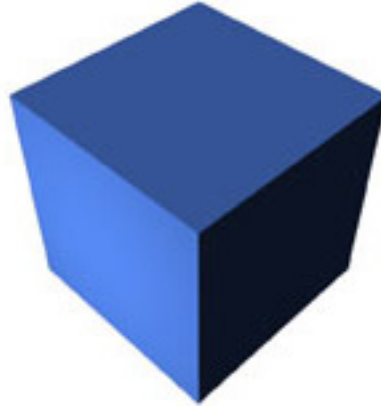


TEST KING



LEADING THE WAY IN IT
TESTING AND CERTIFICATION TOOLS!

Server+

Version 2.1

***Important Note
Please Read Carefully***

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of just cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

We are constantly adding and updating our products with new questions and making the previous versions better so email us once before your exam and we will send you the latest version of the product.

Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that particular pdf file being distributed by you. Testking will reserve the right to take legal action against you according to the International Copyright Law. So don't distribute this PDF file.

Q.1
A Customer wants to add memory to an existing server while preserving their initial investment. Which of the following actions must be performed before purchasing memory?

- A. Check memory count on POST.
- B. Verify pin count of replacement memory.
- C. Verify the availability of memory slot.
- D. Verify compatibility with existing memory.

Answer: C

Before the purchase you should first check if there the server has available memory slot. The next step would be to check which memory are compatible with the existing memory.

Q.2
A file server has been optimized with the following characteristics:

- 1 GB RAM
- 400 MHz CPU
- 10/100 Ethernet NIC
- Hardware RAID subsystem

The server needs to be reconfigured as a database server. Which of the following upgrades should be added first?

- A. More RAM
- B. An additional NIC
- C. An additional processor
- D. An additional tape drive

Answer: C

A single 400 MHz CPU could become a bottleneck on a database server. We should either add an additional CPU or replace the CPU with a faster one.

A database server needs a lot of RAM, 1 GB should be sufficient.

A 10/100 Ethernet NIC should be sufficient. A database server has less network traffic compared to a file server for example.

A tape drive is only used for recovery. It is not required since SQL Server can make backups over the network.

Q.3

The Vice President of Operations has decided that the company should be running the latest version of the Network OS. A decision was made that the existing Network OS should be removed before the new version is installed. A full backup has been performed. Which of the following should be done first?

- A. Verify the backup
- B. Format the system drive
- C. Partition the data drive
- D. Install the latest Network OS updates.

Answer: A

We must ensure that the backup is correct. If the backup is corrupt we would be unable to return to the previous state.

Q.4

All of the following need to be checked after an update to an SNMP agent **EXCEPT** that the

- A. PUTs are enabled
- B. MIBs require updating
- C. traps are still configured
- D. SNMP installation is still valid

Answer: D

Reconfiguration of SNMP agents would not change the SNMP installation.

Incorrect Answers

An SNMP agent update could have an impact on PUTs, MIBs and traps. PUTs are used in SNMP agent scripts, management information base (MIB) files contain SNMP agent information, and traps are configured for SNMP agents.

Q.5

A new UPS has been installed with a signal cable that connects the server to the UPS. However, the server cannot communicate with the UPS. Which of the following is the likely cause?

- A. The UPS is the wrong model.
- B. The UPS batteries are not fully charged.
- C. The UPS software is not properly configured.
- D. The UPS is not configured to a power source.

Answer: C

The most likely cause is that the UPS software has not been properly configured.

Incorrect Answers

A wrong model is not a likely problem, since there are standards for UPS.

The batteries do not have to be fully charged in order for the UPS to operate.

An UPS need a power source, though it is not likely that this have been overlooked.

Q.6

What is the bus length limitation of a single-ended UltraWide SCSI with four devices?

- A. 1.5 meters
- B. 3 meters
- C. 6 meters
- D. 12 meters

Answer: B

UltraSCSI supports four devices, up to 3 meters (10 feet).

UltraSCSI supports eight devices, up to 1.5 meters (5 feet).

Q.7

A customer has a system with two 9-GB drivers that are hardware mirrored on an Ultra SCSI RAID controller. Using the same size drivers, they would like to plan for 63 GB of storage space. Which of the following would offer a solution with the highest performance?

- A. RAID 5 with 7 additional drives
- B. RAID 5 with 12 additional drives
- C. RAID 0/1 with 7 additional drives
- D. RAID 0/1 with 12 additional drives

Answer: D

We should use RAID 0/1 combines RAID 0 (disk mirroring which gives fault tolerance) with RAID 1 (disk striping which give highest performance). 6 additional drives could be used on each mirror. Seven -9GB drives give a 63GB striped volume as was required.

Incorrect Answers

RAID 5 also provides fault tolerance but not as high performance as RAID 0/1.

7 additional drives in a RAID 0/1 is not enough to provide 63 GB of storage space. 12 additional drives are needed.

Q.8

A customer asks a technician to install a new Ultra2 SCSI controller to an existing server. The new controller will replace a Fast SCSI controller that is in the server. The only device that will be connected is a Fast SCSI external tape drive. The customer will want to add new SCSI devices in the future.

What should the technician tell the customer?

- A. The new configuration will work, however Ultra2 devices may operate at single-ended speeds.
- B. The new configuration will work and Ultra2 devices will operate at Ultra speeds.
- C. The new configuration will work and all devices will operate at Ultra2 speeds.
- D. The new configuration will not work.

Answer: B

Ultra2 is compatible with existing SCSI devices allowing older, non-Ultra2-capable controllers to be used with newer, Ultra2-capable devices and vice versa.

Q.9

After a server's processor is upgraded, the server will not POST. What is the most likely cause of this?

- A. The BIOS was not flashed.
- B. The processor is not correctly seated.
- C. The jumper settings on the processor are incorrect.
- D. The original cache size is different from the new cache size.

Answer: B

A possible cause of a failed POST test is an incorrectly seated processor. There should, in general, be no need to flash the BIOS to upgrade a processor. Modern processors do not have jumper settings. The cache size of a processor would not cause the POST to stop.

Q.10

A technician is adding a PCI 2.2-compliant 64-bit, 66-MHz card to a server. Which of the following types of slots can be used for the card?

- I. 32-bit, 33 MHz PCI
- II. 64-bit, 33 MHz PCI

III. 64-bit, 66 MHz PCI

- A. III only
- B. I and II only
- C. II and III only
- D. I, II, and III

Answer: D

The PCI 2.2 specification allows for a 64-bit, 66-MHz compliant card to be used in a 32-bit 33MHz slot, in a 64-bit 33MHz slot, or in 64-bit 66MHz slot.

Q.11

A Wake-on-LAN adapter has been installed on a server. However, the server does not wake up as expected. Which of the following should be done to resolve the problem?

- A. Verify SNMP packets
- B. Verify TCP/IP packets
- C. Verify Magic Packets
- D. Verify ACK packets

Answer: C

Wake On LAN (WOL) is the name for a technical development jointly created by IBM and Intel. The technology allows "enabled" devices to be powered on remotely via a special type of network communication. A WOL-enabled device, when powered off, will still draw a tiny amount of electricity to drive the network interface. The interface remains in a passive, listening mode, sending nothing out on the network. To wake up the device, a specially formed packet is sent to the network port where the device is plugged in.

This special packet, called a **magic packet**, carries a special "signature." When the network interface sees this signature, it recognizes this as a wakeup call.

Q.12

As the server is powered on, POST errors are observed. How can it be determined which FRU (Field Replacement Unit) to replace?

- A. Review the Network OS logs for subsystem errors
- B. Power off the server, disconnect from power, reconnect, restart.
- C. Look up the error codes in the server documentation for the appropriate part to replace.

- D. Contact the server manufacturer's technical support for known failing components that should be replaced.

Answer: C

The POST error codes have to be decoded, for example by using the server motherboard documentation.

Q.13

As part of the installation of a four-way 400 MHz server, a baseline measurement was recorded. In addition, the latest firmware and Network OS patches were applied. Upon rebooting the server, the drives fail to initialize. Which of the following actions will offer the best solution to this issue?

- A. Replace the hard drivers.
- B. Search the vendor's Website for known issues.
- C. Check the Network OS README file.
- D. Install the latest Network OS service patch.

Answer: B

The vendor's Website is the best place to find information on known problems and solutions to these problems.

Q.14

The technician receives a call reporting that a server is down. After arriving at the site, the technician realizes the problem is beyond his technical expertise. What should the technician do in this situation?

- A. Review escalation procedures and contact the responsible individual.
- B. Contact a fellow technician and ask that individual to come in to help.
- C. Continue working on the problem, since the solution may present itself in time.
- D. Tell the client that the system will be down until the next business day.

Answer: A

When a technician is unable to solve a problem, the problem should be escalated so that a person with more expert knowledge can resolve the problem

Q.15

A network server will not boot properly. The server never begins the load of the Network OS and the server technician suspects a POST error. What is the proper way to use a POST diagnostics hardware adapter?

- A. Insert the card into an open bus slot, boot the computer, and the error codes will display on the adapter.
- B. Insert the card into an open bus slot, boot the computer, and the error codes will output on the default printer.
- C. Insert the card into an open bus slot, boot the computer using the supplied floppy disk, and the error codes will be stored on disk.
- D. Connect the adapter to a serial or parallel port, boot the computer, and the error codes will be stored in a memory buffer created by the adapter.

Answer: A

The messages, the post codes, from the POST diagnostics hardware adapter would be shown on a display on the adapter.

Q.16

A technician is trying to determine why a remote alert failed on a server at another location. Which of the following steps should be performed to fix the problem?

- I. Reboot remote server.
 - II. Connect to the remote server.
 - III. Logon with administrator privileges.
 - IV. Determine that the alert criterion is configured correctly.
-
- A. I and II only
 - B. III and IV only
 - C. I, II, and IV only
 - D. II, III, and IV only

Answer: D

Q.17

The hard drive in an organization's certificate authority server has failed. The drive contained the certificate database and certificate revocation list. A replacement hard drive and the appropriate backup tapes from the Grandfather-Father-Son (GFS) rotation are obtained. What should the server technician do first before attempting a restore of the system?

- A. Burn in the new hard drive for at least 24 hours.
- B. Check the certificate authority's Website for software updates.
- C. Locate the organization's server recovery plan.

D. Determine the default server configuration from the certificate authority's software guide.

Answer: C

The server recovery plan, if existing, would be the first to check for the service technician when an import server has failed.

Q.18

A functional server suddenly stops responding to users. Upon a cold reboot of the server, the screen is blank. However, the hard drive and CD-ROM spin up normally. What is most likely causing the problem?

- A. There is a virus problem.
- B. There is an AC power problem.
- C. There is a hardware problem.
- D. There is a software problem.

Answer: D

The behavior could be caused by a virus, a hardware problem, or a software problem. The most common cause of this is a software problem though.

Q.19

The previous month's UPS activity log that is maintained for a server is reviewed. It shows power to the server is repeatedly being lost for about 10 minutes at approximately the same time every Friday night. All system hardware and software diagnostic tests have been unable to locate the cause of the problem.

Who should be contacted regarding the problem?

- A. The UPS manufacturer.
- B. The department manager.
- C. The building maintenance foreman.
- D. The company's outside server consultants.

Answer: C

A building maintenance foreman seems the most likely cause of the problem. He probably shut down some system at the same time each Friday night.

It seems very unlikely that the department manager or the consultants would work Friday night, or that UPS manufacturer would schedule the UPS to perform a specific reoccurring activity.

Q.20

The company server must be shut down for an upgrade. Which of the following sequences is the best practice when shutting down the server?

- A. Perform backup, notify users before shutdown, then shut down server and peripherals together.
- B. Perform backup, notify users before shutdown, shut down server, then shut down the peripherals.
- C. Notify users before shutdown, shut down applications, then shut down peripherals, and then shut down server.
- D. Have all users log off the server, shut down all applications, backup the server, shut down the server, then shut down the peripherals.

Answer: D

Before shutting down the server we should have all users to log off, not just notify them, and shut down all applications. We should then backup the server, shut down the server and finally shut down all peripherals.

Q.21

The Human Resources Department added 50 new users to the network. All of them are using the same application located on the main server in the data center. During peak usage hours the response of the application has slowed to an unacceptable level.

The server is configured with two CPUs, 1GB of memory, a 100 GB SCSI disk array, and one Fast Ethernet NIC. The performance baselines taken during peak hours are:

	Historic	Current
- Average CPU utilization	50%	60%
- Average CPU queue	1.5	1.7
- Average network utilization	25%	40%
- Average network queue	0.2	0.2
- Memory hard page faults	0.1 pages/s	0.12 pages/s
- Memory soft page faults	100 pages/s	200 pages/s
- Average disk subsystem utilization	10%	8%
- Average disk subsystem queue	0.1	0.05

Where is the bottleneck most likely located and how can it be resolved?

- A. Memory is the bottleneck. More RAM needs to be installed.
- B. CPUs are the bottleneck. Faster CPUs need to be installed.
- C. The network is the bottleneck. Replace the hub with a switch.
- D. The disk I/O is the bottleneck. Add an additional SCSI controller.

Answer: A.

100 page faults per second indicate a memory problem. Microsoft gives 20 pages/sec or less as acceptable.

Q.22

A server administrator receives an application-specific error message while logged onto a remote server. A review of the remote server's event logs found no reference to the error. The remote application log files also do no mention the specific error.

Which of the following would be the most appropriate action for the technician to take next?

- A. Examine the Network OS documentation.
- B. Examine the local application event logs.
- C. Examine the remote server vendor's support Website.
- D. Notify the remote server users that the server must be rebooted.

Answer: B

It seems like that error was initiated on the local computer as nothing indicates an error on the server. We should therefore check the local event log.

Q.23

A third-party RAID card has been upgraded to the latest drivers. Since the upgrade, when a cold boot is performed, the connected hard drives are correctly discovered during POST and will boot after a power down, but not after a warm boot of the server. An identical card gives the same results. Which of the following sources of information would be most useful in resolving this problem?

- A. The Network OS vendor's HCL
- B. The Network OS vendor's Website
- C. The server vendor's Website
- D. The adapter vendor's Website

Answer: D

This seems to a software problem since the network adapter works when the OS is cold booted, but not when you warm booted. The information concerning this problem could possibly be found on the Network OS Website, the server vendor's website, or the adapter vendor's website. Most information on the adapter would most likely be found on the adapter vendor's Website.

Q.24

In the event of a single-drive failure of an array, which of the following should be the first step to recovery?

- A. Break the mirror
- B. Restore from backup
- C. Determine the RAID level
- D. Replace the failed drive

Answer: C

Before starting the recovery of the array we should determine the RAID level. Then we will know if we should break the mirror (RAID 1), or replaced the failed drive.

Q.25

When files on an NTFS partition on a new server were configured, an error occurs and the server will no longer boot. Which software is required to recover from the failure and continue configuration?

- A. Novell NetWare CD-ROM
- B. Unix Boot/Root diskette(s)
- C. IBM OS/2 Startup disk and Installation disk
- D. ERD and/or installation disks with CD-ROM

Answer: D

NTFS is only used on Windows NT/2000/XP systems. These systems can be restored by use of the installation CD-ROM/boot disks combined with the ERD diskettes.

Q.26

Some of the users on a customer's network are complaining that they cannot access some servers. Which of the following would be **LEAST** appropriate question to ask upon arriving onsite?

- A. Which servers are not available?
- B. When were the servers last rebooted?
- C. Which users are unable to access the server?
- D. Are any users able to access the unavailable servers?

Answer: B

We should focus at the problem at hand: some users cannot access some servers. The question of when the servers were last rebooted is not so relevant.

