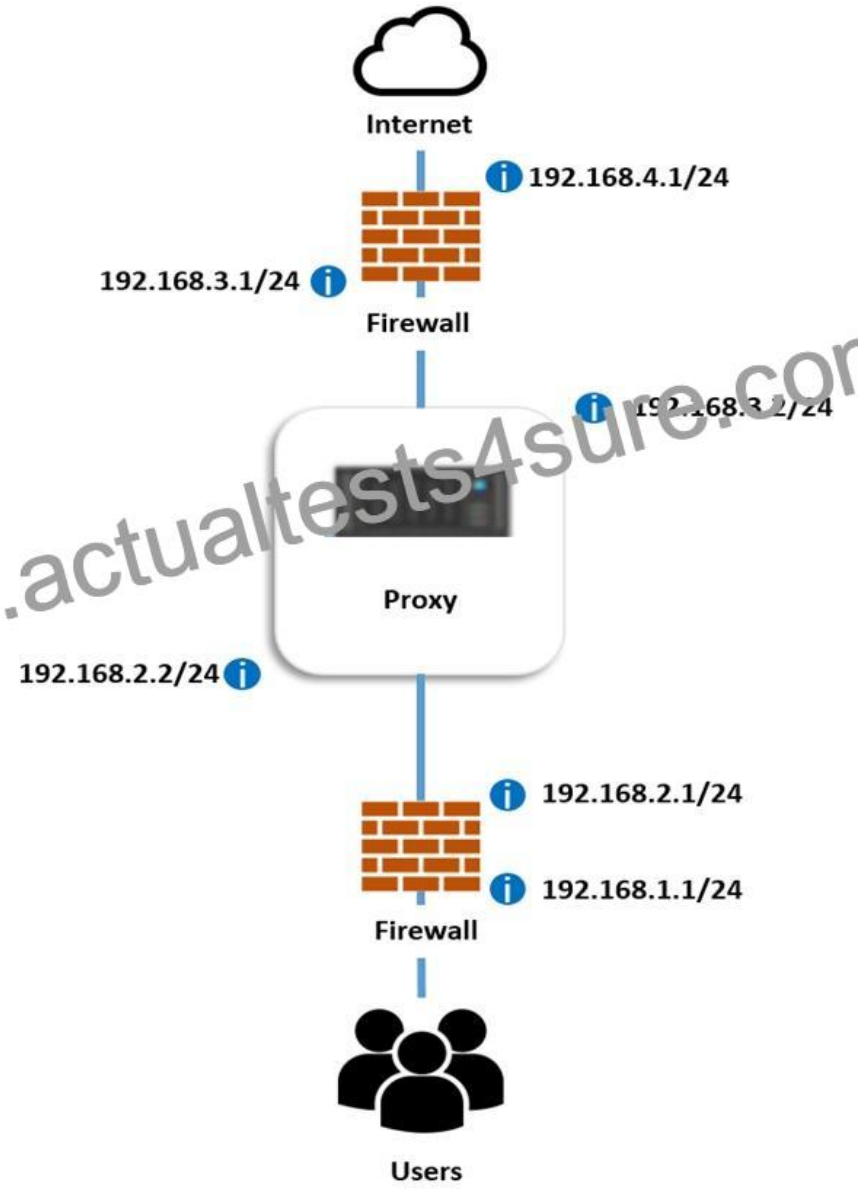
INSTRUCTIONS

Perform the following steps:

