QUESTION 201

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 member server named CK1 is located in an organizational unit (OU) named Servers. CK1 contains a folder named Contracts, which is configured to audit all the activity.
You are directed to review the audit log on Contracts. You want to identify any files that were modified during the past week by a user named Andrew. However, the audit log contains thousands of entries for the past week.
You need to view entries for Andrew's user account only.
What should you do?

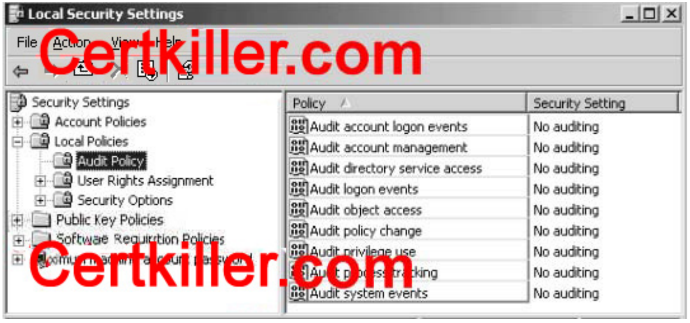
A. In Active Directory Users and Computers, open the properties for Andrew's user account. View the Auditing tab of the Advanced Security Setting dialog box for his account.
B. In Windows Explorer, open Contracts. Add the Owner column for the file pane. Search for files that list Andrew as the owner.
C. On CK1 , use WordPad to open C:\windows\system32\config\SecEvent.evt. Search for entries that contain Adrew's user account.
D. Edit the Group Policy object (GPO) for the Servers OU. Add Andrew's user account to the Generate security audits Group Policy option.
E. In Event Viewer, apply a filter to display only events that contain Andrew's user account in the User field.

Answer: E

Explanation: On the Filter tab, you can select a single entry from the drop-down list and click the Apply button to filter the events. You can also filter the events by populating the Category, Event ID, User, and Computer name fields as arguments and clicking the Apply button. The filtering feature also supports multiple filter criteria.
When a user logs on to a domain, (and auditing is enabled), the authenticating domain controller will log an event in its log. It is likely that multiple domain controllers have authenticated the user at different times; therefore, we must examine the security log on each domain controller. In event viewer, you can set various filters to simplify the search for information. In this case, we can filter the logs to show events for only the user's account.
The default auditing policy setting for domain controllers is No Auditing. This means that even if auditing is enabled in the domain, the domain controllers do not inherit auditing policy locally. If you want domain auditing policy to apply to domain controllers, you must modify this policy setting.
Finding specific logged events After you select a log in Event Viewer, you can:
• Search for events - Searches can be useful when you are viewing large logs. For example, you can search for all Warning events related to a specific application, or search for all Error events from all sources. To search for events that match a specific type, source, or category, on the View menu, click Find. The options available in the Find dialog box are described in the table about Filter options.
• Filter events - Event Viewer lists all events recorded in the selected log. To view a subset of events with specific characteristics, on the View menu, click Filter, and then, on the Filter tab, specify the criteria you want. Filtering has no effect on the actual contents of the log; it changes only the view.
All events are logged continuously, whether the filter is active or not. If you archive a log from a filtered view, all records are saved, even if you select a text format or comma-delimited text format

file.
Incorrect answers:
A: You need to open Event Viewer to be able to view these logs. The Auditing tab of the Advanced Security Setting dialog box is not in the Active Directory Users and Computers.
B: These logs can only be viewed through the Event Viewer.
C: Audit entries alone do not generate audit logs. You must also enable the Audit Object Access policy from Local Security Policy, the Domain Controller Security Policy, or a GPO.
D: Add Andrew's user account to the Generate security audits Group Policy option will not enable you to view Andrew's entries alone.
Reference:
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 231, 235

QUESTION 202



Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

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. The network contains a Windows Server 2003 computer named Certkiller 6 that functions as a file server.
Certkiller 6 contains a folder named PayrollData. Users in the payroll department report that confidential files were deleted. The manager of the payroll department asks you to enable auditing on the Payrolldata folder.
You need to configure the Local Security Policy of Certkiller 6.
Which audit policy should you configure?
To answer, select the appropriate policy in the work area.

Answer: Audit Object Access

Explanation: Audit object access shares the most important spot with the logon events audits. Because you can ask your systems to keep track of who reads, writes, deletes, or creates any file or any group of files on themselves. With object access auditing, you're able to look at the user's workstation's logs and tell exactly when the file met its maker.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering(tm)Windows(r)
Server 2003, Sybex Inc., Alameda, 2003, pp. 604-605

QUESTION 203
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 domain contains two OUs named Clients and Servers. All computer accounts for the client computers are located in the Clients OU. All computer accounts for member servers are located in the Servers OU.
Certkiller .com's written security policy requires you to configure specific permissions for the HKEY_LOCAL_MACHINE hive in the registry on all computers in the domain. The client computers and the servers required a different set of registry permissions.
You create two GPOs named RegistryPermissionsClients and RegistryPermissionsServers.
You configure each GPO with the correct registry permissions.
You need to ensure that the required registry permissions are configured on all client computers and servers in the domain.
Which three actions should you perform? Each correct answer presents part of the solution. Choose three.

A. Link both GPOs to the domain object.
B. Set a WMI filter on the RegistryPermissionsClients GPO that targets all Windows XP Professional computers.
C. Set a WMI filter on the RegistryPermissionsServers GPO that targets all Windows Server 2003 computers.
D. Place a security filter on the GPOs to only apply the GPOs to the Domain Computers group.
E. Link the RegistryPermissionsServers GPO to the Servers OU.

Answer: A, B, C

Explanation: Windows Server offers a WMI filtering option for group policies, which it didn't offer in Windows 2000. WMI filters run queries created in WMI Query Language (WQL) to determine whether or not to apply the entire policy.You can only have one WMI filter per GPO. If you use WMI filters, you'll probably end up creating more GPOs than you normally would. First you would create one or more "generic" GPOs, the ones that apply to the entire site, domain, or OU without any of the hardware or software-dependent settings. Then you would create a bunch of "mini-GPOs" that each use a WMI filter to determine whether or not to deploy. Thus in this scenario you would follow options A, B and C to ensure that the necessary registry requirements are configured on all client computers and servers in the domain.
Incorrect answers:
D: This option will not satisfy the requirements in this question.
E: This option will only apply to servers and to to the client computers.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering(tm)Windows(r)
Server 2003, Sybex Inc., Alameda, 2003, pp. 759-760

QUESTION 204
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain. The domain contains 20 Windows Server 2003 computers and 400 Windows XP Professional computers.
Software Update Services (SUS) is installed on a server named Certkiller 2.
The network security administrator wants you to ensure that the administrative password is not

compromised when an administrator connects to Certkiller 2's SUSAdmin Web site remotely by using HTTP. You want only SSL to be used to connect to the SUSAdmin Web site.
The network security administrator creates a digital certificate and enables communication for SSL on port 443 of Certkiller 2. However, administrators are still able to connect to the SUSAdmin Web site by using HTTP.
You need to ensure that communication to the SUSAdmin Web site is always secure.
What should you do?

A. Disable port 80 on the SUSAdmin Web site.
B. Require 128-Bit SSL on all directories related to the SUSAdmin Web site.
C. Change the default Web site to require 128-Bit SSL.
D. Enable IPSec on Certkiller 2 with the Request Security IPsec template.