Q.27

Users complain that around 3:00 PM each workday, the company's email server operates slowly. What should be done first to determine the cause of the slowdown?

- A. Check the pagefile size.
- B. Add more RAM to the server and do a new baseline.
- C. Do a network trace to determine any issues with the network.
- D. Check logs to determine when maintenance programs are scheduled.

Answer: D

Since the disturbance reoccurs at exactly the same time of the day, it seems that some scheduled task, possibly a maintenance program, is the cause of the problem.

Q.28

A technician is troubleshooting a failed server that cannot connect to the LAN. There are lights on the network card and server that indicate activity. The technician replaced the network cable, and used assorted Network OS vendor, and third-party diagnostic tools, but the server still fails to connect properly. Which of the following is the best source of assistance to help resolve the problem?

- A. IT manager
- B. IS help desk
- C. Network administrator
- D. Disaster recovery team

Answer: C

The network adapter is working, but it seems likely that the server network properties or the network protocol has been misconfigured. The network administrator would know how the server should be configured for this particular network.

Q.29

A client has called to company that their server hums or buzzes. Which of the following is **LEAST** likely to be the problem?

- A. CPU fan
- B. RAID card
- C. Hard drive
- D. Power supply

Answer: B

A RAID card does not have any FAN so it would not hum or buzz.

Q. 30

Users report that the intranet database is slow to respond during peak use times. The database server is on a small 150-user network and is configured with dual processors, 512 MB RAM and a hardware-controlled RAID 5 array with three drives. The server also provides DNS and DHCP services for the intranet. Which of the following changes can be made to help improve server performance?

- I. Set process affinity
 - II. Add a hard drive to the RAID 5 array
 - III. Move the page file to another partition on the RAID 5 array
 - IV. Move the DNS and DHCP services to another server
-
- A. I and IV only
 - B. II and III only
 - C. I, II, and IV only
 - D. I, II, III, and IV

Answer: C

Processor affinity can be used to enable the database server service to exclusively use one processor. This would improve performance.

Adding a hard drive to the RAID 5 array would improve disk access since three drives containing data (one contains the parity bit), instead of two, could be read in parallel.

Removing any network services from the server would improve the performance of the remaining services.

Incorrect Answer

Move the page file on the RAID 5 array would not change the performance. The OS uses the RAID 5 array as a single drive.

Q. 31

An administrator using a Grandfather-Father-Son (GFS) backup rotation needs to restore the system to the state it was in two months previously. How many tape sets will be required to perform this operation?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: A

You use the single tape set from two months ago to restore the system state.

Q. 32

Without bringing the server down, which of the following is the first step in removing a NIC that is in a hot-plug PCI slot?

- A. Reload the NIC driver
- B. Power off the PCI slot
- C. Unload the TCP/IP stack.
- D. Disconnect the Wake-on-LAN cable from the NIC.

Answer: B

Before removing the NIC we should power off the PCI slot.

There is no need to reload the NIC driver or unload the TCP/IP stack.

Q. 33

A server is required to recover after a single disk failure. Which of the following solutions will provide the required level of fault tolerance?

- I. RAID 0
 - II. RAID 1
 - III. RAID 3
 - IV. RAID 5
-
- A. I and IV only
 - B. II and III only
 - C. I, II, and IV only
 - D. II, III, and IV only

Answer: D

RAID 1, RAID 3, and RAID 5 can recover from a single disk failure without any data loss. RAID 0 has no fault tolerance. Data would have to be restored from tape.

Q. 34

A failure occurred while a full backup from a tape set was being restored to a server. During a second attempt, the restore failed at the same point. Which of the following is most likely the cause of the failure?

- A. One of the tapes has failed
- B. The tape backup unit is dirty
- C. The tape drive malfunctioning
- D. All tapes in the backup set are corrupt

Answer: A

Since the failure occur at the same point it seems likely that the backup media, one of the tapes, has failed.

Q. 35

Which of the following is the most important element of an effective disaster recovery plan?

- A. A clear plan for reducing the effects of a disaster.
- B. Adequate personnel to implement the disaster recover plan.
- C. A clear and concise disaster recovery plan stored in hard copy.
- D. A well-documented list of specific vendors used by the company.

Answer: B

The final step in a good disaster recovery plan is training. You need to train your personnel in what the plan is, how it is executed, and how it needs to be maintained. Training is perhaps the most critical yet most neglected task. It helps ensure that new risks and solutions are put into the plan and that everyone knows what is expected when a disaster occurs.

Q. 36

Which of the following types of backup media is recommended to maximize storage on a 24 GB DAT drive?

- A. DDS-1
- B. DDS-2
- C. DDS-3
- D. DDS-24

Answer: C

DDS-3 supports 24GB

DDS-1 supports 2.6GB and 4GB.

DDS-2 supports 8GB.

DDS-4 supports 40GB.

DDS-24 is standard used by Sony. It supports 24GB but might not be compatible with a 24GB DAT drive.

Note: DAT stands for Digital Audio Tape, an audio recording technology based on 4mm wide tape in a helical scan recorder. DDS - Digital Data Storage - was developed from DAT concepts to store computer data with high data density and high reliability. However, many people continued to call DDS drives "DAT drives," and the name is still with us today.

Q. 37

Disaster recovery plans should be prepared at what stage of a server installation?

- A. Before deployment
- B. During the annual budget period
- C. After the server is successfully installed and configured
- D. Immediately upon symptoms of problems developing with the backup system.

Answer: C

The server should first be installed and configured. Then we can make a disaster recovery plan.

Making a disaster recovery plan before deployment seems prudent. It should also be considered (A).

Q. 38

During a test of the disaster recovery plan, it was determined that some servers restored with other servers' data. Which of the following suggestions is most likely to improve disaster recovery in the future?

- A. Implement a differential backup strategy.
- B. Maintain a printed report with tape backups.
- C. Implement a media rotation scheme for offsite tapes.
- D. Create a database that contains the backup logs stored on an incremental server.

Answer: B

Printed instructions could help to avoid tapes from being restored incorrectly.

Q. 39

In addition to backup tapes, which of the following should be stored offsite to help facilitate the recovery of a server in the event of a disaster?

- I. Blank backup tapes
 - II. Duplicate tape drives and cables
 - III. Network OS installation CD-ROMs
 - IV. Backup software and drivers
-
- A. I and II only
 - B. II and IV only
 - C. III and IV only
 - D. II, III, and IV only

Answer: D

Duplicate hardware, such as tape drives and cables, OS installation media, and backup software and drivers would ensure that the backup media could be restored. It eliminates a single point of failure in the recovery process.

Q. 40

When a new disaster recovery plan is reviewed, which of the following should be done first?

- A. Test the existing plan.
- B. Identify critical resources at the department level.
- C. Determine the preventive measures to be taken to minimize risks.
- D. Assess the possible amount of down time that could be experienced.

Answer: A

It is very important to test the existing plan and check if it works or if it has flaws and need improvement.

Q. 41

A company has hired an installation service company to install a server. The SCSI devices are configured to use the same SCSI controller. The installation appeared to be successful. After six hours, the server's SCSI devices are randomly inaccessible. A reboot temporarily resolves the issue.

Which of the following is the most likely cause of this issue?

- A. The devices were not properly terminated.
- B. The system's BIOS was not upgraded prior to installation.
- C. The SCSI adapter is not properly seated in the PCI slot.
- D. The SCSI adapter firmware was not upgraded prior to installation.

Answer: A

SCSI trunks need to be terminated. If it is not terminated it could cause the behavior above.

If a BIOS upgrade would be required, the SCSI adapter not properly seated in the PCI slot, or the SCSI adapter firmware required update, then SCSI adapter would not work for six hours.

Q. 42

A technician is installing the Network OS on a fax server after conducting a pre-installation survey. As part of the plan, the technician performed the following steps:

- Verified the hardware requirements
- Checked the hardware compatibility
- Installed the operating system
- Applied the most current Network OS updates

All items from the plan performed correctly by the technician. The installation proceeds normally but upon testing, it is discovered that the NIC is not functioning. The technician verifies that the cable is connected properly, and that the link light is on. Which of the following should have been included in the pre-installation plan?

- A. Flashing the adapter BIOS
- B. Applying fixes beyond those installed
- C. Getting the latest drivers from the manufacturer
- D. Verifying the NIC's Wake-ON-LAN hardware compatibility

Answer: C

The network adapter is physically in order, but the OS has not been configured with network adapter drivers that work. The latest drivers must be acquired.

Q. 43

A company's main server uses an Ultra2-compatible controller with six Ultra2-compatible devices correctly installed and terminated. The technician is required to install and configured two Ultra3 devices. Which of the following is the most likely result?

- A. The new devices will work at Ultra2 speeds after they are configured.
- B. The Ultra2 controller will not allow the new devices to be installed.
- C. The Ultra3 devices are not compatible with the Ultra2 controller and require an adapter.
- D. All devices will function correctly after the cable length is reduced to include the new devices.

Answer: A

Ultra3 devices are down-compatible with Ultra2 controllers. The Ultra3 devices would work at Ultra2 speeds.

Q. 44

Which of the following factors must be considered when deciding which UPS to install?

- A. Maximum load
- B. Processor load
- C. Primary transformer output
- D. Acceptable downtime

Answer: D

The acceptable downtime is the most crucial factor when deciding which UPS to use.

Q.45

When the location of a server is planned, the power source should be checked for which of the following?

- I. AC Voltage
 - II. DC Voltage
 - III. Amperage
 - IV. Ground
-
- A. I and IV only
 - B. II and III only
 - C. II and IV only
 - D. I, III, and IV only

Answer: D

The AC voltage (not DC voltage), the amperage, and the ground should be checked when deciding the placement of the server.

Q. 46

A technician must perform a pre-installation check prior to installing a new server that required downloading the most recent BIOS and firmware. What is the best resource for acquiring the BIOS and firmware?

- A. The vendor's Website
- B. The vendor's UDP site
- C. A list server resource
- D. The Network OS Website

Answer: A

The motherboard manufacturer, the vendor, should have the most recent BIOS and firmware at their Website.

Q. 47

Which of the following is the best place to confirm current hardware compatibility with Network OS's HCL?

- A. Hardware documentation
- B. Website for the Network OS
- C. Network OS installation media
- D. Hardware compatibility checking utility

Answer: B

The OS manufacturer compiles a Hardware Compatibility List (HCL). This can be acquired from the web site.

Q. 48

A customer has requested a server with a SCSI RAID 5 array. When the equipment arrived, the technician notes are the SCSI RAID card, cables, and three 40-pin hard drives have been delivered. Which of the following should the technician indicate to the administrator?

- A. All required equipment has arrived.
- B. One more hard drive will be needed.
- C. The wrong hard drives were delivered.
- D. The wrong card and cables were delivered.

Answer: C

40-pin hard drives are IDE hard drives, not SCSI drives.

Q. 49

A server technician must move a company's two loaded 42U racks to a new location in the building next door. Which of the following is the best way to accomplish this move?

- A. Load the rack onto a wheeled trolley and move the rack to the new location.
- B. Lower the wheels on the rack, raise the rack feet and move the racks to the new location.
- C. Remove all equipment from the rack and move the racks and equipment to the new location.
- D. Unload enough heavy equipment from the rack to be easily moved and move the racks to the new location.

Answer: C

It would be safer to move the racks and the equipment separately.

Q. 50

During POST, the following message appears:

"2 logical drives found".

There are four SCSI hard drives in the server attached to a single RAID controller. None of the drives is configured as a JBOD.

Which of the following most likely explains this message?

- A. Two of the drives have failed.
- B. The drives are not initializing.
- C. The drive controller is misconfigured.
- D. The drives are configured in two separate arrays.

Answer: D

All drives most configured as a single array.

Q. 51

During the check of all equipment, a technician notices that the installation plan requires Network Adapter Fault Tolerance. The server that was received only has one network adapter. Which of the following procedures will provide the maximum level of Network Adapter Fault Tolerance?

- A. Add an additional router
- B. Add an additional network adapter
- C. Replace adapter with a multiprotocol adapter
- D. Replace adapter with a multiport network adapter

Answer: B

Two network adapters would provide the best fault tolerance.

Q. 52

The only free port on a customer's hub (Hub-1) is the uplink port. The customer purchases an additional 12-port hub (Hub-2) and would like to connect the two hubs. Which of the following cable/port combinations should be used?

- A. Straight cable. Hub-1 uplink port to Hub-2 uplink port.
- B. Straight cable. Hub-1 uplink port to Hub-2 regular port.
- C. Crossover cable. Hub-1 uplink port to Hub-2 uplink port.
- D. Crossover cable. Hub-1 uplink port to Hub-2 regular port.

Answer: B

The uplink port of Hub-1 should be connected to a regular port on Hub-2. A straight cable should be used.

Q. 53

A customer asked for 83 hard drives to be used by all four of their database servers. Which technology would best achieve this configuration?

- A. SCSI
- B. IEEE-1394
- C. Ultra DMA
- D. Fibre Channel

Answer: D

We need to cluster the hard drives so that they can be used by all four database servers. Only the SCSI and Fibre channel technology should be considered. Windows 2000 Clustering services, as an example, only supports SCSI and Fibre channel hard drives in a cluster. To support 83 hard drives we should use Fibre channel, since a single Fibre channel supports up to 126 devices.

Note: Fibre Channel is a high performance interface designed to bring speed and flexibility to multiple disc drive storage systems.

Incorrect answers

The SCSI interface would be inadequate with as many as 83 hard drives. SCSI wide can support only 15 devices.

ULTRA DMA is an IDE standard. IDE drives are not ordinarily used to cluster hard drives. Only two IDE devices can be used on a single IDE channel. By default, a computer has only two IDE channels.

IEEE-1394 (firewire) can support up to 63 devices. It would not, however, be an appropriate solution for hard drives for database servers. IEEE is typically used for external hard drives. IEEE-1394 is comparatively slow with a maximum speed of 400 megabits/s.

Reference:

Seagate knowledge base, Fibre Channel

MCSE Training kit (70-223) Microsoft Windows 2000 Advanced Clustering Services, Configuring the Shared Storage Device, page 44.

Microsoft Article: IEEE 1394: The Time is Right for This Bus

Q. 54

After a new server was installed, a large number of errors occurred during in-page operations. The technician noticed that the memory was not correct for the new server. Which of the following steps did the installing technician neglect to perform?

- A. Verification of virtual memory capacity.
- B. Verification of pre-installation plan
- C. Confirmation of fast page mode capability
- D. Use of single, rather than dual, in-line memory modules.

Answer: B

The pre-installation plan should have included a step for checking the compatibility of the memory of the new server.

Q. 55

A server room contains 15 servers, a 16-port hub, and a patch panel. All of the equipment is on four folding tables. Each server has its own monitor, keyboard, and mouse. All cables are routed behind the tables and around the perimeter of the room. Which of the following recommendations should be made for improving the server room?

- I. Install a KVM (Keyboard Video Monitor) switch
 - II. Install a network switch
 - III. Install a set of server racks
 - IV. Improve cable routing
-
- A. I and II only
 - B. III and IV only
 - C. I, II, and IV only
 - D. I, III, and IV only

Answer: D

With a KVM switch we only need a single monitor, keyboard and mouse, not a separate set for each server. This would save space and resources.

Server racks make better use of the space.

Cable routing should be improved. The cables should be routed behind tables and around the perimeter of the room.

Incorrect answer

A network switch could improve network performance, but could not be considered an improvement for the server room.

Q. 56

Which of the following is the **LEAST** effective method for restricting physical access to servers?

- A. Locking the server cabinet
- B. Requiring complex server passwords
- C. Using biometric identification-based access locks
- D. Installing a monitored alarm system on the server room

Answer: B

Server password would not restrict physical access to the server.