1. Click on the proxy server to display its routing table.

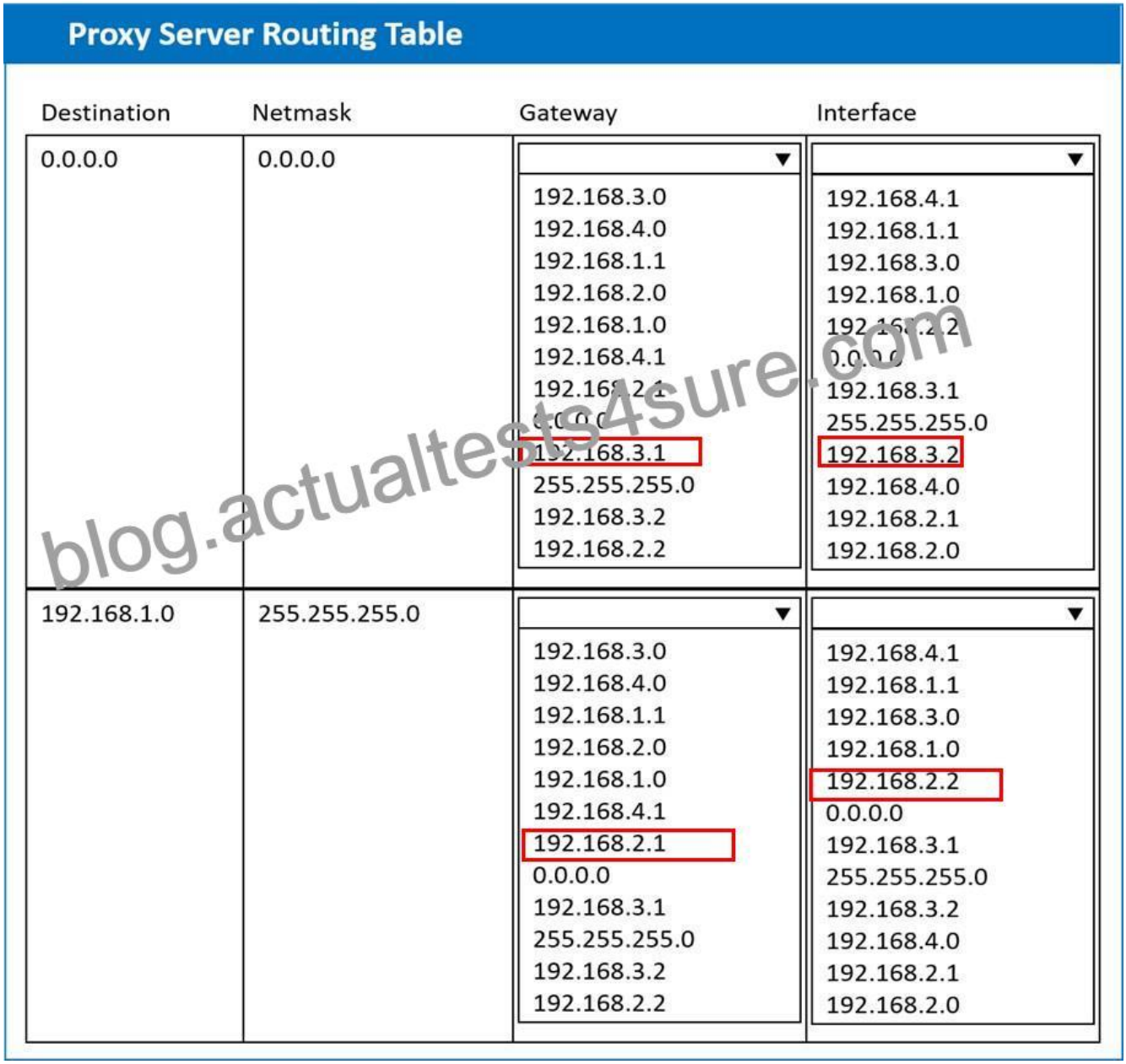
2. Modify the appropriate route entries to resolve the Internet connectivity issue.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Proxy Server Routing Table

Destination	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	▼ 192.168.3.0, 192.168.4.0, 192.168.1.1, 192.168.2.0, 192.168.1.0, 192.168.4.1, 192.168.2.1, 0.0.0.0, 192.168.3.1, 255.255.255.0, 192.168.3.2, 192.168.2.2	▼ 192.168.4.1, 192.168.1.1, 192.168.3.0, 192.168.1.0, 192.168.2.2, 0.0.0.0, 192.168.3.1, 255.255.255.0, 192.168.3.2, 192.168.4.0, 192.168.2.1, 192.168.2.0
192.168.1.0	255.255.255.0	▼ 192.168.3.0, 192.168.4.0, 192.168.1.1, 192.168.2.0, 192.168.1.0, 192.168.4.1, 192.168.2.1, 0.0.0.0, 192.168.3.1, 255.255.255.0, 192.168.3.2, 192.168.2.2	▼ 192.168.4.1, 192.168.1.1, 192.168.3.0, 192.168.1.0, 192.168.2.2, 0.0.0.0, 192.168.3.1, 255.255.255.0, 192.168.3.2, 192.168.4.0, 192.168.2.1, 192.168.2.0



Q203. A server administrator is trying to determine the cause of a slowdown on a database server. Upon investigation, the administrator determines the issue is in the storage subsystem. Which of the following will most likely resolve this issue?

* Increasing IOPS by implementing flash storage
* Implementing deduplication on the storage
* Extending capacity by installing a 4TB SATA disk
* Reformatting the disk as FAT32

Increasing IOPS (input/output operations per second) by implementing flash storage is the most likely solution to resolve a slowdown issue in the storage subsystem of a database server. Flash storage uses solid-state drives (SSDs) that have faster read/write speeds and lower latency than traditional hard disk drives (HDDs). This can improve the performance of database queries and transactions. Implementing deduplication, extending capacity, or reformatting the disk as FAT32 are not likely to resolve the issue, as they do not affect the IOPS of the storage subsystem. References: [CompTIA Server+ Certification Exam Objectives], Domain 3.0:

Storage, Objective 3.5: Summarize hardware and features of various storage technologies.

Free SK0-005 Exam Dumps to Improve Exam Score: https://www.actualtests4sure.com/SK0-005-test-questions.html]