Vendor: CompTIA

Exam Code: SK0-005

Exam Name: CompTIA Server+ Certification Exam

Version: Demo

QUESTION 1
Which of the following BEST measures now much downtime an organization can tolerate Curing an unplanned outage?

A. SLA
B. BIA
C. RTO
D. MTTR

Correct Answer: A

QUESTION 2
Which of the following licenses would MOST likely include vendor assistance?

A. Open-source
B. Version compatibility
C. Subscription
D. Maintenance and support

Correct Answer: C

QUESTION 3
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?

A. Upgrade the application package
B. Tighten the rules on the firewall
C. Install antivirus software
D. Patch the server OS

Correct Answer: D

QUESTION 4
A technician has been asked to check on a SAN. Upon arrival, the technician notices the red LED indicator shows a disk has failed. Which of the following should the technician do NEXT, given the disk is hot swappable?

A. Stop sharing the volume
B. Replace the disk
C. Shut down the SAN
D. Stop all connections to the volume

Correct Answer: B

QUESTION 5
Users in an office lost access to a file server following a short power outage. The server administrator noticed the server was powered off. Which of the following should the administrator do to prevent this situation in the future?

A. Connect the server to a KVM
B. Use cable management

C. Connect the server to a redundant network
D. Connect the server to a UPS

Correct Answer: D

QUESTION 6
Which of the following encryption methodologies would MOST likely be used to ensure encrypted data cannot be retrieved if a device is stolen?

A. End-to-end encryption
B. Encryption in transit
C. Encryption at rest
D. Public key encryption

Correct Answer: C

QUESTION 7
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?

A. Backup recovery
B. Simulated
C. Tabletop
D. Live failover

Correct Answer: C

QUESTION 8
Users at a company work with highly sensitive data. The security department implemented an administrative and technical control to enforce least-privilege access assigned to files. However, the security department has discovered unauthorized data exfiltration. Which of the following is the BEST way to protect the data from leaking?

A. Utilize privacy screens.
B. Implement disk quotas.
C. Install a DLP solution.
D. Enforce the lock-screen feature.

Correct Answer: C

QUESTION 9
A technician is connecting a Linux server to a share on a NAS. Which of the following is the MOST appropriate native protocol to use for this task?

A. CIFS
B. FTP
C. SFTP
D. NFS

Correct Answer: A

QUESTION 10
A remote physical server is unable to communicate to the network through the available NICs, which were misconfigured. However, the server administrator is still able to configure the server remotely. Which of the following connection types is the server administrator using to access the server?

A. Out-of-band management
B. Crash cart access
C. Virtual administrator console
D. Local KVM setup
E. RDP connection

Correct Answer: A

QUESTION 11
A server administrator wants to run a performance monitor for optimal system utilization. Which of the following metrics can the administrator use for monitoring? (Choose two.)

A. Memory
B. Page file
C. Services
D. Application
E. CPU
F. Heartbeat

Correct Answer: AE

QUESTION 12
A global organization keeps personnel application servers that are local to each country. However, a security audit shows these application servers are accessible from sites in other countries. Which of the following hardening techniques should the organization use to restrict access to only sites that are in the same country?

A. Configure a firewall
B. Close the unneeded ports
C. Install a HIDS
D. Disable unneeded services.

Correct Answer: A

QUESTION 13
A technician is attempting to update a server's firmware. After inserting the media for the firmware and restarting the server, the machine starts normally into the OS. Which of the following should the technician do

NEXT to install the firmware?

A.   Press F8 to enter safe mode
B.   Boot from the media
C.   Enable HIDS on the server
D.   Log in with an administrative account

Correct Answer: B

QUESTION 14
A server administrator needs to check remotely for unnecessary running services across 12
servers. Which of the following tools should the administrator use?

A.   DLP
B.   A port scanner
C.   Anti-malware
D.   A sniffer

Correct Answer: B

QUESTION 15
A systems administrator is attempting to connect via RDP to a server that is running Windows.
However, the systems administrator cannot connect to the machine via RDP to reboot it and
apply updates. Which of the following methods should be used to access the machine and
perform a reboot if the server is not physically accessible?

A.   ILO/iDRAC
B.   TCP/IP
C.   SSH/SCP
D.   VNC/VPN

Correct Answer: A

QUESTION 16
The Chief Information Officer (CIO) of a datacenter is concerned that transmissions from the
building can be detected from the outside. Which of the following would resolve this concern?
(Choose two.)

A.   RFID
B.   Proximity readers
C.   Signal blocking
D.   Camouflage
E.   Reflective glass
F.   Bollards

Correct Answer: AB

QUESTION 17
Alter rack mounting a server, a technician must install four network cables and two power cables
for the server. Which of the following is the MOST appropriate way to complete this task?

A.   Wire the four network cables and the two power cables through the cable management arm using