Q. 57

Which of the following is **NOT** usually a server room environmental issue?

- A. Noise
- B. Rodents
- C. Temperature
- D. Fire suppression system

Answer: B

Rodents are usually not considered a server room environmental issue.

Q. 58

A business owner wants a recommendation on who should receive access to secure server rooms. Which of the following is **LEAST** likely to be recommended for having access to server rooms?

- A. Users
- B. System administrators
- C. Data entry supervisors
- D. Database administrators

Answer: A

Users should not have access to the server room.

Q. 59

What is the main benefit of using backup tools supplies by the Network OS vendor?

- A. Speed of operation
- B. Backup media availability
- C. Compatibility with operating system
- D. Advanced features over third party programs

Answer: C

Network OS vendor Backup tools are often integrated directly into the operating system. The same vendor should guarantee compatibility.

Q. 60

A server technician is verifying a new network configuration on a UNIX server and types IPCONFIG at the prompt. Nothing happens. Which of the following commands should have been used to accomplish this?

- A. CONFIG
- B. INETCFG
- C. IFCONFIG
- D. WINIPCFG

Answer: C

UNIX and LINUX use the IFCONFIG command.

Q. 61

Which of the following should be documented for future reference when troubleshooting a hardware configuration?

- I. The initial configuration
 - II. Repairs made to the system
 - III. Monthly password changes
 - IV. Backup procedures
-
- A. I only
 - B. I and II only
 - C. III and IV only
 - D. I, II, and III only

Answer: B

Only hardware related issues like initial configuration and repairs to the system should be documented for hardware troubleshooting purposes.

Password changes and backup procedures would not affect the hardware.

Q. 62

When a multi-homed server is installed, it is sometimes necessary to block TCP/IP traffic between each subnet. Which of the following actions will accomplish this?

- A. Add an SNMP trap
- B. Disable IP forwarding
- C. Remove IPX and NetBEUI
- D. Put the cards on the same subnet but use different IP addresses.

Answer: B

Q. 63

Which of the following features of a network printer will **LEAST** affect performance?

- A. Internal RAM
- B. Network protocol
- C. Print server
- D. Connection interface

Answer: B?

The network protocol would least affect the performance of a network printer.

The RAM would be affect print spooling. The performance of the print server would affect print speed. The connection interface would also influence the speed of the printer.

Q. 64

Which RAID level best provides protection when either two disks fail simultaneously, or when a second disk fails during the reconstruction from the first disk failure?

- A. RAID 0/1
- B. RAID 1
- C. RAID 3
- D. RAID 5

Answer: A

RAID 0/1 is combination of RAID 0 (disk striping) and RAID 1 (disk mirroring). Each mirror consists of a striped volume of disks. It could handle failure of two disks.

Q. 65

Within a printer pools, print devices can have which of the following characteristics?

- I. Be on the same server
- II. Use the same IP address
- III. Have the same make and model
- IV. Use the same print drivers

- A. I and IV only
- B. II and IV only
- C. I, II, and III only
- D. I, III, and IV only

Answer: A

Printer pooling must use printers connected to a single server. The print devices must use the same print driver.

Incorrect answers

The print devices cannot have the same IP address.

The print devices are often of the same make and model, but it is not a requirement. They must use the same print driver however.

Q. 66

A technician is configuring a new server CTIA45 in the "comptia.org" domain using the IP address of 10.10.10.50 with a subnet mask of 255.255.255.0 and a gateway address of 10.10.10.1. The technician is unable to ping the other servers by the IP address. Which two of the following are possible causes and solutions?

- I. The other servers are on the same segment, but using a different subnet mask. Correct the subnet mask by making it match the other servers.
 - II. The DNS hostname entered into the new server is incorrect. Use a different hostname.
 - III. The other servers are on a separate segment and the gateway address is incorrect. Correct the gateway address.
 - IV. The other servers have DNS entries, but the new server does not. Add a new entry to the BIND host file
-
- A. I and III
 - B. I and IV
 - C. II and III
 - D. II and IV

Answer: A

The client could have an incorrect mask or an incorrect default gateway (or an incorrect IP address).

Since the ping attempts do not use host names there is no name resolution problem. The problem is not DNS related.

Q. 67

A company experienced a drive failure on one of its email servers and lost all of the data. The company decided to modify the RAID solution on all of its email servers. The servers are currently using RAID 0 on a set of six disk drives. The new solution will be RAID 5 on a set of six disk drives.

Which of the following is most likely to result from the new solution?

- A. The solution will create redundancy
- B. The solution will not create redundancy.
- C. The solution will create redundancy and improve disk reads only.
- D. The solution will create redundancy and improve disk read/writes.

Answer: A

RAID-5 uses one hard drive for parity so it creates redundancy. The parity drive would decrease both read and write performance compared to a RAID 0 (disk striping).

Q. 68

The Network OS on a server has recently been updated. Some of the hardware on the system is no longer operating. Which of the following should be done to fix the problem?

- A. Reinstall the old Network OS
- B. Replace the hardware in question.
- C. Test the hardware on another system.
- D. Check for drivers specific to the new Network OS.

Answer: D

To solve the problem, to make the hardware work on the new OS, we should check for the latest device drivers for the new Network OS.

Q. 69

When the software on the "/" file system of a new server was configured, an error occurs and the server will no longer boot. Which software is required to recover from the failure and continue configuration?

- A. Novell NetWare CD-ROM
- B. Unix Boot diskette(s)
- C. IBM OS/2 Startup disk and installation disk.
- D. ERD and/or installation disks with CD-ROM

Answer: B

The root directory of the UNIX file system is denoted "/". The entire system appears to be one contiguous file system, starting from the root directory "/".

Q. 70

A technician has created an array composed of four 9-GB hard drives. Two weeks later, the server is working fine; however, the customer calls to complain that the system only recognizes 27 GB of disk space. What would best explain the situation?

- A. The customer is running RAID 5.
- B. One of the hard drives has failed.
- C. One of the logical drives has failed.
- D. The customer is running RAID 5 with a hot spare.

Answer: A

RAID-5 uses one disk for parity. In a four-disk RAID-5 configuration only three disks would be available for data.

Q. 71

During initial installation of a Network OS on a server, the technician configures OEM SCSI and NIC drivers. After completing the installation, the latest Network OS patch is applied. During the installation of the patch, the technician is prompted to overwrite newer files several times. He does as prompted. When rebooting, the system halts. Which of the following could have prevented this problem?

- I. Reinstalling the SCSI and NIC drivers after the patch
 - II. Not overwriting newer files
 - III. Replacing all overwritten files before rebooting
 - IV. Upgrading OEM drivers from the Web before rebooting
-
- A. III and IV only
 - B. I, II, and III only
 - C. I, II, and IV only
 - D. I, II, III, and IV

Answer: C

The OS patch overwrites the OEM SCSI and NIC drivers. We could avoid this problem by:

- reinstalling the SCSI and NIC drivers after the patch was applied. (I)
- Not overwriting newer files. (II)

- Upgrading OEM drivers before rebooting.

We should replace all overwritten files before rebooting since that would nullify the OS patch.

Q. 72

When should a new BIOS version be implemented on an existing server?

- A. After the BIOS data expires
- B. When functionality will be affected
- C. Whenever a new version becomes available
- D. Within one year of purchasing the server

Answer: B

A new BIOS version should only be applied to the server when it is required. It should only be installed if the functionality of the server requires a BIOS upgrade.

Q. 73

A company wants to establish measurements and performance checks. The technician recommends that the company start comparing the server baselines to current server performance. Which of the following is the best time to be considered for this analysis?

- A. During non-business hours
- B. During server-backup periods
- C. During planned maintenance periods
- D. During average network utilization

Answer: D

The baseline should be established during average network utilization.

Q. 74

The server is set to perform a full data backup to a single tape every Friday, and a differential backup Monday through Thursday. Each backup is overwritten to a different tape. Four tape sets are maintained. If the system requires full restoration on Wednesday before the daily backup. How many tapes will be used to restore?

- A. 1
- B. 2

- C. 3
- D. 4

Answer: B

First we must restore the full backup from Friday, then we only need to apply the latest differential backup since a differential backup includes all changes made since the last full backup.

Q. 75

Where are SNMP thresholds set?

- A. ARP Table
- B. SNMP monitor
- C. SNMP service layer
- D. Vendor-provided MIB file

Answer: D

SNMP thresholds are set in vendor-provided MIB files.

Note: The job of communicating the meaning of the parameters exposed via SNMP is assigned to a file known as a management information base (MIB). This file contains detailed information about the information exposed by a device or agent and a description of what the exposed information means. MIBs are simple text files based on the Abstract Syntax Notation (ASN).

Q. 76

Which of the following should be done to ensure the redundant hardware components will be functional in the event of a failure?

- A. Simulate a hardware failure.
- B. Check the system and health logs for the appropriate systems.
- C. Remove each redundant component and test them in a test server.
- D. Remove each component and test them individually with a multimeter.

Answer: A

The redundant components should be tested in order to ensure that they would be functional in the event of failure. The most realistic test would be to simulate a hardware failure and check if the redundant hardware will work.

Q. 77

A drive in a RAID 5 array has failed. The administrator was not aware of this issue. Users complained about server access being slow. What is the most efficient method of alerting the administrator about the drive failure?

- A. Enable event logs
- B. Configure remote notification
- C. Schedule daily hardware visual checks
- D. Enable Network OS alerts on drive enclosure

Answer: D

We should make sure that the administrator should be notified one disk in the RAID-5 array has failed. This will be established by enabling the Network OS alerts on drive enclosure.

Note: The vendor-supplied software will be able to monitor the drive cabinet and report on failures, such as power supply or drive failures. The information provided by the drive cabinet's monitoring software is not otherwise available to the server until a failure occurs. This early warning is important if you have established a RAID array for fault tolerance, because the array is still susceptible to a drive enclosure failure if more than one of the drives in the array is located in the enclosure.

Incorrect answers

Event logs would not immediately notify the administrator of the problem. He would have to check the log files on a regular basis.

Remote notification would not inform the administrator of a failure of disk in a RAID-5 array. The OS would only be able to detect if the RAID-5 disk fails. We must use the monitor software in the Drive Cabinet.

Daily hardware checks would not minimize administrative effort. A more automatic approach is preferred.

Reference: Server+ Training kit, Installing a Drive Cabinet

Q. 78

The IT department is responsible for maintaining the company's 25 Web servers. It was determined that two additional Web servers of the same make and model were needed to provide adequate performance. Which of the following actions must be taken to ensure that the new servers are performing as expected?

- A. Download and install the most recent Network OS patches.
- B. Perform a baseline and compare the two new servers to each other.
- C. Download and install the most recent BIOS and firmware on the new servers.
- D. Perform a baseline and compare it to the baselines of previous server installs.

Answer: D

By comparing the baseline of the new servers with the baseline of existing web servers we can easily ensure that the new servers has the same performance.

Q. 79

A technician performs daily backups. The backup solution contains a verification tool for every backup. A file server experienced catastrophic failure. Recovery attempts failed. Which of the following can be done to minimize the risk of this happening again?

- A. Install a UPS.
- B. Replace the verification tool.
- C. Develop a plan to test backups.
- D. Install vendor patches for the verification tool.

Answer: C

It is not enough to verify backups. The backups should be tested as well.

Q. 80

Which of the following connectors are used on SCSI cables?

- I. 68-pin VHDCI.
 - II. 36-pin Centronics
 - III. 50-pin Centronics
 - IV. 68-pin High Density
-
- A. I and III only.
 - B. II and III only.
 - C. I, II, and IV only.
 - D. I, III, and IV only.

Answer: D

VHDCI, Sometimes called SCSI-5. Very popular in RAID cards



68-pin High Density



Centronics C50:



Incorrect Answer:

36-pin Centronics is a printer interface, not a SCSI interface.

Q. 81

A customer's file server is connected to three external storage enclosures. After a new UPS is installed, users complain that they are unable to access their private storage, but they can access public storage. Which of the following most likely caused this problem?

- A. The UPS is not working.
- B. File sharing was disabled.
- C. The server was powered on before all of the external storage enclosures.
- D. Data was corrupted during the installation of the UPS causing missing files.

Answer: C

The external storage enclosures must be powered on first. This will enable the Server to detect them when the OS boots.

Q. 82

A company's server technician has installed an external tape device. The drive is connected to the same channel on the SCSI adapter as an internal drive, and termination on the drive is enabled. Upon rebooting, the server does not recognize the tape device. Which of the following is the most likely cause of this failure?

- A. Termination on the SCSI adapter was not disabled.
- B. Termination on the tape device was not disabled.
- C. Termination on the internal drive was not disabled.
- D. A SCSI adapter cannot support both internal and external devices.

Answer: B

The SCSI channel is already terminated twice. Once on the adapter and once on the internal drive. We must disable termination on the external tape device. We cannot have three terminations.

Q. 83

During the setup of a new site, an external Ultra2 RAID storage unit is to be installed. Which of the following is **NOT** likely to cause a problem when the external RAID storage unit is installed?

- A. Using passive termination on the enclosure.
- B. Using a SCSI cable between one and five meters in length.
- C. Attaching the subsystem to the server while it is powered up.
- D. Powering off the RAID subsystem when the server is turned on.

Answer: B

Ultra2 can use a cable up to 12 meters in length. A SCSI cable between one and five meters would not cause a problem.

Q. 84

A server, external RAID array, external tape library, and UPS need to be mounted in a rack. Which of the following best describes the recommended installation practice?

- A. Lay out the rack according to the vendor's specification.
- B. Lay out the rack from top to bottom, installing the lightest equipment first.
- C. Lay out the rack from bottom to top as UPS, RAID controller, tape library, server and then any peripherals.
- D. The order of equipment makes no difference as long as all components fit in the rack, cables reach all equipment, and heat-producing items are the top of the rack.

Answer: C

The rack should always be stacked from bottom to the top in order to ensure a stable and safe rack.

Q. 85

A UPS needs to be purchased to protect two new servers that have been ordered. Which of the following is most important to consider when purchasing the UPS?

- A. VA rating.
- B. UL rating.
- C. Clamping voltage.
- D. Length of the UPS cord.

Answer: A

The Volt Ampere (VA) rating of the UPS is the most factor when decide which UPS should be acquired.

Note: How to decide which UPS that would be adequate.

Determine the volt amp (VA) required for all of the equipment. This is done by adding the amperes drawn by the equipment and multiplying the total by the output voltage. Add roughly 15% to allow for future growth and round up to the nearest VA rating available in the product series you have selected.

Q. 86

A technician is verifying a pre-installation plan that calls for a RAID 5 array with a hot spare. The RAID 5 array must be able to store a slow-growing database, currently containing 20 GB of data. The server technician receives four SCSI drives (each 5 GB in size) and an external hot-swappable drive enclosure. The technician needs to report on the availability of the RAID 5 array to support the plan.

Which of the following, if anything, is needed for this installation?

- A. One additional 5 GB drive.
- B. Two additional 5 GB drives.
- C. Three additional 5 GB drives.
- D. The current configuration is acceptable.

Answer: C

We need to support a 20GB slow-growing database on a RAID 5 array. The RAID 5 array must include one hot spare drive. We cannot use exactly 20GB for the database since it slowly growing. We must use five 5 GB drive, which gives 25GB, to store the data. Then we need one drive for parity and one drive as a hot spare. In total we need seven 5GB drivers. Currently we have four drives, so we need three additional drives: two for the RAID 5 array, and one for the external hot-swappable drive enclosure.

Note: To add more redundancy, you can assign one hot-spare drive to one array or to a set of arrays. This hot spare will replace a failed drive and become part of the RAID 5 array until the failed drive is replaced. This permits two failures in any given array without any loss of data.

