

**QUESTION 1**

You are the network administrator for Certkiller .com. The Certkiller network contains seven application servers. Each application server runs a database application named Certkiller App. Requirements for Certkiller App state that when you add a new user, you must add the user to the server that has the most available disk space.

You need to ensure that you meet the requirements when you add new users to Certkiller App. What should you do?

- A. Use Event Viewer to review the application logs on each of the seven servers.
- B. Use Performance Logs and Alerts to record the PhysicalDisk object on all seven servers.
- C. Use Task Manager to view the performance data on each of the seven servers.
- D. Use System Monitor to generate a histogram view of the LogicalDisk object on all seven servers.

Answer: D

Explanation: System Monitor shows real-time performance data based on Object counters, and can display the log data recorded by Performance Logs And Alerts either in the form of Counter (interval polling) logs, or Trace (event-driven) logs. Logs written by Performance Logs And Alerts can be loaded into System Monitor for analysis. The System Monitor is designed for real-time reporting of data to a console interface, and can be reported in graph, histogram, or numeric form. This should aid you in ensuring that you meet the stated requirements.

Incorrect answers:

A: The Application log contains data written to it by software programs, it records events that are generated by application programs and network application services. Using Event Viewer to review application logs would thus not ensure that you add a new user to the server with the most available space.

B: The Performance Logs And Alerts snap-in can do no configuration, only reporting data through Counter Logs as reported by providers (object counters) on a configured interval, or through Trace Logs as reported by event-driven providers. Thus this option will not work.

C: Viewing performance data through the Task Manager is not what you need.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6

---

**QUESTION 2**

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. The network includes a file server named Certkiller 1. Certkiller 1 contains a single disk for system files and two SCSI hard disks that comprise a 72-GB mirrored volume with 65 GB of read-only data.

Users connect to this data by using shortcuts on their desktops.

Certkiller 1 is scheduled for replacement. You have a scheduled maintenance window to complete this task. Before the maintenance window, you build a new server.

You need to bring the new server online with current data and re-establish redundancy as quickly as possible. You must also ensure that the desktop shortcuts will continue to function.

What should you do?

- A. Name the new server Certkiller 1.  
Create a new mirrored volume by using two 72-GB disks.

Connect Certkiller 2 to the network and copy the data from Certkiller 1.

When copying is complete, shut down the old Certkiller 1.

B. Name the new server Certkiller 1.

Move both disks from the old Certkiller 1 to the new Certkiller 1.

Scan the disks for changes.

Import the disks.

Connect the new Certkiller 1 to the network.

C. Name the new server Certkiller 1.

Break the mirror on the old Certkiller 1.

Move one of the disks from the old Certkiller 1 to the new Certkiller 1.

Scan the disk for changes.

Initialize the disk.

Select the spare disk and create the mirror.

Connect the new Certkiller 1 to the network.

D. Name the new server Certkiller 1.

Remove one of the disks in the mirror from the old Certkiller 1.

Move the disk on the new Certkiller 1.

Scan the disk for changes.

Import the disk,

Shut down the old Certkiller 1 and connect the new Certkiller 1 to the network.

Answers: B

Explanation: You have to make use of the existing old Certkiller 1 disks to make sure that the current data will be brought online. When moving disks from one computer to another keep in mind that before disconnecting the disks from the old Certkiller 1 you must make sure the status of all volumes on each of the disks is healthy. For any volumes that are not healthy, repair the volumes before you move the disks. After you physically connect the disks to the new Certkiller 1, in Disk Management, open the Action menu and choose Rescan Disks. The scanning will detect changes. The new disk will show up as Dynamic/Foreign. By default, Dynamic/Foreign disks and should be brought online automatically, but if not, bring it online by right-clicking the disk and selecting Online.

To make Dynamic/Foreign disks useable, you must import it. The disk group remain as is and the database does not change.

When connecting new Certkiller 1 to the network you will enable users to use their existing shortcuts.

Incorrect answers:

A: Since Certkiller 1 is scheduled for replacement you need no mirroring to be done for the question states pertinently that you have to re-establish redundancy which means that redundancy used to be in place before.

A mirrored volume (also known as RAID Level 1 or RAID-1) consists of two identical copies of a simple volume, each on a separate hard disk. Mirrored volumes provide fault tolerance in the event that one physical disk fails. Besides, Certkiller 2 is irrelevant in this scenario.

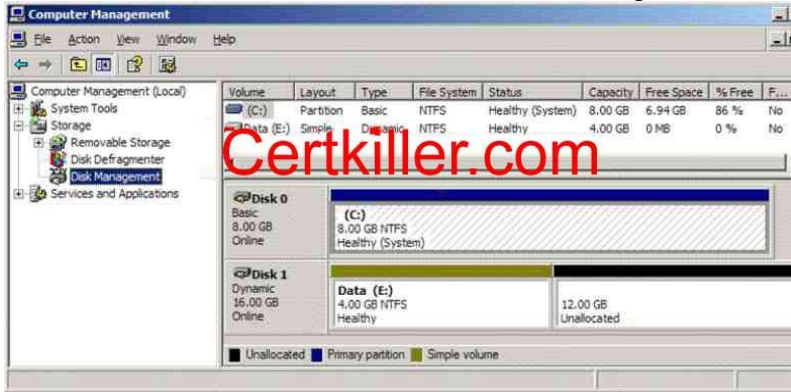
C: By moving only one disk from the old Certkiller 1 to the new Certkiller 1 will affect not only the current amount of data available, but will also result in a lack of possible redundancy.

D: Removing one old Certkiller 1 disk from the mirror will not enable you to accomplish your task successfully.

Reference:

**QUESTION 3**

You are the administrator of a Windows Server 2003 computer named Certkiller 1. Two hard disks are installed on Certkiller 1. The hard disks are configured as shown in the exhibit.



The data volume, which resides on Disk 1, is low on space. You need to provide additional space for the data volume. What should you do?

- A. Use Disk Management to extend the data volume.
- B. Run the fsutil volume command on the data volume.
- C. Using Diskpart.exe, run the extend command on the data volume.
- D. In Device Manager, select Disk 1. On the Volumes tab, click the Populate button.

Answer: A

Explanation: To increase a volume's capacity is to extend the volume. You can extend a simple or spanned volume on a dynamic disk so long as that volume is formatted as NTFS and so long as the volume is not the system or boot volume. And this is done through Disk Management.

Incorrect Answers:

B: With fsutil, Windows Server 2003 administrators can perform tasks such as managing disk quotas, managing mount points, and several other advanced disk-related tasks. Thus this command does not provide additional space.

C: Diskpart.exe command is used in converting disks and also to extend simple volumes, and not to extend disk volumes as is needed in this case which will have to be a spanned volume.

D: Populating Disk1 does not mean providing additional space.

Reference:

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 11, 15

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 3

---

**QUESTION 4**

You are the network administrator for Certkiller .com. Your network includes a computer named

Server1, which runs Windows Server 2003. All file and print services, all user home folders and all user profiles reside on Server1.

Certkiller merges with Acme. Users from both companies will store their files and folders on Server1. You run Diskpart.exe to view the disk configuration of Server1, as shown:

```
Diskpart> list volume
```

Volume #	Letter	Label	File System	Volume Type	Size	Status	Info
Volume 0	F	021234	NTFS	RAID-5	4096 MB	Healthy	
Volume 1	G	023411	FAT32	Stripe	6144 MB	Healthy	
Volume 2	H	023441	NTFS	Mirror	2048 MB	Healthy	
Volume 3	I	023332	FAT32	Spanned	9 GB	Healthy	
Volume 4	D		UDFS	CD-ROM	0 B		
Volume 5	C		NTFS	Partition	2047 MB	Healthy	System
Volume 6	E		FAT32	Partition	2063 MB	Healthy	Boot

Now you need to increase storage space on Server1. You will not create any additional volumes. What should you do to accomplish this task?

- A. Make use of Diskpart.exe, run the Extend command on volume G:\ Then convert volume G:\ to FAT.
- B. Make use of Diskpart.exe, run the Extend command on volume C:\ Then convert volume C:\ to NTFS.
- C. Make use of Diskpart.exe, run the Extend command on volume I:\ Then convert volume I:\ to NTFS.
- D. Make use of Diskpart.exe, run the Extend command on volume E:\ Then convert volume E:\ to FAT32.

Answer: C

Explanation: You can use the Diskpart.exe utility to manage disks, partitions, and volumes from a command-line interface. You can use Diskpart.exe on both Basic disks and Dynamic disks. If an NTFS volume resides on a hardware RAID 5 container that has the capability of adding space to the container, you can extend the NTFS Volume with Diskpart.exe while the disk remains a Basic disk.

Note: When you use Diskpart.exe to extend an NTFS partition, Microsoft recommends that you perform this task in Safe mode or Active Directory Restore mode. By doing so, you prevent open handles to the drive that cause the process to fail.

Use the extend command to incorporate unallocated space into an existing volume while preserving the data. Incorrect answers:

A: Volume G is a striped volume which will not lend itself to being extended safely and without risks. A striped volume (RAID-0) combines areas of free space from multiple hard disks into one logical volume. Unlike a spanned volume, however, data is written to all physical disks in the volume at the same rate. Because multiple spindles are in use, read and write performance is increased almost geometrically as additional physical disks are added to the stripe. But like extended simple volumes and spanned volumes, if a disk in a striped volume fails, the data in the entire volume is lost.

B: Volume C contains the system information and it is thus not recommended to use that specific volume to create space for data storage. NTFS can be extended.

D: FAT32 volumes cannot be extended. Also you cannot extend boot volumes.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 3

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 423

---

**QUESTION 5**

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. A server named Server1 hosts several applications. This server contains two hard disks, Disk0 and Disk1. Each disk is connected to a different EIDE channel. Each disk is configured as a basic disk and formatted as NTFS. System files are installed on Disk1.

You install a third hard disk on Server1. You configure it as a basic disk and format it as NTFS.

When you restart Server1, you receive the following message:

"Windows could not start because of a computer disk hardware configuration problem. Could not read the selected boot disk. Check boot path and disk hardware. Please check Windows documentation about hardware disk configuration and your hardware reference manuals for additional information."

You press a key. Server1 restarts, but it displays the same message.

You need to ensure that Server1 will start correctly. Your solution must not require reinstalling any applications on Server1.

What should you do?

- A. Start Server1 from the Windows Server 2003 installation CD-ROM. Use the Recovery Console to repair the system.
- B. Start Server1 in Safe Mode with Command prompt.
- C. Start Server1 from the Windows Server 2003 installation CD-ROM. Press F6 to replace the Mass Storage driver.
- D. Reconfigure the new disk drive so it is enumerated after the existing drives. Restart Server1.

Answer: A

Explanation: Adding the extra hard disk has probably caused the problem. The boot.ini file needs to be corrected to reflect the new disk configuration. We can use the Bootcfg utility in the Recovery Console to correct this problem.

Use the Bootcfg utility in the Recovery Console to correct the Boot.ini file:

1. Use the Windows XP CD-ROM to start your computer.
2. When you receive the message to press R to repair Windows by using the Recovery Console, press the R key.
3. Select the Windows installation that you want, and then type the administrator password when prompted.
4. Type bootcfg /rebuild, and then press ENTER.
5. When the Windows installation is located, the following instructions are displayed:

Add installation to boot list? (Yes/No/All)

[Type Y in response to this message.]

Incorrect Answers:

B: If the boot.ini file is wrong, you won't be able to boot into safe mode.

C: This is not a driver problem. The mass storage driver worked before we added the new disk.

D: The disk drives are on different EIDE controllers, so this won't be possible (without moving the disk to the other EIDE controller).

Reference:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 15

---

**QUESTION 6**

You are the network administrator for Certkiller .com. Your network includes a computer named Certkiller Srv1, which runs Windows Server 2003 and Windows XP Professional in a dual boot configuration. Certkiller Srv1 has two basic disks, which are configured as shown in the following table.

<b>Partition</b>	<b>Disk 1</b>	<b>Size</b>
1	System	3 GB
2	Boot	4 GB
N/A	Unused	9 GB
3	Backup data	8 GB

<b>Partition</b>	<b>Disk 2</b>	<b>Size</b>
1	Boot	4 GB
2	Application files	8 GB
N/A	Unused	5 GB
3	N/A	N/A

You need to create a 10 GB partition on Server 1 to store user data. Certkiller Srv1 must retain its dual boot functionality.

What should you do?

A. Convert both disks to dynamic disks.

Create a 10 GB extended volume by using the unused space on Disk 1 and Disk 2.

B. Back up Partition 2 on Disk2.

Remove Partition 2 from Disk 2 and restore it on Disk 1 by using the unused space on Disk 1.

Create a 10 GB partition on Disk 2.

C. Back up partition 2 on Disk 1.

Remove Partition 2 from Disk 1 and restore it on Disk 2 by using the unused space on Disk 2.

Create a 10 GB partition on Disk 1.

D. Convert both disks to dynamic disks.

Back up Volume 2 on Disk 2.

Remove Volume 2 from Disk 2 and restore it on Disk 1 by using the unused space on Disk 1.

Create a 10 GB volume on Disk 2.

Answer: B

Explanation: You are presented with two choices, one, you could move the Application files from disk 2 to disk 1 or, two, you could move the boot files from disk 1 to disk 2. However, none of these options are

desirable; however, moving the application files is a better option. It is not advisable to move the boot files. Because you cannot convert basic disks to dynamic disks if they contain multiple installations of Windows 2000, Windows XP Professional, or the Windows Server 2003 family of operating systems. Moreover, after the conversion, it is unlikely that you will be able to start the computer using that operating system. After the disk is converted to dynamic, you can start the operating system that you used to convert the disk, but you will not be able to start the other operating systems on the disk.

Here are some considerations to keep in mind:

- You can convert a basic disk containing the system or boot partitions to a dynamic disk.
- After the disk is converted, these partitions become simple system or boot volumes (after restarting the computer).
- You cannot mark an existing dynamic volume as active.
- You can convert a basic disk containing the boot partition (which contains the operating system) to a dynamic disk.
- After the disk is converted, the boot partition becomes a simple boot volume (after restarting the computer).

Incorrect Answers:

A: Because you cannot convert basic disks to dynamic disks if they contain multiple installations of Windows 2000, Windows XP Professional, or the Windows Server 2003 family of operating systems. Moreover, after the conversion, it is unlikely that you will be able to start the computer using that operating system. After the disk is converted, the boot partition becomes a simple boot volume (after restarting the computer).

C: It is not advisable to move the boot files even if it is possible.

D: Do not convert basic disks to dynamic disks if they contain multiple installations of Windows Operating systems. After the conversion, it is unlikely that you will be able to start the computer using that operating system.

Reference:

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 433  
Server Help

---

## QUESTION 7

You are the network administrator for Certkiller .com. You administrate a Windows Server 2003 computer named Certkiller 12. Certkiller 12 has a single disk. The disk is configured so that it has four primary partitions, which are formatted as FAT32. The disk also has unallocated space available. You need to use the unallocated disk space to store user data.

What should you use?

- A. Convert all existing partitions to NTFS.
- B. Using Diskpart.exe, run the create command.
- C. Convert the disk to a dynamic disk, and create a new volume.
- D. Using Diskpart.exe, run the extend command.

Answer: C

Explanation: Converting the disk to a dynamic disk and then creating a new volume will enable you to use

the unallocated disk space to store data.

Incorrect answers:

A: Merely converting all existing partitions to NTFS is not the answer. This is only part of the solution.

B: Diskpart.exe command is used in converting disks and also to extend simple volumes, and not to extend disk volumes as is needed in this case which will have to be a spanned volume.

D: You can use the Diskpart.exe utility to manage disks, partitions, and volumes from a command-line interface. You can use Diskpart.exe on both Basic disks and Dynamic disks. Use the extend command to incorporate unallocated space into an existing volume while preserving the data. However, FAT32 volumes cannot be extended.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 3

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 423

---

### QUESTION 8

You are the network administrator for Certkiller .com. You manage a Windows 2003 computer named Certkiller 3 that functions as a file server.

The data volume on Certkiller 3 is mirrored. Each physical disk is on a separate controller. One of the hard disks that contain the data volume fails. You discover that the failure was caused by a faulty SCSI controller. You replace the SCSI controller.

You need to restore the data volume to its previous state. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do?

- A. Run the diskpart active command on the failed volume
- B. Convert both disks to basic disks, and then restore the data.
- C. Break the mirror, and then re-create the mirror.
- D. Select a disk in the mirror, and then reactivate the volume.

Answer: D

Explanation: To restore the volume, replace the failed disk, rescan the disks, and reactivate the disk. If this doesn't make the volume healthy again, then right-click the volume and choose Reactivate Volume. The computer will chug away for a couple of minutes, rebuilding the missing data with the parity information on the remaining disks, and the stripe set will be back in one piece. Thus if you select a disk in the mirror and then reactivate the volume you will solve the problem in this case.

Incorrect answers:

A: Replaces the FDISK tool with which you're probably familiar. Creates or deletes disk partitions. Only use this command on basic disks-it can damage dynamic disks. This is not what is needed here.

B: This is unnecessary.

C: There is no need to break the mirror since the problem only arose due to a failed SCSI controller.

Reference:

Mark Minasi, Christa Anderson, Michele Beveridge, C.

A. Callahan & Lisa Justice, Mastering(tm)Windows(r) Server 2003, Sybex Inc., Alameda, 2003, pp. 867, 891



## QUESTION 9

### Exhibit



You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All domain controllers run Windows Server 2003, and all client computers run Windows XP Professional.

Dr King, one of the users in the domain, report that she cannot access a server named Certkiller 2.

Answer: Re-enable the NIC.

Explanation: In the exhibit the 3Com 3C920 Integrated Fast Ethernet Controller is mark with a red cross. This means that Dr. King will first have to enable this card to re-establish a connection to the server Certkiller 2.

If you disable a listener connection, no one will be able to connect to Terminal Services on the NIC for which it is configured until you re-enable it.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 547

---

## QUESTION 10

You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003. You use Microsoft Operations Manager (MOM) to monitor all servers.

An e-mail server named Mail CK1 is located at a remote data center. Mail CK1 runs Microsoft Exchange Server 2003.

Mail CK1 restarts unexpectedly during business hours. The event log indicates a problem with the SCSI CD-ROM.

You need to ensure that Mail CK1 remains continuously available during business hours.

What should you do?

A. Use Device Manager to disable the SCSI CD-ROM.

- B. Create and implement a new hardware profile to exclude the SCSI CD-ROM.
- C. Use Device Manager to update the driver for the SCSI CD-ROM.
- D. Use Device Manager to update the driver for the SCSI controller.

Answer: A

Explanation: The problem lies with the SCSI CD-ROM as indicated by the Event Log. This means that if you circumvent the problem you will avoid the problem of Mail CK1 restarting at unexpected times. Thus you only need to disable the SCSI CD-ROM and not remove it. You can enable and disable devices for a specific hardware profile through their properties dialog boxes in Device Manager.

Incorrect answers:

B: It is not necessary to create a new hardware profile.

C: Updating the driver may solve the problem. However, disabling the device will make sure of it.

D: Updating the driver for the SCSI controller by making use of Device Manager will not solve the problem of the server starting unexpectedly.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 2

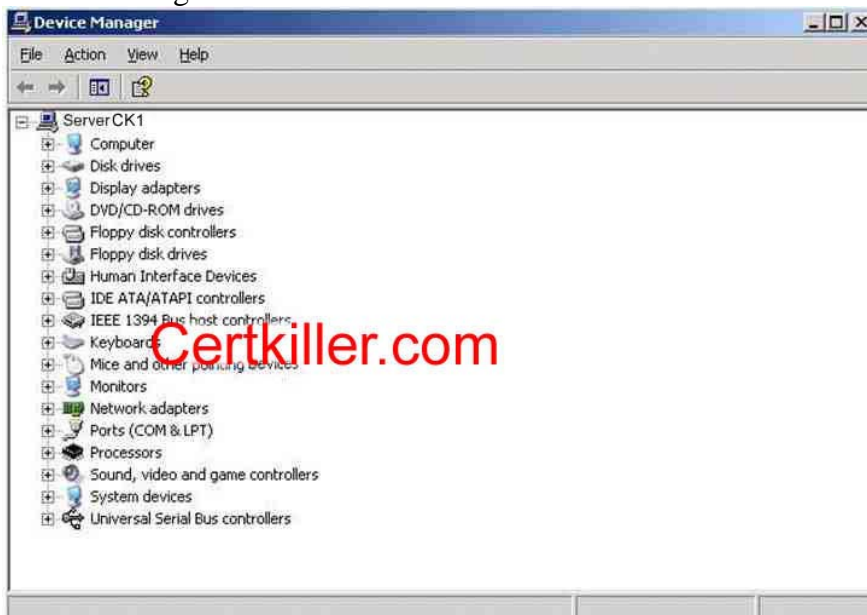
---

### QUESTION 11

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. Your network includes one branch office in addition to the main office. A server named Server CK1 connects the main office to the branch office by using an external dial-up modem.

One morning, users report that the connection to the branch office is not functioning.

On investigation, you discover that the modem is turned off. You restart the modem. Then you open Device Manager and see the information shown in the exhibit:



You need to ensure that the connection between the main office and the branch office functions correctly. Your solution must involve the minimum amount of change to Server CK1 and the minimum amount of interruption in network service.

What should you do?

- A. Restart Server CK1 .
- B. Create a new dial-up connection to the branch office.
- C. Open Device Manager to scan Server CK1 for changes in hardware.
- D. Use the Add Hardware Wizard to detect and install the modem.

Answer: C

Explanation: According to the exhibit, there is no modem found. This is evident from the lack of modem subsection. You should thus Open Device Manager to scan Server CK1 for changes in hardware in an effort to find the modem. This will ensure that you do not add any changes to the existing network and with the minimum amount of server downtime.

Incorrect answers:

A: Restarting the server as suggested here does not mean restoring the settings and establishing the connection from the branch office to the head quarters because the modem has been unplugged.

B: Creating a new dial-up connection to the branch office will involve unnecessary changes.

D: You do not need to add any hardware as the modem was installed and was operational before. You use the Add Hardware Wizard when you want to add new hardware to the computer and the modem is not new it was just turned off.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4

---

## **QUESTION 12**

You are the file server administrator for Certkiller . The company network consists of a single Active Directory domain named Certkiller .com. The domain contains 12 Windows Server 2003 computers and 1,500 Windows XP Professional computers.

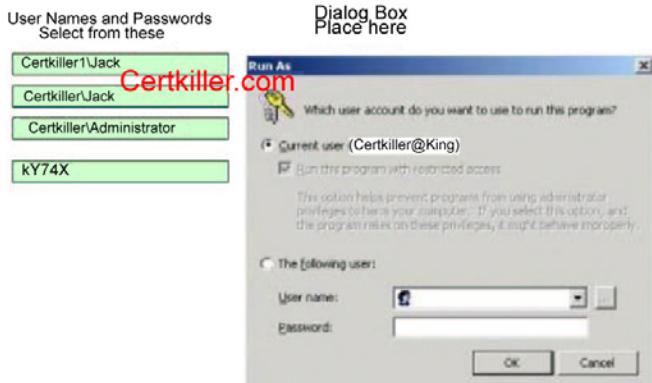
You manage three servers named Certkiller 1, Certkiller 2, and Certkiller 3. You need to update the driver for the network adapter that is installed in Serve1.

You log on to Certkiller 1 by using a nonadministrative domain user account named King. You open the Computer Management console. When you select Device Manager, you receive the following error message: "You do not have sufficient security privileges to uninstall devices or to change device properties or device drivers".

You need to be able to run the Computer Management console by using the local administrator account. The local administrator account on Certkiller 1, Certkiller 2, and Certkiller 3 has been renamed Tess. Jack's password is kY74X.

In Control Panel, you open Administrative Tools. You right-click the Computer Management shortcut and click Run as on the shortcut menu.

What should you do next?



Answer:

Users Names and Passwords  
Select from these

- Certkiller\Jack
- Certkiller\Administrator

Dialog Box  
Place here



Explanation: You need to make use of "The following User" setting because you want to run the program under a different account to the one you're logged in with, by entering " Certkiller 1\Tess" in the User Name field, enter kY74X" in the password field. Certkiller 1\Tess indicates a user account named Jack on a computer named Certkiller 1; in this scenario, this is the local administrator account.