Answer: C

Explanation: SSL works by using a combination of public and private keys. The Session or Encryption key that is used to encrypt communication with the server and the client is created according to the security certificate. The strength of the encryption applied is measured by the length of the encryption key, or in bits. The encryption strength selected would depend on the sensitivity or importance of the data. Encryption strength can be 40-Bits or 128-Bits. Requiring 128-Bit SSL on all directories related to the SUSAdmin Web site would ensure that communication to the SUSAdmin Web site is always secure. Web page encryption is implemented using the Secure Sockets Layer (SSL) protocol. This protocol uses TCP port 443. If administrators can still connect to SUSAdmin through HTTP, then you should change the setting of the default website to require 128-Bit SSL if you want only SSL to be used to connect to SUSAdmin.
Incorrect Answers:
A: Disabling port 80 will not mean that the SUSAdmin site will stay secure. TCP port 80 handles World Wide Web (WWW) service.
B: Requiring 128-bit SSL on all directories related to the USAdmin would be overkill in this situation as all you need to do is to change the default Web site to require 128-bit SSL.
D: Enabling IPSec in this situation would be irrelevant.
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, p. 968
Tony Northrup and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-299): Implementing and Administering Security in a Microsoft Windows Server 2003 Network, Chapter 11 - Deploying, Configuring, and Managing SSL Certificates

---

QUESTION 205
You are the network administrator for Certkiller .com. The network consists of a single IP subnet. All servers are Windows Server 2003. All client computers run Windows XP Professional.
The corporate firewall blocks all requests from the local client computers to port 80 in the Internet. Requests sent over port 443 are allowed through the firewall. Server computers can communicate by using port 80 are 443 to the Internet.
You need to install Software Update Services (SUS) on a computer named Certkiller 5. Certkiller 5 has limited hard drive space and stores a minimal amount of information daily. Client computers must

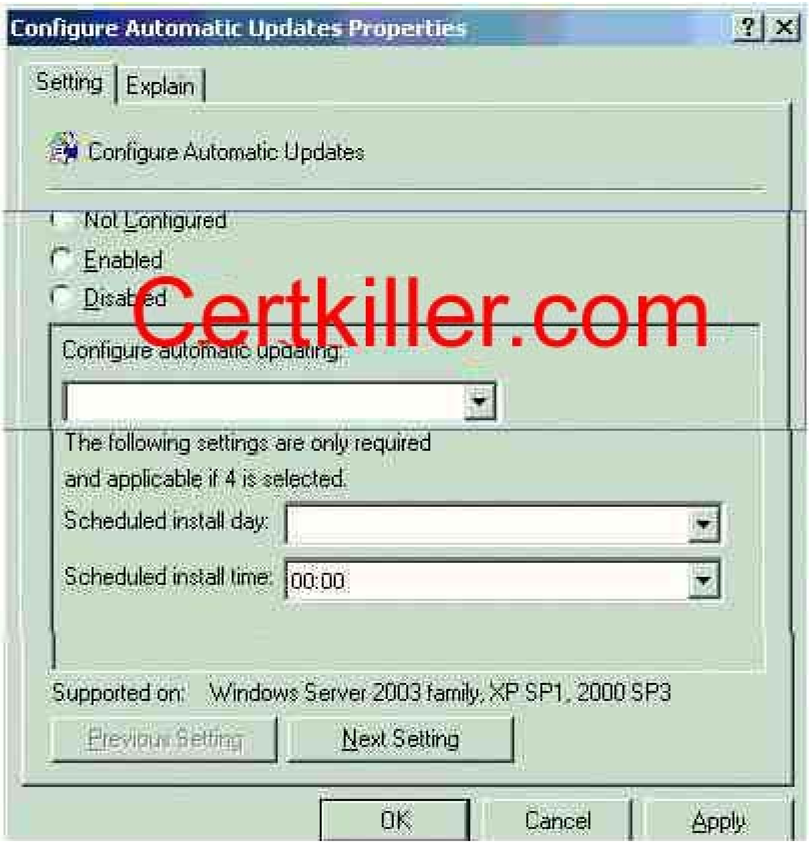
install Microsoft critical updates.
You need to ensure that Certkiller 5 does not run out of hard drive space after the installation of SUS.
What should you do?

A. On Certkiller 5, clear the selection of all locales not used on your network.
B. On Certkiller 5, select the option to maintain the updates on a Windows Update server.
C. Modify the default home page for all client computers to https://windowsupdate.microsoft.com.
D. Modify the proxy server setting for all client computers to http:// Certkiller 5.

Answer: A

Explanation: The options when selecting a storage location for updates are to maintain the updates on a Microsoft Windows Update server or to save the updates to a local folder. Each locale that is selected will increase the amount of storage space necessary to maintain updates on your server. Thus if you clear the selection of all locales not used on your network, you will prevent the SUS from using that specific hard drive space as well.
Incorrect answers:
B: The options available are to maintain the updates on a Microsoft Windows Update server or to save the updates to a local folder. However, deselecting locales after synchronization has already occurred will not free up disk space because the packages that have already been downloaded will remain on the SUS server.
C: Modifying the default home page for all client computers to https://windowsupdate.microsoft.com will not solve the problem because SUS has to be installed on Certkiller 5.
D: This problem will only be solved by clearing the selection of all locales not used on the network, not by modifying the proxy server settings for the client computers to http:// Certkiller 5.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, pp. 802-803

QUESTION 206
You are the network administrator for Certkiller .
You install and configure Software Update Services (SUS) on a Windows Server 2003 computer named Certkiller 2. You install the Automatic Updates client on all Windows XP Professional computers. All Windows XP Professional computer accounts are in the Clients organization unit (OU).
You need to configure Automatic Updates on all Windows XP Professional computers to automatically download and install updates whether users log on to their computers with administrative credentials or nonadministrative credentials. The day and time that updates are installed is not important.
What should you do?
To answer, configure the appropriate option or options in the dialog box.



Configure Automatic Updates Properties
Setting
Explain
Configure Automatic Updates

○ Not Configured
○ Enabled
○ Disabled

Configure automatic updating:

The following settings are only required and applicable if 4 is selected.

Scheduled install day:

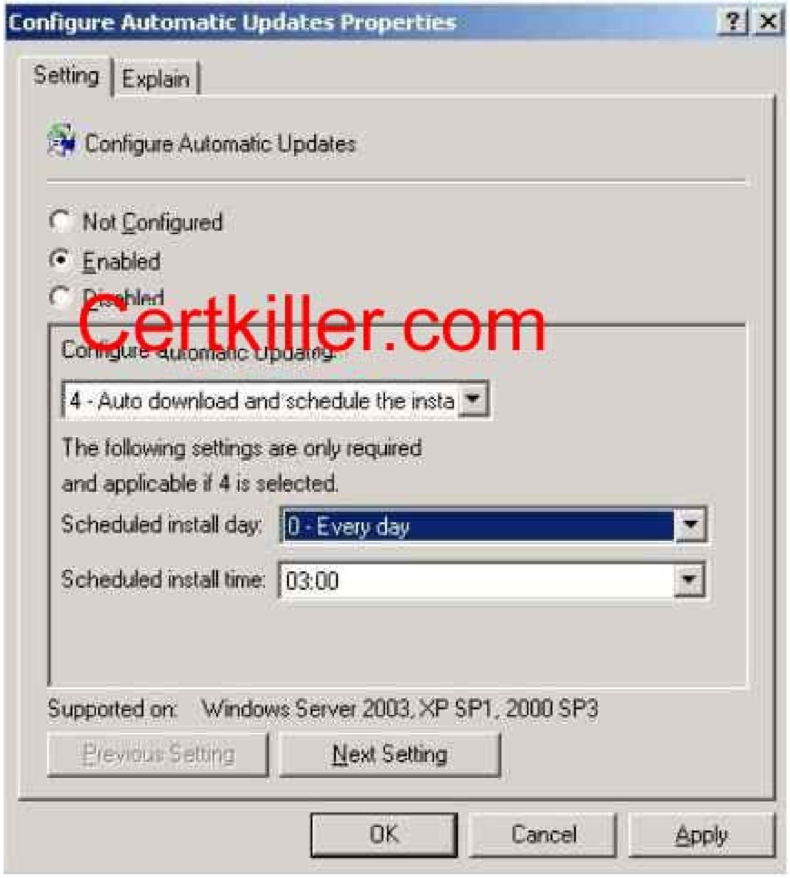
Scheduled install time: 00:00

Supported on: Windows Server 2003 family, XP SP1, 2000 SP3

Previous Setting
Next Setting
OK
Cancel
Apply

Certkiller.com

Answer:



Configure Automatic Updates

○ Not Configured

● Enabled

○ Disabled

Certkiller.com

Configure automatic updating:

4 - Auto download and schedule the insta

The following settings are only required and applicable if 4 is selected.

Scheduled install day: 0 - Every day

Scheduled install time: 03:00

Supported on: Windows Server 2003, XP SP1, 2000 SP3

QUESTION 207

The network is connected to the Internet through a Microsoft Internet Security and Acceleration (ISA) Server computer named Certkiller 4. Certkiller 4 is set to automatically configure client proxy settings.

Your supervisor tells you to install Software Update Services (SUS) on a computer named Certkiller 5. Certkiller 5 is the only SUS server on your network. SUS installation must comply with the following limitations:

- Use the least amount of disk space on Certkiller 5.
- All updates must be tested offline before being deployed to the client computers.
- The IP addressing schemes in Certkiller change often. Certkiller 5 should return its NetBIOS name when client computers connect.

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

A. Configure Certkiller 5 to maintain the updates on a Windows Update server.
B. Configure Certkiller 5 to not automatically approve new versions of previously approved updates.
C. Configure the Specify the name that your clients use to locate this update server setting to Certkiller 5.
D. Configure Certkiller 5 to not use a proxy server to access the Internet.
E. Configure Certkiller 5 to synchronize from a local SUS server.