Q. 87

When following an installation plan, the technician should verify availability of which of the following?

- I. Power source.
- II. UPS capacity.
- III. Physical space.
- IV. Network access.

- A. I and II only.
- B. II and III only.
- C. I, III, and IV only.
- D. I, II, III, and IV.

Answer: C

The following activities should be included in the verification of an installation plan:

- Verify the power outlet for the network server is available and active (I)
- Verify the location where the server is to be installed is ready for installation (III)
- Verify the network connection is available and active (IV)
- Verify all the hardware for the network server has arrived
- Verify all the hardware for the network is as specified in the installation plan

UPS capacity is not included in an installation plan.

Q. 88

When a server installation is being planned, which of the following resources should be used to obtain the most current hardware compatibility information?

- A. Operating system CD.
- B. Hardware installation CD.
- C. Hardware installation manual.
- D. Operating system vendor Website.

Answer: D

The OS vendor website would include the latest Hardware Compatibility List (HCL).

Q. 89

After having five new cables added by a certified cable vendor, a system engineer notices that the new cables have not been labeled on the punch down block. Which of the following uses best industry practice in determining where each network cable terminates?

- A. Use cable tester to trace each new cable to its termination point and label accordingly.
- B. Use network sniffing equipment to determine the MAC address of each cable and label accordingly.

- C. Disconnect each of the net network cables and connect a PC to each termination point. Reconnect the new network cables and label accordingly when the PC is connected to the network.
- D. Do nothing, there is no need to know where the cabling terminates.

Answer: A

We should use a cable tester to test to trace the termination point of each cable.

Q. 90

Before installing new, pre-tested server hardware, a technician performed the following tasks: Inventoried the hardware, checked the HCL, and checked the network port. Upon startup of the system, the UPS starts beeping. Which of the following did the technician fail to verify?

- A. The available power.
- B. The presence of a UPS serial cable.
- C. The KVM (Keyboard Video Mouse) installation.
- D. The temperature of the room is within proper parameters.

Answer: A

The available power is not enough.

Incorrect Answers

The lack of UPS serial cable would not make the UPS beep when the system is started.

KVMs does not influence a UPS in any way, they are used to control several servers from a single keyboard, mouse, and monitor.

The temperature of the room will not cause the UPS to beep.

Q. 91

A customer provided web server hosting for a number of clients. Each server and their storage subsystems must also be secured. Which of the following will provide the required physical access protection?

- A. BIOS passwords.
- B. Server keyboard locks
- C. Cabinets with locking doors.
- D. KVM (Keyboard Video Mouse) switch.

Answer: C

Cabinets with doors that have locks would provide physical access protection.

Q. 92

An external SCSI hard drive has been added to a file server. The hard drive has been configured to use an available SCSI ID. The SCSI controllers BIOS is unable to see the drive. Which of the following actions should be performed first to resolve the issue?

- A. Reinitialize the drive
- B. Low-level format the drive
- C. Check and reconfigure termination if necessary
- D. Change the SCSI ID to the lowest available number

Answer: C

A SCSI segment must be terminated. This is the first we should check.

Q. 93

A technician performing an audit of the server room environment notices a few problems. Which of the following observations should figure most prominently on the audit report?

- A. The server cabinet is unlocked.
- B. There is a trashcan in the server room.
- C. There is a box of spare parts on the floor.
- D. There is a full cup of coffee on top of the server.

Answer: D

A cup of coffee on top of the server is a physical threat to the server.

Q. 94

A client desires to install a dial-up server for remote access to allow 100 telecommuters to logon to the network for daily file transfers. Which of the following deployment consideration is **LEAST** critical to successful deployment?

- A. Adequate power source.
- B. Availability of modems.
- C. Availability of active phone lines.
- D. Availability of Virtual Private Network (VPN).

Answer: D

The remote access server must have an adequate power source, there must be enough modems to support many simultaneous connections, and there must be available active phone lines.

VPN would increase security but is not strictly required. VPN is more common for connections through the Internet.

Q. 95

ESD (Electrostatic Discharge) can be reduced by installing:

- A. A UPS.
- B. A dehumidifier.
- C. Adequate grounding.
- D. Fluorescent lighting.

Answer: B

Adequate grounding, for example a grounding mat, would reduce ESD.

Incorrect Answers

An UPS would not prevent ESD.

Dry air can cause ESD. Humidifier, not dehumidifier, is used to decrease ESD:

Fluorescent lighting has no impact on ESD.

Q. 96

A server currently uses an Ultra2 SCSI controller. A directive to install an Ultra ATA 100 drive is ordered by management. Which of the following reasons would prevent a technician from using this drive?

- A. Ultra2 to Ultra 100 requires a converter.
- B. Ultra2 does not support Ultra ATA 100 drives.
- C. Ultra2 uses a 50-pin connector; Ultra ATA 100 uses 68 pins.
- D. Ultra2 uses an 80-pin connector; Ultra ATA 100 uses 40 pins.

Answer: B

Ultra2 is a SCSI controller, but Ultra ATA 100 driver is an IDE drive. SCSI and IDE are incompatible.

Q. 97

A server technician has been brought in to perform the following to a server:

- Relocate the server to another room
- Add a SCSI controller and external CD tower to the server
- Apply the latest patch to the Network OS

When preparing for the system upgrade, the technician should perform which of the following first?

- A. Perform system backup
- B. Update the Network OS version
- C. Disconnect the server from the network
- D. Unplug the server from the power source

Answer: A

First we should perform a system backup to enable recovery in case of failure.

Q. 98

A technician performs a full backup of the file servers every Monday at 7:00 PM. The tapes are sent to an offsite storage center the following morning. He uses one tape per server. Differentials are performed daily throughout the rest of the week at 7:00 PM. One of the servers fails Saturday at 5:00 PM and must be recovered. What would be the best course of action?

- II. Restore the Monday Full backup tape.
 - III. Restore all of the previous week's Differential backup tapes.
 - IV. Restore the Friday Differential backup tape.
 - V. Restore the Saturday Differential backup tape.
-
- A. III only
 - B. I and II only
 - C. I and III only
 - D. I and IV only

Answer: C

We must first restore the full backup. Then we only need to restore the last differential backup since each differential backup includes all changes made since the last full backup.

Q. 99

A company maintains all backup tapes in a server room that is not fireproof. Management would like a solution that will offer timely recall and data protection, and has defined timely recall as getting the tape in the hands of

the person responsible for recovery, within four hours. Data protection is defined as protection of the backup tapes from fire or flood.

Which of the following is the best solution for this company?

- A. Store the tapes in a fireproof safe at the local facility.
- B. Store the tapes at the administrator's home ten minutes away.
- C. Store the tapes at a remote location one hour away in an unused secured closet.
- D. Store the tapes at a professional storage facility with a two-hour turn-around.

Answer: D

Offsite storage of the tapes at a professional storage facility gives the best security. The time constraint is also met by this proposed solution.

Q. 100

When planning an installation of a server, Network OS, and a third-party device, the technician notes that the third-party hardware is not on the Network OS vendor's HCL. Under which of the following circumstances would the technician proceed with the installation?

- A. The third party device is Plug-and-Play.
- B. The server hardware vendor is manufacturer of the device.
- C. The device manufacturer provides a driver for that Network OS.
- D. The Network OS HCL lists a similar device from the same manufacturer.

Answer: C

If the network adapter manufacturer provides a device driver for this particular OS it is likely that the adapter would function without any further problems even though it is not listed on the HCL.

Q. 101

A new application server arrived configured with an Ultra ATA drive. The pre-installation plan requires that the server technician add a set of ten 18-GB SCSI hard drives and make a SCSI drive the boot drive. The technician installed and configured the drives and rebooted the system. The server continues to boot from the Ultra ATA drive. Which of the following is the likely cause of this problem?

- A. The SCSI device is not properly terminated.
- B. The SCSI device is not configured as a boot device.
- C. The BIOS automatically routes Int40 to the IDE bus.
- D. The Ultra ATA drive has been set to Master and not Slave.

Answer: B

A SCSI hard drive must be configured as the boot device.

Q. 102

A customer has complained about repeated network failures. The server's network cable is frequently found loose or disconnected. Which of the following solutions is **NOT** appropriate solution to the problem?

- A. Replace the cable connector.
- B. Solder the cable to the server.
- C. House the server in a lockable cabinet.
- D. Restrict access to the server to administrators.

Answer: B

We could replace the cable connector, or make the cabling inaccessible by using a lockable cabinet or restricting access to the server to administrators.

We should solder the cable to the server as it would be awkward to replace the cable or the network adapter of the server in case of failure.

Q. 103

A client has identified a room to install a new server rack. Which of the following environmental issues is **LEAST** critical to the server specialist?

- A. Heavy dust on the floor.
- B. Discolored ceiling tiles.
- C. A painted concrete floor.
- D. Overhead sprinkler system.

Answer: C

A painted concrete floor would have little or no environmental impact.

Discolored ceiling tiles could indicate a water leakage which could be very harmful to computers.

A dusty environment could be harmful to the servers.

A sprinkler system cannot be accepted in a server room.

Q. 104

An EISA server at a client site has an ISA NIC. The administrator has noted that an EISA NIC is available, and wants to upgrade to the EISA NIC. Which two of the following applies to this potential upgrade?

- II. The ISA bus is faster than the EISA bus, therefore there is no performance gain.
 - III. The EISA card will need to be configured in the system configuration tool.
 - IV. The EISA card will process incoming packets faster, due to the faster system bus.
 - V. EISA technology was made for video and should not be used for network I/O.
-
- A. I and II
 - B. I and IV
 - C. II and IV
 - D. II and III

Answer: D

ISA and EISA cards are not Plug and Play enabled. We need to configure it manually. (II)
Extended ISA is an improvement over ISA. It has a faster system bus. (III)

Q. 105

A user would like to increase network bandwidth to the server. Which of the following technologies would **NOT** provide bandwidth?

- A. Multi-homing
- B. Load balancing
- C. Port aggregation
- D. Subnetting

Answer: D

Subnetting would decrease network traffic by dividing the network into subnets. It would not, however directly increase the network bandwidth to the server.

Incorrect Answers

Multihoming is achieved by installing more than one network adapter on the server. This will increase the network bandwidth to the server.

Load balancing would increase the performance of the server. The server and its load balancing partners would be able to process more network traffic.

Port aggregation is the combining of two NIC ports with one IP address. This enables fault tolerance and optimizes server availability. It also increases network bandwidth.

Q. 106

A server hardware upgrade requires the use of a legacy NIC. Which of the following steps ensures that this upgrade produces no hardware conflicts?

- A. Plug-and-Play should be disabled on the system board.
- B. The Network OS should be configured to run in ISA-compatibility mode.
- C. Verify that system resources are available.
- D. All other expansion cards should be removed from the system before installing the new card.

Answer: C

To ensure that the legacy NIC will function we must verify the system resources it demands are available.

Q. 107

A server exists in a remote location. Last week as service/daemon on the server crashed, and while the application fault was logged, no one in the IT department noticed it. Major departmental functions were affected. Which of the following would have allowed the problem to be recognized immediately?

- A. Implementing systems management software.
- B. Routinely logging into the server using remote software.
- C. Routinely monitoring server health, system, and application logs.
- D. Enabling automated system recovery to bring server down after service/daemon halts.

Answer: A

To immediately be notified by any failed or crashed network services we must configure alerts. Systems management software is needed to implement this.

Incorrect Answers

Routinely checking server status would improve the detection but it would not immediately alert administrators of the occurring problems.

An automated recovery system could handle many errors and bring the system online after a crash. It would not be able to restart from all problems, and it would not make the administrators aware of the problems immediately.

Q. 108

A company has a pair of servers: a primary server and a secondary server for failover. The primary server is backed up and verified on a routine basis. Both servers are on a UPS. Which of the following should be done to insure maximum system reliability?

- A. Install redundant NICs in the primary server.
- B. Create SNMP traps to report server hardware failure.

- C. Install redundant heartbeat links between the servers.
- D. Routinely test the secondary server in the production environment.

Answer: D

The secondary server should routinely be tested in the production environment.

Q. 109

A fan-cooled server rack cabinet contains three servers and a UPS. The temperature in the cabinets is always significantly higher than the room temperature. Which of the following activities would offer the best solution for lowering the temperature inside each of the server cases?

- A. Take the case covers off the three servers.
- B. Install an additional cooling fan to each server.
- C. Install a higher performance CPU fan in each server.
- D. Increase the airflow through the rack cabinet with better fans.

Answer: D

We should replace or add better fans to the rack cabinet.

Incorrect Answers

Removing the case covers could decrease the air flow and make the problem worse.

Adding better cooling fans to the rack is a more practical solution than replacing or adding fans on each server.

Q.110

A server has been running with not trouble for the past two years. The system has RAID 5 and is backed up and verified on a regular schedule. The server is on UPS and all the components are secured via key locks in a server room with a raised floor. What else could be done to improve system reliability?

- A. Install a second CPU.
- B. Arrange to store a set of backup tapes offsite.
- C. Apply the latest version of Network OS patch and/or upgrade.
- D. Routinely press the self-test button on the UPS after hours.

Answer: B

System reliability could be improved by storing backup tapes off site.

Incorrect Answers

The system has been running for two years without problems so there is no need to change either hardware (adding a second CPU) or apply latest Network OS patch/upgrade.

Testing the UPS could improve reliability. But it is not a major issue since most UPS are self-monitred.

Q.111

A company server is connected to a RAID 5 storage subsystem. A drive failure occurs and goes unnoticed. Three weeks later, an additional drive fails and all data is lost. Which of the following would have prevented the array failure?

- A. Using hot-swappable drives.
- B. Performing regular tape backups.
- C. Flashing the RAID controller BIOS.
- D. Enabling remote notification of the drive failure.

Answer: D

We should have enabled remote notification of drive failures. This would have notified the administrator as soon as the first disk in the RAID 5 array failed.

Q.112

A company that has expanded from two servers to ten servers continues to perform daily full backups. The company would like to significantly reduce the amount of time used to backup the systems, while having the shortest possible restore time in the event of failure. Which of the following solutions would best fit the company's needs?

- A. Maintain the current solution of daily full backups.
- B. Perform an incremental backup every Monday through Sunday.
- C. Perform a full backup every Monday and a differential backup Tuesday through Sunday.
- D. Perform a full backup every Monday and an incremental backup Tuesday through Sunday.

Answer: C

Differential backups are quicker than full backups since they only backup information that has changed since the last full backup. Restoring a differential backup is fast as well. First we restore the full backup and then we restore the last differential backup. Incremental backups take more time to restore.

Q. 113

A server had two 64-MB DIMMS and a 256 MB DIMM was added. After installing the additional memory, POST errors are generated. What is the most likely cause of the failure?

- A. 64 MB DIMMs and 256 MB DIMMS are not compatible.
- B. The server's existing memory is slower than the new memory.
- C. The server has both registered and nonregistered memory installed.
- D. POST messages are normal when mixing DIMM capacities.

Answer: A

The most likely problem is that the 64MB and the 256MB are not compatible.

Incorrect Answers

Different memory speeds would not be a likely problem. The faster memory would run at the slower speed.

Memory does not have to be registered in order to function.

POST messages are not a normal with any type of memory.

Q. 114

A customer has three identical servers (WEB_01, WEB_02, WEB_03) configured in their web farm. Downtime has been scheduled for the web farm on Friday evening. During software installations WEB_01, the monitoring agents were updated to the latest version.

What is the recommended additional procedure, if any, for the web farm?