Reference:

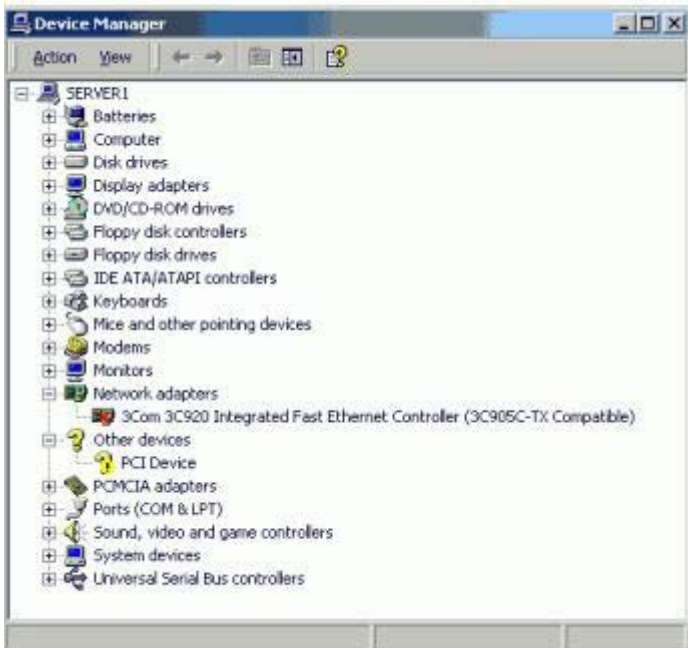
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 2

### QUESTION 13

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.

A user reports that she cannot access a server named Certkiller B.

First, you verify that the network adapter on Certkiller B has the correct driver installed. Then, you open Device Manager on Certkiller B. You see the display shown in the exhibit.



Now you need to use Device Manager to restore network connectivity on Certkiller B. What should you do?

- A. Enable the network adapter.
- B. Change the IRQ setting of the network adapter.
- C. Change the IP address of the network adapter.
- D. Adjust the link speed of the network adapter to match the link speed of the network.
- E. Resolve all possible hardware conflicts between the network adapter and the unknown device.

Answer: A

Explanation: The exhibit shows that the network card is disabled. The question also mentions that the correct driver is installed. Therefore, by enabling the network adapter will render it operational.

Incorrect Answers:

B: Interrupt request (IRQ) - One of a set of possible hardware interrupts, identified by a number. The number of the IRQ determines which interrupt handler will be used. If the IRQ was wrong, the network adapter would have an exclamation mark in a yellow circle over it.

C: If the IP address was wrong, the network adapter would seem to be operational in Device Manager.

D: If the link speed was wrong, the network adapter status will appear as operational in Device Manager.

E: If there was a hardware conflict, the network adapter status will be marked with an exclamation mark in a yellow circle over it.

Reference:

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 763

## QUESTION 14

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. All network servers run Windows Server 2003.

Certkiller operates 10 branch offices in addition to the main office. Each branch office has one filer

server with two logical disks, P:\ and U:\. Each disk has a capacity of 20 GB. For each department in the branch office, P:\ hosts one folder in which departmental users save shared documents. For all users in the branch office, U:\ hosts home folders.

The main office includes a network operations center that monitors servers and network status. However, branch office users frequently report that their servers have no more disk space. In such cases, local support technicians log on to the servers and delete unnecessary files.

You need to create a proactive monitoring strategy for the network operations center. Monitoring must alert the network operations center before the branch office servers run out of disk space.

Monitoring must also report which disks on the servers are approaching capacity. The monitoring strategy must require the minimum amount of administrative effort.

What should you do?

A. Configure a server in the main office to report performance alters on the branch office servers. Use the logicaldisk(\_total)\ &Free Space counter to indicate when free space is less than 5 percent. Use the logicaldisk(\_total)\Free megabytes counter to indicate when free space is less than 100 MB.

B. On each branch office server, create a performance alert. Use the logicaldisk(\_total)\ %Free Space counter to indicate when free space is less than 5 percent. Use the logicaldisk(\_total)\Free megabytes counter to indicate when free space is less than 1000 MB.

C. Configure a server in the main office to report performance alerts on the branch office servers. Use the logicaldisk(P)\ %Free Space counter and the logicaldisk(U)\ %Free Space counter to indicate when free space is less than 5 percent.

D. On each branch office server, create a performance alert. Use the logicaldisk(P)\ %Free Space counter and the logicaldisk(U)\ %Free Space counter to indicate when free space is less than 5 percent.

Answer: C

Explanation: The monitoring must alert the network operations centre before the branch office servers run out of disk space and monitoring must also report which disks on the servers are approaching capacity. LogicalDisk: % Free Space is a counter that indicates the amount of free space available on the disk as a percentage of the total disk capacity. Paging problems can occur if you have little disk space to which the system can swap data out of memory, and operating system errors can occur if the partition on which the OS is installed becomes too full.

Incorrect Answers:

A: It is necessary is to know which disks are near capacity, so we cannot monitor the total disk space - we must monitor the individual logical disks.

B: We need to know which disks are near capacity, so we cannot monitor the total disk space - we must monitor the individual logical disks.

D: The monitoring must alert the network operations centre before the branch office servers run out of disk space; therefore, the monitoring should be done from the main office.

Reference:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 748

---

**QUESTION 15**

You are the network administrator for Certkiller .com. You administer a Windows Server 2003 computer named Certkiller 5. The hardware vendor for Certkiller 5 notifies you that a critical hotfix is available. This hotfix is required for all models of this computer that have a certain network interface card.

You need to find out if the network interface card that requires the hotfix is installed in Certkiller 5. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

- A. Open Network Connections, and then examine the properties of each connection that is listed.
- B. Open the Component Services snap-in, expand Computers, expand My Computer, and then examine the list.
- C. Run the netsh interface command, and then examine the list.
- D. Open Device Manager, expand Network adapters, and then examine the list.

Answer: A, D

**Explanation:**

A: The Network Connections tab contains settings for network connections and a Wizard to create new connections. From there you will be able to examine the properties of each connection that is listed. This will reveal if the network interface card that requires the hotfix is installed on Certkiller 5.

D: The Device Manager utility is a graphically-based utility that provides information about all of the devices that your computer currently recognizes. Through Device Manager, you can see a summary of all of the currently installed hardware; view and change hardware settings; view, uninstall, update, or roll back a device driver; disable and enable devices; and print a summary of all of the hardware devices that have been installed on your computer. You can also run the Hardware Troubleshooting Wizards from Device Manager. If you make use of Device Manager and then expand the Network Adapters tab, you will be able to find out if the appropriate network interface card is installed on Certkiller 5.

**Incorrect answers:**

B: This option will not display the relevant information needed.

C: You can use commands in the Netsh Interface IP context to configure the TCP/IP protocol (including addresses, default gateways, DNS servers, and WINS servers) and to display configuration and statistical information.

**Reference:**

Microsoft Knowledge Base: 306794: How to Install the Support Tools from the Windows XP CD-ROM  
Network Monitor is provided with Windows Server products and Microsoft Systems Management Server (SMS). Microsoft Corporation, 2004

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, pp. 686, 854-856, 926

Lisa Donald & Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r) Server 2003 Environment Management and Maintenance: Study Guide, Sybex Inc, Alameda, 2003, Chapter 2, pp. 84 &116

---

**QUESTION 16**

You are the network administrator for Certkiller .com. You are the administrator of a Windows Server 2003 computer named Certkiller 3.

Newly hired employees recently started storing files on Certkiller 3. Now users report that Certkiller 3 is responding much slower than it did before the additional users were added. You suspect the disk subsystem needs to be upgraded to accommodate the additional user load.

You need to confirm whether the disk subsystem on Certkiller 3 needs to be upgraded.

What should you do?

- A. Configure a Performance Logs and Alerts on the %Free space counter.
- B. Use Device Manager to populate volume settings and examine the properties of the disk drives on Certkiller 3.
- C. Use Event View to examine the system logs and search the system logs for event logs for events generated by the disk event source.
- D. Use System Monitor to monitor counters based on the PhysicalDisk object.

Answer: D

Explanation: One adds key counters to track for the processes subsystem and how to tune and upgrade the processes subsystem to the System Monitor. The PhysicalDisk object is the sum of all logical drives on a single physical drive. Adding this object counter to the System Monitor should give you the relevant information necessary to confirm whether an upgrade of the disk subsystem is needed.

Incorrect answers:

A: The %Free space counter tracks how much free space is available on the hard drive. It is a way to track disk space usage proactively so users do not experience "out of disk space" errors. This is not the information needed to confirm whether an upgrade of the disk subsystem is needed.

B: Device Manager is a Windows Server 2003 utility used to view information about the computer's hardware configuration and set configuration options. This is not what is required.

C: Event Viewer is a Windows Server 2003 utility that tracks status information about the computer's hardware and software, as well as security events. This information is stored in multiple log files dependent upon the configuration of the server. The minimum number of logs is three: the Application log, the Security log, and the System log. However, you should rather make use of System Monitor to monitor counters based on the PhysicalDisk object in this case.

Reference:

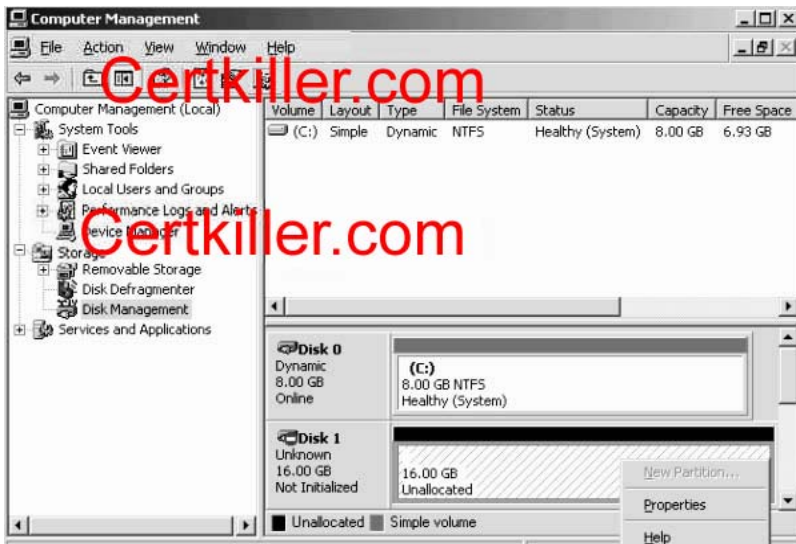
Lisa Donald & Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r) Server 2003 Environment Management and Maintenance: Study Guide, Sybex Inc, Alameda, 2003, Chapter 9, p. 460

---

**QUESTION 17**

Exhibit





You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. A Windows Server 2003 computer named Certkiller 2 functions as a mail server. Certkiller 2 has a single disk that is configured as a basic disk. You add a second disk. In Disk Management, you right-click the unallocated file system. You discover that the "New Partition" menu command is unavailable, as shown in the exhibit.

You need to create a new partition.

What should you do?

- A. Restart the server, and then select the New partition menu command.
- B. Right-click the disk, select Initialize, and then select the New partition menu command.
- C. Replace the disk that you added, and then select the New partition menu command.
- D. Ask the appropriate administrator to assign you Administrator rights on Certkiller 2, and then select the New partition menu command.

Answer: B

Explanation: When you attach a new disk to your computer, you must first initialize the disk before you can create partitions. When you first start Disk Management after installing a new disk, a wizard appears that provides a list of the new disks that are detected by the operating system. When you complete the wizard, the operating system initializes the disk by writing a disk signature, the end of sector marker (also called a signature word), and a master boot record (MBR). The question states that a second disk has been added thus you will need to initialize the disk and then select the new Partition menu command to create a new partition.

Incorrect answers:

A: Restarting the server is not the way to go when you first need to initialize the disk as the question states that a second disk has been added.

C: This does not make sense considering that a second disk has already been added. What is needed is to initialize the disk and only then will the New Partition menu command be available.

D: This is not a matter of administration rights.

Reference:

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 11.38

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 3

Lisa Donald & Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r) Server 2003 Environment Management and Maintenance: Study Guide, Sybex Inc, Alameda, 2003, Chapter 4, p. 216

---

**QUESTION 18**

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. The network includes a file server named Certkiller 17. Certkiller 17 contains a single disk for system files and two SCSI hard disks that comprise a 72-GB mirrored volume with 65 GB of read-only data. Users connect to this data by using shortcuts on their desktops. Certkiller 17 is scheduled for replacement. You have a scheduled maintenance window to complete this task. Before the maintenance window, you build a new server. You need to bring the new server online with current data and re-establish redundancy as quickly as possible. You must also ensure that the desktop shortcuts will continue to function. What should you do?

- A. Name the new server Certkiller 20. Create a new mirrored volume by using two 72-GB disks. Connect Certkiller 20 to the network and copy the data from Certkiller 17. When copying is complete, shut down the old Certkiller 17.
- B. Name the new server Certkiller 17. Move both disks from the old Certkiller 17 to the new Certkiller 17. Scan the disks for changes. Connect the new Certkiller 17 to the network.
- C. Name the new server Certkiller 17. Break the mirror on the old Certkiller 17. Move one of the disks from the old Certkiller 17 to the new Certkiller 17. Scan the disk for changes. Initialize the disk. Select the spare disk and create the mirror. Connect the new Certkiller 17 to the network.
- D. Name the new server Certkiller 17. Remove one of the disks in the mirror from the old Certkiller 17. Move the disk to the new Certkiller 17. Scan the disk for changes. Import the disk. Shut down the old Certkiller 17 and connect the new Certkiller 17 to the network.

Answer: B

Explanation: The "Scan For Hardware Changes" option allows you to force a manual scan to see if any new hardware changes have been detected. To be able to bring the server online with the current data and reestablishing redundancy as soon as possible whilst ensuring that desktop shortcuts stay functional, you will need to give the same name to the new server, namely Certkiller 17 and use the two disks from the old Certkiller 17. You should then scan it for any changes and then connect the new Certkiller 17 to the network. Incorrect answers:

A: There is no need to create a new mirrored volume in this case. Besides where will you get the two new disks from to copy the existing data of Certkiller 17 onto. What is needed is to use the old Certkiller 17 disks to provide continuity for users insofar as desktop shortcuts are concerned.

C & D: This is not necessary. All that has to be done is to use the existing Certkiller 17 disks and put them on the newly created and named Certkiller 17 server. Scanning the disk for changes and then connecting new Certkiller 17 to the network.

Reference:

Lisa Donald & Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r) Server 2003 Environment Management and Maintenance: Study Guide, Sybex Inc, Alameda, 2003, Chapter 2, p. 91

**QUESTION 19**

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. A server named CK1 contains a simple volume that stores mission critical data files. CK1 experiences hardware failure and stops functioning. Replacement parts will be available within 72 hours.

A second file server named CK2 is available. However, CK2 has insufficient disks space to hold the data on CK1 .

You need to provide immediate access to the data on CK1 .

First, you install the disks from CK1 on CK2 and restart CK2 . However, the disks do not appear in Disk Management.

Which action or actions should you perform? (Choose all that apply)

- A. Install the disks from CK1 on CK2 . In Disk Management, initialize the disks.
- B. Install the disks from CK1 on CK2 . In Disk Management, rescan the disks.
- C. In Disk Management, select each disk from CK1 . Then, select the option to import foreign disks.
- D. In Disk Management, select each disk from CK1 . Then, select the option to repair the volume.
- E. On CK2 , run the mountvol /p command from a command prompt.
- F. On CK2 , convert the dynamic disks to basic disks.

Answer: B, C

Explanation: It is imperative that you rescan disks after you move hard disks between computers.

Following is the reason: When Disk Management rescans disk properties; it scans all attached disks for changes to the disk configuration. It also updates information about removable media, CD-ROM drives, basic volumes, file systems, and drive letters.

When you move a dynamic disk from one computer to another, Windows Server 2003 considers the disk as a foreign disk by default. When Disk Manager indicates the status of a new disk as foreign, you have to import the disk before you can access volumes on the disk.

Incorrect Answers:

A: When you attach a new disk to your computer, you must first initialize the disk before you can create partitions. When you first start Disk Management after installing a new disk, a wizard appears that provides a list of the new disks that are detected by the operating system. When you complete the wizard, the operating system initializes the disk by writing a disk signature, the end of sector marker (also called a signature word), and a master boot record (MBR). If you cancel the wizard before the disk signature is written, the disk status remains Not Initialized.

D: Since replacement parts are underway, you need not repair the disk as this will not make the CK1 data available immediately.

E: The Mountvol command creates, deletes, or lists a volume mount point. Mountvol is a way to link volumes without requiring a drive letter.

F: If you convert the dynamic disks to basic disks you will lose the data and the question pertinently asks for the CK1 data to be made available.

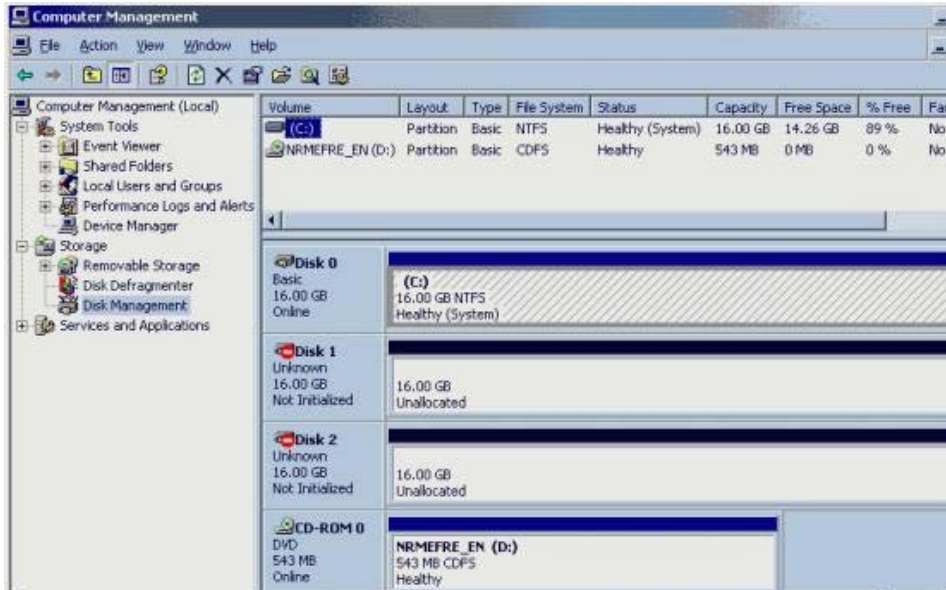
Reference:

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 11.38

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 3

**QUESTION 20**

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. Certkiller A hosts highly confidential files. The Disk Management console for Certkiller A is shown in the exhibit.



You need to ensure the security of all files on Certkiller

A. In the event of disk failure, you need to minimize the time required to make these files available again. You also need to improve file system performance.

How will you go about accomplishing these objectives?

- A. Configure the unallocated disks in a RAID-0 configuration and then convert the disks to basic disks.
- B. Configure one of the unallocated disks in a RAID-1 configuration and then convert the disks to dynamic disks.
- C. Store a shadow copy of disk C on one of the unallocated disks and then convert the disks to basic disks.
- D. Configure the unallocated disks as an extended volume and then convert the disks to dynamic disks.

Answer: B

Explanation: Part of the objectives state that you must minimize the time needed to make these files available again in case of disk failure. This can be accomplished through mirroring Disk0 to another disk. A disk mirror is also known as RAID-1. You have to convert the disks to dynamic disks to accomplish this. A mirrored volume is a fault-tolerant set of two physical disks that contain an exact replica of each other's data within the mirrored portion of each disk. Mirrored volumes are supported only on Windows Server computer versions.

If you convert the disk containing the boot and system partitions to a dynamic disk, you can mirror the boot and system volumes onto another dynamic disk. Then, if the disk containing the boot and system volumes fails, you can start the computer from the disk containing the mirrors of these volumes.

Incorrect Answers:

A: A RAID-0 is fast but it offers no redundancy. Redundancy is necessary if you need to consider using the minimum time needed to make these files available after possible disk failure. The disks are already basic disks there is no need for any conversion. Furthermore the objectives will only be met through converting the disks to dynamic volumes.

C: A shadow copy will keep copies of previous versions of the files. You won't be able to access these though if Disk0 fails. The disks are already basic disks there is no need for any conversion. Furthermore the objectives will only be met through converting the disks to dynamic volumes.

D: An extended volume offers no redundancy which if needed to minimize the time needed to make these files available in case of disk failure. Though dynamic disks will allow mirroring, the extended volume configuration will negate that possibility.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 3

---

### **QUESTION 21**

You are the network administrator for Certkiller .com. You administer a Windows Server 2003 computer named Certkiller 4. Certkiller 4 has a single physical disk that is configured as a simple volume.

You plan to store the files for a large database on Certkiller 4. You plan to install additional physical disks on Certkiller 4.

You need to reconfigure the disks on Certkiller 4. Your solution must provide fault tolerance for the operating system and the database files.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Install three additional physical disks. Create a new RAID-5 volume. Place the database files on the new volume.

B. Install three additional physical disks. Create a new striped volume. Place the database files on the new volume.

C. Install one additional physical disk. Configure the simple volume as a mirrored volume.

D. Install one additional physical disk. Configure the simple volume as a spanned volume.

Answer: A, C

Explanation: RAID (Redundant Array of Independent Disks)-5 volume or striped set with parity volume is a fault-tolerant collection of equal-sized partitions on at least three physical disks, in which the data is striped and includes parity data. The parity data helps recover a member of the striped set if the member fails. If a single disk fails in a RAID-5 volume, data can continue to be accessed as is the case here. During read operations, any missing data is regenerated on the fly through a calculation involving remaining data and parity information thus taking care of redundancy in the sense that work will continue and no information will be lost. RAID-5 can only sustain a single drive failure. Thus RAID-5 is a volume configuration that stripes data over multiple disk channels and places a parity stripe across the volume for fault tolerance. A mirrored volume set contains a primary volume and a secondary volume. The data written to the primary volume is mirrored to the secondary volume. Mirrored volumes provide fault tolerance, because if one volume in the mirrored volume fails, the other volume still works without any interruption in service or loss of data. Mirrored volumes are copies of two simple volumes stored on two separate physical

drives. So, if you are to provide fault tolerance for the operating system and the database files in your reconfiguration of Certkiller 4, you should install three additional physical disks, create a new Raid-5 volume and place the database files on the new volume. You should also install another physical disk and configure it as a mirrored volume.

Incorrect answers:

B: A striped volume is a dynamic disk volume that stores data in equal stripes between 2 to 32 dynamic drives. Typically, administrators use striped volumes when they want to combine the space of several physical drives into a single logical volume and increase disk performance. You should not create a new striped volume, RAID-5 will provide fault tolerance since Certkiller 4 is configured as a simple volume.

D: A spanned volume is a dynamic disk volume that consists of disk space on 2 to 32 dynamic drives. Spanned volume sets are used to dynamically increase the size of a dynamic volume. With spanned volumes, the data is written sequentially, filling space on one physical drive before writing to space on the next physical drive in the spanned volume set. Certkiller 4 is a simple volume.

Reference:

Lisa Donald & Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r) Server 2003 Environment Management and Maintenance: Study Guide, Sybex Inc, Alameda, 2003, Chapter 4, p. 208

---

### QUESTION 22

You are the network administrator for Certkiller .com. You manage a Windows Server 2003 computer that functions as a file server.

The data volume on the server is configured as a software RAID-5 array. One of disks that contain the data volume fails. You replace the failed disk. You start the Disk Management utility and view the status listed in the following table.

<b>Disk</b>	<b>Status</b>	<b>Type</b>
Disk1	Online	Dynamic
Disk2	Online	Dynamic
Disk3	Not initiated	Unknown
Missing	Offline	Dynamic

You need to restore fault tolerance.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Create a striped set that includes Disk1 and Disk2.
- B. Initialize Disk3 and convert it to a dynamic disk.
- C. Reactivate the RAID-5 array volume.
- D. Repair the RAID-5 array volume to include Disk3.
- E. Initialize Disk3 and configure it as a basic disk.
- F. Reactivate the missing disk.

Answer: B, D

Explanation: The question states that Disk3 is not initiated. Thus to restore fault tolerance you should make sure that their type are all the same, hence the need to initialize Disk3 and converting it to dynamic.

A RAID-5 volume is where data is written to 3 to 32 physical disks at the same rate, and is interlaced with parity to provide fault tolerance for a single disk failure. Since the question mentions that the data volume that is configured as a software RAID-5 array has one failed disk, you should also repair the array to restore fault tolerance.

Incorrect answers:

A: A mere striped set that includes only Disk1 and Disk2 will not restore the lost fault tolerance since those two disks are still operational and available and not Disk3.

C: You need to repair the RAID-5 array and not reactivate it.

E: Configuring Disk3 as a basic disk will not restore fault tolerance. Disk3 needs to be converted to dynamic disk so as to make it the same type as the other two disks.

F: Reactivating the missing disk is not going to restore fault tolerance.

Reference:

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 11.38

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 3

Lisa Donald & Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r) Server 2003 Environment Management and Maintenance: Study Guide, Sybex Inc, Alameda, 2003, Chapter 4, p. 203

---

## QUESTION 23

Exhibit

Physical disk	Drive	Data
1	C	Operating system
1	D	Shared folder
2	E	Temp file
2	F	Sales database

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. A server named Certkiller 2 functions as a file server. The hard disks in Certkiller 2 are configured as shown in the table displayed in the exhibit.