Answer: A, B, C

Explanation: When selecting a storage location while configuring a SUS server, the options are to store the updates on a Microsoft Windows Update server or to store the updates on a local folder. When using the Microsoft Windows Update server option, you can control which updates your clients will receive. This option also leads to a reduction in the amount of free disk space needed on the Certkiller 5 SUS server. You have to use the Set Options screen to configure the Specify the name that your clients use to locate this update server setting to Certkiller 5.
Incorrect Answers:
D: A proxy server acts on behalf of the client to establish an IP connection with a remote machine. Since Certkiller 4 is set to automatically configure client proxy settings as well as being the network's connection to the Internet, this option will leave you without an Internet connection which must be used to download the updates.
E: To have Certkiller 5 synchronizing from the local SUS server is impractical since Certkiller 5 is the only SUS server in this scenario.
Reference:
Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Chapter, p. 351
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. 802-803

QUESTION 208
You are the administrator of an Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional with Service Pack 2.
You install Software Update Services (SUS) on a computer named Certkiller 1, and you approve all downloaded updates. You apply the appropriate Group Policy object (GPO) settings to configure domain computers to download critical updates from Certkiller 1.
You discover that no updates were applied since you installed SUS on Certkiller 1. You confirm that all the Windows Server 2003 computers receive updates from Certkiller 1.
You need to ensure that all client computers receive updates from Certkiller 1.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Install Service Pack 3 on all client computers.
B. Move all client computers out of the Computers contain and into a new organizational unit (OU).
C. Enable the No Override GPO setting.
D. Install the Automatic Updates client on all client computers.
E. Configure Certkiller 1 to authenticate against a proxy server to receive updates from the Windows Update servers.

Answer: A, D

Explanation: Automatic Updates can be configured on client computers to access the local SUS server in place of the Windows Update site. The client computers need the Automatic Update feature installed in order to connect to the SUS server, Certkiller 1, to download critical updates. Servers running Windows Server 2003 and client computers running Windows 2000 Service Pack 3 can be configured to automatically

receive their SUS updates.
Incorrect Answers:
B: Organizational unit containers and default containers serve the same purpose. They organize objects within a domain. Moving all client computers into a new OU will thus not ensure that all client computers receive their updates from Certkiller 1. You need to ensure that client computers have Automatic Updates installed in order to be connected to Certkiller 1.
C: The No Override GPO setting is irrelevant is this case as there is already an appropriate GPO to download updates. Furthermore the problem is that the client computers should also have Automatic Updates installed.
E: This is not necessary. All that is needed is to have Service Pack 3 and Automatic Updates installed on the client computers since Certkiller 1 is already reconfigured.
Reference:
Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Chapter 9, pp. 354, 362

QUESTION 209
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. Servers run either Windows 2000 Server or Windows Server 2003. Client computers run either Windows 2000 Professional Service Pack 2 or Windows XP Professional.
You need to implement a new software update infrastructure. You discover that security patches, critical updates, and service packs have never been installed on any client computer on the network.
You install Software Update Services (SUS) on a Windows Server 2003 computer named Certkiller 5.
You must ensure that all client computers receive all Microsoft security patches, critical updates, and service packs. You want to achieve this goal as quickly as possible.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

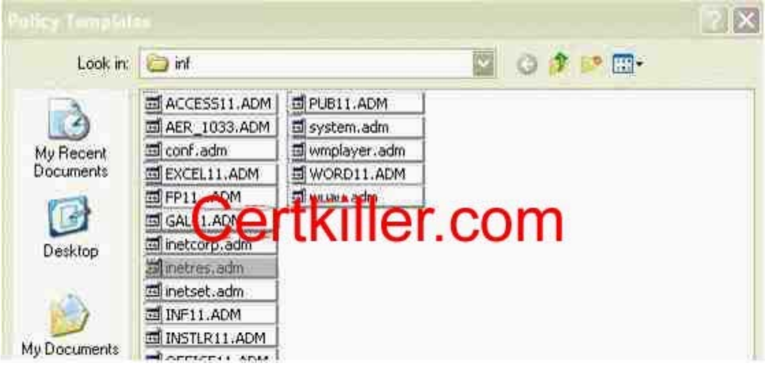
A. Install the Automatic Updates client on all Windows 2000 Professional client computers.
B. Install the Automatic Updates client on all Windows XP Professional client computers.
C. Install SUS on a Windows 2000 Server computer.
D. Modify the Windows Update settings of the Default Domain Controller organizational unit (OU) Group Policy object (GPO) to point client computers to http:// Certkiller 5.
E. Modify the Windows Update settings of the Default Domain Policy Group Policy object (GPO) to point client computers to http:// Certkiller 5.
F. Upgrade all Windows 2000 Professional client computers to Windows XP Professional.

Answer: A, B, E

Explanation:
The Automatic Updates client software is necessary for some Windows 2000 and Windows XP machines to use Microsoft Software Update Services (SUS). You only need to install Automatic Updates on computers running Windows 2000 with SP2 or earlier or Windows XP without SP1. Automatic Updates is a Windows feature that notifies you when critical updates are available for your computer. This feature replaces Critical Update Notification, if it is already installed. Critical Update Notification will no longer offer critical updates. Download and install to receive notifications of critical Windows updates.

Incorrect Answers:
C: We already have SUS installed on windows 2003. That will work great.
D: We want all client computers to have the updates. Not only the domain controllers.
F: There is no need to upgrade the windows 2000 machines. The automatic Updates client will be sufficient.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 4

QUESTION 210
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 2000 Server. All client computers run Windows XP Professional.
You install Software Update Services (SUS) on a Windows Server 2003 computer named Certkiller 2. You want all client computers on the network to use Certkiller 2 to receive their software updates. You decide to modify the Default Domain Policy Group Policy object (GPO) to set Certkiller 2 as the SUS server for all computers in the domain.
When you open the Default Domain Policy GPO, you notice that there are no settings for Windows Update. You realize that you need to load an administrative template to configure SUS by using Group Policy.
You need to load the appropriate administrative template into the Group Policy Object Editor.
Which template should you load?
To answer, select the appropriate template in the dialog box in the work area.



Answer: wuau.adm

Explanation: The WUAU.adm file holds Windows Update settings for Windows 2000 and Windows Server 2003 clients. It describes the new policy settings for the Automatic Updates client, and is automatically installed into the %windir%\inf folder when installing Automatic Updates. You should Load WUAU.adm as an administrative template in the Group Policy Object Editor.
Reference:
Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Chapter 9, p. 364

QUESTION 211
You are the network administrator for Certkiller . The network consists of a single Active directory domain named Certkiller .com. The domain contains 20 Windows Server 2003 computers and 5,000 Windows XP Professional computers. All client computer accounts are in the Clients organizational

unit (OU).
The client computers do not have any service packs installed.
You install and configure Software Update Services (SUS) on a server named Certkiller 4. All client computers must download security updates from Certkiller 4.
You need to prepare the client computers so they can connect to Certkiller 4 to download Windows security updates.
What should you do?

A. Create a logon script that connects to the Windows Update Catalog Web site, scans for available security updates, and downloads security updates to the client computes,
B. Install the automatic Updates client on all client computers. Configure the client computers to use Automatic Updates to connect to Certkiller 4.
C. Create a new Group Policy object (GPO) and link it to the clients OU. Configure the GPO to create a software package that assigns security updates from Certkiller 4 to the client computers.
D. Add http:// Certkiller 4 as the value for WUStatusServer registry entries on all client computers.

Answer: B

Explanation: A local administrator can use the Automatic Updates applet in the Control Panel to configure Automatic Update or to modify the settings. If Group Policy has been configured for Automatic Updates, it will override the local settings.
With Automatic Updates installed and configured on the client computers, security updates can be automatically downloaded from Certkiller 4. Once the client computers are configured, Windows Server 2003 will automatically search for any Windows security updates for your client computers from the Windows Update website and download these via Background Intelligent Transfer Services (BITS).
Incorrect Answers:
A: To prepare the client computers to be able to receive updates you need to install the Automatic Updates client on them and not create log on scripts as if the client computers have already been installed.
C: Linking GPOs to the clients as described in this option is not preparing them to receive updates from Certkiller 4.
D: UseWUServer - Set this to 1 to enable Automatic Updates to use the server running Software Update Services as specified in WUServer and sets the s Sets the SUS server as well as the SUS statistics server by HTTP name thus this option will not work.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Study Guide and DVD Training System, p. 81

QUESTION 212
You are the network administrator for Certkiller . The network consists of a single Active Directory domain Certkiller .com. The domain contains 25 Windows server 2003 computers and 5,000 Windows 2000 Professional computers.
You install and configure Software Update Services (SUS) on a server named Certkiller Srv. All client computer accounts are in the Clients organizational unit (OU). You create a Group Policy object (GPO) named SUSupdates and link it to the Clients OU. You configure the SUSupdates GPO so that client computers obtain security updates from Certkiller Srv.