- A. Update WEB_02 and Web_03 to the same version monitoring agents.
- B. Disable the agents on WEB_02 and WEB_03 until they can be updated.
- C. Configure the agent on WEB_01 to communicate with the older agents on WEB_02 and WEB_03.
- D. No action is required.WEB_02 and WEB_03 will be automatically updated.

Answer: C

We should configure the updated monitoring agent to communicate with the older agents.

We should not be forced to upgrade the agents on the other web servers.

Q. 115

An existing UPS has succeeded in preventing immediate, unplanned shutdown, but the run time on a fully-charged battery is too short for a clean shut down of the Network OS. What step should be taken to improve the amount of available battery run time?

- A. Install a higher capacity UPS.
- B. Increase the charge time on the UPS.
- C. Connect the UPS to a dedicated circuit.
- D. Configure the advanced power management on the server.

Answer: A

We must replace the UPS with an UPS with increased battery time that will ensure that the server can be shut down gracefully.

Incorrect Answers

Changing the charge time or connecting the UPS to a dedicated circuit would not increase the available battery run time.

The advanced power management on the server can be configured for an unattended operating system shutdown in the event of an extended power outage. The advanced power management cannot be used to improve the amount of available battery run time in any way though.

Reference: American Power Conversion Delivers Uninterruptible Power Supply Management in Windows XP

Q. 116

After Network OS installation, the clients can log into the new server, but cannot ping the server. Any of the following may cause problem **EXCEPT**

- A. There server has no DNS entry.
- B. TCP/IP is not loaded on the server.
- C. There is no entry in the HOSTS file.
- D. The ping daemon is not loaded on the server.

Answer: D

There is no such thing as a ping daemon. The 'ping' command generates "ICMP echo request" packets (ICMP is the "internet control messaging protocol"). There is no daemon that generates the ICMP echo replies. Those are generated by the kernel.

Note: A daemon on a UNIX/LINUX system is approximately the same thing as a service on a Windows system.

Incorrect Answers

A name resolution problem, for example a missing entry in the DNS zone or in a HOSTS file, could prevent a computer from pinging the server by name, but it would still be able to logon to the server using the IP address of the server.

There could be another network protocol in use instead of a TCP/IP. The Ping utility only works with the TCP/IP protocol.

Q. 117

While auditing a client site, the technician notices that the SNMP monitor has a high volume of messages from the servers indicating that each server has reached 5% network utilization. The alerts were configured by the previous administrator. Which of the following actions should be taken?

- A. Raise the SNMP network utilization threshold.
- B. Call in a network cabling expert to resolve the errors.
- C. Subnet the network to decrease the size of the collision domain.
- D. Set a filter on the SNMP monitor to stop displaying the network utilization messages.

Answer: A

Every time the network utilization has reach 5% a network alert is generated. The alert threshold should be raised. Too many alerts are generated with such a low threshold.

Q. 118

A file server is experiencing a dramatic increase in memory pages per second and a simultaneous decrease in CPU utilization. Which of the following is most likely the cause?

- A. The server's CPU cache is malfunctioning.
- B. The server is running out of virtual memory.
- C. The server is running out of physical memory.
- D. The server's processor is inadequate for the task.

Answer: A

The increase in memory pages/second normally indicates that the server is running out of physical memory. This would also cause an increase in the CPU utilization since the CPU would have to swap content between the physical memory and the virtual memory. But in this scenario a decrease in CPU utilization is reported instead. This indicates that there is some problem with the CPU, possibly a malfunctioning CPU. The malfunctioning CPU is causing the increase in memory pages per second.

Q.119

A small company owns a file server that shuts down frequently. After a great deal of troubleshooting, the server technician discovers the system is overheating and that there is a large buildup of dust in the server. What can be done to improve reliability?

- A. Use compressed air to clean out the server.
- B. Clean the server and set up a cleaning maintenance schedule.
- C. Obtain an air compressor and use it to clean out the server.
- D. Bring in his vacuum from home and use it to clean out the server.

Answer: B

We should clean out the server and ensure that in the future we do it on a regular basis.

Q. 120

A technician tasked with creating backup procedures needs to provide a company with a backup plan. Which of the following provides minimal risk of data loss in the event of a hard drive failure?

- A. Weekly full backup.
- B. Daily incremental with weekly full backup.
- C. Daily differential with weekly full backup,
- D. Weekly full backup to a remote data facility.

Answer: C

A weekly full backup with daily differential backups provides minimal risk of data loss. Incremental backups are somewhat less secure since all incremental backups since the last full backup are required, but a differential restore only requires the last differential backup.

Q. 121

A server at a client site failed for the second time last week. The network management software was never alerted that any thresholds had been reached. Which of the following should be done first?

- A. Add more memory to the server.
- B. Verify the SNMP configuration.
- C. Move the server to another subnet.
- D. Replace/Update the mass storage subsystem.

Answer: B

The Simple Network Management Protocol (SNMP) configuration must be adjusted since the alerts never fired.

Q. 122

A company's IT department is adding additional CPUs for SMP (symmetrical multiprocessing). Where should they check first to verify that the additional CPUs are recognized?

- A. In the BIOS setup

- B. In the system log
- C. During the Network OS load
- D. In the Network OS monitor utility

Answer: A

The BIOS setup would show all detected CPUs.

Q. 123

A server uses a RAID 5 array, tape drive, NIC, and a Grandfather-Father-Son (GFS) backup scheme. Which of the following will increase the availability of the server?

- A. Change the RAID 5 to RAID 0
- B. Add another NIC for failover
- C. Add another tape drive for failover
- D. Change the differential backup scheme

Answer: B

A second NIC for failover would increase the availability of the server.

Incorrect Answers

Changing from RAID 5 to RAID 0 would decrease availability.

Another tape drive would not increase availability of the server.

The Differential backup scheme would not be an improvement of the full backup scheme in terms of availability.

Q. 124

A technician is concerned about how natural disasters would affect their existing disaster recovery plan. Which of the following disaster recovery plan modifications should be implemented to address this situation?

- A. Use a remote hot site.
- B. Use a local media safe.
- C. Stock adequate hardware.
- D. Backup to another local server for redundancy.

Answer: A

A remote hot site would not be affected by a natural disaster at the main location.

Incorrect answers

Local facilities, like a local media safe or backing up to a local server, would give protection from a natural disaster.

Stacking up hardware would not be of much help addressing the problem of a natural disaster.

Q. 125

Which of the following would **NOT** provide redundancy for a server in the event of failure?

- A. RAID 0
- B. RAID 1
- C. Disk duplexing
- D. Network adapter teaming

Answer: A

RAID 0, disk striping, improves disk performance but does not provide redundancy.

Q. 126

A server recently had its video card replaced under warranty by the manufacturer. Since the repair, the system only displays in VGA mode. Which of the following would be the most effective solution to apply first?

- A. Replace the monitor, as it is damaged.
- B. Replace the video card, as it is defective.
- C. Replace the system board, as it is defective.
- D. Replace the device driver, as it is incorrect.

Answer: D

A video adapter with an incorrect driver would only use VGA mode. We need to install a correct device driver for the video card.

Q. 127

Of the following actions, which is the best way to create a server baseline?

- A. Run an SNMP agent continuously for a week.
- B. Run an SNMP agent at random times each day during the week.
- C. Run performance monitoring software continuously for 72 hours.
- D. Run performance monitoring software at the same time each day for a week.

Answer: D

To establish a baseline we should monitor the performance with monitoring software (system monitor on Windows 2000/XP systems), not running an SNMP agent. We should try to monitor typical network performance. It is not necessary to continuously monitoring the system for a prolonged amount of time. Instead we should monitor at several occasions.

Q. 128

Two servers need a connection between them to establish a heartbeat monitor for a software monitoring tool. The System Administrator requests that COM1 be used on each server to establish this connection. This technician must obtain a cable to accomplish this task.

Which of the following types of cables is most likely to be used?

- A. DB9 cable
- B. IEEE-1284 cable
- C. Null modem cable
- D. Standard serial cable

Answer: C

We need a null modem cable, a twisted serial cable, to connect two computers using the serial (COM) interface.

Q. 129

When a performance baseline was created, a peak of 100% CPU utilization was observed more than once. The performance sample was taken at 5-second intervals during normal business hours. The application response time has been acceptable. Which of the following is the most likely reason for this serve behavior?

- A. The CPU is probably faulty.
- B. The system behavior is normal.
- C. The server is unable to handle the required load.
- D. The baseline has to be taken over a 24-hour period.

Answer: D

We should take longer samples. Too short samples could give a false view.

Q. 130

A customer uses a 24 GB DAT drive for backup purposes. The drive has been intermittently failing during backup jobs. To resolve the problem, the customer cleaned the drive and purchases new DDS-3, 120m tapes. The drive now fails on all jobs. Which of the following will most likely resolve this problem?

- A. Use compatible media.
- B. Replace the tape drive.
- C. Replace the SCSI controller.
- D. Clean the drive additional times.

Answer: B

We need to replace the tape drive. The other alternatives does not apply.

Incorrect Answers

DDS-3 can store 24GB of data. DDS-3 tapes can be used in 24GB DAT drive.

It is not likely that the SCSI adapter should have failed.

Additional cleaning of the drive would not help.

Q. 131

A new server has been installed at the main complex of a company.

- By pinging the local gateway from the new server, a server technician has verified the presence of a good LAN connection.
- Users from a remote site cannot connect to the new server but can connect to all other servers at the remote site.
- When the technician tries to ping the remote site from the new server, it times out.
- The IP stack was removed and reinstalled but that did not help.
- When pinging the router at the remote site from the new server, it also times out.

Which of the following is the most appropriate action to take?

- A. Enable DHCP on the server.
- B. Wait for the new server to be recognized by the routers.
- C. Inform the network administrator responsible for routers.
- D. Plug the network cable into a different port in the switch.

Answer: C

A misconfigured or faulty router could explain the problems.

Incorrect Answers

The server can ping the local gateway so it has proper IP configuration. There is no need to configure it as an DHCP client.

Routers do not recognize servers or computers. They recognize other routers.

The server can ping the default gateway so the connection to the switch works already.

Q. 132

A customer needs to minimize the amount of time required for each weekday backup. The best choice of daily backup for this customer would be

- A. Daily full
- B. Daily incremental and weekly full
- C. Daily differential and weekly full
- D. Grandfather-Father-Son (GFS)

Answer: B

Daily incremental backup with a weekly full backup minimizes the daily backup time (but requires more time for restoring).

Q. 133

In a standard Grandfather-Father-Son (GFS) backup rotation scheme, where is the best place to store the Grandfather media sets when the data is going to be permanently archived?

- A. In a secure onsite storage location
- B. In a secure offsite storage location
- C. In the server room in a fireproof cabinet
- D. In an adjacent room in a fireproof cabinet

Answer: B

Permanently archived data should be stored in a secure offsite storage location.

Q. 134

After a full backup has completed for the previous day, which of the following would be the most effective method of verifying that the backup tape is useable for restoring the data?

- A. Use the backup software "verify" option.
- B. Read the contents of any text file directly from the backup tape.
- C. View the backup session log file to verify all directories and files are present.
- D. Restore sample data to verify success of the backup.

Answer: A

The verify option of the backup software is the most effective method to check the integrity of the backup tapes.

Q. 135

A company has a new disaster recovery requirement. It states that the media have minimum five-year storage life and capability to back up their 80 GB database. Which of the following technologies would provide the best solution for this company?

- A. DLT
- B. CD-RW discs
- C. WORM discs
- D. QIC-80 Tapes

Answer: A

There are DLT tapes and DLT tape drives that supports up to 120 GB of data (or more).

Incorrect Answers

CD-RW and WORM discs does not even support 1GB, typically 650-800MB.

QIC-80 tapes might be able to store 1GB, but nowhere near 80GB.

Q. 136

What is the primary advantage, if any, of implementing RAID 5 over implementing RAID 1?

- A. RAID 5 does not have an advantage over RAID 1.
- B. RAID 5 more efficiently utilizes storage capacity.
- C. RAID 5 provides better data integrity.
- D. RAID 5 generates less processor overhead.

Answer: C

RAID 1, mirroring, only has a 50% storage utilization. RAID 5 with the minimal three disk drives has a 66% utilization of the disk space (one disk is used for parity). RAID 5 with more drives has even higher disk utilization: Four drives: 75%, Five drives: 80%, etc.

Incorrect Answers

RAID 5 has a better disk utilization.

They provide a similar degree of data integrity.

RAID 5 generates more processor overhead since the parity bit must be calculated.

Q. 137

An e-commerce company has a web server with a network adapter that fails under a heavy load. The server technician finds there is a patch available for the Network OS that corrects the problem. Which of the following steps is **LEAST** important to consider when installing the patch?

- A. Reboot the server.
- B. Reinstall the Network OS.
- C. Install other software patches.
- D. Make a full backup of the system.

Answer: B

Before installing a batch we should make a full backup of the system. We should then install the network patch and possibly other network patches as well. After rebooting the server the system should be functional. There is no need to install the OS in order to install a patch.

Q. 138

When files on the SYS: volume of a new server were configured, an error is made and the server will no longer boot. Which software is required to recover from the failure and continue configuration?

- A. NetWare CDRROM
- B. Unix Boot/Root diskette(s)
- C. OS/2 startup disk and Installation disk.
- D. ERD and/or installation disks with CDRROM

Answer: A

Novell NetWare servers use a SYS volume. NetWare software is needed to solve the problem at hand. UNIX, OS/2 or Windows does not use SYS volumes. ERD is only used by Windows systems.

Q. 139

Two physically identical servers were acquired. One will be used for a mail server and one for a file server. Both servers were loaded from the same media. Immediately after installation, the system administrator noticed that each server has a Network OS executable file of slightly different size. Which of the following conclusions is most appropriate?

- A. This is a dynamic file.
- B. The file is infected with a virus.
- C. The servers' hard drive sector sizes vary.
- D. The disk controller is failing on one server

Answer: C

Different sector sizes would give different file sizes.

Q. 140

A remote email alert has been created to inform three key network personnel when any drive in a RAID array fails. While reviewing recent system events, one technician did not receive email alerts. Which of the following best explains why this happened?

- A. The email server is down.
- B. The technician is not on the same subnet.
- C. The technician's email address is misspelled.
- D. The technician is not logged on as an administrator.

Answer: C

His email address could have been misspelled.

Incorrect answers

A downed email server would affect other people as well.

There is no requirement to be on the same subnet to receive emails or alerts.

There is no requirement to be logged on as an administrator to receive emails or alerts.

Q. 141

Two new servers have been purchased and need to be installed to allow sharing of a single external hard drive enclosure. One of the servers is configured as a local file server, and the other as a database server for a different network. The onsite technician notices that when both servers are running at the same time, they each receive SCSI errors. However, when they are running individually, no errors are reported. What is the best source of information to troubleshoot this issue?

- A. The Network OS vendor's Website.
- B. The server vendor's FAQ Website.
- C. The drive enclosure vendor's user manual.
- D. The SCSI controller vendor's user manual.

Answer: C

The SCSI hard drive is shared through the external hard drive enclosure. We should check the manual of the enclosure in order to troubleshoot the problem at hand.

Q. 142

A Unix/Linux server needs to be powered down so that building power can be serviced. Which of the following command could the server technician use to shutdown the server?

- A. tar
- B. logout
- C. init 0
- D. system stop

Answer: C

Unix/Linux systems are shut down with the **init 0** command.

Q. 143

A company's server was crushed in a building collapse. Current data backups were stored offsite. The replacement server has been supplied with a DLT drive, rather than the TRAVAN drive that was in the older server. What impact will this have on the recovery of this server?