Users in the finance department store documents in the shared folder on Certkiller 2. Users report that they experience poor performance when they save files in the shared folder.

You need to use System Monitor to find out if the storage subsystem has a performance problem when users save files in the shared folder on Certkiller 2.

What should you do?

- A. Add the LogicalDisk performance object. Monitor the Free Megabytes counter on drive F.
- B. Add the LogicalDisk performance object. Monitor the Avg. Disk Queue Length counter on physical disk 1.
- C. Add the Paging File performance object. Monitor the % Usage counter.
- D. Add the Server performance object. Monitor the Bytes Total/sec counter.

Answer: B

Explanation: Disk Queue Length indicates the number of outstanding disk requests that are waiting to be processed. The Avg. Disk Queue Length counter forms part of the most useful performance data and will yield the necessary information regarding the storage subsystem.

Incorrect answers:

A: You will not get the necessary information for the purposes of this question.

C: The Paging File > %Usage counter indicates how much of the allocated page file is currently in use. If this number is consistently over 70 percent, you may need to add more memory or increase the size of the paging file. You should use the Paging File > %Usage counter value in conjunction with the Memory > Available Bytes and Memory > Pages/Sec counters to determine how much paging is occurring on your computer.

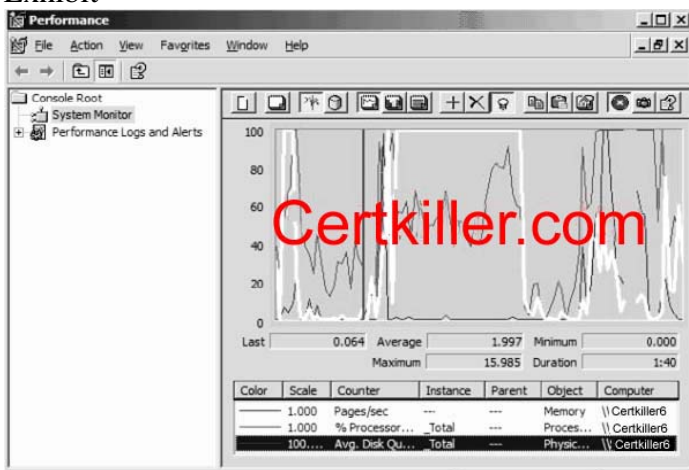
D: This will not yield the proper information needed in this case.

Reference:

Lisa Donald & Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r) Server 2003 Environment Management and Maintenance: Study Guide, Sybex Inc, Alameda, 2003, Chapter 9, pp. 454, 460

## QUESTION 24

### Exhibit



You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. A server named Certkiller 6 functions as a print server.

Users in the sales department print large reports and sales documents on several printers that are attached to Certkiller 6. Users report that during periods of peak activity, Certkiller 6 becomes unresponsive and it is slow to print documents. You use System Monitor to view the performance of Certkiller during a period of peak activity. The results are shown in the exhibit.

You need to improve the performance of Certkiller 6 when documents are printed during periods of peak activity.

What should you do?

- A. Configure a printer pool on Certkiller 6 by using an additional print device.
- B. Install an additional hard disk in Certkiller 6. Move the spool directory to the new hard disk.
- C. Increase the amount of physical RAM that is installed in Certkiller 6.
- D. Upgrade the processor in Certkiller 6.

Answer: B

Explanation: A common problem with printing in larger networks is that the spool folder gets so large that it fills up all available space on the disk drive. To get around this, move the spool folder to a different disk partition that has plenty of free space. Since the problem only occurs during periods of peak activity there is



an indication that you need additional hard drive space so as to be able to print the large documents and reports. With network printing you need to spool the documents before printing as many a time there would be a print queue. Thus to improve Certkiller 6 performance, you need to install an additional hard disk and move the spooler to the new hard disk.

Incorrect answers:

A: Making use of an additional print device will not solve the problem that the print server, Certkiller 6, is experiencing.

C: This is not a matter of insufficient RAM that causes the problem but rather a problem caused by insufficient space to spool the documents.

D: There is no need to upgrade the processor since it is not a processor that is causing the problem.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment: Study Guide & DVD Training System, Syngress Publishing, Rockland, 2003, Chapter 7, p. 611

---

### **QUESTION 25**

You are the network administrator for Certkiller .com. You administer a Windows Server 2003 computer named Certkiller 7. Users report that they experience poor performance when they access resources located on Certkiller 7. You suspect a disk bottleneck. You need to set up performance counters to monitor Certkiller 7.

You need to decide which performance objects to monitor.

Which two counters should you choose? (Each correct answer presents part of the solution. Select two.)

- A. LogicalDisk\% Idle Time
- B. PhysicalDisk\% Disk Time
- C. PhysicalDisk\Avg. Disk Queue Length
- D. Memory\Write Copies/sec
- E. Memory\Commit Limit

Answer: B, D

Explanation: The Memory: Pages/sec counter is used to measure memory usage. And with the PhysicalDisk\%Disk Time counter you will get an indication of whether the disk is being read quickly enough or not. These two counters would be essential if you suspect a disk bottleneck.

Incorrect answers:

A: This counter will not be as crucial to the requirements of this question.

C: The Physical Disk: Ave. Disk Queue Length counter is used to measure hard disk performance.

E: The Commit Charge group box is related to the Kernel Memory group box. The virtual memory details can be found here. (Remember, virtual memory is the maximum size of the page file.) The Peak item in this Commit Charge group box can exceed the physical memory value in the Physical Memory group box since page file can be utilized. The Limit item displays the maximum memory available.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment: Study Guide & DVD Training System, Syngress Publishing, Rockland, 2003, Chapter 9, p. 725

**QUESTION 26**

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. A server named Certkiller 6 functions as a file server. The disk subsystem on Certkiller 6 is configured as shown in the following table.

Physical disk	Volume	Contents
1	C	Operating system
2	C	Mirror of operating system
3	F	Company data (RAID-5)
4	F	Company data (RAID-5)
5	F	Company data (RAID-5)
6	F	Company data (RAID-5)

You need to ensure that you are notified if there is less than 1 GB of available disk space for company data.

What should you do?

- A. Create a performance alert. Configure the alert to monitor LogicalDisk performance objects for volume F.
- B. Create a trace log. Configure the log to record disk input/output for volume F.
- C. Create a performance alert. Configure the alert to monitor the PhysicalDisk performance objects for physical disks 3, 4, 5, and 6.
- D. Create a trace log. Configure the log to record the LogicalDisk performance objects for volume F.

Answer: A

Explanation:

The purpose of an alert is to notify the system administrator that the system is not functioning according to standard operating environment. You can configure alerts to send a network message, start a program, run a script, or log an event in the event log if a performance threshold is reached. Thresholds are limits that you specify (for example, when a disk is 90 percent full), or in this case to monitor LogicalDisk performance object for volume F for volume F: has the company data that is bound to grow larger in volume.

Incorrect answers:

B: You should be creating a performance alert, not a trace log. Furthermore, recording disk input and output will not yield the proper alert.

C: This option is halfway correct except that you need to monitor LogicalDisk performance object for volume F: and not PhysicalDisk performance objects for disks 3, 4, 5 and 6.

D: You should be creating a performance alert and not a trace log.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment: Study Guide & DVD Training System, Syngress Publishing, Rockland, 2003, Chapter 9, p. 788

**QUESTION 27**

You are the network administrator for Certkiller . All network servers run Windows Server 2003. You administer a server named Certkiller 76. You need to configure Certkiller 76 to function as a streaming

media server for Certkiller .com's content team. The content team wants Certkiller 76 to provide the fastest performance and the most available space possible. Redundancy is not important. Certkiller 76 currently has three identical, unpartitioned hard disks available. You need to configure the disks to meet the content team's requirements. What should you do?

- A. Create a simple volume on disk and then expand it to the other two disks.
- B. Create a mirrored volume that uses two of the disks.
- C. Create a RAID-5 volume that uses all three disks.
- D. Create a striped volume that uses all three disks.

Answer: D

Explanation: A striped volume is where data is written to 2 to 32 physical disks at the same rate. It offers maximum performance and capacity but no fault tolerance. Striped volumes use RAID-0, which stripes data across multiple disks. Striped volumes cannot be extended or mirrored, and do not offer fault tolerance. If one of the disks containing a striped volume fails, the entire volume fails. When creating striped volumes, it is best to use disks that are the same size, model, and manufacturer.

With a striped volume, data is divided into blocks and spread in a fixed order among all the disks in the array, similar to spanned volumes. Striping writes files across all disks so that data is added to all disks at the same rate.

Despite their lack of fault tolerance, striped volumes offer the best performance of all the Windows disk management strategies and provide increased I/O performance by distributing I/O requests across disks. For example, striped volumes offer improved performance when:

- Reading from or writing to large databases.
- Collecting data from external sources at very high transfer rates.
- Loading program images, dynamic-link libraries (DLLs), or run-time libraries.

Thus the answer to the problem would be to create a striped volume that uses all three disks.

Incorrect answers:

A: This option will not meet the requirements.

B: Mirrored volumes are used for redundancy purposes.

C: A RAID-5 volume is where data is written to 3 to 32 physical disks at the same rate, and is interlaced with parity to provide fault tolerance for a single disk failure. However, since the problem mentions that redundancy is not important, it would be better to make use of a striped volume that uses all three disks.

Reference:

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 281, 11.49

---

### QUESTION 28

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003. A server named Certkiller 9 functions as an application server. The disks in Certkiller 9 are configured as shown in the following table.

Physical disk	Drive	Data	Size
0	C	Operating system	20 GB

1                      D                      Free space                      20 GB

You purchase four additional 20-GB hard disks for Certkiller 9. You plan to install an inventory database on Certkiller 9. You estimate that you need a total of 60 GB of disk space to hold all the inventory data. You need to protect the data against the failure of any disk that contains either operating system data or inventory database data.

You need to create a new disk configuration on Certkiller 9.

Which two actions should you perform? (Each correct answer presents part of the solution. Select two.)

- A. Use one additional disk to create a mirror for drive C.
- B. Use two additional disks to create a striped set for drive C.
- C. Use three additional disks to create a RAID-5 volume for drive D.
- D. Use two additional disks to create a RAID-5 volume for drive C.
- E. Use one additional disk to create a mirror for drive D.
- F. Use three additional disks to create a striped set for drive D.

Answer: A, C

Explanation: A RAID-5 volume is where data is written to 3 to 32 physical disks at the same rate, and is interlaced with parity to provide fault tolerance for a single disk failure. Good read performance; good utilization of disk capacity; expensive in terms of processor utilization and write performance as parity must be calculated during write operations. Since Drive C holds the operating system, you should make use of an additional disk to create a mirror for drive C.

Incorrect answers:

B & F: Striped volumes are made up of two to 32 disks. Each disk should be the same size to efficiently use all space. It is possible to use different-sized disks, but the stripe size on every disk will be limited to the amount of free space on the smallest disk, so there will be space wasted on the larger disk(s). A striped set, whether making use of two or three additional disks, will not suffice in this case.

D: Two additional disks will not support RAID-5, you need three for Drive D and not Drive C.

E: You should create the mirror for Drive C and not drive D.

Reference:

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 281, 11.49

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment: Study Guide & DVD Training System, Syngress Publishing, Rockland, 2003, Chapter 2, p. 81

---

**QUESTION 29**

Exhibit, hotspot

Policy	Security Setting
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
Devices: Restrict floppy access to locally logged-on user only	Disabled
Devices: Unsigned driver installation behavior	Warn but allow...
Domain member: Digitally encrypt or sign secure schedule tasks	Not Defined
Domain member: Digitally encrypt secure channel data	Not Defined
Domain controller: Reuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Disabled
Interactive logon: Do not display last user name	Disabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Message text for users attempting to log on	
Interactive logon: Menu text for account password to log on	Not Defined
Interactive logon: Require strong (Windows 2000 or later) password	10 logons
Interactive logon: Require strong (Windows 2000 or later) password before expiration	14 days
Interactive logon: Do not display last user name before expiration	Disabled
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Requires smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (always)	Disabled

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. Certkiller .com's written security policy states that all computers are permitted to use only hardware that is listed on the Windows Server Catalog. You need to change the policy settings for the Windows Server 2003 computer so that it complies with the written security policy.

Which policy setting should you modify? To answer, select the appropriate policy in the exhibit.

Answer: Devices: Unsigned Driver installation behavior

Explanation: Driver signing is a method for marking or identifying driver files that meet certain specifications or standards. Windows Server 2003 uses a driver-signing process to make sure drivers are certified to work correctly with the Windows Driver Model (WDM) in Windows Server 2003. By modifying the Unsigned Driver installation behavior, you will be able to comply with company regulations regarding security policy.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 2

### QUESTION 30

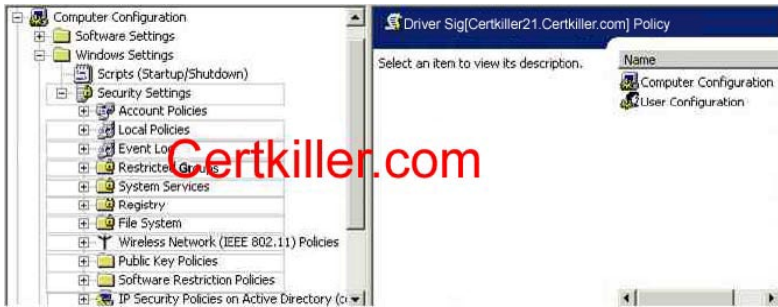
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.

A change in business rules requires you to configure hardware drivers on all network computers. You open the Group Policy Object Editor, as shown in the work area.

You need to configure Driver Signing in the treeview pane.

Which node should you configure?

To answer, select the appropriate node in the work area.



Answers: Select "Local Policies"

Explanation: Every device that is attached to a computer requires software, known as a device driver, is to be installed on the computer to enable it to function properly. Every device requires a device driver to communicate with the operating system.

Device drivers that are used with the Microsoft Windows operating systems are typically provided by Microsoft and the device manufacturer. Each device driver and operating system file that is included with Windows has a digital signature. This setting can be located in the LOCAL POLICIES section.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 2

### QUESTION 31

You are the administrator of a Windows Server 2003 computer named Certkiller 1. There is a driver conflict on Certkiller 1. You suspect that an unsigned driver has been installed for one of the hardware devices.

You need to locate any unsigned drives.

What should you do?

- A. Use the advanced options of the File Signature Verification tool to scan the contents of the Systemroot\System32 folder and all subfolders.
- B. Run the driverquery / si command, and examine the output.
- C. Use the advanced options of the File Signature Verification tool to scan the contents of the Systemroot\System folder and all subfolders.
- D. Run the ver command.

Answer: A

Explanation: The File Signature Verification tool generates the report of unsigned drivers with the least administrative effort. You can use File Signature Verification tool (Sigverif.exe) to identify unsigned drivers on a Windows-based computer by running a scan for unsigned drivers. sigverif.exe is a wizard-driven tool, which scans the system for the presence of unsigned drivers and critical system files. It also creates a report that lists all the files scanned along with relevant version and digital signature information. The report is stored in your

Windows directory and is called sigverif.txt. This information can be helpful when you are troubleshooting system instability in Windows.

Incorrect answers:

B: The driverquery command with the si parameter specifies to display the properties of signed drivers only

and not the location of unsigned drivers.

C: Systemroot\System32 folder is a protected directory in the Windows Server 2003 environment and the Systemroot\System folder is not besides that folder will not indicate whether the driver is signed or not.

D: You need to specify exactly what you want to verify.

Reference:

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 10.6

### QUESTION 32

You are the network administrator for Certkiller .com. You attempt to install a new network adapter in a Windows Server 2003 computer. You receive an error message that states that the software for the hardware that you are attempting to install has not passed Windows Logo testing to verify its compatibility with this version of Windows. The error message also states that the hardware has not installed.

You need to change the policies to ensure that you can install the network adapter on the Windows Server 2003 computer.

Which policy setting should you modify?

To answer select the appropriate policy in the work area.



Answer:

Change the "Unsigned driver installation behaviour" setting to "Allow installation".

Explanation: The exhibit shows that unsigned driver installation behaviour setting is on do not allow. This has to be changed in order for the network adapter to be installed successfully. Each device driver and operating system file that is included with Windows has a digital signature. The digital signature indicates that the driver or file meets a certain level of testing and that it was not altered or overwritten by another programs installation process. Using signed device drivers helps to ensure the performance and stability of your system. Also, it is recommended that you use only signed device drivers for new and updated device drivers.

Reference:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 203-205

### QUESTION 33

You are the network administrator for Certkiller .com. You are the administrator of a Windows

Server 2003 computer named Certkiller 8.

You log on to Certkiller 8 and attempt to access the network. You discover that the server is not communicating on the network. You discover that a service pack and an updated network adapter driver were installed on Certkiller 8 the previous night. A complete backup, including the System State data, was performed before the service pack and the driver were installed.

You need to restore network communications.

What should you do first?

- A. Use Roll Back Driver to reinstall the previous driver for the network adapter.
- B. Use the Backup or Restore Wizard to restore the backup from the previous night.
- C. Restart Certkiller 8 by using Last Known Good Configuration option.
- D. Use the Registry Editor to delete the registry settings for the network adapter driver.

Answer: A

Explanation: When drivers cause problems within a system, you might experience two levels of severity. The first is the device simply not being enabled on system startup or installation. A more severe level will result in the system not starting up due to a bug check (also known as a blue screen or STOP error).

If the problem is caused during a driver upgrade, you can leverage the capability to rollback a driver. To roll back a driver from a previous version, open the device Properties dialog box in Device Manager and select the Driver tab. In that tab is a button called Rollback that you can select to roll back the driver to the previous version.

Incorrect answers:

B: This option would not be advisable in this case as the complete backup was performed before the service pack and the driver were installed. And what is thus needed is to just rollback to the previous driver.

C: When Last Known Good Configuration is used, Windows starts using the Registry information and driver settings saved at the last successful logon. However, all you need to do is to make use of Roll Back Driver to reinstall the previous driver.

D: This would not be necessary.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment: Study Guide & DVD Training System, Syngress Publishing, Rockland, 2003, Chapter 3, p. 235

---

### QUESTION 34

You are the network administrator for Certkiller .com. In particular you administer a Windows 2003 server named Certkiller 4. Certkiller 4 stops responding several times. Each time, the following error message is displayed:

```
"0x00000001 (0x0000000c, 0x00000002, 0x00000000, 0xf27b4e8e) IRQL_NOT_LESS_OR_EQUAL."
```

You suspect that a hardware component is causing the problem, and you contact the vendor. The vendor requires debugging information.

You need to configure Certkiller 4 to generate a file that contains relevant information for the vendor.

What should you do?

- A. Configure Certkiller 4 to perform a memory dump.
- B. Add the /debug option to the Boot.ini file on Certkiller 4.



- C. Enable Physical Addressing Extensions on Certkiller 4.
- D. Install the Recovery Console on Certkiller 4.

Answer: A

Explanation: It is important that you record the information associated with the bug check and driver information sections. Many of the bug check messages have relevant information that you should read and understand if they apply to your situation. Your device vendor and/or Microsoft make use of the memory dumps to help understand the state of the system at the time that the bug check occurred. You can change the memory dump settings through the Startup and Recovery button in the System Properties' Advanced tab. Incorrect answers:

B: Adding the /debug option to the Boot.ini file will not address your problem.

C: Enabling Physical Addressing Extensions will not generate a file with the necessary information to address your problem.

D: Installing the Recovery Console will not yield the necessary information for the vendor.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 236

---

### **QUESTION 35**

You are the network administrator for Certkiller .com. In particular you administer a Windows 2003 server named Certkiller 13. You need to use Disk Management to configure a partition on Certkiller 13.

When you attempt to access Disk Management, you receive the following error message:

"Unable to connect Logical Disk Manager service."

You verify that the Logical Disk Manager service is started.

What is the most likely cause of the problem?

- A. There is not enough available space on the boot partition.
- B. The disk performance counters are disabled.
- C. The Logical Disk Manager Administrative service is disabled.
- D. The Windows 2003 Administration Tools Pack is not installed

Answer: C

Explanation: A disabled Logical Disk Manager Administrative service manifests as an inability to connect to Logical Disk Manager.

Incorrect answers:

A: It is not a matter of enough available space but rather an inability to connect to the Logical Disk Manager service.

B: Disk performance counters are irrelevant in this scenario.

D: This is not the problem; it is the service that needs to be enabled.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 3

---

**QUESTION 36**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003. Terminal Services is installed on your network. You currently use a terminal server farm. Certkiller 1, the first server in the farm, acts as the session directory server. All terminal servers are operating at maximum capacity. An increasing number of users report slow response times when they use these servers. You need to improve the performance of the terminal server farm. You plan to use a server named Certkiller 4, which has hardware identical to that of the other terminal servers in the farm. First, you add Certkiller 4 to the Session Directory Computers group on Certkiller 1. What should you do next?

- A. Add Certkiller 4 to the Session Directory Computers group on the PDC emulator.
- B. On Certkiller 4, select the Terminal Services configuration option to join the existing session directory.
- C. On Certkiller 4, install the Session Directory service.
- D. On Certkiller 4, create a new session directory server.

Answer: B

Explanation: The session directory is a database that can reside on a server that is separate from the terminal servers in the farm, although it is possible to have it on a member of the farm. The session directory database maintains a list of the user names associated with the session IDs connected to the servers in a load balanced Terminal Server farm.

There are two Session Directory components to keep in mind when installing and configuring Session Directory: (1) Session Directory server and (2) Client servers.

- The Session Directory server is the server that is running the Session Directory service. It is not required to be a Terminal Server, or even to have Remote Desktop enabled.
- The client servers are the Terminal Servers which will request data from the Session Directory server. Client servers need to be configured to point towards the Session Directory server for Session Directory requests. Architecturally, one Session Directory server may service multiple load balanced farms, although this may cause confusion if the administrator configures all farms to have the same logical cluster name value.

After adding CK4 to the Session Directory Computers group on CK1 , CK4 must be joined to the existing session directory.

Incorrect answers:

A: The PDC emulator can be used in a situation where you have windows NT4 servers in your domain. This is however not applicable in this scenario.

C: On all editions of the Windows Server 2003 family Session Directory service is installed by default. There is thus no need to install it on CK4 .

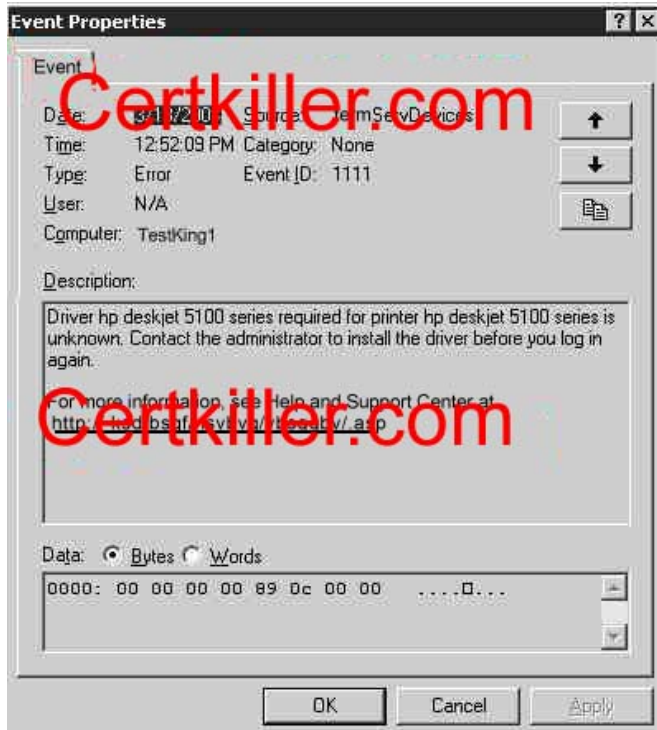
D: It would be superfluous to add another session directory server; a farm only requires one session directory server.

Reference:

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 750

**QUESTION 37**

Exhibit



You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains two domain controllers named Certkiller 1 and Certkiller 2.

During routine monitoring of the domain controllers, you observe numerous errors in the system log. The errors are similar to the one shown in the exhibit.

You need to resolve these errors on your domain controllers as quickly as possible.

What are two possible ways to achieve this goal? (Each answer is a complete solution. Select two.)

- A. Install the appropriate printer drivers on Certkiller 1 and Certkiller 2.
- B. Modify the Default domain controller GPO. Enable the Do not allow client printer redirection policy.
- C. Add the Domain Admins group to the built-in Print Operators group.
- D. Add the Domain Users group to the built-in Print Operators group.

Answer: A, B

Explanation: The System log records events generated by the operating system and its subsystems, such as its device drivers and services. It could be that the incorrect drivers were installed on the domain controllers. Thus if you install the appropriate driver on Certkiller 1 and Certkiller 2 you will solve the problem. If the Default To Main Client Printer setting is disabled, the Terminal Server session will use the default printer of the Terminal Server computer. Printer redirection settings can be specified by a GPO. This option should also solve your problem.