Three days later, you examine the Windowsupdate.log file on several client computers and discover that they have downloaded Windows security updates from only windowsupdate.microsoft.com.
You need to configure all client computers to download Windows security updates from Certkiller Srv.
What should you do?

A. Open the SUSupdates GPO and configure the Configure Automatic Update policy to assign the Auto download and notify for install setting for Windows security updates.
B. Open the SUSupdates GPO and configure the Configure Automatic Update policy to assign the Auto download and schedule the install setting for Windows security updates.
C. Create software distribution policy for the SUSupdates GPO that assigns the package WUAU22.msi to all client computers.
Restart all client computers.
D. On all client computers, configure the UseWUServer registry value to enable Automatic Updates to use Certkiller Srv.

Answer: D

Explanation: The Windows 2000 clients aren't able to use the GPO setting that configures which server they should receive their updates from. You can import a template file to correct this problem, but that isn't listed as an answer. The only answer that will work is to edit the registry of the client computers to configure them to receive their updates from Certkiller Srv.
Incorrect Answers:
A: This won't affect which server the clients download the updates from.
B: This won't affect which server the clients download the updates from.
C: WUAU22.msi is the automatic updates client software. The clients in this case already have this installed (it comes as part of Windows 2000 Service Pack 3).
Reference: http://www.jsiinc.com/SUBL/tip5800/rh5809.htm

QUESTION 213
You are the domain administrator for Certkiller 's Active Directory domain named Certkiller .com. All client computers run Windows XP Professional.
You need to implement a solution for managing security updates on client computers. You plan to use a Windows Server 2003 computer to manage security updates. Your solution for managing security updates must meet the following requirements:
• You must not purchase additional software or licences.
• Security updates must be installed automatically.
• You must be able to control which updates are available to install.
• Security updates must synchronize automatically with the latest updates offered by Microsoft.
You need to implement a solution for managing security updates that meets the requirements.
What should you do?

A. Publish the security updates by using a Group Policy object (GPO).
Assign the GPO to the client computers that require updates-
B. Install Software Update Services (SUS).
Configure the SUS software to synchronize daily with Microsoft.
Use Group Policy to configure the appropriate Windows Update settings on the client computers.

C. Install Microsoft Internet Security and Acceleration (ISA) Server on a Windows Server 2003 computer.
D. Create a process to run Windows Update on all client computers.

Answer: B

Explanation: You can use Software Update Services to download all critical updates to servers and clients as soon as they are posted to the Windows Update Web site.
You install the server component of Software Update Services on a server running Windows 2000 Server, Windows XP, or Windows Server 2003 inside your corporate firewall.
A corporate service allows your internal server to synchronize content with the Windows Update Web site whenever critical updates for Windows are available.
The synchronization can be automatic or the administrator can perform it manually.
By synchronizing with the Windows Update Web site, your internal server that is running Software Update Services can pull the update packages and store them until an administrator decides which ones to publish. Then, all the clients that are configured to use the server running Software Update Services will install those updates.
You can control which server each client computer connects to and then schedule when the client performs all installations of critical updates either manually by means of the registry or by using Group Policy from the Active Directory directory service.
Incorrect answers:
A: Assigning a GPO to update all client computers that require updates does not necessarily mean that the updating will be synchronized.
C: Installing ISA is more of a heavy duty firewall protection measure.
D: Creating a process to run Windows Update on all client computers will not meet all requirements.
Reference:
Michael Cross, Jeffery
A. Martin and Todd
A. Walls, MCSE Exam 70-294: Planning, Implementing, and
Maintaining a Windows Server 2003 Active Directory Infrastructure Study Guide & DVD Training System, p 698.

QUESTION 214
You are the network administrator for Certkiller . Your network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all 200 client computers run Windows XP Professional.
Software Update Services (SUS) is installed with default settings on a server named Certkiller 5.
You discover that a critical security update for Internet Explorer is not installed on any client computer. You verify that the update was downloaded from the Internet to Certkiller 5. You also verify that more recent security updates are installed.
You need to investigate the cause of this problem. You will use the SUS administration console on Certkiller 5.
Which data should you evaluate? (Choose two)

A. The security update in the synchronization log.
B. The security update in the approval log.

C. The status of Internet Explorer 5.5x in the Monitor Server window.
D. The status of Internet Explorer 6.x in the Monitor Server window.

Answer: A, B

Explanation:
A synchronization log is maintained on each server running SUS to keep track of the content synchronizations it has performed.
This log contains the following synchronization information:

- Time that the last synchronization was performed.
- Success and Failure notification information for the overall synchronization operation.
- Time of the next synchronization if scheduled synchronization is enabled.
- The update packages that have been downloaded and/or updated since the last synchronization.
- The update packages that failed synchronization.
- The type of synchronization that was performed (Manual or Automatic).

The log can be accessed from the navigation pane of the administrator's SUS user interface.
You can also access this file directly using any text editor.
An approval log is maintained on each server running SUS to keep track of the content that has been approved or not approved. This log contains the following information:

- A record of each time the list of approved packages was changed.
- The list of items that changed.
- The new list of approved items.
- A record of who made this change; that is, the server administrator or the synchronization service.

The log can be accessed from the navigation pane in the administrative user interface.
You can also access this file directly using any text editor.

QUESTION 215
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, and all client computer objects are store din the Clients organizational unit (OU). Client computers receive critical security patches from servers at Microsoft.
A server named Certkiller 1 runs Software Update Services (SUS). You enable Certkiller 1 to obtain and store security patches for distribution on the internal network.
Now you need to ensure that all client computers receive future security patches from Certkiller 1 only.
You open the Group Policy object (GPO) for the Clients OU.
Which setting should you configure?

A. Computer Configuration\Software Settings\Software Installation
B. User Configuration\Software Settings\Software Installation
C. Computer Configuration\Administrative Templates\Windows Components\Windows Installer
D. User Configuration\Administrative Templates\Windows Components\Windows Installer
E. Computer Configuration\Administrative Templates\Windows Components\Windows Update
F. User Configuration\Administrative Templates\Windows Components\Windows Update
Answers: E

Explanation: Group Policy settings - Automatic Updates clients can be configured to synchronize from an SUS server rather than the Windows Update servers by modifying the clients' registries or, more efficiently, by configuring Windows Update policies in a Group Policy Object (GPO).
Reference:
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 9: 4.

QUESTION 216
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.
The information technology (IT) department recently installed Software Update Services (SUS) to manage security updates. The server that runs SUS is configured to synchronize automatically every day at 7:00 A.M. New critical updates were released today at 9:00 A.M.
You need to manually update the SUS server.
What action should you take?

A. Log on to the SUS server. Download the new security updates from Windows Update.
B. Download the new security updates from Windows Update to your local computer. Copy and paste the updates on the SUS server.
C. On the SUS home page, synchronize the server.
D. Log on to the SUS server. Run Wupdmgr.exe by using the appropriate command to manually synchronize the server.

Answer: C

Explanation: An SUS server can retrieve software updates directly from Microsoft, or it can retrieve them from another SUS server. To have the SUS server retrieve updates from Microsoft, select Synchronize Directly from the Microsoft Windows Update Servers. To have the SUS server retrieve updates from another SUS server, select Synchronize from a Local Software Update Services Server and specify the name of the server.
An administrator can also change how the SUS server handles updated content. This enables you to specify what the SUS server should do when software packages that are previously approved are updated. You can select from two options:
- Automatically Approve New Versions of Previously Approved Updates.
- Do Not Automatically Approve New Versions of Previously Approved Updates. I Will Manually Approve These Later.

Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 4

QUESTION 217
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. All client computers run Windows XP Professional.
CK1 is your global catalog server. CK2 runs Software Update Services (SUS). The Set Options

console on CK2 uses all default settings. You configure the client computers to access the service on CK1 and CK2 .
Three months later, Microsoft releases a critical security update for Windows XP Professional. From a test client computer, you use Windows Update to download the update. You test the update and receive no error messages.
Now you need to deploy the update to all client computers as quickly as possible. You must ensure that the update is not deployed to any servers.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

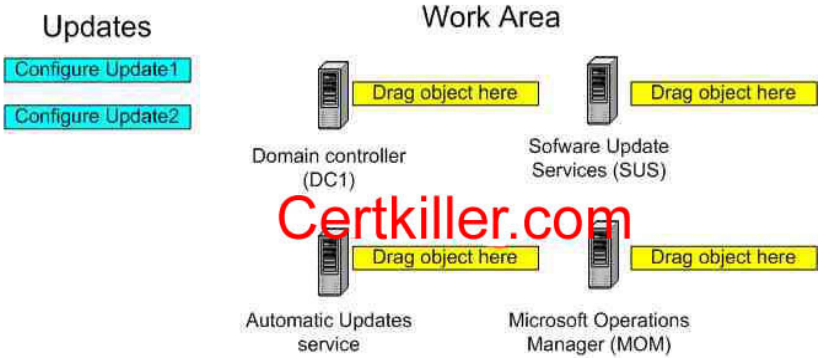
A. On CK1 , configure the Default Domain Group Policy object (GPO) to distribute the security update.
B. On CK1 , initiate replication.
C. On CK2 , initiate synchronization.
D. On CK2 , approve the security update.

Answer: C, D

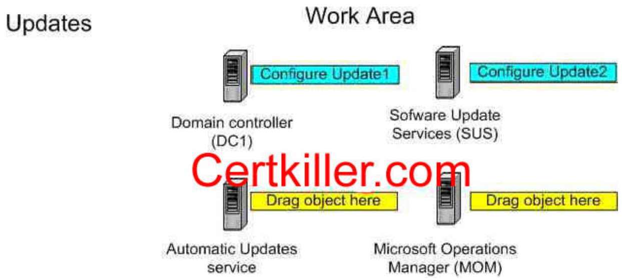
Explanation: Only approved updates can be installed on the client computers. The two main tasks that you can perform with SUS are synchronizing content and approving content. Before you can perform those actions, you need to configure your server. You can configure all of your SUS options after running Setup by using the SUS Web administration tools.
SUS is dependant on the IIS services. In this case the first step is to restart IIS services and check if all services start again. After that we will need to look for error codes generated by SUS. During synchronization, the Aucatalog1.cab file is always downloaded. As the administrator, you have the choice of whether or not to download the actual package files referenced in the metadata.
The file name for Synchronization log is named history-Sync.xml and it is stored in the <Location of SUS Website>\AutoUpdate\Administration directory.
The file name for Approval log is History-Approve.xml and it is stored in the <Location of SUS Website>\AutoUpdate\Administration directory.
SUS uses the Background Intelligent Transfer Service (BITS) to perform the download by using idle network bandwidth.
If you change your SUSconfiguration from Maintain the updates on a Microsoft Windows Update server to Save the updates to a local folder, immediately perform a synchronization to download the necessary packages to the location that you have selected.
The question mentions that the clients are configured to receive updates. When using Software Update Services to deploy security updates, the updates must be approved before they will be downloaded by the clients and installed.
References:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6

QUESTION 218
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.
Certkiller has several branch offices. One branch office contains four servers, whose roles and applications are shown in the work area. All servers except DC1 are member servers.

The same branch office contains 250 client computers. All of them run Windows XP Professional and Microsoft Office XP.
The Microsoft Windows Update Web issues two updates. Update1 is an MSI file that applies to Office XP. Update2 is a critical security update that applies to Windows XP Professional.
You need to configure the appropriate servers to deploy these updates.
What should you do?
To answer, drag the appropriate updates to the correct servers in the work area.



Answer:



Explanation: Update2 for Windows XP will be deployed with SUS services.
Update1 for Office will be deployed using a group policy from a domain controller.
Since all clients run on Windows XP and Update1 is an MSI file that applies to Office XP, the domain controller should be configured with Update1. In accordance the Software Update Services should be configured with Update2 that has a critical security update applicable to Windows XP Professional.
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. 594-595

QUESTION 219
You are the network administrator for Certkiller .com. The network contains Windows Server 2003 computers and Windows XP Professional computers.
You install Software Update Services (SUS) on a server named Certkiller Srv.
You scan the client computers to find out if any current hotfixes are installed. You notice that no client computers have been updated during the past seven days. You are unable to access the synchronization logs on Certkiller Srv.
You need to ensure that SUS is functioning properly.
What should you do on Certkiller Srv?

A. Delete the History_Approve.xml file and restart the computer.

B. Delete the Aucatalog.cab file and restart the computer.
C. Restart the Background Intelligent Transfer Service (BITS).
D. Restart all IIS-related services.

Answer: D

Explanation: SUS is dependant on the IIS services. In this case the first step is to restart IIS services and check if all services start again. After that we will need to look for error codes generated by SUS.
During synchronization, the Aucatalog1.cab file is always downloaded. As the administrator, you have the choice of whether or not to download the actual package files referenced in the metadata. The file name for Synchronization log is named history-Sync.xml and it is stored in the <Location of SUS Website>\AutoUpdate\Administration directory.
The file name for Approval log is History-Approve.xml and it is stored in the <Location of SUS Website>\AutoUpdate\Administration directory. SUS uses the Background Intelligent Transfer Service (BITS) to perform the download by using idle network bandwidth.
Incorrect answers:
A: Deleting the History-Approve.xml file and restarting the computer will not ensure that SUS functions properly as it is the file for the Approval log only. This on its own is not enough.
B: The Aucatalog1.cab file is always downloaded during synchronization only. This is but one aspect of SUS.
C: Restarting the Background Intelligent Transfer Service (BITS) is not going to ensure that SUS functions properly because it is only used to perform download using idle network bandwidth. What is needed is to restart all IIS-related services.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6

QUESTION 220
You are the network administrator for Certkiller .com. The company has a main office at Toronto and several branch offices in North America. You work in Toronto.
The network contains Windows Server 2003 computers and Windows XP Professional computers.
A user named Jack works in a branch office. She reports that her client computers cannot connect to a remote VPN server. You suspect that her client computer did not receive a recent hotfix.
You need to verify which hotfixes are installed on Jack's computer.
What should you do?

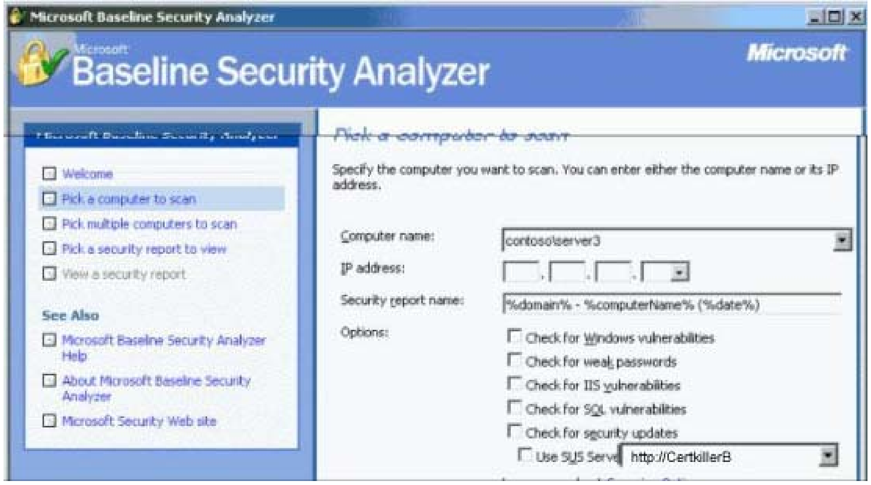
A. From a command prompt, run the update.exe command.
B. From a command prompt, run the wmic qfe command.
C. View the History-synch.xml file.
D. View the History-apprive.xml file.

Answer: B

Explanation: WMIC extends WMI for operation from several command-line interfaces and through batch scripts.
Incorrect answers:

A: Running the update.exe command installs hotfixes; it will not allow you to see which hotfixes has already been installed.
C: Viewing the History-synch.xml file does not necessarily synchronize the server and have connecting ability with the VPN server. It just gives you the ability to view the synchronization log.
D: Viewing the History-approve.xml file will not enable Jack to connect to the VPN server. It is the approval log that you will be viewing.
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. 207

QUESTION 221
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.
The written company security policy states that unnecessary services must be disabled and that servers must have the most recent, company-approved updates. You install and configure Software Update Services (SUS) on a server named Certkiller B.
You install Windows Server 2003 Standard edition on a computer named Certkiller
A. Certkiller A is
used only as a file and print server. Certkiller A has two local user accounts, and the administrator account has been renamed.
You need to find out whether Certkiller A is running unnecessary services and whether it has all available approved security updates. To reduce the amount of network bandwidth and time requirements, you need to scan for only the required information.