- A. The administrator will not be able to recover the data.
- B. The administrator must use a TRAVAN drive to recover the data and must buy new tapes for future backups.
- C. The administrator will be able to recover data using the DLT driver, but must buy new tapes for backing up data.
- D. The administrator will be able to recover data using the DLT drive and continue to backup on existing tapes.

Answer: A

DLT and TRAVAN are incompatible standards.

Q. 144

A server has lost two disks on its data array running RAID 5. The company deploys a Grandfather-Father-Son (GFS) backup rotation using incremental backups during the week. The company's disaster recovery plan stipulates any data that cannot be recovered from local tape resources must be acquired from the offsite tape storage location. The incremental backup was completed on Wednesday night, shortly before the server crashed. Backup media is still available locally.

Which of the following is the best procedure to recover the data?

- A. The tapes should be recovered from the onsite facility using tapes from Friday's full backup and Wednesday's incremental backup.
- B. The tapes should be recovered from the offsite facility using Friday's full backup and Wednesday's incremental backups.
- C. The tapes should be recovered from the onsite facility using Friday's full backup and Monday, Tuesday, and Wednesday's incremental backups.
- D. The tapes should be recovered from the offsite facility using Friday's full backup and Monday, Tuesday, and Wednesday's incremental backups.

Answer: C

The local tapes are still available. We are able to use the local tapes. We are only required to use offsite tapes if data cannot be recovered from the local tapes.

We must start to restore the full backup followed by each incremental made after the full backup in order.

Q. 145

RAID and system logs are showing that a drive in a RAID 5 array is reporting PFA (Predictive Failure Analysis) drive failures. Which of the following steps should be taken?

- A. Use the backup program to copy all the data from the drive to the tape. Replace the drive. Restore all of the data from the tape.
- B. Use a cloning utility program to create an exact mirror image of the drive. Replace the drive. Restore the cloned image to the next drive.
- C. Use the RAID utility program to "fail" or take the drive offline. Remove the drive. Replace with a new drive. Using the RAID utility program, rebuild the RAID 5 array.
- D. Use the RAID utility program to "fail" or take the drive offline. Remove the drive. Replace with a new drive. Using the RAID utility program, rebuild the RAID 5 array. Restore the data in the array from the latest backup.

Answer: C

PFA alerts us that a disk in the RAID-5 is having problems. We should fail that drive, remote it, replace it with a new drive, and rebuild the RAID 5 array (this is possible thanks to the parity bit).

Q. 146

When a RAID 5 array is established, which of the following will provide the fastest read solution?

- A. 3 drives, 10 GB each
- B. 5 drives, 6 GB each

- C. 5 drives, 10 GB each
- D. 10 drives, 3 GB each

Answer: D

With RAID 5 the number of drives decides the read performance. Since the data is read in parallel from all drives, the more drives available in the RAID 5 array the more data can be read and the better performance is achieved.

Q. 147

Which of the following details is **LEAST** important to include when the server and network configuration is documented?

- A. Complete network map.
- B. Detailed hardware inventory.
- C. Computer naming convention for all locations.
- D. The name of the technician who performed the installation.

Answer: D

In a server and network configuration documentation a complete network map, detailed hardware inventory, and computer naming conventions are more important than the name of the technician who performed the installation.

Q. 148

Which of the following external connection types provides the fastest interface?

- A. SCSI
- B. RS-232
- C. IEEE-1394
- D. USB

Answer: A

SCSI is the fastest interface by a huge margin. It is almost 8 times faster than IEEE-1394 for example. SCSI-4 (Ultra320) has a maximum speed of 320MB/s. 1394 can transmit data at up to 400 megabits per second, more 30 times the speed of USB.

Reference:

Server+ Certification Training Kit, SCSI Terminators and Timing
Microsoft article: IEEE 1394: The Time is Right for This Bus

Q. 149

When the functionality of a new UPS connected to a server is tested, the UPS does not perform as expected. The new system is configured to wait one minute and implement an orderly shutdown. The computer remains on several minutes until the UPS loses power and shuts down abruptly. Which of the following should be checked to determine the cause of the problem?

- II. A DMA conflict
 - III. Conflict from a serial mouse
 - IV. Bad battery array
 - V. Incorrect polarity setting
-
- A. II only
 - B. I and III only
 - C. II and IV only
 - D. III and IV only

Answer: C

A conflict from a serial mouse could prevent communication between the UPS and the OS. This would prevent a clean shut down.

Wrong polarity setting (e.g. positive instead of negative) can make the UPS alert service not work. Instead of getting warnings and a clean shutdown, you'll get an abrupt power off when the juice is gone from the UPS.

Incorrect Answers

UPS devices use an IRQ and not any DMAs when communicating with the OS.

The battery array in this scenario is not bad, since it the UPS gives the system power for several minutes.

Q. 150

A file server for a remote network location needs to be remotely powered on so that remote troubleshooting can take place. Which of the following Wake-on-LAN compatible components on the remote file server are necessary to perform this task?

- I. Network OS.
 - II. Network drivers.
 - III. Mainboard
 - IV. NIC.
-
- A. IV only.
 - B. II and IV only.
 - C. III and IV only.

D. I, II, III, and IV.

Answer: D

All of the above is required. We need a network OS, a network adapter (NIC), a driver for the NIC, and a motherboard (mainboard) to connect the NIC to the computer.

Q. 151

A server hardware technician has installed a new NIC in a server, connected the correct network cabling, and installed the driver included with the NIC. After rebooting the server, the NIC does not function. The technician reviews the vendor's installation manuals and repeats the installation procedures. The technician further confirms that the installation procedure taken was correct, but that the NIC still will not function. Following best practices, what is the next best step to correct this problem?

- A. Remove and reinstall all network protocols.
- B. Reseat the NIC by removing and reinstalling the card.
- C. Remove the defective NIC and return it to the manufacturer.
- D. Search the NIC manufacturer's Website for software patches and updates to the installation guide.

Answer: D

We should try to find the latest device driver (or software patch/update) at the NIC vendor's web site.

Q. 152

At a company with a file server and a router for Internet access, a user reports that the network is down. None of the users can print or retrieve files. Last night, the company has some work done on the air conditioning ducts in the ceiling. The technician checks the server, router, and hub and everything appears normal. He plugs his laptop into the hub and has no problem connecting, opening, and printing files. What would be the likely explanation for this situation?

- A. DHCP is not working.
- B. There are bad ports on the hub.
- C. The network cabling is damaged.
- D. Users are not logging into the LAN.

Answer: C

Since work were performed on the air conditioning ducts, which often contain network cabling, the work could have damaged the network cabling.

Incorrect Answers

Everything appears normal at the server. The network services, including the DHCP service, should be up and running.

Bad hub ports would not affect all users.

Users know how to log on to the network. Not all users would forget this at the same time.

Q. 153

What troubleshooting limitation is created by using vendor-specific systems on the hard drives of a server (NTFS, HPFS, Ext2FS)?

- A. They are not recoverable after a crash.
- B. Data cannot be recovered from a corrupt volume.
- C. Log files are not compatible for troubleshooting tools.
- D. Local access is available only from within the Network OS.

Answer: C

If we use a vendor-specific file system we can only access the locally with the vendor OS.

Incorrect Answers

If the network OS support the file system then it would be able to recover from a crashed drive or recover from corrupt volumes which use that vendor specific file system.

File formats might be compatible even if the file systems are incompatible.

Q. 154

In the process of adding a network card to a server, a spark was witnessed and the component malfunctioned immediately thereafter. Now the server technician has a new network card and wants to avoid this happening again. The best solution to accomplish this includes which of the following?

- II. Wrist strap and mat
 - III. Rubber gloves
 - IV. Avoiding contact with chassis
 - V. Avoiding contact with the outer edge of the card
-
- A. I only
 - B. I and III only
 - C. II and IV only
 - D. I, III, and, IV only

Answer: A

Wrist strap and a mat is good protection from ESD (electrostatic discharge).

Incorrect answers

Rubber gloves could increase ESD.

Chassis is ground. There is no need to avoid touching the chassis.

The outer edge of the card can be touched.

Q. 155

A company's server hardware technician is assigned the responsibility of verifying the readiness of a room in which a new server will be installed. Which of the following areas should the technician verify prior to the installation?

- II. Wall construction and material source
- III. Power supply availability and stability
- IV. Server manufacturer and Network OS
- V. Environment requirements

- A. I and II only
- B. I and III only
- C. II and IV only
- D. II, III, and IV only

Answer: C

The technician should check for power supply availability and stability. Environment requirements should also be verified.

The server technician should not be required to check the wall construction or any hardware and software issues when verifying the readiness of the server room.

Q. 156

A company works with an external HVD (high voltage differential) SCSI tape drive connected to the main server used for backup. The technician wants to install a new SE (single-ended) SCSI tape drive to work in the same bus with the old tape unit to reduce backup time. Which of the following is the most likely result of the technician's action?

- A. The difference in potential will cause damage to devices.
- B. The bus will require a special 132-ohm active termination.
- C. Tapes will install correctly, but configuration will be required.
- D. Different bus cable connectors in the devices will not allow the connection.

Answer: D

HVD and SE SCSI devices are not compatible and they use different connectors.

Q. 157

Which of the following IP utilities is most commonly used to verify connectivity to the network layer of the OSI model?

- A. arp
- B. ping
- C. telnet
- D. nbtstat

Answer: B

Ping is the utility most frequently used to test for network connectivity.

Q. 158

After upgrading a server from a software RAID solution to a hardware RAID solution, the administrator notices a substantial increase in performance. Which of the following would best explain the increase?

- A. Hardware solutions support additional RAID levels for improved performance.
- B. Processing is now performed by the controller, resulting in less system CPU usage.
- C. The implementation of hardware RAID would no increase performance of the overall system.
- D. The controller works together with the system CPU, providing improved hard drive seek time.

Answer: B

The RAID processing is performed by processor on the RAID controller, not by the system CPU.

Q. 159

Unix is being installed on a server that needs large amounts of memory, but has little physical memory. Which of the following is the best step to increase virtual memory?

- A. Parse the swap file.
- B. Create a large swap partition.
- C. Use a RAMDRIVE to provide virtual RAM.
- D. Use the EMM386.EXE /NOEMS command at startup.

Answer: B

UNIX and LINUX systems, contrary to Windows systems, use a swap partition. The size of the swap partition determines the ability to increase the size of the virtual memory.

Incorrect Answers

Text files are parsed. For example do compilers parse program source code before producing program code. A swap file cannot be parsed.

Windows 3.x used RAMDRIVE and EMM386.EXE for memory handling. UNIX does not use these utilities.

Q.160

A server manager logs into a server with his administrator account and installs a third-party diagnostic tool. No installation problems were encountered. Upon starting the tool for the first time, an error code is displayed that is difficult to understand. The manager attempted to reinstall the tool, but received the identical error. Which of the following actions is the most appropriate next step to resolve the problem?

- A. Review the application documentation.
- B. Search the Network OS support Website for the specific error code.
- C. Review the server performance logs for an easier-to-interpret error code.
- D. Install the latest Network OS service patch to correct recently identified bugs.

Answer: A

The error is specific to the diagnostic tool. Reviewing the application documentation would be the next step to resolve the problem.

Q.161

After a technician installed software on a mission-critical server, the server experienced errors reported to a log file during boot. Which of the following is the best process to determine a course of action?

- A. Delete the log file and see if the problem happens again?
- B. Ignore the log file and test the application, verifying proper operation.
- C. View the log file and the documentation from the previous technician for recent work done to the server.
- D. Refer to the vendor's Web-based knowledge base. If no answer is found, submit a bug report to the vendor.

Answer: C

We should first examine the log file. We should then examine the server documentation for any recent work on the server which could be the cause of the errors.

Q. 162

A server with a preconfigured RAID 5 array is delivered. The four hot-swap drives were shipped in separate packaging. The server is deployed and during POST, the following message appears:

Array configuration has changes please configure array.

Which of the following is the most likely cause?

- A. The array must be configured.
- B. The SCSI drives must be addressed properly.
- C. The SCSI drives are inserted in the wrong order.
- D. The SCSI controller has failed and must be replaced.

Answer: A

The error message indicates that the array should be configured.

Q. 163

The pre-installation plan calls for a particular NIC to be used in all servers. Upon investigation, it is discovered that this NIC is not listed on the HCL of one of the Network OS vendors in a multi-vendor environment. The NIC vendor states nothing about incompatibility with any particular Network OS.

Which of the following is the best way to proceed?

- A. Send the NIC back since it may not work properly.
- B. Contact the affected NIC vendor for compatibility information and test one NIC.
- C. Begin installation immediately, since the NIC vendor did not specify and incompatibility.
- D. Change the installation plan to include a different NIC, because the specified card will not work with the Network OS.

Answer: B

The NIC may be compatible with the OS but we should control this with the NIC manufacturer before the installation.

Q. 164

Three servers connected to a KVM (Keyboard Video Mouse) switch are to be installed in a rack. What is the minimum number of standard network cables, KVM cable sets and monitors needed to support this configuration?

- A. 1 standard cable, 2 KVM cable sets, and 1 monitor
- B. 3 standard network cables, 3 KVM cable sets, and 1 monitor
- C. 1 standard network cable, 3 KVM cable sets, and 3 monitors
- D. 3 standard network cables, 4 KVM cable sets, and 1 monitor

Answer: B

We need a network cable and a KVM cable set for each server. The KVM enables use a single keyboard, mouse and monitor for all servers.

Q. 165

A Magic Packet is a packet that contains 16 contiguous copies of the receiving network adapter's MAC address. What technology utilizes this concept?

- A. WOL (Wake-On-LAN)
- B. CLC (Cluster LAN communication)
- C. SMTP (Simple Mail Transport Protocol)
- D. SNMP (Simple Network Management Protocol)

Answer: A

Wake On LAN (WOL) is the name for a technical development jointly created by IBM and Intel. The technology allows "enabled" devices to be powered on remotely via a special type of network communication. A WOL-enabled device, when powered off, will still draw a tiny amount of electricity to drive the network interface. The interface remains in a passive, listening mode, sending nothing out on the network. To wake up the device, a specially formed packet is sent to the network port where the device is plugged in.

This special packet, called a **magic packet**, carries a special "signature." When the network interface sees this signature, it recognizes this as a wakeup call.

Q. 166

A web server was upgraded to enable data striping with parity to improve performance. It has two UltraWide SCSI adapters, two PNP ISA 100 Mbps NICs, and 256 MB of RAM. The CPU utilization is at 52% and users are complaining of sluggish performance. Which of the following actions should be done to fix the bottleneck?

- A. Add more RAM.
- B. Upgrade the CPU.
- C. Add more hard drive space for swap files.
- D. Replace the NICs with units having bus mastering capabilities.

Answer: D

The ISA technology is old. The ISA NICs should be replaced with faster NICs that have bus mastering capabilities.

Q. 167

In what order should the following steps for flashing the system BIOS be performed?

- II. Run the BIOS flash utility
- III. Restart the server normally
- IV. Record the current BIOS settings
- V. Boot the server using the BIOS flash disk

- A. III, I, II, IV
- B. III, IV, I, II
- C. IV, I, III, II
- D. IV, III, II, I

Answer: B

First we should record the current BIOS settings. We then reboot the system with the BIOS flash disk, run the BIOS flash utility, and finally boot the server normally.

Incorrect answers.

We must the system reboot using the BIOS flash disk in order to run the BIOS flash utility.

Before starting the flashing process we must document the old BIOS settings in order to manually reconfigure them to return to the previous state if necessary. We cannot make this documentation after booting from the BIOS flash disk.

Q. 168

A NIC appears to be causing a network broadcast storm. Which of the following is the best tool to determine the source of the problem?