Incorrect answers:

C, D: The built-in Print Operators group has the right to log on locally. Whether you add the Domain Admins group or the Domain Users group to the built-in Print Operators group, it will not solve your problem as the problem is registered as a different type of error.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6

---

### **QUESTION 38**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

The network contains a domain controller named Certkiller 3. You create a preconfigured user profile on a client computer named TKClient1.

You need to ensure that all users receive the preconfigured user profile when they log on to the network for the first time. All users must still be able to personalize their desktop environments.

What should you do?

- A. From TKClient1, copy the user profile to \\ Certkiller 3\netlogon\Default User.
- B. From TKClient1, copy the user profile to \\ Certkiller 3\netlogon\Default User. Change the User Profile path for all users in the Active Directory to \\ Certkiller 3\netlogon\Default. User.
- C. From TKClient1, copy the user profile to the C:\Documents and Settings\Default User folder. Share the Default User profile on the network.
- D. Create a Folder Redirection policy in Active Directory.

Answer: A

Explanation: The Net Logon service uses it for processing logon scripts. To assign a preconfigured user profile for all first time users on the network, you need to copy TKClient1's user profile to the \\ Certkiller 3\netlogon\Default User. This option will still allow users to personalize their desktop environments.

Incorrect answers:

B: You do not need to change the User Profile path for all users, it is only the first time users that you need to assign the preconfigured user profile.

C: Sharing the Default User profile is not going to ensure that all first time users will be assigned the profile.

D: Folder redirection is not what is required in this scenario.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapters 4 & 5

---

### **QUESTION 39**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003. Some client computers run Windows 2000 Professional, and the rest run Windows XP Professional.

All user accounts in the Sales department are located in the Sales organizational unit (OU).

To store roaming user profiles, you create a shared folder named Profiles on a member server named CK1 . You assign the Allow - Full Control permission on the Profiles folder to the Everyone group. Now you need to create roaming user profiles for the user accounts in the Sales OU. What should you do?

A. Select all user accounts in the Sales OU.

Modify the account properties to specify \\ CK1 \Profiles\%username% as the profile path.

B. Select all user accounts in the Sales OU.

Modify the account properties to specify \\ CK1 \Profiles as the profile path.

C. Create a Group Policy object (GPO) and link it to the Sales OU.

In the User Configuration section of the GPO, configure Folder Redirection to use \\ CK1 \Profiles.

D. Create a Group Policy object (GPO) and link to the Domain Controllers OU.

In the User Configuration section of the GPO, configure Folder Redirection to use \\ CK1 \Profiles.

Answer: A

Explanation: The users will log on the client computers and will be authenticated on domain controllers. The roaming profiles are stored on a member server, so we must enter the UNC path to the shared profiles folder in the profile path. In this case, the UNC path is \\ CK1 \Profiles. To create profiles based on the user names, we can use the %username% variable. The %username% variable will be changed the users log in name when the user logs in. For example, if a user named Jack logs in, \\ CK1 \Profiles\%username% will become \\ CK1 \Profiles\Tess.

Incorrect answers:

B: The account properties should specify the profile path by making use of the %username% variable if you want to create roaming user profiles for the user accounts in the Sales OU.

C: Linking a GPO to the Sales OU as described in this case will not work, you should still make use of the %username% variable to create roaming user profiles for the accounts in the Sales OU.

D: Whether you create a GPO to be linked to the Domain Controllers OU, the folder Redirection should be more specific and point to the %username% variable as well.

Reference:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 285

---

### **QUESTION 40**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. All network servers run Windows Server 2003.

User profiles are stored in a folder named Certkiller Profiles, which is located on a member server named Certkiller 12. Certkiller Profiles is shared as Profiles.

A change in business rules requires you to create a template account for users in the engineering department. All user accounts that are created from the template will use roaming profiles. Each profile name will be based on user name. All profiles must be stored in a central location.

You create the template and name it T-Engineer.

Now you need to add information about profile location to T-Engineer.

What should you do?

To answer, drag the appropriate path or paths to the correct location or locations in the dialog box.

**Paths**  
Select from these

\\Certkiller12\profiles\%username%

C:\profileshome\%username%

\\Certkiller12\profiles\T-Engineer

C:\profileshome\T-Engineer

**Place here**



Answer:

**Paths**  
Select from these

\\Certkiller12\profiles\%username%

C:\profileshome\%username%

\\Certkiller12\profiles\T-Engineer

C:\profileshome\T-Engineer

**Place here**



Explanation:

The users will log on the client computers and will be authenticated on domain controllers. The roaming profiles are stored on a member server, so we must enter the UNC path to the shared profiles folder in the profile path. In this case, the UNC path is \\ Certkiller 12\profiles. To create profiles based on the user names, we can use the %username% variable. The %username% variable will be changed the users log in name when the user logs in. For example, if a user named Jack logs in, \\ Certkiller 12\profiles\%username% will become \\ Certkiller 12\profiles\Tess.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 285

### QUESTION 41

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows 2000 Professional.

You need to standardize the desktop environment for all client computers. Your solution must prevent domain users from permanently modifying their regional settings or the desktop background.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Specify the profile's network path in the user properties in Active Directory Users and Computers.
- B. Specify the profile's local path in the user properties in Computer Management,
- C. Specify the profile's network path in the user properties in Computer Management.
- D. In the network share where profiles reside, rename Ntuser.dat to Ntuser.man.
- E. In the local profile directory, rename Ntuser.dat to Ntuser.man.
- F. In the network share where profiles reside, rename the Ntuser.ini to Ntuser.man.

Answer: A, D

Explanation: Your solution must prevent domain users from permanently modifying their regional settings or the desktop background. The trick here is the word permanently; the user with a mandatory profile can modify his profile, but the mandatory profile will change the settings again next time the user logs on.

A mandatory user profile is a user profile that is not updated when the user logs off.

It is downloaded to the user's desktop each time the user logs on, and it is created by an administrator and assigned to one or more users to create consistent or job-specific user profiles. Only members of the Administrators group can change settings in a preconfigured user profile. The user can still modify the desktop, but the changes are not saved when the user logs off. The next time the user logs on, the mandatory user profile is downloaded again.

User profiles become mandatory when you rename the NTuser.dat file on the server to NTuser.man.

By renaming this file, you have effectively made the user profile read-only, meaning that the operating system does not save any changes made to the profile when the user logs off. Microsoft recommends this method for creating mandatory user profiles.

Incorrect answers:

B: The profile's network path and not the local path should be specified.

C: The profile's network path is specified in the user properties in Active Directory Users and Computers and not in the user properties in Computer Management.

E: Renaming the Ntuser.dat to Ntuser.man in the local profile directory thus making it a mandatory user profile will only be applicable to the local profile directory and not to the network share. If the server where user profiles are stored is not available when a user logs on, the operating system defaults to using an existing local profile for the user. If the user has no local profile on that computer, it creates a local profile for the user from the local default profile. If you want to strictly enforce a policy that states that no user can log on without a roaming profile, you can append the extension of .man to the roaming user profile folder's name.

F: This will not work even if you have the correct location in the network share where the profiles reside.

Reference:

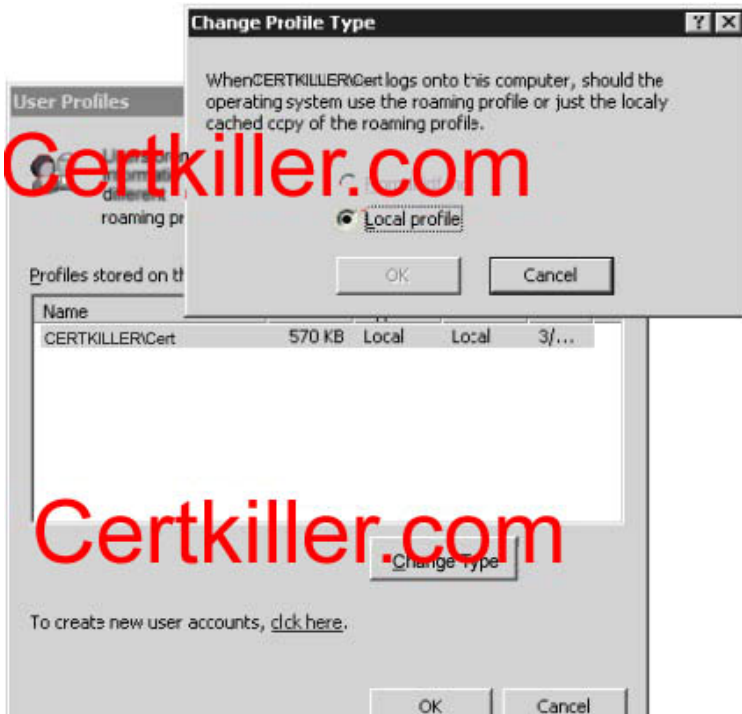
HOW TO: Create a Roaming User Profile in Windows Server 2003 KB article 324749

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4

---

**QUESTION 42**

Exhibit



You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. All users log on to the company's domain.

A user named Jack King logs on to multiple computers on the network. Jack reports that her desktop settings are not retained when she switches between computers. You decide to configure a roaming profile for Tess. From Jack's primary desktop computer, you attempt to copy this profile to the network by using Jack's credentials. You receive the dialog box shown in the exhibit.

You need to copy Jack's profile to the network.

What should you do?

- A. Log on to Jack's computer by using a local Administrator account.
- B. Add Jack's account to the local Administrators group.
- C. Add the Administrator security group to roaming user profiles policy setting to the Default Domain Policy GPO.
- D. Remove the Prevent Roaming Profile changes from propagating to the server policy setting from the Default Domain Policy GPO.

Answer: A

Explanation: A roaming user profile is a server-based user profile that is downloaded to the local computer when a user logs on and is updated both locally and on the server when the user logs off. But in this case you need to log on to Jack computer by using the local Administrator account in order to copy Jack profile to the network using her credentials.

Incorrect answers:

B: Just adding Jack account to the local Administrators group will not enable you to copy her profile to the network.

C: It is just a matter of changing profile type and not changing settings to the GPO as only Jack account is problematic.



D: This is not the solution.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment: Study Guide & DVD Training System, Syngress Publishing, Rockland, 2003, Chapter 3, p. 210

---

**QUESTION 43**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com All network servers run Windows Server 2003. All client computers run Windows XP Professional. Multiple users share the same client computer.

A server named Certkiller 2 functions as a file and print server. You set the profile path for all user accounts to \\ Certkiller 2\Profiles\username. Some domain users were added to the local Administrators group on the Windows XP Professional computers.

A user reports that other users can log on to client computers that he has previously used and gain access to files stored in his My Documents folder on the local hard disk.

You need to permanently prevent users from being able to access the My Documents folder of other domain users on the client computers.

What should you do?

- A. In Active Directory, modify the Default Domain Policy. Disable the Do not check for user ownership of Roaming Profile Folders setting.
- B. In Active Directory, modify the Default Domain Policy. Enable the Delete cached copies of roaming profiles setting.
- C. Log on to all client computers and delete all user profiles from the local hard disks.
- D. Log on to all client computers and configure the Number of previous logons to cache setting to 0.

Answer: B

Explanation: When users on your network regularly move from one profile-creating workstation to another, every machine they use will store a copy of their local profile. You may use System Policy Editor or Group Policies to compel the workstations to delete cached copies of roaming profiles when the user logs out. This is a machine-specific setting that is implemented in the Registry in HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON. What this setting also does is to prevent users from being able to access the My Documents folder of other domain users on the client computers as is the case in this question.

Incorrect answers:

A: Disabling the Do not check for user ownership of Roaming Profile Folders will not prevent users from being able to access folders of other domain users on the client computers.

C: Deleting all user profiles from the local hard disks is not the solution.

D: Configuring the number of previous logons to cache setting to 0 is not the solution.

Reference:

Mark Minasi, Christa Anderson, Michele Beveridge, C.

A. Callahan & Lisa Justice, Mastering(tm)Windows(r) Server 2003, Sybex Inc., Alameda, 2003, p.815

---

**QUESTION 44**

You are the network administrator for Certkiller . All network servers run Windows Server 2003. A server named Certkiller 6 functions as a file server. All client computers run Windows XP Professional and are members of the domain.

Certkiller .com periodically hires temporary employees. You need to prepare a custom user profile for all temporary employees.

You log on to a client computer as an administrator, and you configure the desktop settings. You copy the profile to a folder named \\ Certkiller 6\Profiles\Temp\_profile. You rename the Ntuser.dat file in the \\ Certkiller 6\Profiles\Temp\_profile folder to Ntuser.man. You create three new user accounts for the temporary employees. The user accounts are named temp\_user1, temp\_user2, and temp\_user3.

You need to configure the temporary user accounts to receive the new desktop settings that you created on Certkiller 6. The temporary employees must not be allowed to retain customized desktop settings?

What should you do?

- A. Specify a user profile path of \\ Certkiller 6\Profiles\username for each of the three user accounts.
- B. Specify a user profile path of \\ Certkiller 6\Profiles\username.man for each of the three user accounts.
- C. Specify a home folder path of \\ Certkiller 6\Profiles\username for each of the three user accounts.
- D. Specify a user profile path of \\ Certkiller 6\Profiles\Temp\_profile for each of the three user accounts.
- E. Specify a user profile path of \\ Certkiller 6\Profiles\Temp\_profile.man for each of the three user accounts.

Answer: D

Explanation: Force the user to load a particular profile - If you specify the directory path on the domain controller or server as DIRECTORYNAME.MAN but you do not rename the hive file to NTUSER.MAN, the operating system will not see it as a mandatory profile. If the hive file is not named NTUSER.MAN, the workstation will classify it merely as a roaming profile. In this scenario, users can make changes to their Desktops. At logon, however, the user will not be able to log in if the profile directory does not exist in the specified path.

Renaming the NTUSER.DAT file to NTUSER.MAN so that the user cannot save changes to the profile has been done in this case. What is necessary further is to specify an appropriate user profile path to the \\ Certkiller 6\Profiles\Temp\_profile folder for each of the three user accounts, and then you will prevent temporary employees from retaining customised desktop settings.

Incorrect answers:

A: This will not work.

B: This is inappropriate in this scenario.

C: You should not be specifying a home folder path, but rather a user profile path to the appropriate folder.

E: This is not the solution.

Reference:

Mark Minasi, Christa Anderson, Michele Beveridge, C.

A. Callahan & Lisa Justice, Mastering(tm)Windows(r) Server 2003, Sybex Inc., Alameda, 2003, pp. 816-817

---

**QUESTION 45**

You are the network administrator for Certkiller .com. The network consists of a single Active

Directory domain named Certkiller .com.

The sales department is hiring employees. An OU named Certkiller Sales is created to hold objects for the new sales department users. Each sales department user has a portable computer. Each portable computer runs Windows XP Professional. The sales department users are responsible for joining their portable computers to the domain.

You need to ensure that the computer accounts for the Sales department user's portable computers are created in the Certkiller Sales OU. You need to achieve this goal without granting any unnecessary permissions.

What should you do?

- A. Assign the sales department users the Allow - Read permissions for the Computer container.
- B. Configure the sales department users' user accounts to be trusted for delegation.
- C. Prestage the computer accounts in the Certkiller Sales OU for the sales department users' portable computers.
- D. Assign the sales department users the Allow - Create all Child Objects permission for the Certkiller Sales OU.

Answer: C

Explanation: Pre-staging prevents RIS from deploying an operating system to unknown client computers. And with pre-staging you can add the user accounts with the appropriate permissions in the OU. This option is best suited in this scenario.

Incorrect options:

A: Assigning the Allow - Read permission for the Computer Container to the Sales department users will not work.

B: The Account Is Trusted For Delegation option enables a service account to impersonate a user to access network resources on behalf of a user. This is not recommended in this scenario.

D: Assigning the Allow - Create all child objects permission for the Certkiller Sales OU will be granting unnecessary permissions.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, 3: 9

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4

---

### **QUESTION** 46

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.

You install a new server named Server22 with default settings. During installation, you set the IP configuration shown in the exhibit.

```

c:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : server22
Primary Dns Suffix . . . . . :
Mode Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : AMD PCNET Family PCI Ethernet Adapter
Physical Address. . . . . : 00-50-56-59-01-F8
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.10.100.71
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.10.10.3
DNS Servers . . . . . : 10.10.100.71

```

You make Server22 a member of a workgroup. Then you restart Server22 and use the local Administrator account to log on locally. You join Server22 to the domain. You restart Server22 and use the Domain Administrator account to log on. However, you are unsuccessful. You need to ensure that Server22 is a member of the domain. What should you do?

- A. Open the Active Directory Users and Computers and reset Server22.
- B. From a command prompt on another member server or domain controller, type: `dsmod computer Server22. Certkiller .com-reset`
- C. Log on locally. In the TCP/Ip properties, change the DNS server of Server22.
- D. Log on locally. In the TCP/IP properties, change the subnet mask of Server22.
- E. From a command prompt on another member server or domain controller, type: `nltest /server:Server22. Certkiller .com /trusted_domains`

Answer: E

Explanation: The command "`nltest /server:Server22. Certkiller .com /trusted_domains`" will display a list of domains trusted by the server Server22. Certkiller .com. A trusted domain means the domain that the computer is a member of or other domains trusted by the computer's domain.

Incorrect Answers:

- A: The client workstation hasn't been offline. Therefore, it is unlikely that the account needs resetting.
- B: This command also resets the account.
- C: The questions states, "You join Server22 to the domain". You would have got an error if you had a DNS problem.
- D: The questions states, "You join Server22 to the domain". You would have got an error if you had an IP configuration problem.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 284

---

**QUESTION 47**

You are the network administrator for Certkiller .com. The network contains two Windows Server 2003 computers named Certkiller 7 and Certkiller 8.

You install a new modem on Certkiller 7 to allow an application to dial out to your pager. You install the driver. When you test the modem, it does not dial out successfully. You install an identical hardware and driver configuration on Certkiller 2, and the modem dials out successfully.

You need to find out if the modem card in Certkiller 7 is defective.

What should you do on Certkiller 7?

- A. In Device Manager, right-click the modem, and then click Scan for hardware changes.
- B. In Modem Properties, click the Modem tab, and then set the maximum port speed to the same value as the value for the maximum port speed on Certkiller 8.
- C. In Modem Properties, click the Diagnostics tab, and then click the Query Modem button.
- D. In Device Manager, right-click Ports, and then click Scan for hardware changes.

Answer: C

Explanation: You can manage the modem properties by clicking on and selecting the modem you want to manage on the Modems tab, then clicking the Properties button. This brings up the Modem Properties dialog box, which allows you to configure general properties and modem properties, run diagnostics, set advanced parameters, view and manage the driver, and view the resources the modem is using. Using the Query Modem button will enable you to verify whether the modem card in Certkiller 7 is defective or not.

Incorrect answers:

A: This will not aid you in checking whether the modem card is defective or not.

B: The Modem tab and the setting of the maximum port speed are not causing the problem since an identical situation on Certkiller 2 has the modem dialling out successfully.

D: This is not the place to check whether the modem card is defective or not.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 124

---

**QUESTION 48**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.

You place computer accounts for servers in OUs that are organized by server roles. You apply GPOs to these servers at the OU level.

You need to add a new server to the domain. You need to ensure that the appropriate GPOs are applied to this server.

What should you do?

- A. Prestage a domain computer account for the new server in the appropriate OU. Join the server to the domain by using the prestaged computer account.
- B. On the server, add the domain name for the Active Directory domain to the DNS suffix setting. Join

the server to the domain.

C. Assign a user account the Allow - Create permission for the appropriate OU. Join the new server to the domain by using the user account.

D. Join the new server to the Active Directory domain. On the new server, run the `gpupdate /force` command.

Answer: A

Explanation: With pre-staging you can add the user accounts with the appropriate permissions in the OU. This option is best suited in this scenario since GPOs are applied at OU level.

Incorrect answers:

B: Joining the server to the domain will not ensure that the GPO will be applied to the server.

C: Assigning the Allow-Create permission albeit to the appropriate OU and joining the new server to the domain will not ensure that the appropriate GPOs are applied to the server.

D: This option is not suitable since GPOs are applied at OU level.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, 3: 9

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4

---

## QUESTION 49

Exhibit



You are the network administrator for Certkiller .com. The network consists of a single Active

Directory forest that contains two domain. The functional level of the forest is Windows 2000. The functional level for both domains is Windows 2000 native. All servers run Windows 2003.

You create a group named Certkiller Staff. The Certkiller Staff group includes users from both domains. The group properties are shown in the exhibit.

You need to use the Certkiller Staff group to assign permissions to resources in both domains. However, when you attempt to assign permissions to a shared folder by using the Certkiller Staff group, you receive an error message that states than an object named " Certkiller data" cannot be found.

You need to ensure that the Certkiller Staff group can be used to assign permissions to shared resources in both domains.

What should you do?

- A. Upgrade the forest functional level to Windows Server 2003.
- B. Upgrade the domain functional level for both domains to Windows Server 2003.
- C. Modify the group properties to make the group a global distribution group.
- D. Modify the group properties to make the group a universal security group.
- E. Modify the group properties to make the group a domain local security group.

Answer: D

Explanation: Use security groups for the distribution of e-mail as described for distribution groups, but also use them to assign permissions to Windows resources. You can also use security groups to assign user rights to group members. User rights include actions such as Backup files and directories or Restore files and directories, both of which are assigned to the Backup Operators group by default. You can delegate rights to groups to enable the members of the group to perform a specific administrative function that is not normally allowed by their standard user rights. You can also assign permissions to security groups to enable them to access network resources, such as printers and file shares.

Universal groups can include other groups and user/computer accounts from any domain in the domain tree or forest. Permissions for any domain in the domain tree or forest can be assigned to universal groups. Universal groups are only available if your domain functional level is set to Windows 2000 native mode.

Incorrect answers:

A, B: Upgrading the forest functional level or even the domain functional level for both domains to Windows Server 2003 will not work because once you have raised the domain functional level, domain controllers running earlier operating systems cannot be used in that domain. As an example, should you decide to raise domain functional level to Windows Server 2003, Windows 2000 Server domain controllers cannot be added to that domain.

C: Distribution groups are used for distributing messages to group members. And global groups can include other groups and user/computer accounts from only the domain in which the group is defined.

Modifying the group to be a global distribution group will not work

E: Making the group a domain local security group will not ensure permissions to shared resources on both domains.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 319-320

---

**QUESTION 50**

Your network consists of a single Active Directory forest containing two domains. hq. Certkiller .com and manu. Certkiller .com. The functional level of both domains is Windows 2000 mixed.

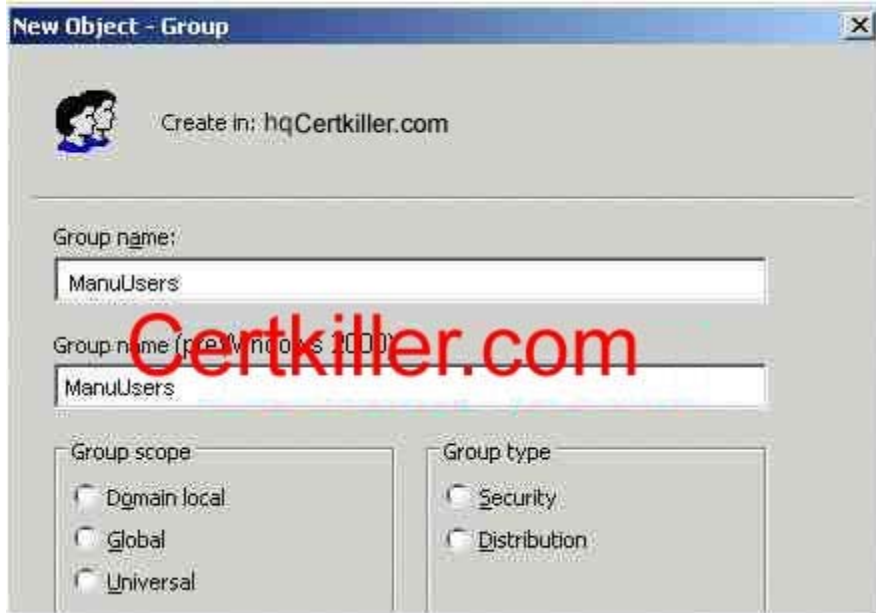
hq. Certkiller .com contains two domain controllers running Windows Server 2003 and three domain controllers running Windows 2000 Server.

You are the network administrator for hq. Certkiller .com. The domain controllers in your domain host applications and shared folder to which users in manu. Certkiller .com require access.

You need to create a group that will grant the required access to users in manu. Certkiller .com.

What should you do?

To answer, configure the appropriate options in the dialog box.



Answer: Domain local - Security.