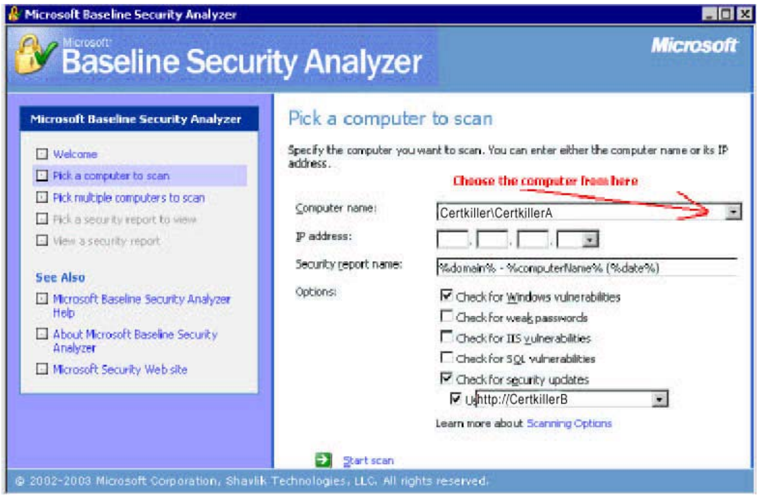

Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site

Pick a computer to scan

Specify the computer you want to scan. You can enter either the computer name or its IP address.

Computer name: contoso\server3
IP address: . . .
Security report name: %domain% - %computerName% (%date%)
Options:
☐ Check for Windows vulnerabilities
☐ Check for weak passwords
☐ Check for IIS vulnerabilities
☐ Check for SQL vulnerabilities
☐ Check for security updates
☐ Use SUS Serve http://CertkillerB

Answer:
Check for windows vulnerabilities
Check for security updates
If you have this option to select Check Use SUS service and select server http:// Certkiller B


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Start scan
© 2002-2003 Microsoft Corporation, Shavlik Technologies, LLC. All rights reserved.

Pick a computer to scan

Specify the computer you want to scan. You can enter either the computer name or its IP address.

Choose the computer from here

Computer name: Certkiller\CertkillerA

IP address:

Security report name: %domain% - %computerName% (%date%)

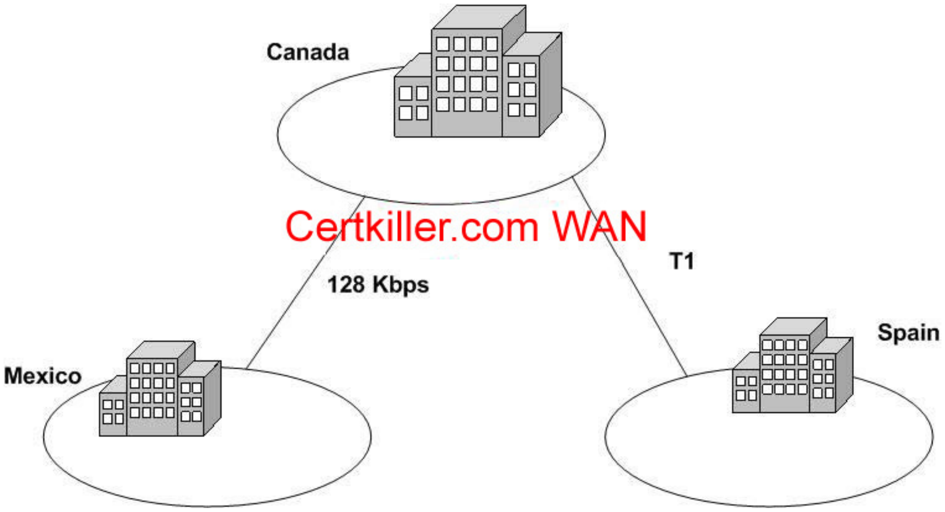
Options:

☑ Check for Windows vulnerabilities
☐ Check for weak passwords
☐ Check for IIS vulnerabilities
☐ Check for SQL vulnerabilities
☑ Check for security updates
☑ U http://CertkillerB

Learn more about Scanning Options

They give to you three options on this combo box and also in computer name combo box
Select box Check for Unnecessary Services
Windows checks
Check for missing security updates and service packs
Check for account password expiration
Check for file system type on hard drives
Check if autologon feature is enabled
Check if the Guest account is enabled
Check the RestrictAnonymous registry key settings
Check the number of local Administrator accounts
Check for blank and/or simple local user account passwords
Check if unnecessary services are running
List the shares present on the computer
Check if auditing is enabled
Check the Windows version running on the scanned computer
Select box Security Updates Scan - By default, a security update scan executed from the MBSA GUI or from mbsacli.exe (MBSA-style scan) will scan and report missing updates marked as critical security updates in Windows Update (WU), also referred to as "baseline" critical security updates. When a security update scan is executed from mbsacli.exe using the /hf switch (HFNetChk-style scan), all security-related security updates will be scanned and reported on. A user running an HFNetChk-style scan would have to use the -b option to scan only for WU critical security updates. When the SUS option is chosen, all security updates marked as approved by the SUS Administrator, including updates that have been superseded, will be scanned and reported by MBSA.
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. 230, 244

QUESTION 222
You are the network administrator for Certkiller .com. Certkiller has offices in three countries. The network contains Windows Server 2003 computers and Windows XP Professional computers. The network is configured as shown in the exhibit.



Software Update Services (SUS) is installed on one server in each office. Each SUS server is configured to synchronize by using the default settings.
Because bandwidth at each office is limited, you want to ensure that updates require the minimum amount of time.
What should you do?

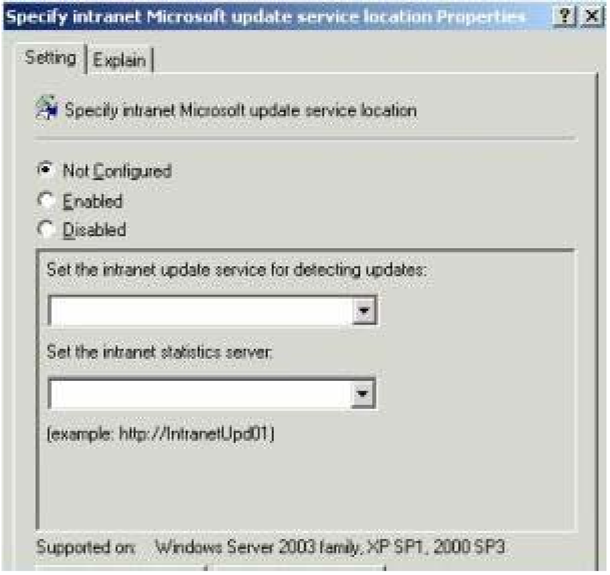
A. Synchronize the updates with an SUS server at another office.
B. Select only the locales that are needed.
C. Configure Background Intelligent Transfer Service (BITS) to limit file transfer size to 9 MB.
D. Configure Background Intelligent Transfer Service (BITS) to delete incomplete jobs after 20 minutes.

Answer: B

Explanation: When you configure SUS, you can select multiple languages for the updates according to your locale. In this scenario, we can reduce the bandwidth used by the synchronization by selecting only the required locales. This will avoid downloading and synchronizing multiple copies of the same updates, but in different languages.
Incorrect Answers:
A: This will not reduce the size of the updates or minimize bandwidth usage.
C: The updates may be more than 9MB, so we shouldn't limit the transfer size.
D: This will not reduce the size of the updates or minimize bandwidth usage.
References:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6

QUESTION 223
You are the network administrator for Certkiller .com. The network contains Windows Server 2003 computers and Windows XP Professional computers.
You install Software Update Services on a server named Certkiller
A. You create a new Group Policy
object (GPO) at the domain level.
You need to properly configure the GPO so that all computers receive their updates from Certkiller A.

How should you configure the GPO?
To answer, configure the appropriate option or options in the dialog box.