- A. SNMP
- B. Cable tester.
- C. LAN analyzer
- D. Performance monitor.

Answer: C

A LAN analyzer would be able to analyze the packets on the network. We would be able to obtain the source of the packets.

Q. 169

Users suddenly lost connectivity to an existing server. The server technician can ping the loopback address and the server's own IP address. However, no other device on the network can be pinged. The LAN cable is plugged in. Which of the following should the server technician check next?

- A. The router.
- B. The subnet mask.
- C. Link integrity.
- D. The DNS server.

Answer: C

We should check the simple possible causes of the problem first. Broken, disconnected, improperly terminated, or mis-wired cables are responsible for over 70% of all LAN problems. We check physical connectivity with the link integrity. A green LED indicating good link integrity should be on at the server end, and on the port of the hub where the server is connected.

Note: The IEEE Ethernet standards make use of a feature called 'Link Integrity' to ensure that the physical cable being used to transmit/receive data is intact.

Incorrect Answers.

A malfunctioning router could explain that no other computers can be reached, but we should check the link integrity first.

The server's subnet mask would not change by itself.

Since the PING by IP address fails there is no name resolution problem at hand. The DNS server cannot be blamed.

Q. 170

What should be the first consideration when identifying potential server bottlenecks?

- A. The role of the server.
- B. Amount of installed RAM.
- C. Number of installed processors.
- D. Quantity of installed network adapters.

Answer: A

Different server roles (file server, database server, mail server, domain controller, DNS server, etc) have different bottle necks. The role of the server is first thing to consider when identifying potential bottlenecks.

Q. 171

A server that has been running for several months was scheduled for maintenance and the latest operating system patches was applied. Upon reboot, the message that “no operating system found” was shown. What is the most likely cause?

- A. The master boot record has been corrupted.
- B. The file system has been corrupted by a virus in the patches.
- C. The RAID configuration has not been synchronizes in some time.
- D. The operating system patches overwrote the OEM driver for the drive controller.

Answer: D

The last change made on the server made before the reboot was the installation of the latest operating system patches. It seems like that the error is related to that. The patches might have overwritten the OEM driver for the drive controller.

Q. 172

While installing a new server, a server technician performed the following actions:

- Inventoried the server hardware components
- Downloaded and applied the latest BIOS and firmware
- Loaded the Network OS and patches

The tape drive failed initialize during Network OS startup. Which of the following is most likely causing the failure?

- A. The tape drive device driver was not enabled in the system BIOS.
- B. The Network OS patches were not applied correctly.
- C. The tape drive is not on the Network OS HCL.
- D. The BIOS and firmware upgrades were not properly applied.

Answer: C

A failed installation of a device could be explained by an incorrect or old driver (not listed here) or by a device that is incompatible with the OS (not included on the HCL).

Q. 173

An installation plan requires plugging a 64-bit, 66 MHz, PCI 2.2-compliant SCSI controller into a 32-bit, 33 MHz PCI slot. Which of the following steps, must be performed?

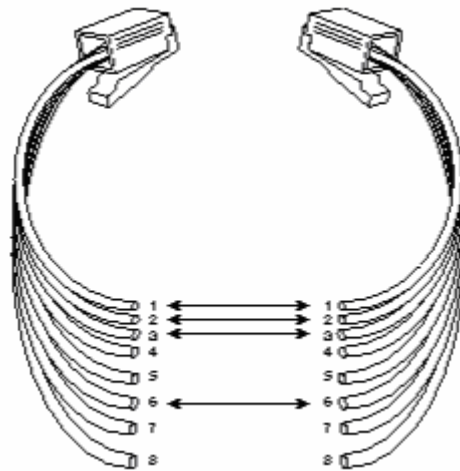
- A. Nothing can be done. 64-bit, 66 MHz cards are not backward-compatible with 32-bit, 33 MHz slots.
- B. 64-bit cards are already compatible with a 32-bit slot. Bus speed compatibility must be set with a jumper on the PCI card.
- C. Remove the perforated cutout on the edge connector of the PCI card. This will allow a 66 MHz card to be plugged into a 33 MHz slot.
- D. Do nothing. The 64-bit, 66 MHz card is compatible with the 32-bit, 33 MHz slot.

Answer: D

The PCI 2.2 specification ensures that a 64-bit 66MHz cards can be used in a 32-bit, 33MHz PCI slot. The slot can be used by the card.

Q. 174

Exhibit: Wiring diagram



The wiring diagram reference in the exhibit should be used in which of the following situations?

- A. A network card to a CSU/DSU connection
- B. A network card to a network card connection
- C. A network hub to a network card connection
- D. A network hub to a network hub connection.

Answer: C

The exhibit shows a straight cable. A straight cable is used to connect a network adapter to a network hub.

Q. 175

A server error indicates that a service or driver failed during system startup. When a technician tries to start the service manually, it again fails to load and displays a specific error code. Which of the following is the most appropriate next step to resolve the problem?

- A. Reinstall the current patches.
- B. Reboot the server and observe any real-time errors.
- C. Determine if other services or functions also failed to start.
- D. Reinstall the service from the original install disks and apply appropriate patches.

Answer: C

Services are often dependant of other services. We should initially determine if other services or functions also failed to start. This could help use to find the cause of the problem. We should start by checking the system logs.

Incorrect Answers

We should not start by reinstalling the current patches. Instead we should try to locate the source of the problem.

Rebooting the server and checking for any errors could be useful, but most likely no further information would be gained by this.

Initially we should try to locate the source if the problem instead of reinstalling services or applying patches.

Q. 176

A server with a virus infection was recovered by repartitioning and reformatting the hard disk drive. The Network OS was reinstalled using a boot floppy and the vendor CD-ROM. However, the server was infected again. Which of the following most likely caused the problem?

- A. The file allocation table is infected.
- B. The boot disk is infected.
- C. The vendor CD-ROM is infected.
- D. The active partition is infected.

Answer: B

If the boot disk is infected the system would be re-infected during the installation process.

Q. 177

While performing a daily review of the system logs, a server manager notices that the latest error entry in the log indicates that a specific service or function has stopped operating. What should be the next diagnostic step taken by the server manager?

- A. Attempt to manually restart the service or function.
- B. Examine the log for previous instances of this error.
- C. Determine which enterprise functions are being affected by this stoppage.
- D. Erase the log to make it easier to locate the next occurrence of this error.

Answer: B

We want to diagnose the problem. We should try to locate the source of the problem. A good first step is to check the system logs for similar event that has occurred earlier, maybe locating the first occurrence and possibly what cause the first occurrence.

Incorrect Answers

A manual restart of the service (or function) might start the service (or function) but it would not help diagnosing the cause of the problem.

Determine which enterprise functions that are affected by this problem might be a good precaution. It would not, however, help to diagnose the problem.

The log contains information that could be helpful for diagnosing the problem. The log must not be erased.

Q. 178

A working server's monitoring tool identifies a problem with a PCI NIC in the server. Which of the following steps should be performed next?

- A. Assign an IRQ to the card.
- B. Move the card to another slot.
- C. Install an identical spare card.
- D. Install a PC diagnostic tool in the server.

Answer: D

We should replace the card with an identical card. The identical card should work immediately since it uses the same device drivers.

Incorrect answers

An IRQ problem seems unlikely since the NIC used to work.

Moving the card to another slot would most likely not change anything.

It is simpler and more straightforward just to replace the card, compared to installing and using additional diagnostic software.

Q. 179

A hot-plug PCI card needs to be replaced in a server supporting this technology. Before replacing the card, which of the following actions, if any, must be performed before removing the card from the server?

- A. Shut down the server.
- B. Unplug the power cord from the server.
- C. Remove power to the expansion slot.
- D. No action is required.

Answer: C

Hot plug PCI cards can be deactivated, allowing for removal and replacement of a PCI card while the system is in operation. Power should be removed from the expansion slot before removing or inserting the PCI card.

Incorrect answers

Hot-pluggable PCI cards can be replaced while the server is running. There is no need to shut down the server or unplug the power cord from the server.

Power should be removed from the expansion slot before removing or inserting the PCI card.

Q. 180

In a mixed protocol environment, a local server is viewable throughout the LAN, however, it cannot connect to the Internet. Which of the following diagnostic tools should be used first to determine where the problem exists?

- A. Ping 127.0.0.1 ensure TCP/IP stack is functioning.
- B. Check the error log file of the server to determine what errors have been received.
- C. Use the NSLOOKUP command to determine what host name should be used to access the Internet.
- D. Check the system error log file and the network file to determine if any errors have been encountered.

Answer: A

The network may use some other network than TCP/IP on the local network. We must ensure that TCP/IP, the protocol of Internet, is properly installed and functioning.

Q. 181

A customer has purchased a new file server and wishes to retire their three-year old file server, making it into a department print server. The print server will run a newer version of the operating system. The print server's hardware is on the new operating system's HCL. However, the customer is having problems keeping the server running reliably. The system log shows operating faults and not all Network OS features are available. Which of the following should be done next to resolve this issue?

- A. Install alternative operating system on the print server.
- B. Inspect hardware and firmware versions and compare to latest revisions.
- C. Install the previous operating system and perform an upgrade to the new version.
- D. Inform the customer that the server is not compatible with the new operating system.

Answer: B

The server is on the OS HCL so it should be functioning correctly. We need to ensure that the BIOS is upgraded and that the latest device drivers are used. The server should then be able to function correctly.

Q. 182

There are 4U of available space in a server rack mount unit. How much space is available to install additional devices?

- A. 4 inches (10.2 cm)
- B. 7 inches (17.8 cm)
- C. 8 inches (20.3 cm)
- D. 14 inches (35.5 cm)

Answer: B

A 4U rack is a 7" rack.

Q. 183

After the four pieces of equipment listed below were connected, the UPS went into an overload condition. Which of the following pieces of equipment is the most likely cause of the problem?

- A. Desktop system
- B. 17" monitor
- C. Laser printer
- D. 48-port hub

Answer: C

A laser printer should never be connected to an UPS since a laser printer consumes a lot of power when it print pages. This would cause problems for the UPS.

Q. 184

A company wants to install an internal Ultra3-compatible controller with two external Ultra2-compatible tape devices. The technician requests two 50-pin cables and two passive (132 ohm) external terminators. Which two of the following must be done to accomplish the installation?

- II. Change the controller to an Ultra2 compatible.
- III. Change Tapes devices to UltraWide compatible.
- IV. Change cables to 68-pin cables
- V. Change terminators

- A. I and II
- B. I and IV
- C. II and III
- D. III and IV

Answer: D

We must use the 68-pin connector for the Ultra2 devices. We must replace the 50-pin connector. Passive termination use 132 ohm terminators. Passive termination is an older technology which cannot be used with Ultra2 or Ultra3.

Incorrect Answers

Ultra3 is backward compatible with Ultra2. There is no need to replace the Ultra SCSI controller.

Q. 185

When the installation of a new server is planned, using which of the following is most likely to result in the greatest number of problems when the operating system is installed?

- A. Untested memory
- B. Third-party NICs and SCSI controllers
- C. Server listed on Network OS vendor's HCL
- D. Drivers supplied by Network OS instead of hardware vendor

Answer: B

We should avoid third-party NICs and SCSI controllers. We should use the ones recommended and tested by the server manufacturer.

Incorrect Answers

Untested memory could cause problems but it is not the most likely cause.

It would be good, not bad, if the server was listed on the OS vendor's HCL.

The latest drivers should be obtained from the hardware vendor. The drivers supplied by the OS vendor have been tested with the OS and should be adequate most of the time.

Q. 186

A customer is using a DAT drive for data backup. The drive will backup intermittently, usually stopping towards the end of the backup job. The customer claims to have cleaned the drive just two days ago, but the problem still exists. What should be the next step in troubleshooting the backup problem?

- A. Ask the customer to replace the backup tapes.
- B. Ask the customer to reload the backup tapes.
- C. Replace the tape drive with a known good drive.
- D. Replace the controller with a known good controller.

Answer: A

Since the backup jobs stops at the same point it seems likely that the backup media is corrupted and should be replaced.

Q. 187

During a midnight shift a technician upgrades a server two new processors. During the next work shift, users complain that the server is slower that it was the day before. What is the first thing that the current shift's server technician should do to resolve the problem?

- A. Down the server to check if the processor is seated properly.
- B. Check the documentation from the previous shift's installation.
- C. Check the pre-installation checklist that was used for the upgrade.
- D. Call the server support help desk to determine what happened during the install.

Answer: B

The server technician should check for any documentation from the previous shift. Any recent irregularities or problems should be found in that documentation.

Q. 188

A customer who needs to restore their system from tape has been creating differential backups since their last full backup. How many tape sets will be required to restore the system to the most recent backup?

- A. One, the full backup.
- B. One, the last differential backup.
- C. Two, the full backup and incremental backup.
- D. Two, the full backup and the last differential backup.

Answer: D

To restore from a differential backup we must first restore the full backup and then restore only the last differential backup.

Q. 189

While maintaining fault tolerance, which of the following would provide the greatest disk performance?

- A. RAID 0/1
- B. RAID 0
- C. RAID 1
- D. RAID 5

Answer: A

We should use RAID 0/1 combines RAID 0 (disk mirroring which gives fault tolerance) with RAID 1 (disk striping which give highest performance).

Incorrect Answers

RAID 0, disk striping, does not provide fault tolerance.

RAID 1, disk mirroring, provides fault tolerance, but not as good performance as RAID 0/1.

RAID 5 also provides fault tolerance and good performance but not as high performance as RAID 0/1.

Q. 190

A customer has been using a QIC-80 (Quarter-Inch Cartridge) tape drive for their server backups. Due to increased drive capacity they want to upgrade the tape drive to store more data on each tape. Which of the following tape drives allow backward compatibility with their existing QIC-80 tapes and provide additional capacity?

- A. DAT
- B. DDS
- C. DDS-2
- D. TRAVAN

Answer: D

QIC-80 and Travan are compatible technologies. DDS and DDS-2 are not compatible with either QIC-80 or Travan.

Q. 191

Which of the two following options would require an update of a disaster recover plan?

- I. Adding new hardware.
 - II. A move to a new location.
 - III. Replacing failed hardware.
 - IV. Adding workstations to the network.
-
- A. I and II.
 - B. I and III
 - C. II and IV
 - D. III and IV

Answer: B

New hardware and a move to a new location would force use to make changes in the disaster recovery plan.-

Incorrect Answers

Replacing failed hardware would not change the disaster recovery plan as we still would use the same type of hardware.

Adding more workstations to the network would not change the disaster recovery plan. The vital information is stored on the servers, not on the workstations.

Q. 192

A server technician discovers that a drive in a RAID 5 array has failed during the night. The array was protected with a hot-spare drive. What is the best first step in restoring the RAID array to its pre-failure state?

- A. Rebuild the RAID 5 array.
- B. Assign another drive as the hot spare in the array.
- C. Replace the defective drive.
- D. Verify completion of rebuilding of RAID array to the hot space.

Answer: B

We should:

1. Replace the failed drive.
2. Rebuild the RAID 5 array.

Q. 193

After a pre-installation walkthrough, the server technician observed that the power outlets, rack dimensions, physical security, and network cabling were all acceptable. However, one factor was missing in the pre-installation planning, so the technician decided not to install the server in this location.

Which of the following factors was missing from the pre-installation planning?

- A. Location
- B. Environment
- C. Wall materials
- D. Electrostatic discharge

Answer: B

The pre-installation planning should include Environment assessment.

Q. 194

A server is consistently rebooting every day at the same time. Which of the following environmental elements has most likely caused this behavior?

- A. ESD (Electrostatic Discharge)
- B. Humidity
- C. Temperature
- D. Electrical

Answer: D

Only an electrical problem could reoccur at the same time every day. It could for example be caused by some electrical maintenance or by some micro-wave ovens being used at the same time each day.