Explanation: Distribution groups can be used only with e-mail applications (such as Exchange) to send email to collections of users. Distribution groups are not security-enabled, which means that they cannot be listed in discretionary access control lists (DACLS) discretionary access control lists (DACLS) The part of an object's security descriptor that grants or denies specific users and groups permission to access the object. Only the owner of an object can change permissions granted or denied in a DACL; thus, access to the object is at the owner's discretion. If you need a group for controlling access to shared resources, create a security group.

Security groups are used with care; security groups provide an efficient way to assign access to resources on your network. Using security groups, you can:

- Assign user rights to security groups in Active Directory.
- Assign permissions to security groups on resources.

A group can be converted from a security group to a distribution group, and vice versa, at any time, but only if the domain functional level is set to Windows 2000 native or higher. No groups can be converted while the domain functional level is set to Windows 2000 mixed.

Domain local groups can contain other domain local groups in the same domain, global groups from any domain, universal groups from any domain, user accounts from any domain, and computer accounts from any domain.



Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 320, 329

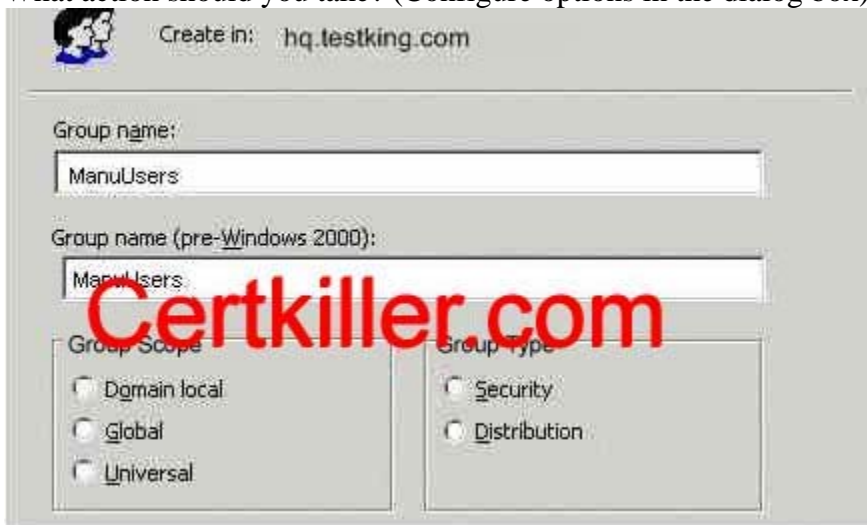
---

**QUESTION 51**

You are an employee at Certkiller . The network consists of a single Active Directory forest containing two domains helsinki. Certkiller .com and mumbai. Certkiller .com. The functional level of both domains is Windows 2000 mixed. helsinki. Certkiller contains two domain controllers running Windows Server 2003 and three domain controllers Windows 2000 Server.

You are the network administrator for helsinki. Certkiller .com. Users in your domain require access to applications and shared folders that reside on member servers in mumbai. Certkiller .com.

What action should you take? (Configure options in the dialog box)



Answer: Select "Global" and "Security".

Explanation: Global groups can include other groups and user/computer accounts from only the domain in which the group is defined. Permissions for any domain in the forest can be assigned to global groups. The group's Security tab is used to add and remove permissions to this group for other accounts (users and groups). Use the Add button to add the accounts, and then use the check boxes at the bottom to select the permissions for the newly added accounts. Read is the default permission assigned when you add an account to the security tab of a group. The Advanced button enables you to manage permissions to the group on a more granular level. This is also where you manage auditing, ownership, as well as view effective permissions.

Using security groups, you can:

- Assign user rights to security groups in Active Directory.
- Assign permissions to security groups on resources.

A group can be converted from a security group to a distribution group, and vice versa, at any time, but only if the domain functional level is set to Windows 2000 native or higher. No groups can be converted while the domain functional level is set to Windows 2000 mixed.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, MCSA/MCSE:

**QUESTION 52**

Your company network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows 2000 Native. The network contains 20 member servers running Windows 2000 and 5 domain controllers running Windows Server 2003.

The user accounts for employees in the Finance department are members of a global distribution group named Finance\_Users. You create a shared folder named Finance\_Docs on a Windows 2000 member server.

You need to enable the Finance users to access the Finance\_Docs folder.

What should you do?

- A. Change Finance\_Users to a security group.
- B. Change the scope of Finance\_Users to Universal.
- C. Change the scope of Finance\_Users to Domain Local.
- D. Raise the domain functional level to Windows Server 2003.

Answer: A.

Explanation: Groups are special objects that contain users, and security groups are used to simplify management of multiple user accounts by enabling you to apply permissions, user rights, and so forth to an entire group of users in a single operation instead of having to apply them to individual user accounts. You cannot assign permissions to file shares to a distribution group. The group must be converted to a security group. Note: you must be in at least Windows 2000 Native Functional Level in order to be able to convert a distribution group to a security group.

Incorrect Answers:

B: You cannot assign permissions to file shares to a universal distribution group.

C: You cannot assign permissions to file shares to a distribution group, regardless of what functional level the forest is in. Finance\_Users is a distribution group.

D: You cannot assign permissions to file shares to a distribution group, whatever functional level the domain is in. Finance\_Users is a distribution group.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 256

---

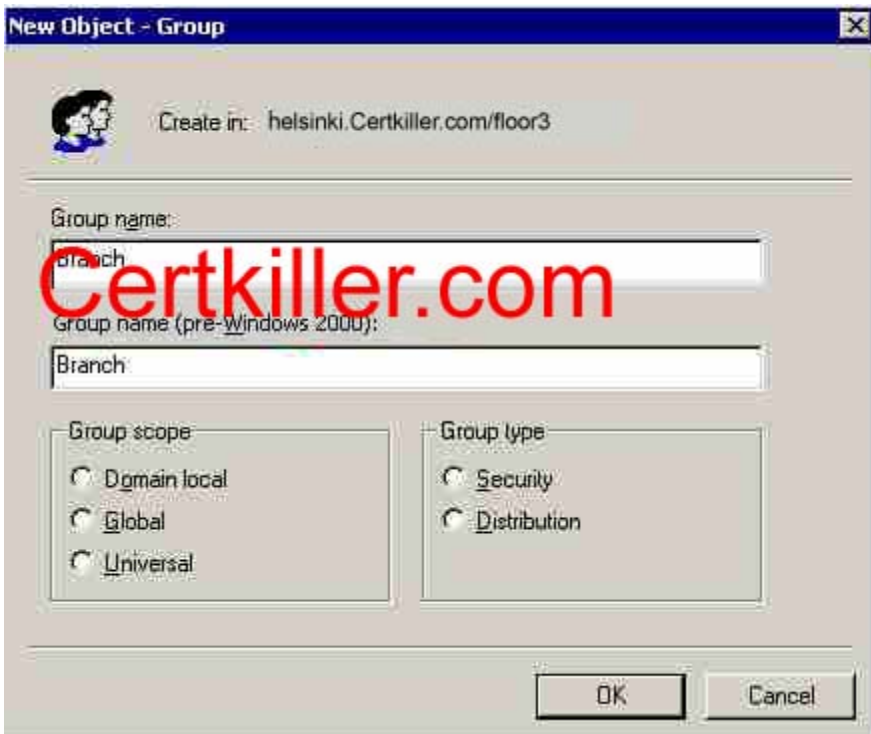
**QUESTION 53**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest containing two domains, hq.hmopslab.com and mm. hmopslab.com. The functional level of both domains is Windows 2000 mixed. hq.hmopslab.com contains 2 domain controllers running Windows Server 2003 and 3 domain controllers running Windows 2000 server.

You are the network admin for hq.hmopslab.com. Users in your domain require access to applications and shared folders that reside on member servers in mm.hmopslab.com.

You need to create a group in hq.hmopslab.com that will provide the required access.

What should you do?



Answer: Global, Security.

Explanation: We should use Global Security groups because the users in the domain require access to the applications and shared folders that are on the member servers. Global groups can include other groups and user/computer accounts from only the domain in which the group is defined. Permissions for any domain in the forest can be assigned to global groups.

The group's Security tab is used to add and remove permissions to this group for other accounts (users and groups). Use the Add button to add the accounts, and then use the check boxes at the bottom to select the permissions for the newly added accounts. Read is the default permission assigned when you add an account to the security tab of a group. The Advanced button enables you to manage permissions to the group on a more granular level. This is also where you manage auditing, ownership, as well as view effective permissions.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 320, 329

#### **QUESTION 54**

You are a network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com.

A user named Mrs. King works in the information technology (IT) security department. Mrs. King is a member of the ITSecurity global group. Mrs. King reports that no one in the ITSecurity global group can access the security log from the console of a computer named Certkiller 1.

You need to grant the ITSecurity global group the minimum rights necessary to view the security log on Certkiller 1.

How should you modify the local security policy?

- A. Assign the Generate security audits user right to the ITSecurity global group.
- B. Assign the Manage auditing and security logs user right to the ITSecurity global group.
- C. Assign the Allow logon through Terminal Services user right to the ITSecurity global group.
- D. Assign the Act as part of the operating system user right to the ITSecurity global group.

Answer: B

Explanation: Security events are logged in the security log, accessible by administrators via the Event Viewer. An audit entry can be either a Success or a Failure event in the security log. A list of audit entries that describes the life span of an object, file, or folder is referred to as an audit trail. Security auditing enables you to track access to and modifications of objects, files, or folders, and to determine who has logged on (or attempted to do so) and when. The right to manage the security event log is a powerful user privilege that should be closely guarded. Anyone with this user right can clear the security log, possibly erasing important evidence of unauthorized activity. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to enforce the default Administrators in the High Security environment.

Incorrect answers:

A: Being able to generate security audits does not mean that that specific group can view the security logs. Security logs can only be viewed with administrator rights via the Event Viewer.

C: Having the Allow logon through Terminal Services user right will not grant the ability to view security logs.

D: The Act as part of the operating system user right will not do, you need to be an administrator.

References:

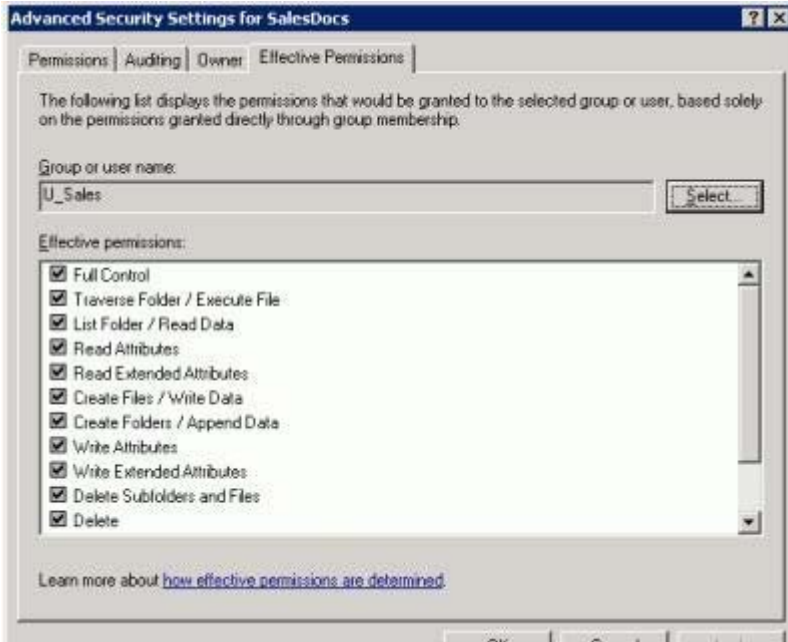
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 749.

---

### **QUESTION 55**

You are the network administrator for Certkiller . The network consists of several domains in a single Active Directory forest Certkiller .com. The functional level for all child domains is Windows 2000 mixed.

A server named Certkiller A.litwareinc.com runs Windows Server 2003. You share a folder named SalesDocs on this server. In the properties for SalesDocs, you assign the Allow - Full Control permissions to a universal group named U\_Sales in Certkiller .com. Effective permissions for U\_Sales are shown in the U\_Sales exhibit.



In each domain in the forest, you create a global group named G\_Sales, whose membership consists of users in that domain's department. You add every G\_Sales group to the U\_Sales group. Ben Smith is a member of G\_Sales in child1. Certkiller .com. He reports that he cannot access SalesDocs. On Certkiller A, you verify the effective permissions for Ben Smith, as shown in the Ben Smith exhibit.



You need to ensure that Ben Smith can access SalesDocs. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

- A. Add Ben Smith's user account to U\_Sales in litwareinc.com
- B. Change the group scope of U\_Sales to domain local.
- C. Change the group type of U\_Sales to distribution.
- D. Assign the Allow - Full Control permissions to G\_Sales in child1.litwareinc.com.

E. Instruct Ben Smith to log on by using his user principal name.

Answer: B, D

Explanation: Ben Smith is unable to access SalesDocs because the child domains are in mixed mode thus cannot use the Universal group.

Only Certkiller .com is in native mode because Universal group U\_sales was created there.

We need to change the scope For U\_Sales Universal to domain local. This will give Ben the required permissions because the Global Group G\_Sales is a member of U\_Sales.

Alternatively, we could assign the permission directly to the G\_Sales group in child1. Certkiller .com.

Incorrect answers:

A: U\_Sales was created in Certkiller .com, but adding Ben Smith's account to U\_Sales will not work as U\_Sales' group scope will have to be changed from global to domain local.

C: Windows Server 2003 has two group types: security and distribution. Security groups are used to assign permissions for access to network resources. Distribution groups are used to combine users for e-mail distribution lists. Security groups can be used as a distribution group, but distribution groups cannot be used as security groups.

E: Logging on by making use of a UPN is irrelevant in this scenario as one needs to change the groups scopes first and then assign the appropriate permissions that will allow Ben Smith access to SalesDocs.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4

---

### **QUESTION 56**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. The functional level of the domain is Windows 2000 native. Some network servers run Windows 2000 Server, and others run Windows Server 2003.

All users in your accounting department are members of an existing global distribution group named Global-1. You create a new network share for the accounting users.

You need to enable the members of Global-1 to access the file share.

What should you do?

A. Raise the functional level of the domain to Windows Server 2003.

B. Change the group type of Global-1 to security.

C. Change the group scope of Global-1 to universal.

D. Raise the functional level of the forest to Windows Server 2003.

Answer: B.

Explanation: You cannot assign permissions to file shares to a distribution group. The group has to be converted to a security group. Note: you must be in at least Windows 2000 Native Functional Level in order to be able to convert a distribution group to a security group.

Incorrect Answers:

A: You will not be able to assign permissions to file shares to a distribution group, whatever functional level the domain is in.

C: You will not be able to assign permissions to file shares to a universal distribution group.

D: You will not be able to assign permissions to file shares to a distribution group, whatever functional level the forest is in.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 321-323

---

**QUESTION 57**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain in its own forest. All network servers run Windows Server 2003.

Certkiller .com merges with Foo.com, which also has a single Active Directory domain in its own forest. A cross-forest trust from Certkiller .com to Foo.com is created.

You need to ensure that all users have access to personal payroll tools located in the Certkiller .com domain. The built-in users group for Certkiller .com has the appropriate permissions on the payroll tools.

What should you do?

A. Create a new universal group in the Foo.com domain. Add all Foo.com users to the group. Place the new group in the built-in Users group for Foo.com.

B. Create a new universal group in the Certkiller .com domain. Add all Certkiller .com users to the group. Place the new group in the built-in Users group for Certkiller .com.

C. Create a new universal group in the Foo.com domain. Add all Foo.com users to the group. Place the new group in the built-in Users group for Certkiller .com.

D. Create a new universal group in the Certkiller .com domain. Add all Certkiller .com users to the group. Place the new group in the built-in Users group for Foo.com.

Answer: C

Explanation: Universal groups are used to logically organize global groups and appear in the Global Catalog. Universal groups can contain users from anywhere in the domain tree or forest, other universal groups, and global groups. For all users to have access to the personal payroll tools in the Certkiller .com domain you need to create a new universal group for the Foo.com domain and then place it in the built-in users group for Certkiller .com since the Certkiller .com domain contains the tools.

Incorrect answers:

A: This option is suggesting the wrong group of users to be added to the new universal group and the wrong built-in Users group to add it to.

B: The Certkiller .com domain does not need to be given access to the personal payroll tools.

D: You should add the Foo.com users to the group and not the Certkiller .com users. Furthermore, you should place the new group in the built-in users for Certkiller .com and not Foo.com

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 167

---

**QUESTION 58**

Exhibit



You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. Files and folders for the network users are stored on a member server named Certkiller 8. Folders are shared on the network by assigning the Allow - Full Control permission to the Authenticated Users group.

A folder named Budget contains financial information. Permissions for Budget are shown in the exhibit.

A new employee named Jack King is hired to manage Certkiller 's financial information. You create a user account for her. However, Jack reports that she cannot create new files in Budget.

You need to ensure that Jack can perform these actions.

To which group should you add her user account?

- A. Group1
- B. Group2
- C. Group3
- D. Administrators
- E. Users

Answer: B

Explanation: The group2 account has the Allow - Modify permission applied to the budget folder only. The Allow - Modify permission involves: View and list folders and files; view the contents of files; write data to files; add folders and files; delete folders, files, and file contents; view and set attributes and extended attributes. This should enable Jack to perform her duties since the Budget folder contains the financial information.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 5



**QUESTION 59**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.

An administrator named Jack King attempts to perform troubleshooting tasks on a file server. However, when she attempts to open the security event log, she receives the error message shown in the exhibit.



You need to ensure that Jack can complete her troubleshooting tasks. What should you do?

- A. Add Jack's user account to the Server Operators domain group.
- B. Add Jack's user account to the local Administrators group on the file server.
- C. Configure Jack's client computer to enable the IPSec Server (Request Security) policy.
- D. Assign Jack's user account the Allow logon through Terminal Services user right for the file server.

Answer: B

Explanation: You can configure the security logs to record information about Active Directory and server events. These events are recorded in the Windows security log. The security log can record security events, such as valid and invalid logon attempts, as well as events that are related to resource use, such as creating, opening, or deleting files. You must log on as an administrator to control what events are audited and displayed in the security log.

Security log files are also stored in the systemroot/system32/config directory.

Security logs can be exported and archived in the following file formats:

- Event log files (.evt) (Default).
- Comma delimited (.csv).
- Text file (.txt).

Tess needs to troubleshoot tasks on the file server; therefore we need to add her to the local administrators group. Making Jack part of the Administrator's group will allow her access to the security log which will enable her to perform troubleshooting.

Incorrect answers:

A: To be able to access the security log one has to be part of the administrator's group on that specific server, thus making Jack part of the Server Operators will not grant her enough permissions to view the security log.

C: Enabling the IPsec Server (Request Security) policy permission for Jack's client computer will not suffice in allowing her to view the security log. She still needs to be an administrator on the server.

D: The Allow logon through Terminal Services user right for the file server will not grant the same rights as an administrator account. Thus this option will not grant Jack the ability to view the security log.

References:

Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 230-233

---

### **QUESTION 60**

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All domain controllers run Windows Server 2003.

The sales department recently hired 10 new employees. User accounts for these employees were created in Active Directory. The manager of the sales department sent you a list of a new users and asked you to add the user accounts to an existing global group named SalesDept.

You need to add the users to the SalesDept global group.

What are two possible ways to achieve this goal? Each correct answer presents a complete solution. Choose two.

- A. Use the dsadd user command to add the user accounts to the SalesDept global group.
- B. Use the dsadd group command to add the user accounts to the SalesDept global group.
- C. In Active Directory Users and Computers, select all 10 user accounts. Right-click the selected users, and then select the Properties menu command.
- D. In Active Directory Users and Computers, select all 10 user accounts. Right-click the selected users, and then select the Add to a Group menu command.

Answer: B, D

Explanation: You can automate the process of creating users, groups, and computers through the Dsadd command-line utility. Each Dsadd command offers a series of switches (which can be viewed from a command prompt window by typing Dsadd /?) that can be used to configure the object that is being created. Active Directory Users and Computers on Windows Server 2003 domain controllers, is the main tool used for managing the Active Directory users, groups, and computers. To set up and manage domain user accounts, you use the Active Directory Users And Computers utility. The Add to a Group menu command will enable you to add the users to the SalesDept global group.

Incorrect answers:

A: The Dsadd user command includes parameters for almost all of the options that can be configured for a user through the Active Directory Users And Computers utility. This is not the appropriate parameter in this case.

C: The properties menu command would be the inappropriate choice in this matter.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r)Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, p. 227

---

**QUESTION 61**

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All domain controller run Windows Server 2003.

Certkiller .com employs three database administrators who administer seven database servers that run Windows Server 2003. The database administrators occasionally restore a database server after a disaster. To restore a server, database administrators need the rights required to perform the following tasks:

- Back up files and folders
- Restore files and folders.
- Restore the System State data.

You need to assign the database administrators the rights that they require to perform the specified tasks. For security reasons, you must not assign the administrators more rights than they require to perform the tasks.

What should you do?

- A. Add the database administrators' user accounts to the Administrators group on each of the database servers.
- B. Add the database administrators' user accounts to the Power Users group on each of the database servers.
- C. Add the database administrators' user accounts to the Backup Operators group on each of the database servers.
- D. Add the database administrators' user accounts to the Backup Operators group on one of the domain controllers.
- E. Add the database administrators' user accounts to the Server Operators group on one of the domain controllers.

Answer: C

**Explanation:** The members of the Backup Operators group have rights to back up and restore the file system, even if the file system is NTFS and they have not been assigned permissions to the file system. However, the members of Backup Operators can access the file system only through the Backup utility. To be able to directly access the file system, they must have explicit permissions assigned. Thus by adding the database administrator's user accounts to this group on each of the database servers, you will be granting them the appropriate rights to perform their tasks.

**Incorrect answers:**

A: The Administrators group has full rights and privileges on all domain controllers within the domain. Its members can grant themselves any permissions they do not have by default to manage all of the objects on the computer. (Objects include the file system, printers, and account management.) By default, the Administrator user account and the Domain Admins and Enterprise Admins groups are members of the Administrators group. Because of the permissions associated with this group, you should add users to this group with caution. This should work, but it would be granting the database administrators too much

permissions.

B: This option would also give them too much permissions.

D: This is the correct group to make them members of, but it should be done on all the database servers.

E: The Server Operators group members can administer domain servers. Administration tasks include creating, managing, and deleting shared resources, starting and stopping services, formatting hard disks, backing up and restoring the file system, and shutting down domain controllers. The Server Operators Group would be the wrong choice to add the database administrators to.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, pp. 168-173

---

### **QUESTION 62**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.

You create an organizational unit (OU) named Engineering, which will hold all objects associated with the users and computers in the engineering department. You also create a global group named Engineering Admins, whose members will administer these objects.

Now you need to assign the appropriate permissions to the Engineering Admins group so its members can administer the objects in the Engineering OU.

First, you use Active Directory Users and Computers to view the properties of the Engineering OU. However, the Security tab is not available.

What should you do next?

A. Convert the system partition to NTFS.

B. Enable the Advanced Features option in the View menu of Active Directory Users and Computers.

C. Enable the Users, Groups, and Computers as Containers option in the View menu of Active Directory Users and Computers.

D. Log on by using a user account that has Administrator permissions for the Engineering OU.

Answers: B

Explanation: The Security tab is available for modification in the Advanced Features option of the View menu. If you select that entry and click View/Edit, you will see the specific permissions assigned to. By default we cannot see the security tab. Therefore we must enable the advanced features option in the View menu of Active Directory Users and Computers.

Incorrect answers:

A: Converting the system partition to NTFS does not facilitate the viewing of the security tab as this tab is available in the view menu of Active Directory Users and computers and converting any system partition will not make it available as it has to be enabled in that view menu.

C: A Container is an object in a directory that contains other objects. By enabling the Users, Groups and Computers as containers, you grant yourself the ability to organize the objects. Though, you still have to enable the Advanced Features option to get the security tab available.

D: Administrator permissions - Members of the administration group have complete and unrestricted access to the domain and to servers and other resources within the domain. Administrators have the power to grant themselves any rights or permissions that they do not already have. Because the security context for members of the Administrators group is so high, the server and the network is vulnerable to attacks from Internet-related sources and email-related virus-infected attachments if accounts in the

Administrators group are compromised. For these reasons, members of the Administrators group should log on using an administrative account only when necessary. The Runas command enables administrators to log on to the machine with their ordinary user accounts yet launch support tools under an administrative security context. However, to make the security tab available, they still have to enable the Advanced Features option.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 166

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

---

### **QUESTION 63**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains three domains. The functional level of the forest is Windows Server 2003. The domain names are Certkiller .com, europe. Certkiller .com, and asia. Certkiller .com. Each domain contains 500 user accounts.

Certkiller .com is in the process of acquiring several other companies whose networks will be added to the Certkiller .com Windows Server 2003 domain. These acquisitions will entail the addition of several new offices, which will be connected to Certkiller 's network by means of dedicated 56-Kbps WAN connections.