Specify intranet Microsoft update service location Properties

Specify intranet Microsoft update service location

● Not Configured
○ Enabled
○ Disabled

Set the intranet update service for detecting updates:

Set the intranet statistics server:

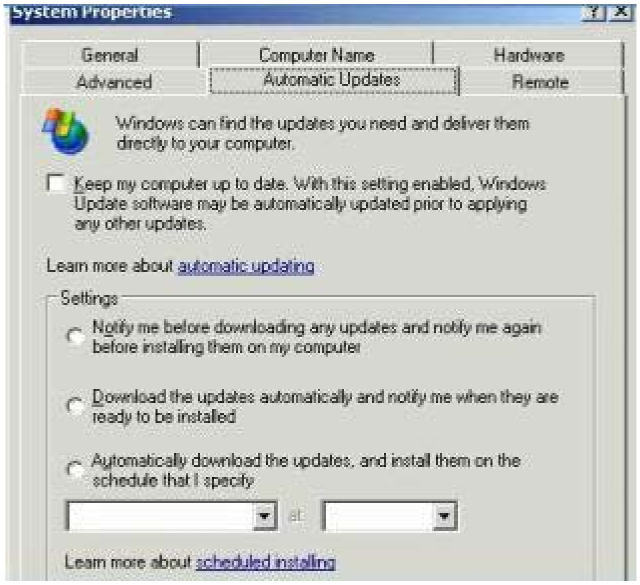
(example: http://IntranetUpd01)

Supported on: Windows Server 2003 family, XP SP1, 2000 SP3

Answer: Select the "Enabled" radio button. In the "Set the intranet update service for detecting updates" box, enter the name of the server; in this case you would enter http:// Certkiller
A. You should also enter
http:// Certkiller A as the address of the intranet statistics server.

Explanation: Since the Software Update Services has been installed on Certkiller A, the group policy object on the domain should enable the intranet update services to detect and set from Certkiller A.
References:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Que Publishing, Indianapolis, 2003, Chapter 6

QUESTION 224
You are the network administrator for Certkiller .com. The network contains Windows Server 2003 computers and Windows XP Professional computers. You are configuring Automatic Update on the servers.
The written company network security policy states that all updates must be reviewed and approved before they are installed. All updates are received from the Microsoft Windows Update servers.
You want to automate the updates as much as possible.
What should you do?
To answer, configure the appropriate option or options in the dialog box.



Windows can find the updates you need and deliver them directly to your computer.

□ Keep my computer up to date. With this setting enabled, Windows Update software may be automatically updated prior to applying any other updates.

Learn more about automatic updating

Settings

○ Notify me before downloading any updates and notify me again before installing them on my computer

○ Download the updates automatically and notify me when they are ready to be installed

○ Automatically download the updates, and install them on the schedule that I specify

at

Learn more about scheduled installing

Answer: Check the "Keep my computer up to date" checkbox. Select the "Download the updates automatically and notify me when they are ready to be installed" radio button.

Explanation: The updates will be automatically downloaded, but you will be able to review the updates before they are installed.
References:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6

QUESTION 225
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 20003, and all client computers run Windows XP Professional.
A member server named Certkiller SrvA runs Software Update Services (SUS). Certkiller SrvA is configured to synchronize directly from the Microsoft Windows Update servers every day.
All client computers are configured to use the Automatic Updates client software to receive updates from Certkiller Srv
A. All client computers are located in an organizational unit (OU) named Clients.
Microsoft releases a critical security update for Windows XP Professional computers. Server1 receives the update.
Client computers on the network do not receive this update. However, they receive other updates from Certkiller SrvA.
You need to ensure that all client computers receive the critical security update.
What should you do?

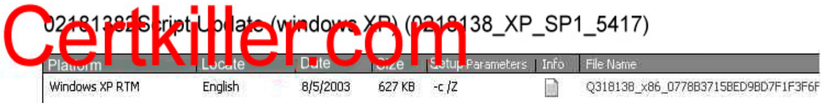
A. In the System Properties dialog box on each client computer, enable the Keep my computer up to date option.
B. Edit the Group Policy object (GPO) for the Clients OU by enabling the Reschedule Automatic Updates scheduled installations settings.
C. On Server1, open the SUS content folder.

Select the file that contains the security update, and assign the Allow - Read permissions on the file to all client computer accounts.
D. Use Internet Explorer to connect to the SUS administration page.
Approve the security update.

Answer: D

Explanation: The question states that the clients are configured to receive updates. When using Software Update Services to deploy security updates, the updates must be approved before they will be downloaded by the clients and installed.
Incorrect Answers:
A: The question states that the clients are configured to receive updates; therefore, this option is already set.
B: The Reschedule Automatic Updates scheduled installations setting means that a computer will re-run the update process if the computer was offline at the time of the last scheduled update.
C: This is not a permissions problem. The update must be approved before it can be installed.
References:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapters 2 & 6

QUESTION 226
Exhibit


Certkiller.com

Q318138: Script Update (windows XP) (Q318138_XP_SP1_5417)

Platform	Locate	Date	Size	Setup Parameters	Info	File Name
Windows XP RTM	English	8/5/2003	627 KB	-c /Z	📄	Q318138_x86_0778B3715BED9BD7F1F3F6F

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.
A new low-priority update is released and is synchronized with the Software Update Services (SUS) server on the network. You decide to approve the update without testing.
After the update is applied to client computers, users report that they can no longer runt their account application. On the SUS server, you view the details of the update as shown in the exhibit.
You need to remote the update from all client computers until you can test the update.
What should you do?

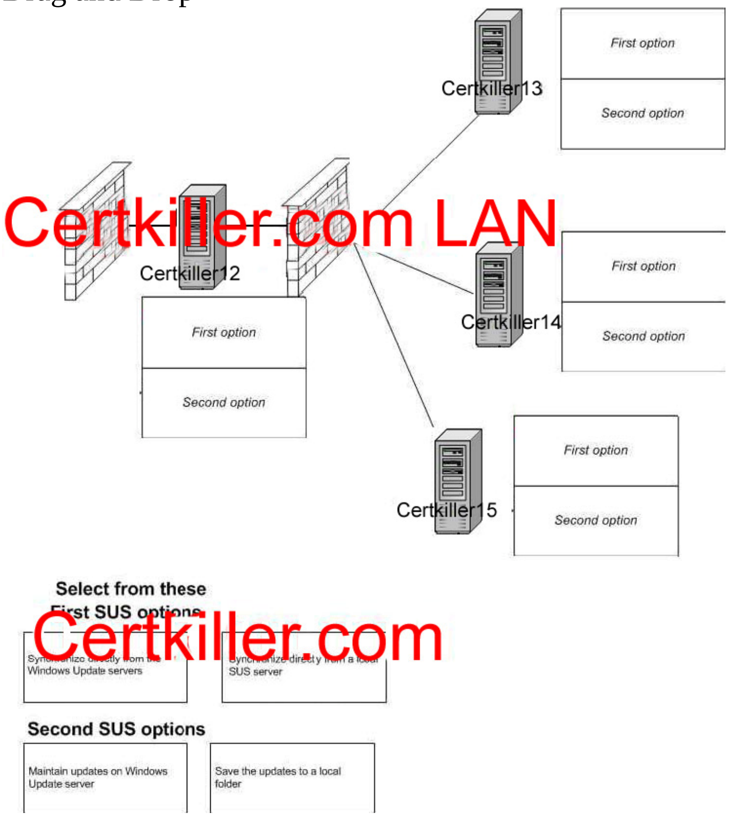
A. Clear the Automatically approve new versions of previously approved updates option on the SUS server.
B. Clear the update for approval on the SUS server, and the resynchronize the server with the Windows Update servers.
C. Run the spuninst command from Systemroot\$NtUninstallQ318138$\spuninst directory on each client computer.
D. Delete the Systemroot\$NtUninstallQ318138£ directory on each client computer.

Answer: C

Explanation: This command will remove the update from all the client computers as this is what is necessary in this scenario.