Incorrect Answers

It seems unlikely that ESD, high humidity, or high temperature would occur at same time every day.

Q. 195

A client has set up a new data center. Which of the following is **LEAST** important to install at the new data center?

- A. Raised floor
- B. Dehumidifier/humidifier
- C. Physical locks on all entrances to the data center
- D. Waterless-based sprinkler system in data center.

Answer: D

A waterless-based sprinkler system in data center is very rare.

Incorrect Answers

A raised floor could make cabling of the data center easy.

Dehumidifier/humidifier could be important to keep the humidity at acceptable levels.

Physical locks would protect the servers from physical access.

Q. 196

A technician is troubleshooting a server problem. Immediately after a reboot, the following error message was received:

"setup did not find any hard drives on the computer"

Which of the following should be checked first?

- A. Determine whether the Network OS is corrupted.
- B. Determine whether the first hard disk crashed.
- C. Check that the SCSI adapter is seen at POST.
- D. Verify that the DMA is not set to the "on" position.

Answer: B

The first hard disk could have crashed. We must check this possibility.

Incorrect Answers

The error message indicates a problem with the hard drive, not any problem with the OS.

The POST does not check for SCSI adapters. SCSI adapters are checked after the POST. Furthermore, we do not know if they server use any SCSI adapter.

This is not a DMA problem.

Q. 197

On Monday morning many users find they are unable to log into the network. The server technician has been at work over the weekend and has no trouble connecting from his workstation. The server is apparently up and running fine. The NICs on the failing workstations have link status-lights lit.

Which of the following actions will most likely correct the problem?

- A. Restart DHCP.
- B. Replace the hub.
- C. Update workstation client software.
- D. Replace the patch cable between server and hub.

Answer: A

The DHCP service might have been stopped. This would explain why the server technician is able to connect from his workstation. DHCP is initiated when the OS is started and his computer has been online during the whole weekend. Restarting the DHCP service could solve the problem.

Incorrect Answers

Some users are able to connect so it does not seem to be any hardware or cabling problems. There should be no need to replace either the hub or cabling between the hub and the server.

It seems unlikely that we suddenly would be some problem with the workstation client software.

Q. 198

A server crashed where the data was locally stored on a RAID 0 configuration. According to the organization's disaster recovery plan, data should be recovered via disk fault tolerance strategies before going to the tape archive. What should be done to recover the lost data?

- A. The data is safe. Replace the failed disk and regenerate the mirror set.
- B. Replace the failed disk in the RAID array and it will regenerate itself automatically.
- C. Replace the failed disk in the RAID array and restore data from the most current backup.
- D. Replace the failed disk when it is convenient, because a copy of the data is on a disk on the second RAID controller.

Answer: C

RAID 0, disk striping, does not include any fault tolerance. We must restore the data from the most current backup.

Q. 199

Two of the server's data disks in a customer's RAID 5 array fail. The Network OS is mirrored on a separate drive set and RAID controller. According to the company's in-place disaster recovery plan, all data should be restored from onsite tape before recovering from tape stored at the offsite storage location. A full backup and two incremental backups were performed before the crash. What must be done to return the system to operational status?

- A. Replace the two failed disks in the array so the array will start to regenerate itself.
- B. Replace the two failed disks in the array, and then use the last incremental backup to restore the data.
- C. Replace the two failed disks in the array, and then use the full backup and one incremental backup to restore the data.
- D. Replace the two failed disks in the array, and then use the full backup and all (two) incremental backups to restore the data.

Answer: D

A RAID 5 disk array can recover from one failed disk, but not from two or more failed disks. We need use tape backups. We must restore the full backup, followed by all incremental backups applied in the correct order. In this scenario we must apply both the incremental backups.

Q. 200

A small company is backing up mission-critical data and wants to implement a disaster recovery plan. The network administrator is tasked with developing the disaster recovery plan. Which of the following should be the first step in developing the plan?

- A. Practicing the disaster recover drills.
- B. Exploring disaster prevention techniques.
- C. Create a step-by-step restoration plan.
- D. Determining the Information Technology configuration.

Answer: D

The first step in developing a disaster recovery plan is to determine what the risks to your business operation are. In order to evaluate the risks we need to determine the present Information Technology configuration.

Incorrect Answers

Practicing the disaster recover drills, training, should be the final, not first, step in a good disaster recovery plan. Exploring disaster prevention techniques has no place in a disaster recovery plan. We want to have a plan how to recover from a disaster, not how we prevent a disaster.

Creating a step-by-step restoration plan should be included in the restoration plan, but not as the first step. We need to determine the risks first.

Q. 201

A company's server room flooded and five years of data were lost. Server administrators implemented a disaster recovery plan before the flood that included a backup process with a daily tape rotation schedule. Which of the following would have best minimized the impact of the flood?

- A. Establishing a cold site.
- B. Establishing remote notification for flooding.
- C. Installing a raised floor in the server room.
- D. Storing backup tapes at an offsite location.

Answer: D

The impact of the flooding would be minimized if the tapes were stored at an offsite location which presumably would not be affected by the flooding.

Q. 202

Open access needs to be maintained to the server room so that work flow is not impeded. Data on the servers is extremely sensitive and physical security should be maintained. Which of the following actions most effectively meets these criteria?

- A. Installing alarms on servers.
- B. Disabling removable media drives on the servers.
- C. Placing servers in a locked room with a human guard.
- D. Using lockable server cabinets with keys issued to authorized users.

Answer: D

Preventing physical access to the servers would be the most effective precaution.

Incorrect Answers

Alarms on the servers would be awkward.

Disabling removable media in the servers would not prevent any users from copying sensitive data from the servers to other computers on the network.

A locked room with a human guard would be an expensive solution.

Q. 203

A technician is called to perform maintenance on a server. While performing his tasks, he notices that the tape backups are located on a bookshelf outside the server room. Which of the following recommendations, if any, should be made to the system administrator?

- A. The tapes should be stored in a lockable cabinet outside the server room.
- B. The bookshelf should be moved inside the server room.
- C. The tapes should be stored in a secure offsite location.
- D. No recommendation is necessary. This is a common practice to allow quick access in the event of a server failure.

Answer: A

The tapes should not be publicly accessible. Where the tapes should be stored depends on several factors that are not listed in this scenario:

- Is the access to the server room restricted?
- What type of backups are stored in the cabinet?
- Do the company store some backups off-site already?

However, it seems most prudent to recommend that the tapes should be stored in a lockable cabinet outside the server room.

Incorrect Answers

Moving the bookshelf inside the server room might not help if access to the server room is not restricted.

The tapes might be daily backup tapes that are rotated during the week. The company may already have an off-site storage procedure for backup tapes.

Public access to the backup tapes is unacceptable. We must make a recommendation.

Q. 204

A company is building a new server. After the operating system is installed and the drivers are configured, the system log contains errors that are difficult to understand. Everything appears to be correctly configured and the drivers are up to date. Which of the following should be done next?

- A. Research the error code.
- B. Obtain an OS patch from the vendor.
- C. Begin disabling services, rebooting each time.
- D. Replace each peripheral one at a time until the errors go away.

Answer: A

We should try to investigate the error code and see if the issue is known by the OS vendor or the some hardware vendor. We could, for example, search the knowledge base of the OS vendor.

Incorrect Answers

Before installing an OS patch we should research the error code for known issues.

Disabling services or replacing peripheral would not be the first troubleshooting steps since they require a lot of effort.

Q. 205

A server is maintained by a group of administrators. When a commonly accessed application is used, the server crashes. After discussing the issue with the server team, the technician learns that the problem has happened several times in the recent past. What troubleshooting step should be taken first?

- A. Check the application manufacturer's knowledge base.
- B. Call the software vendor to see if there is a patch to correct this issue.
- C. Call the hardware technical support to see if this is a known hardware limitation.
- D. Check the server's logbook to determine what changed prior to the server's first crash.

Answer: D

Often a problem is caused by a change in the system. Locating the change, if any, that occurred before the first crash would most certainly be very useful for troubleshooting the problem.

Q. 206

A customer is contemplating creating a two-node cluster with a SCSI shared storage configuration to provide quick fault recovery. For which of the following failures will this cluster provide quick fault recover?

- A. One server in the cluster loses all power.
- B. The computer room loses all power for an hour or more.
- C. The shared SCSI storage system for the cluster loses all power.
- D. The shared SCSI storage system for the cluster loses two disk drives.

Answer: A

A cluster is used for failover protection. If one node fails another node in the cluster takes its place.

Note: The cluster service can detect a hardware or a software failure (for example that one server stops due to a power loss) and quickly assign the application or service responsibility to another node in the cluster. This process is called failover.

Reference: MCSE Training kit (70-223) Microsoft Windows 2000 Advanced Clustering Services, Overview of Microsoft Cluster Service, page 6.

Incorrect answers

If the computer room loses power both the nodes in the cluster would be shut down.

If the shared SCSI storage system fails both nodes in the cluster would be unable to operate.

Q. 207

An onsite technician is at a client's site to perform a warranty replacement of a FRU (Field Replacable Unit) in Novell IntranetWare 4.11 server. The technician is unsure of how to shut down the server properly. When calling into the help desk, the technician inquired about which commands should be entered before powering off the server. Which commands should the help desk tell the technician to use?

- II. Shutdown
 - III. Exit
 - IV. Down
 - V. Killservices
-
- A. I then II
 - B. II then III
 - C. III then II

D. IV then I

Answer: C

First we must down the server with the DOWN command, then we exit to DOS with the EXIT command. We DOWN command must precede the EXIT command, not vice versa.

Note: NetWare 4.11 console commands

DOWN - Shuts down Server activity

EXIT - Returns to DOS after the server has been DOWN(ed)

Q. 208

A system administrator has been notified twice this week that an application has failed, causing a critical server to crash. The server has generated an output file. He decided to run a set of performance monitors on the server to evaluate what is the most likely cause of the crash. What else should be done, if anything, to aid in problem determination?

- A. Cluster the server with another for load balancing.
- B. Send the output file to the application group or vendor for analysis.
- C. Move the application to a new server with more RAM and a faster processor.
- D. Do nothing, because it is probably an anomaly and is unlikely to happen again.

Answer: B

The output file could be send either to the application developer or to the OS vendor for further analysis. This could be costly however.

Incorrect Answers

Clustering is used for failover workload distribution. Clustering would not solve any problem with a critical server.

More RAM and faster processor would improve performance, but moving the application to another server not aid in determining the cause of the crash.

The problem has already occurred twice. It is not anomaly.

Q. 209

Hot-plug PCI card technology relies on the Network OS to support this feature. Which of the following items is most relevant for implementing this technology?

- A. Adapter BIOS
- B. Server design
- C. Adapter driver

D. Server manufacturer

Answer: A

The Adapter BIOS must support Hot-plugging.

Q. 210

Several users have had problems accessing the company's intranet server named SERVER1. A technician has attempted to ping the server and receives the following message:

```
C:\ ping server1
Unknown host server1
```

Which of the following should be done next?

- A. Try to "tracert server1".
- B. Reboot the intranet server.
- C. Reload the TCP/IP protocol stack on the server.
- D. Put the server in the local machine's host table.

Answer: A

Several users, but not all users, have problem accessing SERVER1. This indicates that it is a local problem.

If ping fails we already know that tracert would fail. However, the tracert command could show where in the path between the client and the server the error occurs. The clients could have an incorrect default gateway setting or a router may work incorrectly. Since it is very easy to test a tracert command it seems like the best troubleshooting step to try next.

Incorrect Answers

Since only some of the users have this problem there is no need to make any changes on the server: there is no need to reboot the server or reconfigure the TCP/IP protocol on the server.

There could be a name resolution problem. The client may not be able to resolve the host name server1 to an IP address. We could add a mapping from Server1 to the IP address of server at the local hosts file on the clients. However, this would require considerable administrative effort. Furthermore this file is not known as a host table.

Q. 211

The file servers regularly download antivirus updates from the vendor's FTP server. The automatic updates have not occurred on these servers for the last three updates. Which of the following actions should be taken to isolate this problem?

- II. Verify connectivity to the vendor's FTP server.
- III. Ping another server on the network.
- IV. Check the server logs for errors.
- V. Reboot the server to restart all services.

- A. I and II only
- B. II and IV only
- C. I, II, and III only
- D. I, II, III, and IV

Answer: C

We could verify the connectivity of these servers. We should check both the connectivity with the vendor and local connectivity. (I and II)

We should also check the server logs for any related errors or warning. (III)

Rebooting the server and restarting all services should only be used as a last desperate attempt. It would not be particularly useful for isolating the problem.

Q. 212

A sever technician is called to a customer site to troubleshoot SCSI timeouts. The customer has a mix of Fast-Wide SCSI drives and UltraWide SCSI drivers. Which of the following should be performed first?

- A. Run diagnostics and look for information to diagnose the error.
- B. Power cycle the server and drives to start from a known-good position-
- C. Replace the UltraWide drives so that only Fast-Wide drives are in the system.
- D. Recommend that the jumpers on the UltraWide drives be changed to work with Fast-Wide drives on the same bus.

Answer: A

We should run diagnostics in order to diagnose the problem.

Incorrect Answers

UltraWide and FastWide drives are compatible. There is no need to replace the UltraWide drives. There is no need to change any jumpers for compatibility.

Q. 213

While offsite, a network administrator receives a page from the server that a drive in the array has failed. From the current location, how can the administrator confirm the failure and determine whether corrective action has taken place?

- A. Return to the server site, check the drive, and replace if necessary.
- B. Using a dial-up connection to the server, check the RAID log to confirm the rebuild with the hot spare.
- C. Contact an administrator at the server site and have them stop RAID services, perform a data integrity check, and then restart RAID services.
- D. Using the system management software, stop RAID services, have an administrator at the server site check the drive, and then restart the service.

Answer: B

From the current location the network administrator can use connect remotely, using a dial-up connection for example, to the server and check the RAID logs. He could diagnose the problem and determine the action that need to be taken. The problem might even be fixed remotely.

Incorrect Answers

It is not necessary to physically visit the site, or get help from an on-site administrator, just to confirm the failure and decide the action. This can be done remotely.

Q. 214

A customer reports that the new server shows only one of the two installed PCI Ethernet controllers. They request a service call to have one of the controllers replaced. Before ordering the replacement controller, which of the following actions should be taken first?

- A. Remove the drivers for the controllers and reinstall.
- B. Update the controller's drivers to the latest version.
- C. Remove each controller to determine the faulty controller.
- D. Examine controller configuration data and vendor specifications.

Answer: C

Before replacing the faulty controller we must be sure we replace the correct one.

Incorrect Answers

We have already decided to replace the controllers. It is too late to reinstall or update the driver of the controller. It would also be a waste of time to check the controller's configuration data and vendor specifications.

Q. 215

The server diagnostic tool is reporting a faulty memory module in a non-mission-critical server. What should the technician attempt next?

- A. Buy a new memory module and clear the error in the diagnostic tool.

- B. Check to see if the error moves with the module when it is placed in a different slot.
- C. Replace all the modules in the bank with known good ones and clear the error in the diagnostic tool.
- D. Cold boot the system, clear the error in the diagnostic log, and wait to see if the error occurs again.

Answer: C

We should replace the all memory modules in the bank with good ones. This would make the server run again. It would not, however, locate the faulty memory module.

We could also try to locate the faulty memory module by checking if the error moves when the module is placed in a different slot.

Since the server is a non-mission critical server it seems prudent to try to locate and replace only the faulty memory module.

If the server was mission-critical we should immediately replace all memory with known good ones.