You create a new shared folder named NewProjects on a file server in Certkiller .com. Several users in each existing domain need access to the NewProjects folder. These users are not in the same group in any domain. All users who need access to the NewProjects folder must be able to add, delete, and modify files and folders in the NewProjects folder. Users in the acquired companies also will require access to this folder.

You need to create the required Active Directory groups and configure the required permissions for the NewProjects folder. Your solution must minimize ongoing administrative effort as you add new companies to the network. You must also minimize unnecessary traffic across the WAN connections. What should you do?

- A. Create a single universal security group. Add all users that require access to the folder to the group. Create a domain local group in the Certkiller .com domain. Add the universal group to the domain local group. Assign permissions to the shared folder by using the domain local group.
- B. Create a global security group in each domain. Add all users that require access to the folder to the global group in their domain. Create a domain local group in Certkiller .com domain. Add the global groups to the domain local group. Assign permissions to the shared folder by using the domain local group.
- C. Create a universal security group in each domain. Add all users that require access to the folder to the group in their domain. Assign permissions to the shared folder by using the universal groups.
- D. Create a global security group in each domain. Add all users that require access to the folder to the group in their domain. Assign permissions to the shared folder by using the global groups.

Answer: B

Explanation: Applying security permissions to groups of users instead of to individual users greatly eases the administrative burden of managing control over data and other resources. You can change the type of a

group from security to distribution or from distribution to security at any time, provided that the domain is set at the Windows 2000 native or the Windows Server 2003 domain functional level.

Domain local group scope - a group assigned as domain local can only specify permissions on resources within a single domain.

Global group scope - a global group can contain users, groups, and computers from its own domain as members. Global groups are available under any domain functional level.

Following this it would make sense to create a global security group in each domain, add all users that needs access to the global group in their domain. Create a domain local group and add the global group to this domain local group. After which you can assign permissions to the shared folder.

Incorrect answers:

A: Creating a universal security group will result in too much overhead in terms of bandwidth usage. The question pertinently states that you should minimize traffic over the WAN connections.

C: A universal group can contain users, groups, and computers from any domain in its forest. The membership list of universal groups is maintained by global catalog (GC) servers, unlike global groups and domain local groups. Certain DCs must be assigned as GCs so that applications and computers can locate resources within the Active Directory database. When a member is added to or removed from a universal group, global catalog servers must track the change, and each change must be replicated to all the global catalog servers in the forest. This result in increased overhead and network replication traffic for universal groups and thus will not serve the purpose.

D: Assigning permissions to the shared folder by using the global groups will not work in this scenario. You need to assign permissions to the shared folder by making use of the domain local group.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4

---

### **QUESTION 64**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows 2000 native.

A global group named Travelling contains 7,000 users. All of these users are assigned portable computers, which they will use to run new POSIX-compliant application.

You create a global group named POSIX. For all 7,000 users in Travelling, you change the primary group to POSIX.

Members of Travelling now report that they cannot access necessary domain resources.

How should you solve this problem?

A. Ensure that each site on your network is connected to at least one other site by a replication link that uses the SMTP protocol.

B. Create two new global groups, Travelling1 and Travelling2.

Place one half of the members of Travelling in each new group.

Then place both new groups in Travelling.

C. Remove all domain users from the Users group, and then add all domain users to the group again.

D. Remove all users from Travelling.

Change Travelling to a universal group.

Add the same users to the new Travelling group.

Answer: B

Explanation: Per Microsoft: Updates to the Active Directory store must be made in a single transaction. One consequence of this is that you should not create groups with more than 5,000 members. Because group memberships are stored in a single multi-valued attribute, a change to the membership requires that the whole attribute—that is, the whole membership list—be updated in a single transaction. Microsoft has tested and supports group memberships of up to 5,000 members.

Global groups are used primarily to provide categorized membership in domain local groups for individual security principals or for direct permission assignment (particularly in the case of a mixed or interim domain functional level domain). Often, global groups are used to collect users or computers in the same domain and share the same job, role, or function. Global groups:

- Exist in all mixed, interim, and native functional level domains and forests
- Can only include members from within their domain
- Can be made a member of machine local or domain local group
- Can be granted permission in any domain (including trusted domains in other forests and pre-Windows 2003 domains)
- Can contain other global groups (Windows 2000 native or Windows Server 2003 domain functional level only) A global group is a group that can be used in its own domain and in trusting domains.

However, it can contain user accounts and other global groups only from its own domain.

A domain local group can contain users and global groups from any domain in the forest, universal groups, and other domain local groups in its own domain. A local group used on ACLs only in its own domain.

Global group (scope) is a group that is available domain-wide in any domain functional level.

Incorrect answers:

A: Replication on network computers enables the contents of a directory, designated as an export directory, to be copied to other directories, called import directories. Active Directory changes are replicated to all domain controllers on a regular schedule. Thus the contents of a directory do not mean access to domain resources.

C: Removing all domain users from the group and then re-adding them to the group will not help as the Microsoft recommended amount of members per group will still be exceeded.

D: Converting travelling to a new universal group and in the process getting rid of the existing travelling group, but universal groups are used primarily to grant access to resources in all trusted domains, but universal groups can only be used as a security principal (security group type) in a Windows 2000 native or Windows Server 2003 domain functional level domain. Thus this option is not viable.

References:

Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 4: 5-21, 770

---

### **QUESTION 65**

You are the network administrator for Certkiller Oil. The network consists of three Active Directory domains in a single forest. All domain controllers run Windows Server 2003.

Certkiller Oil enters into a business partnership with Oil Importers. The Oil Importers network consists of four Active Directory domains in a single forest. To enable the two companies to share resources, a two-way forest trust relationship with selective authentication is created.

Now you need to ensure that the research data of Certkiller Oil will remain inaccessible to all users in Oil Importers.

First, you create a local group named No Oil. Then, you assign the Deny - Full Control permission to No Oil.

What should you do next?

- A. Add the Domain Guests group from each of the four domains of Oil Importers to No Oil.
- B. Add the Other Organization group to No Oil.
- C. Add the Users group from each of the four domains of Oil Importers to No Oil.
- D. Add the Proxy group to No Oil.

Answer: C

Explanation: Using Active Directory Domains and Trusts, you can determine the scope of authentication between two forests that are joined by a forest trust.

You can set selective authentication differently for outgoing and incoming forest trusts. With selective trusts, administrators can make flexible forest-wide access control decisions.

If you use forest-wide authentication on an incoming forest trust, users from the outside forest have the same level of access to resources in the local forest as users who belong to the local forest. For example, if ForestA has an incoming forest trust from ForestB and forest-wide authentication is used, users from ForestB would be able to access any resource in ForestA (assuming they have the required permissions).

If you decide to set selective authentication on an incoming forest trust, you need to manually assign permissions on each domain and resource to which you want users in the second forest to have access. To do this, set a control access right Allowed to authenticate on an object for that particular user or group from the second forest. Therefore we need to add the Users group from each of the four domains of Oil Importers to No Oil.

With the Deny-Full Control permission activated to the No Oil local group, and by adding the users of all the four domains to No Oil, you will ensure the integrity of the research data by keeping it inaccessible.

Incorrect answers:

A: For the data to remain inaccessible to all users you need to add all the users from all the groups to the No Oil local group. If you add the Domain Guests group from each of the four domains of Oil Importers to the No Oil local group then you are not including all the users.

B: Adding the Other Organization group to No Oil will not have the desired effect.

D: By adding only the Proxy group to No Oil, will not work as Proxy servers only provide security by shielding the IP addresses of internal clients from the Internet.

Reference:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 829

Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 769

---

## **QUESTION 66**

You are the network administrator for Certkiller .com Active Directory domain. The domain includes Windows Server 2003 domain controllers and Windows XP Professional client computers.

A new administrator named Sandra is hired to assist you in deploying Windows XP Professional to 100 new computers. Sandra installs the operating system on a new computer named Certkiller 11.

However, when Sandra tries to log on to the domain from Certkiller 11, she is unsuccessful. The logon box does not allow her to view and select the domain name.

You need to ensure that Sandra can log on to the domain from Certkiller 11.

What should you do?



- A. Enable the computer account for Certkiller 11.
- B. Configure Certkiller 11 as a member of the domain.
- C. Add Sandra's user account to the Enterprise Admins group.
- D. Add Sandra's user account to the Server Operators group.

Answer: B

### QUESTION 67

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. The network consists of 10 offices located across Europa. The OU structure consists of one top-level OU for each branch office. Each top-level OU contains eight or more child OUs, one for each department. User accounts are located in the appropriate departmental OU within the appropriate office OU.

For security purposes, you routinely disable user accounts for terminated employees. As part of an internal audit, you need to create a list of all disabled user accounts.

You need to generate the list of disabled user accounts as quickly as possible.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

- A. In Active Directory Users and Computers, create a new saved query.
- B. Run the dsget user command.
- C. Run the dsquery user command.
- D. Run the netsh command.

Answer: A, C

### QUESTION 68

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.

Some client computers run Windows NT 4.0 Workstation, others run Windows 2000 Professional, and the rest run Windows XP Professional.

You need to create a new global group by modifying an existing script written in Microsoft Visual Basic, Scripting Edition (VBscript). Client computers will access the new global group by using the name Accounting.

How should modify the script? (Drag suitable lines of code to the corrections to the work area. Use only code that apply.)

#### Lines of Code

```
Set oGroup = oOU.Create("Group", "cn=Accounting")
oGroup.Put "sAMAccountName", "Accounting"
oOU.SetInfo
oOU.SetInfo
Set oGroup = ogroup.Create("Group", "cn=accounting")
```

**Work Area**

addgroup1.vbs - Notepad

File Edit Format View Help

```
Set oRoot = GetObject("LDAP://rootDSE")
Set oDomain = GetObject("LDAP://" & oRoot.Get

Set oOU=oDomain.Create("organizationalunit", "
oOU.Put "Description", "Employee OU"
oOU.SetInfo

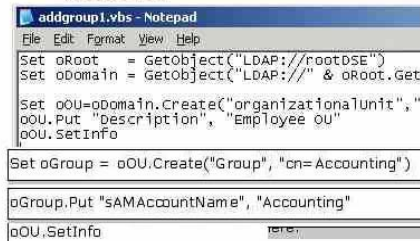
Drag object here.
Drag object here.
Drag object here.
```

Answer:

## Lines of Code

```
Set oGroup = oOU.Create("Group", "cn=Accounting")
oGroup.Put "sAMAccountName", "Accounting"
oOU.SetInfo
oOU.SetInfo
Set oGroup = ogroup.Create("Group", "cn=accounting")
```

## Work Area



```
addgroup1.vbs - Notepad
File Edit Format View Help
Set oRoot = GetObject("LDAP://rootDSE")
Set oDomain = GetObject("LDAP://" & oRoot.Get
Set oOU=oDomain.Create("organizationalUnit", "
oOU.Put "description", "Employee OU"
oOU.SetInfo
Set oGroup = oOU.Create("Group", "cn=Accounting")
oGroup.Put "sAMAccountName", "Accounting"
oOU.SetInfo
```

Explanation: Since all client computers will access the new global group by making use of the name Accounting, the group setting should be set accordingly. Global groups can include other groups and user/computer accounts from only the domain in which the group is defined. Permissions for any domain in the forest can be assigned to global groups. Global group can contain users, groups, and computers from its own domain as members. Global groups are available under any domain functional level.

## Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 320

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4

**QUESTION 69**

You are the network administrator for Certkiller .com. The network consists of two Active Directory domains in a single forest. The functional level of each domain is Windows 2000 mixed. Your engineering department has 3,000 users. The engineering users are members of various global groups.

Certkiller plans to open a new office where engineering users will test products. Engineering users will need to dial in to the company network when they work at the new office.

You need to ensure that all new user accounts in the engineering department will have the appropriate group memberships. These accounts must be allowed to connect to the network by using remote access permissions. You must achieve your goal by using the minimum amount of administrative effort.

First, you create a template account for engineering users.

Which two additional actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Modify the schema for the office and street attributes by selecting the Index this attribute in the Active Directory check box.
- B. Modify the schema for the group attribute by selecting the Index this attribute in the Active Directory check box.
- C. Manually add the Allow Access remote access permission to each new user account that you create.
- D. Manually add the group membership information to each new user account that you create.
- E. Add the group membership information to the template account.
- F. Add the Allow Access remote access permission to the template account.

Answer: C, E

Explanation: You can add the template account to the appropriate groups. When you copy the template account, the copy will have the same group membership as the template account. This does not apply however, to remote access permission. When you copy the template account, the copy will have the default remote access permission. Therefore, we need to manually assign the appropriate remote access permission to the new user accounts.

Incorrect Answers:

A: Modifying the schema would be obsolete as it would result in additional administrative efforts.

B: If you want to avoid adding to the administrative efforts that has to be done, then you do not have to modify the schema.

D: When you copy the template account, the copy will have the same group membership as the template account.

F: The copy will have the default remote access permission when one copies the template account. Therefore, we need to manually assign the appropriate remote access permission to the new user accounts.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, *Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System*, p. 283

---

### **QUESTION 70**

You are the network administrator for Certkiller .com. All user accounts and groups in the domain are in the container named Users.

Company naming conventions require that names of global groups begin with G\_ and names of domain local groups begin with DL\_. A domain local group named HRServices does not meet the requirements. The HRServices group has one global group member named G\_HRUsers. The HRServices group is assigned to Allow - Full Control permission for a shared folder named HRFiles. The shard folder is located on a file server.

You need to rename the HRServices group to meet the naming convention requirements. In addition, you need to ensure that user access to the HRFiles shared folder is not disrupted while you perform the procedure.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A. Open Active Directory Users and Computers, and then delete the existing HRServices domain local group. Create a new domain local group named DL\_HRServices. Add the G\_HRUsers group to the DL\_HRServices group. Assign the DL\_HRServices group the Allow - Full Control permission for the HRFiles shared folder.

B. Open the Active Directory Users and Computers, and then change the name of the HRservices group to DL\_HRServices.

C. Run the following command: `dsadd group CN=DL_HRServices,CN=Users,DC= Certkiller .com,DC=com - member CN=G_HRUsers,CN=Users,DC= Certkiller ,DC=com`

D. Run the following command: `dsmove CN=HRServices,CN=Users,DC= Certkiller ,DC=com - newname DL_HRServices`

Answer: B, D

Explanation: The Dsmove command-line utility is used to rename or move a single object within the Active Directory. When you use the Dsmove command-line utility, you specify the object's distinguished name, then the new name of the object (if you are changing the object's name) and the new location of the object. Active Directory Users and Computers on Windows Server 2003 domain controllers, is the main tool used for managing the Active Directory users, groups, and computers. To set up and manage domain user accounts, you use the Active Directory Users And Computers utility. You need to change the name of the HRservices group to DL\_HRServices. And then run the appropriate dsmove command.

Incorrect answers:

A: You only need to change the name and not assign the DL\_HRServices group Full Control permission.

C: You can automate the process of creating users, groups, and computers through the Dsadd command-line utility. However, in this case you should rather run the dsmove command with the appropriate parameters.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r)Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, p. 227

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, pp. 189-191

---

## QUESTION 71

You are the network administrator for Certkiller . The network consists of a single Active Directory forest that contains three domains. The functional level of the forest is Windows 2000. The NetBIOS names of the domains are Certkiller 1, Certkiller 2, and Certkiller 3. The functional level of all three domains is Windows 2000 mixed. You manage resources in Certkiller 1.

A new file server is added to Certkiller 1. Users in all three domains need access to resources on the file server.

You need to create a group that will be used to grant access to the file server in Certkiller 1.

Which two actions should you perform? Each correct answer presents part of the solution. Select two.

- A. Create a security group.
- B. Create a distribution group.
- C. Configure the group to be a global group.
- D. Configure the group to be a universal group.
- E. Configure the group to be a domain local group.

Answer: A, E

Explanation: The group type security group is a logical group of users who need to access specific resources. Security groups are listed in Discretionary Access Control Lists (DACLS) to assign permissions to resources.

A domain local group is a type of group used to assign permissions to resources. It can contain user accounts, universal groups, and global groups from any domain in the tree or forest. It can also contain other domain local groups from its own local domain.

These two options should allow you to create a group that will be used to grant access to the file server in Certkiller 1 under the given circumstances.

Incorrect answers:

B: A distribution group type is a logical group of users who have common characteristics. Applications and

e-mail programs (for example, Microsoft Exchange) can use distribution groups. Distribution groups can't be listed in DACLs and therefore have no permissions. This is not what is required.

C: Global groups are used to organize users who have similar network access requirements. A global group is simply a container of users. This will not do in these circumstances.

D: Universal groups are used to logically organize global groups and appear in the Global Catalog (a search engine that contains limited information about every object in the Active Directory). Universal groups can contain users (not recommended) from anywhere in the domain tree or forest, other universal groups, and global groups. But this is not what is required.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, pp. 167-170

---

## QUESTION 72

Exhibit, multiple hotspot



You are the network administrator for Certkiller .com. The network contains a third-party application that runs as a service. The application service is secured with a domain-level service account. The properties of the service account are displayed in exhibit.

Users report that the application is no longer available. The application service is stopped.

An administrator reports that the password of the service account had expired and was changed. You reset the password on the service to match the new password of the service account. You unsuccessfully attempt to restart the service.

You need to ensure that the service will start. You need to prevent this problem from happening again while retaining administrative control over the service account password.

What should you do?

Answer: Enable Password never expires.

Explanation: Since the question states that the password of the service account had expired and was changed, you need to enable the Password never expires option especially in lieu of you already having has the password reset to match the new password of the service account and you still unable to restart the service. This option will enable you to start the service and also prevent this situation from occurring again, whilst it will allow you to retain administrative control over the password.

References:

Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft Press, pp. 7:12-13

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 317-318.

---

**QUESTION 73**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains Windows Server 2003 computers and Windows XP Professional computers.

You use a non-administrative user account named Joseph to log on to a client computer. You need to change the password for a domain user account named Sophia.

You open the Active Directory Users and Computers console. When you attempt to change Sophia's password, you receive the following error message: "Access is denied".

You need to remain logged on to the client computer as Joseph, and you need to be able to change Sophia's password.

What should you do?

- A. Add the non-administrative domain user account to the local Administrators group.
- B. Use the runas command to run Active Directory Users and Computers with domain administrative credentials.
- C. From a command prompt, run the net user Sophia /add /passwordreq:yes command.
- D. From a command prompt, run the net accounts /uniquepw: /domain command.

Answer: B

Explanation: The runas command can be used to perform administrative tasks. Run as, also called secondary logon, is a useful tool that allows a user to run a specified program with permissions that are different from those belonging to the account with which the user is currently logged on. You can use this command to run executable files, and Control Panel items, among other tasks. It allows you to run a specified program with permissions that are different from that associated to the account (user account named Joseph) with which you are currently logged on. Therefore, you can use the runas command to run Active Directory Users and Computers with domain administrative credentials to change Sophia's password.

Incorrect Answers:

A: Adding a non-administrative account to the local administrators group will allow you to complete this task. But the question states that you need to remain logged on the client computer as Joseph. This results in you needing a secondary logon rather than being added to the local administrators group.

C: This command allows you to add or modify user accounts or display user account info. And as this command is used in this scenario, it also specifies that the user must have a password. This will not allow you to change Sophia's password because you need to have either administrator status or use the run as command especially since the question states that you need to remain logged on to the client computer as Joseph who is a non-administrative account.

D: This specific command updates user accounts database and modifies password and logon requirements for all accounts. Furthermore it requires the user not to use same password for the number of password changes and it performs the operation on the primary domain controller of the current domain, else the modification will be performed on the local computer. However, this assumes that you are working from an administrator's account rather than a non-administrative user account named Joseph.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Chapter 1, p. 36

---

**QUESTION 74**

You are the network administrator for Certkiller . Your network consists of three Active Directory domains in a single forest. You do not have administrative rights to the forest. All domain controllers run Windows Server 2003. Universal group membership caching is enabled. Certkiller has a main office in Madras and five branch offices located worldwide. Each office is configured as an Active Directory site, as shown in the exhibit.



Each office contains three domain controllers, one for each domain.

A new employee named Dr King is hired in the Berlin office. You create a new user account for Dr King from a domain controller in Berlin. However, Dr King reports that he cannot log on to his domain. Other users from Berlin report no difficulties.

You need to ensure that Dr King can log on successfully.

What should you do?

- A. Delete the user account in Berlin.  
Recreate the user account in Madras.
- B. Force directory replication between all domain controllers in Berlin.
- C. Restore network connectivity between the domain controllers in Berlin and Madras.
- D. Instruct Dr King to use his user principal name when he logs on for the first time.

Answer: C

Explanation: When a new user logs on to a native mode domain, the authenticating domain controller needs to be able to contact a Global Catalog server to obtain universal group information. The Global Catalog servers are in the Madras office, so a lack on network connectivity between Berlin and Madras would prevent the new user from being able to log on. The reason no one else has a problem logging on is that Universal Group caching is enabled. However, the information in the cache on the Berlin domain controller is out of date in the sense that it doesn't contain information about the new user.

Incorrect Answers:

- A: The account does not need to be created in Madras. It can be created on any domain controller in the domain.
- B: The domain controllers in Berlin are in separate domains. They do not need to replicate to each other.
- D: You don't have to log on using your UPN name. The question states that the user couldn't log on to "his" domain. This implies that he either attempted to log on using his UPN or he entered his downlevel username and selected the correct domain in the drop down box.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, p. 426

**QUESTION 75**

You are the network administrator for Certkiller .com. The network consists of a single Active

Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.

A new management directive states that users can log to the domain only during business hours.

Users who remain logged on after business hours must be automatically disconnected from network resources.

You need to enforce this directive by using the minimum amount of administrative effort.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Configure the Default Domain Policy Group Policy object (GPO) to increase scheduling priority for all users.

B. Configure the Default Domain Policy Group Policy object (GPO) to force users to log off when their logon hours expire.

C. Select all user accounts.

Modify the account properties to restrict logon hours to business hours.

D. Create a domain user account named Temp.

Configure the account properties to restrict logon hours to business hours.

E. Modify the DACL on the Default Domain Policy Group Policy object (GPO) to assign the Allow - Read permission to the Users group.

Answer: B, C

Explanation: When you restrict logon hours, you might also want to force users to log off after a certain point. If you apply this policy, users cannot log on to a new computer, but they can stay logged on even during restricted logon hours. To force users to log off when logon hours expire for their account, apply the Network security: Force logoff when logon hour's expiry policy.

You can assign logon hours as a means to ensure that employees are using computers only during specified hours. This setting applies both to interactive logon, in which a user unlocks a computer and has access to the local computer, and network logon, in which a user obtains credentials that allow him or her to access resources on the network.

Incorrect answers:

A: Increasing the scheduling priority will not affect logon hours.

D: Restricting logon hours to business hours by configuring the account properties will work, but this option does not mention measures to cut down on administrative effort.

E: A DACL is a list of ACEs that lets administrators set permissions for users and groups at the object and attribute levels. This list represents part of an object's security descriptor that allows or denies permissions to specific users and groups. Modifying the DACL by assigning the Allow-Read permission will not work as you first need to force all users to log off when their logon hours expire.

References:

Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 582

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 58, 442.

---

## **QUESTION 76**

You are responsible for administering the Production OU. You are assigned the Allow - Full Control



permission for the OU. All computer objects in the Production OU are administered by another administrator named Tom.

The Production OU contains the computer account for a Windows Server 2003 computer named Certkiller 1. Tom submits a list of configuration settings that he wants to apply to Certkiller 1 by means of a Group Policy object (GPO). A GPO that contains Tom's required settings is created in another OU by the domain administrator.

You only want to allow Tom to link existing GPOs to the Production OU. He must not have any more rights than he needs to perform the required tasks.

What should you do?

- A. Add Tom's user account to the Group Policy Creator Owners group in the domain.
- B. Run the Delegation of Control Wizard and assign Tom's user account the Allow - Manage group policy links permission for the Production OU.
- C. Run the Delegation of Control wizard and assign Tom's user account the Allow - Change permission for the Production OU.
- D. Run the Delegation of Control wizard and assign Tom's user account the Allow - Apply group policy permission for all GPOs that are linked to the Production OU.

Answer: B

Explanation: You can delegate permissions to manage Group Policies of the Production OU. This is done through delegation of control. Right click the designated container in Active Directory Users and Computers. Select Delegate Control. Once the Delegate Control Wizard runs, select the user (Tom) whom should be granted control in the container. Then, add Manage Group Policy Links from the Permissions list, and complete the Delegate Control Wizard. Tom will only be able to create GPO links in containers where he has been allowed the particular permission. Thus restricting him to only what he needs to be able to do his job.

Incorrect Answers:

A: This type of group permissions should be applied at the root of the volume. The Creator Owner group e.g. is a special group that determines the access that a user has to files and folders he or she has created. By default, the Full Control special permissions assigned to this group automatically apply to every folder created on the volume. Thus the default permissions of being Creator Owner would grant Tom too much permission than is necessary.

C, D: Active Directory enables you to efficiently manage objects by delegating administrative control of the objects. You can use the Delegation of Control Wizard and customized consoles in Microsoft Management Console (MMC) to grant specific users the permissions to perform various administrative and management tasks. You use the Delegation of Control Wizard to select the user or group to which you want to delegate control. You also use the wizard to grant users permissions to control organizational units and objects and to access and modify objects. However, these options, whether Allow- change or Allow - Apply group policy permission, will grant Tom more than the necessary permissions to perform his tasks.

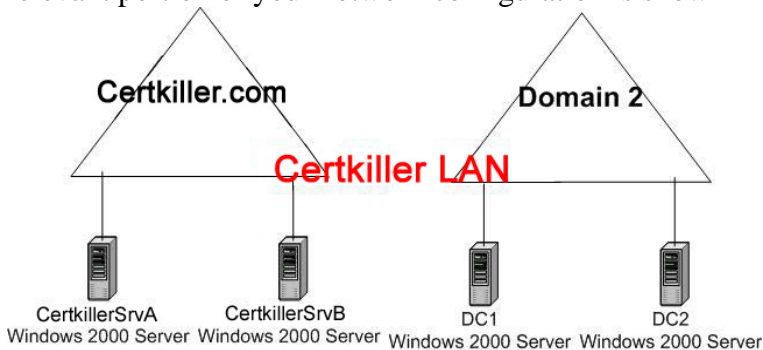
Reference:

Jill Spealman, Kurt Hudson, and Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Chapter 10, p. 601

---

**QUESTION 77**

You are the network administrator for Certkiller . The network consists of two Active Directory domains: Certkiller .com and Domain 2. All client computers run Windows XP Professional. The relevant portion of your network configuration is shown in the exhibit.



A support technician named Jack needs to create user accounts in both domains. You delegate the appropriate permissions to her. Then you run Adminpak.msi from the Windows Server 2003 CDROM on Jack's computer.

Later, Jack reports that she cannot connect to Certkiller SrvA or Certkiller SrvB by using her administrative tools. However, she can access all other resources in both domains.

How should you solve this problem?

- A. On Jack's computer use Registry Editor to disable signing and encryption of LDAP traffic.
- B. On Certkiller SrvA and Certkiller SrvB, use Registry Editor to change the LDAP port value to 380.
- C. On Certkiller SrvA and Certkiller SrvB, run Adminpak.msi from the Windows Server 2003 CD-ROM.
- D. On Jack's computer, change the domain membership from Domain 2 to Certkiller .com.

Answer: A

**Explanation:**

To use the Windows Server 2003 Active Directory administrative tools to manage Windows 2000-based domain controllers with Windows 2 Service Pack 2 (SP2) or earlier installed when NTLM authentication is negotiated, you can configure the administrative tools to communicate by using non-secured LDAP traffic. To turn off the signature and encryption of LDAP traffic for the Windows Server 2003 Active Directory tools, set the ADsOpenObjectFlags value to 0x03.

Incorrect Answers:

B: It is not necessary to change the LDAP port value.

C: You cannot install the Windows 2003 adminpak.msi on a Windows 2000 computer.

D: It is not necessary to change the domain membership of the computer.

Reference: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;325465>

**QUESTION 78**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.

All user accounts in the Sales department are located in the Sales organizational unit (OU). You suspect that one or more user accounts in the OU have compromised passwords.

You need to force all users in the Sales department to reset their passwords.

What should you do?

- A. Select all user accounts in the Sales OU.  
Disable the accounts and re-enable them.
- B. Select all user accounts in the Sales OU.  
Modify the account properties to force all passwords to be changed on next logon.
- C. Create a Group Policy object (GPO) and link it to the Sales OU.  
Modify the password policy to set the maximum password age to 0.
- D. Create as Group Policy object (GPO) and link it to the domain.  
Modify the password policy to set the maximum password age to 0.

Answer: B

Explanation: To force all the users in the Sales OU to reset their passwords, we must select all user accounts in the Sales OU and modify the account properties to force all passwords to be changed on next logon.

User rights can be assigned in a domain environment by editing a GPO assigned to the domain. To access the default domain policy and set user rights on its GPO, open Active Directory Users and Computers console from the Administrative Tools menu, right-click the domain name in the left console pane, select Properties. Click the Group Policy tab, select the GPO, and then click Edit. This opens the Group Policy Object Editor. Under Computer Configuration in the left pane, expand Windows Settings, expand Security Settings, expand Local Policies, and select User Rights Assignment.

Incorrect answers:

A: Disabled accounts have as a consequence the inability to log on with the account. It does not alter or modify password settings.

C: Maximum password age determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. Linking the GPO to the OU will not compel users to reset their passwords.

D: Linking a GPO where the maximum password age is set to 0 to the domain will not force users to reset their passwords.

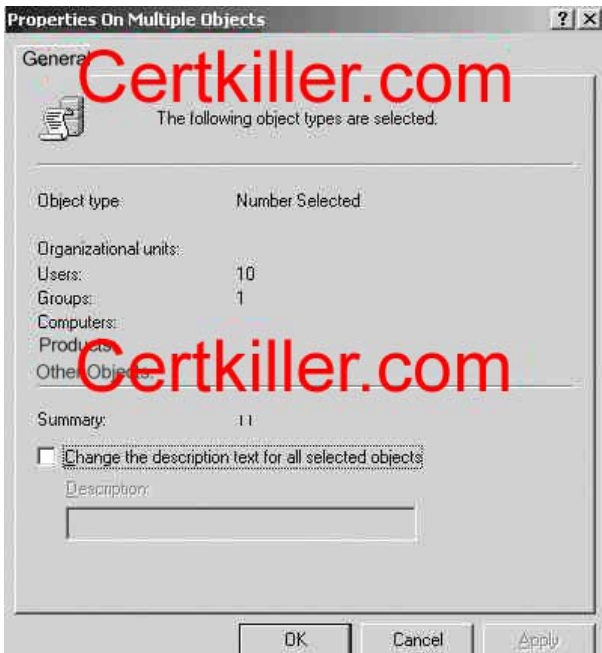
References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 297, 442.

---

**QUESTION 79**

Exhibit



You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows 2000. Your sales department employs 100 users. All users accounts for sales employees are located in an OU named Sales.

To reduce the size of the sales department, the company terminates 10 sales users.

You need to disable these 10 user accounts by using the minimum amount of administrative effort.

You use the Active Directory Users and Computers in an attempt to disable all 10 users accounts simultaneously. You see the dialog box in the exhibit.

What should you do?

- A. Disable each of the 10 affected user accounts, one by one.
- B. Log on by using an account that has administrative access to the domain. Disable all user accounts in the Sales OU simultaneously.
- C. Select all user accounts in the Sales OU. Disable all user accounts simultaneously.
- D. Select only the 10 affected user accounts in the Sales OU. Disable all 10 user accounts simultaneously.

Answer: D

Explanation: Active Directory Users and Computers is used to manage Active Directory objects such as users, groups, and machines within the domain. To make space available and thus reduce the size of the Sales OU in an efficient manner with the least amount of administrative effort, you can make use of Active Directory Users and Computers to disable several user accounts simultaneously.

Incorrect answers:

A: Disabling each of the 10 affected user accounts one by one can be made more efficient. Though this option will work, it is not the answer as it results in too much administrative effort and does not disable the accounts simultaneously.

B, C: Disabling all the user accounts will not be advisable in this scenario as you will then have to reenable all the user accounts other than the 10 affected user accounts afterward. Also option B has even

more administrative effort attached to it than is already mentioned for option C and B together.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, *Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System*, pp. 259-267, 337

---

**QUESTION 80**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.

A user named King will leave Certkiller in one week. A replacement will be hired in one month.

The replacement will need the same access to network resources that King currently has. The

replacement will also need ownership of all files that currently reside in King's home folder.

You need to minimize the administrative effort that will be required when the replacement is hired.

You also need to ensure that no one can use King's user account to log on to the domain until the replacement is hired.

What should you do?

- A. Move King's user account to the LostAndFound organizational unit (OU).
- B. Disable King's user account.
- C. Configure King's user account to require a change in password at next logon.
- D. Delete King's user account.

Answer: B.

Explanation: The quickest way is to disable King's user account. When the replacement starts, we can enable and rename the account.

To ensure no unauthorized use of King's account it should be disabled only because the question also poses the scenario of wanting to use the King user account with all its work, documents, etc for the new replacement. Disabling the account will not destroy the information and the documents residing in that account. It will leave the option there for the administrators to use it for the new replacement.

Incorrect answers:

A: Placing files in whatever OU will not render it safe from other users who might still be able to access it.

C: A change in password at the next logon configuration will not preclude tempering with the account till the replacement arrives.

D: Deleting King's user account would be folly as his replacement will need that account and the data that it holds. Deleting the account will destroy the information and the documents residing in that account.

References:

Dan Holme and Thomas Orin, *MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment*, pp. 173-178

---

**QUESTION 81**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. All domain controllers run Windows Server 2003.

Users who enter an invalid password more than twice in one day must be locked out.

You need to configure domain account policy settings to enforce this rule.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose

two)

- A. Set the minimum password age to one day.
- B. Set the maximum password age to one day.
- C. Change the Enforce password history setting to three passwords remembered.
- D. Change the Account lockout duration setting to 1440 minutes.
- E. Change the Account lockout threshold setting to three invalid logon attempts.
- F. Change the Reset account lockout counter after setting to 1440 minutes.

Answer: E, F

Explanation: An Account lockout policy disables a user account if an incorrect password is entered a specified number of times over a specified period. These policy settings help you to prevent attackers from guessing users' passwords, and they decrease the likelihood of successful attacks on your network. Account lockout threshold is a security setting that determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts.

If you set the value to 0, the account will never be locked out.

Reset account lockout counter after is a security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 99,999 minutes. If an account lockout threshold is defined, this reset time must be less than or equal to the Account lockout duration.

Thus when you choose Account lockout threshold to 3, by default Windows Server 2003 will put 30 minutes value for: Reset account lockout and Account lockout duration, but if you change Reset account lockout default value to 1440. Windows Server 2003 will change for you the value for Account lockout duration to match Reset account lockout.

Incorrect answers:

A: Setting the minimum password age to one day will not work as it is a case of entering a wrong invalid password, whether it is once, twice, or even many times, in a single day that has to be prevented.

B: Setting the maximum password age to one day is irrelevant as this scenario calls for preventing the entering of invalid passwords more than twice in a single day.

C: Changing the enforce password history setting to three password remembered will result in Active Directory maintains a list of recently used passwords, and will not allow a user to create a password that matches a password in that history. The result is that a user, when prompted to change his or her password, cannot use the same password again, and therefore cannot circumvent the password lifetime. The policy is enabled by default, with the maximum value of 24. To make this setting to three passwords remembered will result in users being allowed to enter invalid passwords more than twice.

D: This policy defines how long locked-out accounts remain locked out. The default setting is none (or undefined) because you must enable the Account Lockout Threshold policy for this policy to be in effect. The available range is from 0 minutes through 99,999 minutes. This does not include a setting for a quantity of invalid password entering.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 282, 317-318

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4

---

**QUESTION 82**

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com.

You add a Windows Server 2003 computer to the domain. This server is used to store critical business applications and confidential data. You create several local accounts on the server to manage the applications.

Some users report that they are having difficulty accessing an application that is stored on the server. The application uses local accounts.

You need to enable auditing to track all attempts to access the server through a local account in order to gather more information. You must not track more data than is necessary.

What should you do?

To answer, drag the appropriate setting or settings to the correct policy or policies in the work area.

Policy	Setting
Audit account logon events	Place setting here
Audit account management	Place setting here
Audit directory service access	Place setting here
Audit logon events	Place setting here

**Settings, select from these**

No auditing

Success

Failure

Success and failure

Answer:

Policy	Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	Success and failure

Settings, select from these

No auditing

Success

Failure

Success and failure

Explanation: Success Audit - Indicates the occurrence of an event that has been audited for success. For example, a Success Audit event is a successful logon when system logons are being audited. Failure Audit - Indicates the occurrence of an event that has been audited for failure. For example, a Failure Audit event is a failed logon due to an invalid username and/or password when system logons are being audited.

These would be the only necessary information in this case.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 490

---

### QUESTION 83

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.

Certkiller .com purchases a new server to test applications in a stand-alone environment.

Certkiller .com's written security policy includes the following requirements:

- User passwords on stand-alone computers must be changed every 45 days.



- Users can change their passwords immediately after they change their passwords once.
- Users must not be able to use the same password again until at least 10 different passwords are used.

You need to configure the password settings so that the new server conforms to the written security policy.

What should you do?

Drag and Drop.

	Setting
Minimum password age	<input type="text" value="0"/>
Maximum password age	<input type="text" value="45"/>
Enforce password history	<input type="text" value="10"/>

Settings, select from these

Certkiller.com

Answer:

**Setting**

Minimum password age	<input type="text" value="10"/>
Maximum password age	<input type="text" value="45"/>
Enforce password history	<input type="text" value="10"/>

Settings, select from these

**Certkiller.com**

Explanation: Minimum Password Age defines the minimum number of days a user must keep a password before they can change the password.

Maximum Password Age defines how many days a user can keep the same password before having to create a new password.

Enforce Password History, specifies how many passwords are remembered and is used to prevent users from re-using the same password when they configure new passwords.

Setting the minimum password age to 0, Setting the maximum password age to 45 and Setting the enforce password history to 10 will comply with the written requirements.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, pp. 141-142

---

**QUESTION 84**

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003. All client computers run Windows XP Professional and are members of the domain.

The domain has security settings that are applied that are applied the Default Domain Policy GPO. The current password policy shown in the Policy Exhibit.

A new user named Jack King logs on to the domain for the first time and is prompted to reset her password. Jack successfully sets a new password. Later the same day, she attempts to change her password. You view the properties of her account in Active Directory Users and Computers. The

properties for Jack King's account are shown in the Account Properties exhibit. You need to ensure that Jack can change her password. What should you do?

- A. In the properties of Jack King's user account, select the Store password using reversible encryption check box.
- B. In the properties of Jack King's user account, on the Account tab, select the User must change password at next logon check box.
- C. In the properties of Jack King's user account, on the Account tab, select the Password never expires check box.
- D. In the properties of Jack King's user account, on the Account tab, configure the account to expire today.

Answer: B

Explanation: User Must Change Password At Next Logon If selected, forces the user to change the password the first time they log on. This is done to increase security and moves password responsibility to the user and away from the administrator. And in this case it will ensure that Jack can change her password.

Incorrect answers:

- A: This will not ensure that Jack will be able to change her password.
- C: Password Never Expires - if selected specifies that the password will never expire, even if a password policy has been specified. For example, you might select this option if this is a service account and you do not want the administrative overhead of managing and changing passwords. This is not what is required.
- D: This will not ensure that Jack will be able to change her password.

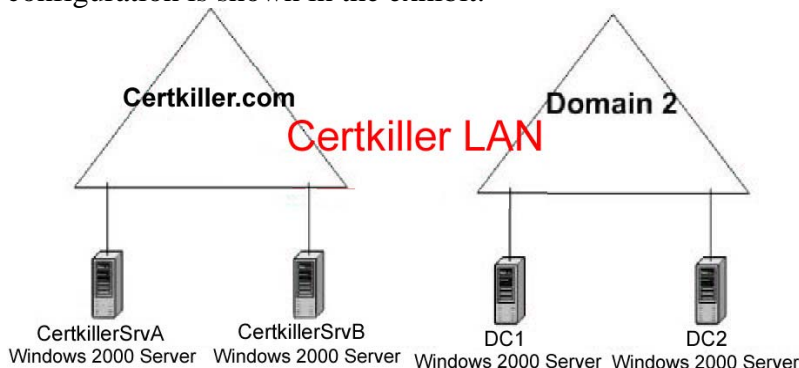
Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 145

---

### QUESTION 85

You are the network administrator for Certkiller .com. The network consists of two Active Directory domains. All client computers run Windows XP Professional. The relevant portion of your network configuration is shown in the exhibit.



A support technician named Sandra needs to create user accounts in both domains. You delegate the appropriate permissions to her. Then you run Adminpak.msi from the Windows Server 2003 CDROM on Sandra's computer.

Later, Sandra reports that she cannot connect to DC1 or DC2 by using her administrative tools. However, she can access all other resources in both domains.

How should you solve this problem?

- A. On Sandra's computer, use Registry Editor to disable signing and encryption of LDAP traffic.
- B. On DC1 and DC2, use Registry Editor to change the LDAP port value to 380.
- C. On DC1 and DC2, run Adminpak.msi from the Windows Server 2003 CD-ROM.
- D. On Sandra's computer, change the domain membership from Domain 2 to Domain 1.

Answer: A

Explanation: Because Active Directory is based on the Lightweight Directory Access Protocol (LDAP), you can reference each object within Active Directory using different types of LDAP naming conventions. Distinguished names (DNs) and relative distinguished names (RDNs) are two of the naming conventions that Active Directory uses for its objects. DN and RDN use specific naming components to define the location of the objects that they are identifying. There is a need to import and export data into and out of Active Directory and other Lightweight Directory Access Protocol (LDAP) directory services. In the above scenario Sandra is unable to connect to DC2 or DC2 and to solve her problem you need to use the Registry Editor on her computer to disable signing and encryption of LDAP traffic since she can access all other resources in both the domains.

Incorrect answers:

B: The problem that is being described stems from Sandra's computer and not the domain controllers, thus changing the LDAP port value on the domain controllers will not address the problem. Sandra can access the other resources in both the domains; she just is unable to connect by means of her administrative tools.

C: Running the Adminpak.msi from the Windows Server 2003 CD-ROM will not work; the problem is with Sandra's computer and not the domain controllers.

D: You do not need to change domain membership on Sandra's computer.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 315

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows(r) Server 2003 Environment Exam Cram(tm) 2 (Exam 70-290), Chapter 4

---

### **QUESTION 86**

You are the network administrator for Certkiller . The network originally consists of a single Windows NT 4.0 domain.

You upgrade the domain to a single Active Directory domain. All network servers now run Windows Server 2003, and all client computers run Windows XP Professional.

Your staff provides technical support to the network. They frequently establish Remote Desktop connections with a domain controller named DC1.

You hire 25 new support specialists for your staff. You use Csvde.exe to create Active Directory user accounts for all 25.

A new support specialist named King reports that he cannot establish a Remote Desktop connection with DC1. He receives the message shown in the Logon Message exhibit:



You open Gpedit.msc on DC1. You see the display shown in the Security Policy exhibit:

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Shut down system immediately if unable to log security audits	Disabled
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Devices: Unsigned driver installation behavior	Do not allow installation
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	None
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled

You need to ensure that King can establish Remote Desktop connections with DC1. What should you do?

- Direct King to establish a VPN connection with DC1 before he starts Remote Desktop Connection.
- Direct King to set a password for his user account before he starts Remote Desktop Connection.
- In the local security policy of DC1, disable the Require strong (Windows 2000 or later) session key setting.
- In the local security policy of DC1, enable the Disable machine account password changes setting.

Answer: B

Explanation: The exhibit shows us that logons by accounts with blank passwords are limited to console logons only (this is also the default setting). The error message indicates that this is the reason that King is unable to connect with a Remote Desktop connection. We can solve this problem by instructing King to set a password for his user account before he starts a Remote Desktop Connection.

Incorrect Answers:

- It is not necessary to create a VPN connection before starting a Remote Desktop Connection.
- This will not help. The client computer is running Windows XP Professional, which can use a strong session key.
- This is unrelated to Remote Desktop connections.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, p. 574

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, pp. 545-546

### QUESTION 87

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.

You use a script written in Microsoft Visual Basic, Scripting Edition (VBScript) to create new user accounts.

You need to modify the script and enable all new user accounts created from the script.

What should you do?

To answer, drag the appropriate line or lines of code to the correct location or locations in the work area.

Lines of Code	Work Area
oRoot.AccountDisabled = False	<pre> AddSales.vbs - Notepad File Edit Format View Help Set oRoot = GetObject("LDAP://rootDSE") Set oDomain = GetObject("LDAP://" &amp; oRoot.Get("defaultNamingContext")) Drag object here.  Set oOU=oDomain.Create("organizationalunit","ou=Employee ou") oOU.Put "description", "Employee OU" Drag object here.  oOU.SetInfo  Set user = oOU.Create("user", "cn=Employee Admin user") user.Put "sAMAccountName", "EmpAdminUser" user.Put "description", "Employee Admin User" Drag object here.  oUser.SetInfo  oUser.SetPassword "5qwI#z7" Drag object here.  oUser.SetInfo  Set oOU = GetObject("LDAP://ou=Employee OU,dc=contoso,dc=com") Set oOU=oOU.Create("organizationalunit","ou=Sales OU") oOU.Put "description", "Sales OU" Drag object here.  oOU.SetInfo  For i = 1 To 5 Set oLeaf = oOU.Create("user", "cn=Salesuser" &amp; i) oLeaf.Put "sAMAccountName", "Salesuser" &amp; i oLeaf.SetInfo  oLeaf.SetPassword "x7&amp;fg0" Drag object here. oLeaf.SetInfo </pre>
oUser.AccountDisabled = False	
oLeaf.AccountDisabled = False	
oDomain.AccountDisabled = False	

Answer:

Lines of Code	Work Area
oRoot.AccountDisabled = False	<pre> AddSales.vbs - Notepad File Edit Format View Help Set oRoot = GetObject("LDAP://rootDSE") Set oDomain = GetObject("LDAP://" &amp; oRoot.Get("defaultNamingContext")) Drag object here.  Set oOU=oDomain.Create("organizationalUnit","ou=Employee ou") oOU.Put "description", "Employee OU" Drag object here. oOU.SetInfo  Set oUser = oOU.Create("User", "cn=Employee Admin user") oUser.Put "sAMAccountName", "EmpAdminUser" oUser.Put "description", "Employee Admin user" Drag object here. oUser.SetInfo  oUser.SetPassword "5ow!#27" oUser.AccountDisabled = False oUser.SetInfo  Set oOU = GetObject("LDAP://ou=Employee ou,dc=contoso,dc=com") Set oOU=oOU.Create("organizationalUnit","ou=Sales ou") oOU.Put "description", "Sales OU" Drag object here. oOU.SetInfo  For i = 1 To 5 Set oLeaf = oOU.Create("User", "cn=Salesuser" &amp; i) oLeaf.Put "sAMAccountName", "Salesuser" &amp; i oLeaf.SetInfo  oLeaf.SetPassword "x7&amp;fg0" oLeaf.AccountDisabled = False oLeaf.SetInfo </pre>
oUser.AccountDisabled = False	
oLeaf.AccountDisabled = False	
oDomain.AccountDisabled = False	

**Explanation:**

The key here is that we need to enable all new user accounts.

This script creates two different sets of user accounts, one to create the Empadminuser and one counter to create salesuser from 1 to 5.

We need to enable all new accounts, in this way we had to drag and drop.

oUser.AccountDisabled = False for enable user Empadminuser. to oUser set info part

oLeaf.AccountDisabled = False for enable users SalesUser1, SalesUser2, SalesUser3, SalesUser4, SaleUser5 to oLeaf set info part

**Reference:**

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/ctasks022.asp>

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 692

**QUESTION 88****Exhibit:**

You are the network administrator for Certkiller . All network servers run Windows Server 2003. A server named Certkiller 5 is joined to the domain. Certkiller 5 functions as a printer server.

Your user account is a member of only the Domain Admins group and the Domain Users group.

You attempt to establish a Remote Desktop connection to Certkiller 5. You receive the error message displayed in the exhibit.

What should you do?

- A. Enable the Digitally sign secure channel data security setting on Certkiller 5.
- B. Add your user account to the Remote Desktop Users group in the Certkiller .com domain.
- C. Add your user account to the Remote Desktop Users group on Certkiller 5.
- D. Enable Remote Assistance on Certkiller 5.
- E. Configure the appropriate remote settings on Certkiller 5 by using System Properties in Control panel.

Answer: D

Explanation: Remote Desktop allows you to remotely take control of a Windows Server 2003 server from another location. For example, you could access a server located in a remote office from your company's corporate headquarters. Remote Assistance is used to request assistance from another user or an expert user. Common examples of when you would use Remote Assistance include:

1. When you are diagnosing problems that are difficult to explain or reproduce. By using Remote Assistance, you can remotely view the computer and the remote user can show you what the error is or step you through processes that caused the error to occur.
2. When an inexperienced user needs to perform a complex set of instructions. Instead of asking the inexperienced user to complete the task, you can use Remote Assistance to take control of the computer and complete the tasks yourself.

Incorrect answers:

A: You need to enable Remote Assistance to establish a Remote Desktop connection and not the Digitally sign secure channel data.

B & C: Adding your user account to the Remote Desktop Users group in the Certkiller .com domain or on Certkiller 5 is not going to work in this case. You should enable Remote Assistance on Certkiller 5.

E: This is not the solution.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, pp. 545, 553

---

**QUESTION 89**

Exhibit #1



Exhibit #2



Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Shut down system immediately if unable to log security audits	Disabled
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Devices: Unsigned driver installation behavior	Do not allow installation
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	None
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Do not display last user name	Disabled

You are the network administrator for Certkiller .com. The network originally consists of a single Windows NT 4.0 domain.

You upgrade the domain to a single Active Directory domain. All network servers now run Windows Server 2000, and all client computers run Windows XP Professional.

Your staff provides technical support to the network. They frequently establish Remote Desktop connections with a domain controller named Certkiller 1.

You hire 25 new support specialists for your staff. You use Csvde.exe to create Active Directory user accounts for all 25.

A new support specialist named Sandra reports that she cannot establish a Remote Desktop connection with Certkiller 1. She receives the message shown in the Logon Message exhibit.

You open Gpedit.msc on Certkiller 1. You see the display shown in the Security Policy exhibit.

You need to ensure that Sandra can establish Remote Desktop connections with Certkiller 1.

What should you do?

- Direct Sandra to establish a VPN connection with Certkiller 1 before she starts Remote Desktop Connection.
- Direct Sandra to set a password for her user account before she starts Remote Desktop Connection.
- In the local security policy of Certkiller 1, disable the Require strong (Windows 2000 or later) session key setting.
- In the local security policy of Certkiller 1, enable the Disable machine account password changes setting.

Answer: B

Explanation: The exhibit shows us that logons by accounts with blank passwords are limited to console logons only (this is also the default setting). The error message indicates that this is the reason that King is unable to connect with a Remote Desktop connection. We can solve this problem by instructing King to set a password for his user account before he starts a Remote Desktop Connection.

Incorrect Answers:

- It is not necessary to create a VPN connection before starting a Remote Desktop Connection.

C: This will not help. The client computer is running Windows XP Professional, which can use a strong session key.

D: This is unrelated to Remote Desktop connections.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, *Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System*, p. 574  
Lisa Donald, Suzan Sage London & James Chellis, *MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide*, Sybex Inc. Alameda, 2003, pp. 545-546

---

### **QUESTION 90**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. All domain controllers run Windows Server 2003, and all client computers run Windows XP Professional.

Certkiller acquires a subsidiary. You receive a comma delimited file that contains the names of all user accounts at the subsidiary.

You need to import these accounts into your domain.

Which command should you use?

- A. ldifde
- B. csvde
- C. ntdsutil with the authoritative restore option
- D. dsadd user

Answer: B

Explanation: The csvde (CSV Directory Exchange) command can be used to import and export Active Directory information using files formatted in the Microsoft comma-separated value (CSV), or comma delimited, format. The csvde command can also support batch operations. The csvde command only allows you to add new objects. It does not allow you to modify existing objects.

Incorrect Options:

A: The ldifde (LDIF Directory Exchange) command can be used to create, modify, and delete directory objects on Windows Server 2000, Windows Server 2003 and Windows XP Professional. You can also use ldifde to extend the schema, export Active Directory user and group information to other LDAP (Lightweight Directory Access Protocol) applications or services, and populate Active Directory with data from other directory services. The ldifde command, however, uses the LDAP Data Interchange Format (LDIF) file format, which is a draft Internet standard for a file format that may be used to perform batch operations against directories that conform to the LDAP standards.

C: The ntdsutil command is used to perform an authoritative restore of Active Directory. The ntdsutil is used to mark the restored Active Directory database as authoritative. However, in this scenario we are not restoring the Active Directory database, but importing user accounts into it from a CSV file.

D: The dsadd user command allows you to add a single user to Active Directory directory. The dsadd user command has a number of parameters that allows you to specify various attributes of the user account, such as first name, last name, password, etc. The dsadd user command, however, does not allow you to import objects into Active Directory from a CSV file.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp 300-303, 315.

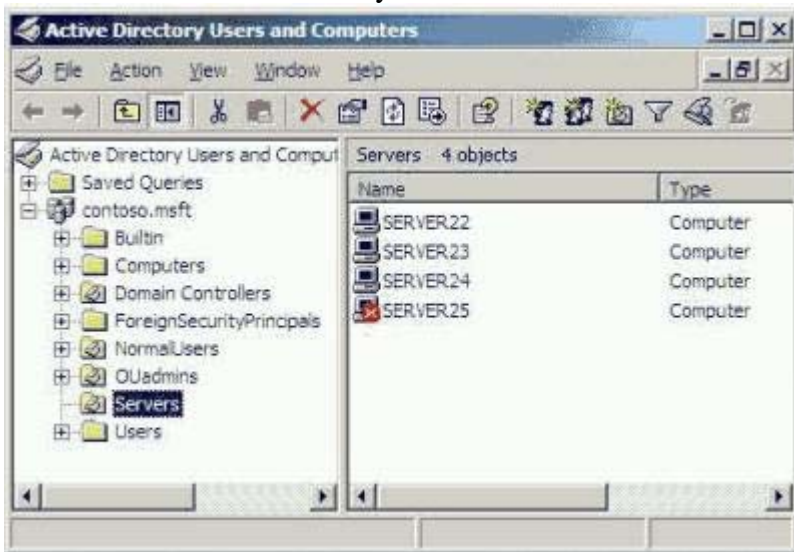
### QUESTION 91

You are the network administrator for Certkiller .com.com. All network servers run Windows server 20003, and all client computers run Windows XP Professional.

A user named King manages an application server named Server25. One morning, King tries to log on to the network from Server 25. He receives the message shown in the Logon message exhibit.



King notifies you of the problem. You open Active Directory Users and Computers and see the display shown in the Active Directory exhibit.



You need to enable King to log on to Server 25. Your solution must require the minimum amount of administrative effort.

What should you do?

- A. Enable the computer account for Server 25
- B. Reset the computer account for Server 25.
- C. Remove Server 25 from the domain, and then rejoin Server25 to the domain.
- D. Delete the computer account for Server25, and then create a new account with the same name.

Answer: A

Explanation: You need a valid user account as well as a valid computer account to be able to log on to a domain. In this case the red balloon means that Server25 account has been disabled.

Incorrect Answers:

B: The exhibit shows that the account is disabled and it thus resetting the account is not needed.

C: This would be unnecessary.

D: This will not work due to the new account having a different Security Identifier (SID) from the original computer account. Security Identifier (SID) is a unique identifier associated with a specific resource, such as a user account object or a computer.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 411

---

### **QUESTION 92**

You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain Certkiller .com. All network servers run Windows Server 2003.

Certkiller has offices in Chicago, New York and Los Angeles. Each office has one domain controller. Each office also has its own organization unit (OU), which contains all user accounts and computer accounts in that office.

The Chicago OU is accidentally deleted from Active Directory. You perform an authoritative restoration of that OU.

Some users in Chicago now report that they receive the following error message when they try to log on to the domain.

"The session setup from the computer DOMAINMEMBER failed to authenticate. The name of the account referenced is the security database in DOMAINMEMBER\$. The following error occurred: Access is denied".

How should you solve this problem?

- A. Reset the computer accounts of the computers that receive the error message.  
Instruct the affected users to restart their computers.
- B. Perform a nonauthoritative restoration of Active Directory.  
Force directory replication on all domain controllers.
- C. Restart the Kerberos Key Distribution Center service on each domain controller.
- D. Run Nltest.exe on the computers that receive the error message.  
Restart the Net Logon service on the domain controller on Chicago.

Answer: A

Explanation:

You have restored the computer accounts. The result is that you restored computer accounts have an older password to the password that the computers are currently using. The password is used for the secure channel between the client computer and the domain controller. You must reset the computer accounts to synchronize the passwords.

Incorrect Answers:

B: A nonauthoritative restoration of Active Directory will be overwritten by the existing copy of Active Directory. We need an authoritative restore of the OU.

C: The Kerberos Key Distribution Center service is irrelevant to this scenario.

D: The security channel is used by the Net Logon service on the client and on the domain controller to communicate. However, then problem doesn't lie with the Net Logon service. Furthermore, Nltest.exe can be used only to test the trust relationship between the client and the domain controller on which its machine account resides. It doesn't resolve the problem.

**QUESTION 93**

You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.

You install a new file and print server named File1. You configure standard company policies and other local options. You use third-party software to create and save an image of the server. Then you join File1 to the domain.

Six weeks later, you reapply the saved image to File1 and restart the server. You try to log on to the domain by using domain credentials. However, you are unsuccessful.

You need to log on to File1 and re-establish its domain membership. Your solution must require the minimum amount of administrative effort.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Reset the computer account for File1 in Active Directory Users and Computers.
- B. Reset the password for Administrator account by logging on locally to File1 as a member of the local Power Users group.
- C. Reinstall and reconfigure File1.
- D. Join File1 to the domain.
- E. Remove File1 from the domain.

Answer: A, D

Explanation: Resetting the password for domain controllers using this method is not allowed. Thus resetting a computer account breaks that computer's connection to the domain and requires it to rejoin the domain. This is also the quickest way.

Since the print server named File1 was joined to the domain after the image of the server was saved, it resulted in File1 not being present when the saved image was reapplied. In order to successfully log on to the domain, File1 must be added to the domain.

Incorrect answers:

B: You should be resetting the computer account for File1 and not the password for the administrator account. Although this can also be done to achieve this goal, it involves more administrative effort.

C: Reinstalling and reconfiguring File1 will result in unnecessary administrative effort.

E: Removing File1 from the domain will not make it available to all users and will inevitably amount to more administrative effort.

Reference:

Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 86-88

---

**QUESTION 94**

You are the domain administrator for Certkiller .com's Active Directory domain. All client computers run Windows XP Professional.

A user reports that she attempted to log on six times unsuccessfully. She reports that she logged on successfully yesterday. You discover that the user reset her password three days ago to comply with a new security policy that requires strong passwords.

The account policies that are applied in the Domain Security Group Policy object (GPO) as shown in the following table.

<b>Policy setting</b>	<b>Value</b>
MinimumPasswordAge	1
MaximumPasswordAge	42
MinimumPasswordLength	7
PasswordComplexity	1
PasswordHistorySize	24
LockoutBadCount	5
ResetLockoutCount	30
LockoutDuration	30

You need to ensure that the user can log on to the domain.  
What should you do?

- A. Reset the password for the computer account.
- B. Unlock the user account.
- C. In the user account properties, select the Password never expires check box for the user account.
- D. In the user account properties, select the User must change password on next logon check box for the user account.

Answer: B

Explanation: As you can see in the exhibit, the user account will be locked out if someone tries to login 5 times (LockOutBadCount).

The most common problems with user accounts are due to group membership, password problems, or account lockouts. Group membership problems manifest themselves by users not being able to access resources that are assigned through group membership. This can easily be verified and corrected via Active Directory Users and Computers or from the command line using the dsget.exe and dsmod.exe commands. Password problems are usually due to users forgetting their password and needing it reset. This can be accomplished via Active Directory Users and Computers or via the dsmod.exe command. Lastly: users often lockout their accounts due to them entering their password incorrectly. This is usually due to them forgetting their password because they just changed it recently, in which case you would need to unlock their account and reset their password. Sometimes they just cannot type or CAPS LOCK is on and they enter in their password incorrectly too many times and lock their account. User accounts can be unlocked by using Active Directory Users and Computers or by using the dsmod.exe command. The user said she attempted to log on six times, but failed. As a result the account is locked out. Therefore we can simply unlock the user account, and she can logon again.

Incorrect answers:

- A: Resetting the password for the user account does not necessarily grant log on rights to the domain. You need to unlock the account first.
- C: Modifying the properties of the account to password never expires will not affect the situation. The account must first be unlocked. Whether the password expires or not, she will still need to use a strong password once the account has been unlocked. She obviously went over the account lockout count

threshold.

D: The user's problems stems from going over the account lockout threshold too many times. Her account has to be unlocked first to be able to log on to the domain. The User must change password on next logon check box in her user account properties will not help in this case as her account has been locked out.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 317-318.

---

### **QUESTION 95**

You are the network administrator for Certkiller .com. The network consists of single Active directory domain Certkiller .com.

The domain contains a Windows Server 2003 domain controller named Certkiller 3. The securews.inf security policy has been applied to the domain. A network application requires a service account. The network application runs constantly.

You create and configure a service account named SrvAcct for the network application. The software functions properly using the new account and service.

You discover an ongoing brute force attack against the SrvAcct account. The intruder appears to be attempting a distributed attack from several Windows XP Professional domain member computers on the LAN. The account has not been compromised and you are able to stop the attack, you restart Server6 and attempt to run the network application, but the application does not respond.

- A. Reset the SrvAcct password,
- B. Configure the default Domain Controllers policy to assign the SrvAcct account the right to log on locally.
- C. Unlock the SrvAcct account.
- D. Restart the NetAppService service.

Answer: C

Explanation: Disabling the Interactive logon: Require Domain Controller authentication to unlock workstation will weaken the security configuration, but it will allow the application to run smoothly.

Incorrect Answers:

A: Resetting the password for that specific account will not work in this scenario. You want to be able to run the network application after the attack has been stopped and thus locked the account which first has to be unlocked to enable the application to run smoothly.

B: Assigning the log on locally permission to the SrvAcct account is not sufficient; you still need to unlock the account.

D: Restarting the backup application is not sufficient as the account has to be unlocked for the application to respond.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, p. 401

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 317-318.

**QUESTION 96**

You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain named Certkiller .com. The Default Domain Group Policy object (GPO) uses all default settings.

The network contains five servers running Windows Server 2003 and 800 client computers. Half of the client computers are portable computers. The other half are desktop computers. Users of portable computers often work offline, but users of desktop computers do not.

You install Windows XP Professional on all client computers with default settings. Then you configure user profiles and store them on the network.

Some users of portable computers now report that they cannot log on to their computers. Other users of portable computers do not experience this problem.

You need to ensure that all users of portable computers can log on successfully, whether they are working online or offline.

What should you do?

- A. Configure all portable computers to cache user credentials locally.
- B. Ensure that all users of portable computers log on to the network at least once before working offline.
- C. In all portable computers, rename Ntuser.dat to Ntuser.man.
- D. For all portable computers, configure the Loopback policy setting.

Answers: B

Explanation: If a user is logging on to the domain for the first time, then a profile will be created on his workstation. So the workstation has to be connected to the network for this to work. If the workstation is not connected to the network, then the user login cannot be validated and a profile will not be created. After the user has logged on to the domain and logged out again, the workstation can be disconnected from the network. The user can now log in using cached credentials. By compelling the portable users to log on to the network at least once is a logical way of finding out which of the portable users can log on successfully.

Incorrect answers:

A: This setting is default: ENABLED.

C: You can protect both local and roaming profiles from being permanently changed by users if you simply rename the ntuser.dat file to ntuser.man. By renaming this file, you have effectively made the user profile read-only, meaning that the operating system does not save any changes made to the profile when the user logs off. If you enable user profiles on Windows 9x computers, the file that stores the user settings is named user.dat instead of ntuser.dat. You can rename user.dat to user.man to make the user profile mandatory (read-only). Thus this action will create mandatory profiles meaning the profile settings cannot be changed.

D: The User Group Policy loopback processing mode policy setting is an advanced option that is intended to keep the configuration of the computer the same regardless of who logs on. This option is appropriate in certain closely managed environments, such as servers, terminal servers, classrooms, public kiosks, and reception areas. Setting the loopback processing mode policy setting applies the same user settings for any user who logs onto the computer, based on the computer.

Reference:

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4



**QUESTION 97**

You are the administrator of an Active Directory domain named Certkiller .com. A user reports that he forgot his password and cannot log on to the domain. You discover that yesterday morning the user reset his password and successfully logged on to the domain.

You need to enable the user to log on to the domain.

What should you do? (Choose two)

A. Use Active Directory Users and Computers to move the account to the default organizational unit (OU) named Users.

Instruct the user to restart his computer.

B. Use Active Directory Users and Computers to open the account properties for the user's user account.

Clear the Account is locked out check box, and select the User must change password at next logon check box.

C. Use Active Directory Users and Computers to reset the user's password.

Give the user the new password.

D. Use Computer Management to reset the password for the local Administrator account.

Give the user the new password.

Answer: B, C

Explanation: It is possible that he typed in his password several times; as a result his account is locked. Therefore we must unlock his account and reset his password since he has forgotten it.

Password problems are usually due to users forgetting their password and needing it reset. This can be accomplished via Active Directory Users and Computers or via the dsmod.exe command.

Users often happen to lockout their accounts. This is usually due to them forgetting their password because they just changed it recently, in which case you would need to unlock their account and reset their password.

Sometimes they just cannot type or CAPS LOCK is on and they enter in their password incorrectly too many times and lock their account. User accounts can be unlocked by using Active Directory Users and Computers or by using the dsmod.exe command.

Incorrect answers:

A: You would need to open the account properties to get access to the Account is locked out check box.

That is the checkbox that has to be accessed to get to the User must change password at next logon option. Moving the account to the default organizational unit (OU) named Users will not solve the problem

D: Resetting the password for the local Administrator account will not grant a user account right to log on to the domain.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 317-318.

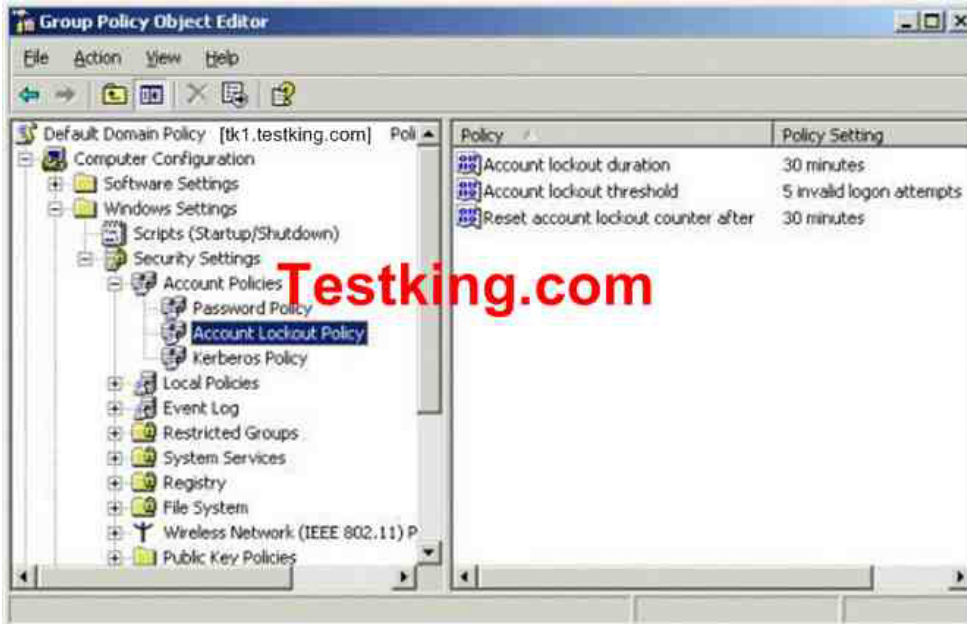
---

**QUESTION 98**

You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.

Robert's user account is located in the standard Users folder of the domain. One day, Robert tries to log on to his computer. When he enters the password he receives an error message indicating that his account is locked out. Robert cannot remember the correct password.

You examine the domain's Account Lockout Policy, which is shown in the exhibit.



You need to ensure that Robert can log on as soon as possible.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Unlock Robert's account.
- B. Increase the value for the Reset account lockout after option.
- C. Decrease the value for the Reset account lockout after option.
- D. Reset Robert's password.
- E. Increase the value for the Account lockout threshold option.
- F. Decrease the value for the Account lockout threshold option.

Answer: A, D

Explanation: Account lockout policy disables users account if an incorrect password is entered a specified number of times over a specified period. These policy settings help you to prevent attackers from guessing users' passwords, and they decrease the likelihood of successful attacks on your network. Account lockout is based on the lockout security policy, a user will be denied access, or locked out, after a predefined number of failed logon attempts. The duration of the lockout is also set in the lockout security policy. You need to enable Robert to access his account by unlocking it. And then you need to reset Robert's password to grant him the ability to log on in a speedy manner.

Robert's account will be locked out because he entered a wrong password at least five times. Therefore we need to unlock Robert's account. We can do this manually or we can wait for 30 minutes. The question states that you need to ensure that Robert can log on as soon as possible so we'll unlock the account manually.

Robert can't remember his password so we can set a new password.

Users often lockout their accounts due to entering incorrect passwords due to them forgetting their password because they just changed it recently, in which case you would need to unlock their account and reset their password. Sometimes they just cannot type or CAPS LOCK is on and they enter in their password incorrectly too many times and lock their account. User accounts can be unlocked by using Active Directory Users and Computers or by using the dsmod.exe command.

Incorrect answers:

B: Reset account lockout counter after is a security setting that determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 99,999 minutes. Thus increasing this value setting is not going to allow Robert to be able to log on as soon as possible. Manual unlocking of the account would be best suited.

C: For the same reason as option B, decreasing the value setting will not ensure Robert the ability to log on as soon as possible.

E: Account lockout threshold is a security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out. Thus increasing the threshold will not aid Robert as his account is already locked out.

F: A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out. Unlocking and resetting the user account manually will grant Robert the ability to log on as soon as possible.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 317-318

---

### **QUESTION 99**

You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.

Certkiller has 16 different office locations. Each office is a separate Active Directory site. You work in the main office.

A user named Anne works in a branch office. Every morning for one week, Anne reports that her user account is locked out. Each time, you are obliged to unlock her account. You suspect that Anne's account is being misused or attacked outside of regular business hours.

You need to investigate the cause of the account lockout.

Where should you search for security events?

- A. Only in the event log of a domain controller in your site.
- B. Only in the event logs of the domain controllers in Anne's site.
- C. In the event logs of all domain controllers in all sites.
- D. Only in the event log of Anne's computer.

Answer: C

Explanation: The Event Viewer displays event log data. There are at least three different event log files:

the application, security, and system logs. Security log - Events that affect system security are included in this event log.

These events include failed or successful logon attempts, creating, opening or deleting files, changing properties or permissions on user accounts and groups, etc.

Domain logons give users access to resources throughout the domain. Domain user accounts are stored in an Active Directory domain. Active Directory is deployed on each domain controller and domain user accounts are replicated throughout a domain.

Before a user can log on to a computer using a domain account, the computer must be joined to a domain. If the computer has access to a network connection, the user can log on to a domain provided that the user has an account in the domain's Active Directory.

The computer must transparently authenticate to the domain's Active Directory. This form of logon is called a computer logon. Both users and computers are considered equal security principals in Active Directory; to be granted access to network resources, both must be able to verify their identities.

Therefore to investigate the cause of the account lockout we must look at all eventlogs of all the domain controllers in all sites.

Incorrect answers:

A: Checking the event log of the domain controllers in your site will not yield the information that you need.

B: If Anne's account is being misused or even attacked outside of regular business hours, then you need to check the event logs of all the domain controllers in all the sites. Because it could be that the attack can be launched from outside of the office where Anne's account resides.

D: If you are to check only the event log on Anne's computer then you will not be able to see who or from where an attack has been launched on her account. Both users and computers are considered equal security principals in Active Directory; to be granted access to network resources, both must be able to verify their identities. Thus you need to check the event log of all the domain controllers in all the sites.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 760, 762.

---

### **QUESTION 100**

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows 2000 Professional.

Certkiller is organized in three departments. Each department corresponds to a separate organizational unit (OU). Computer accounts for each department reside in the corresponding OU.

Domain users report that their accounts are locked out after three unsuccessful attempts to log on. You need to increase your account lockout setting to five unsuccessful attempts to log on. You also need to ensure that you can review all unsuccessful attempts to log on to the domain or to log on locally to client computers. The new settings must be applied to a limited number of objects.

What should you do?

To answer, drag the appropriate security policy settings to the correct locations in the work area.

Security Lockout Settings  
Select from these

- Account Lockout Settings
- Audit Account Logon Events
- Audit Logon Events

Place here

- Certkiller.com
- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Users
- Marketing
- Finance
- Research

Answer:

Security Lockout Settings  
Select from these

- Account Lockout Settings
- Audit Account Logon Events
- Audit Logon Events

Place here

- Certkiller.com: Account Lockout Settings
- Domain Controllers: Audit Account Logon Events
- Marketing: Audit Logon Events
- Finance: Audit Logon Events
- Research: Audit Logon Events

Explanation:

Account Lockout Settings must always be applied at domain level. If they are applied at any other level such as an OU for example, they will not apply to domain user accounts.

Audit Account Logon Events: This is for auditing logon events for domain accounts; therefore, this policy must be applied to the domain controllers.

Audit Logon Events: This is for auditing local logon events. The Marketing, Finance and Research OUs all contain computer accounts, so we must apply this policy to all three OUs.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 317