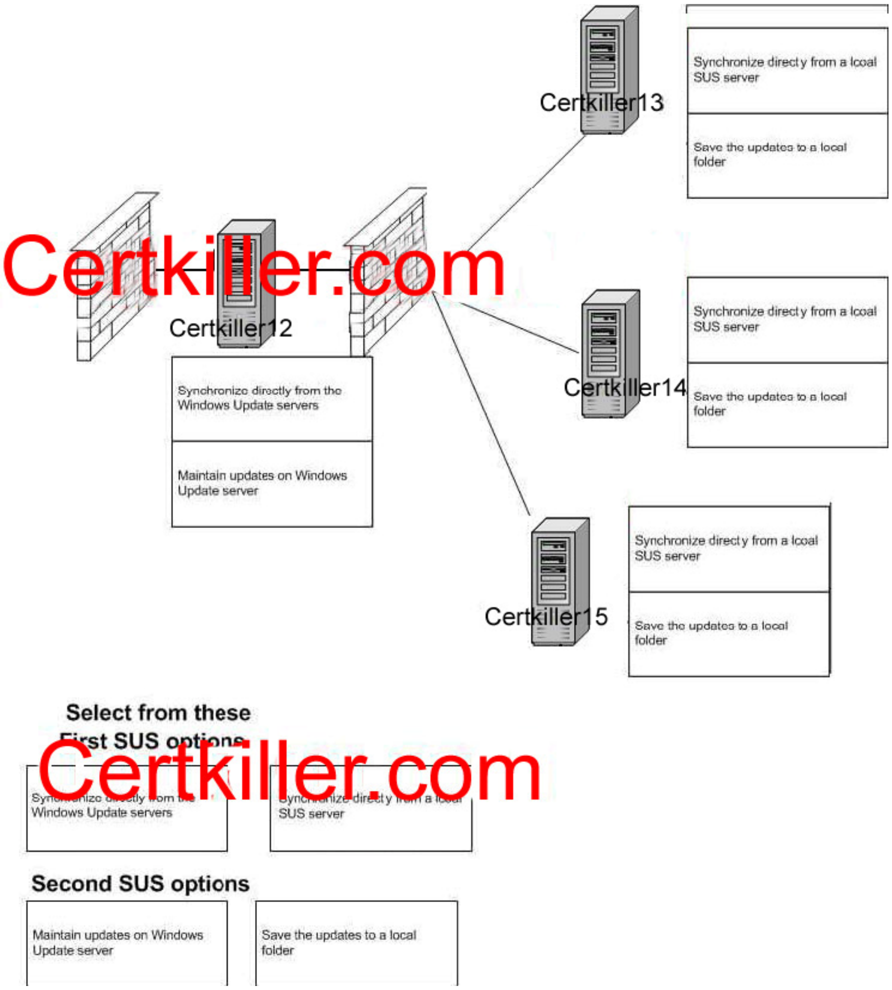
Incorrect answers:
A: This option in the light of this specific scenario is reactionary and the damage is already done. Clearing the Automatically approve new versions of previously approved updates option will not help.
B: You cannot clear an update for approval if it was already applied to the server as well as the client computers, what you need to do is to uninstall it.
D: This option will not help as the update has to be uninstalled since it was already applied to the client computers and the server.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure: Study Guide & DVD Training System, pp. 811-816

QUESTION 227
You are the network administrator for Certkiller .com. The network contains 25 servers and 1,000 client computers.
The network architect has designed a software update infrastructure. You need to configure the software update infrastructure. The configuration must meet the following requirements:
• Client computers must receive critical updates from a Software Update Services (SuS) server.
• Three SUS servers must be available for critical updates.
• Only servers in the perimeter network must be able to connect to the Internet.
• Client computers must not be able to connect to servers in the perimeter network.
You install SUS on four servers on the network.
Which configuration should you apply to the four SUS servers?
Drag and Drop



Certkiller.com LAN
Certkiller.com

Answer:


Certkiller13
Synchronize directy from a lcoal SUS server
Save the updates to a local folder
Certkiller.com
Certkiller12
Synchronize directly from the Windows Update servers
Maintain updates on Windows Update server
Certkiller14
Synchronize directy from a lcoal SUS server
Save the updates to a local folder
Certkiller15
Synchronize directy from a lcoal SUS server
Save the updates to a local folder
Select from these
First SUS options
Certkiller.com
Synchronize directly from the Windows Update servers
Synchronize directy from a lcoal SUS server
Second SUS options
Maintain updates on Windows Update server
Save the updates to a local folder

Explanation: By default, SUS server synchronization is not defined. You can manually synchronize your server with the Windows Update server or you can set a synchronization schedule to automate the process. If you want to meet the stated requirements then you should have only Certkiller 12 synchronize directly from the Windows Update Service and maintain the updates on Windows Update server since it is the server that is firewall protected and connected to the Internet from whence it gets its updates. Certkiller 13, -14 and -15 should be configured to synchronize directly from the local SUS server and to save the updates to a local folder.

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. 60-68

QUESTION 228

You are the network administrator for Certkiller . 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.

You install Software Update Services (SUS) on a network server named Certkiller 1. When you attempt to synchronize Certkiller 1 with the Windows Update servers, you receive an error message. You suspect that your proxy server requires authentication. You open Internet Explorer and verify that

you can communicate with an external Web site by using the proxy server.
You need to ensure that Certkiller 1 can communicate with the Windows Update servers.
What should you do on Certkiller 1?

A. Restart the IIS administration tool.
B. Configure the Internet Explorer settings to bypass the proxy server.
C. In the SUS options, configure authentication to the proxy server.
D. Install the Microsoft Firewall Client.

Answer: C

Explanation: If you are running Windows Server 2003 as a proxy server so your internal clients can surf the Web, or if you're running it as an e-mail server, dial-up connections to the Internet are an option worth looking into.
Incorrect answers:
A: Internet Information Services (IIS) is software that serves Internet higher-level protocols such as HTTP and FTP to clients using web browsers. The IIS software that is installed on a Windows Server 2003 computer is a fully functional web server and is designed to support heavy Internet usage. But this is not the issue here.
B: It is not necessary to bypass the proxy server.
D: SUS is used to deploy a limited version of Windows Update to a corporate server, which in turn provides the Windows updates to client computers within the corporate network. This allows clients that are limited to what they can access through a firewall to still keep their Windows operating systems up-to-date. However, there is no need to install the Microsoft Firewall Client 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. 59
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering(tm)Windows(r)
Server 2003, Sybex Inc., Alameda, 2003, p. 1588

QUESTION 229
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The domain contains 15 Windows Server 2003 computers and 3,000 Windows XP Professional computers. All client computers are running the most recent service pack.
You install and configure Software Update Services (SUS) on a server named Certkiller 1. You install the Automatic Updates client on all client computers. All client computer accounts are in the Clients organization unit (OU).
Currently all client computers obtain their Windows security updates from Windows Update. You want all client computers, and no other computers, to obtain their updates from Certkiller 1.
You need to configure all client computers to obtain Windows security updates from Certkiller 1. You need to accomplish this task with the minimum amount of administrative effort.
What should you do?

A. Create a Group Policy object (GPO) named SUS and link it to the Clients OU. Open the SUS GPO and enable the Configure Automatic Update policy to automatically download updates.

B. Create a Group Policy object (GPO) named SUS and link it to the Clients OU. Open the SUS GPO and enable the Specify intranet Microsoft updates service location policy to use http:// Certkiller 1 as the value for the update and statistics server.
C. Create a Group Policy object (GPO) named SUS and link to the domain. Open the SUS GPO and enable the Specify intranet Microsoft update service location policy to use http:// Certkiller 1 as the value for the update and statistics server.
D. Create a Group Policy object (GPO) named SUS and link it to the domain. Open the SUS GPO and enable the Configure Automatic Update policy to automatically download updates.

Answer: B

Explanation: To configure which server will provide automatic updates, you should click the Next Setting button in the Configure Automatic Updates Properties dialog box. This brings up the Specify Intranet Microsoft Update Service Location Properties dialog box. The properties that can be configured through group policy are as follows: (1) The status of the intranet Microsoft update service location as not configured, enabled, or disabled, (2) The HTTP name of the server that will provide intranet service updates and (3) The HTTP name of the server that will act as the intranet SUS statistics server. Thus if you want to configure all client computers to obtain Windows security updates from Certkiller 1 with theleast amount of administrative effort, you should create an appropriate GPO anf link it to the Clients OU (all the client computers are located in this OU), and then do the proper configuration regarding the Specify intranet Microsoft updates service location.
Incorrect answers:
A: The first part of the option is correct, but you should not enable the Configure Automatic Update policy to automaticvally down load updates as this could result in the client computers not obtaining their updates from Certkiller 1.
C: This option could work but it would not be appropriate in this case as the GPO should be linked to the Clients OU and not the domain.
D: Linking the newly created GPO to the domain would be wrong in this case as well as enabling the Configure Automatic Updates policy to automatically download updates.
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. 147-149

QUESTION 230
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All client computers run either Windows 2000 Professional or Windows XP Professional. All servers run either Windows 2000 Server or Windows Server 2003. There are no service packs installed on any network computers.
You install Software Update Services (SUS) on a server named Certkiller 1.
You must ensure that all network computers can connect to Certkiller 1.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Install Windows 2000 Service Pack 3 on all Windows 2000 Server computers and Windows 2000 Professional computers. Install the Automatic Updates client on all Windows XP Professional computers.

B. Install Windows 2000 Service Pack 3 on all Windows 2000 Server computers and on all Windows 2000 Professional computers. Install Windows XP Service Pack 1 on all Windows XP Professional computers.
C. Configure the Internet browser home page for all Windows XP Professional computers to point to http://windowsupdate.microsoft.com. Install the Active Directory client on all Windows 2000 Server computers and on all Windows 2000 Professional computers.
D. Configure the Internet browser home page for all Windows 2000 Professional computers to point to http://windowsupdate.microsoft.com. Install Windows XP Service Pack 1 on all Windows XP Professional computers.
E. Upgrade all client computers to Windows XP Professional. Install Active Directory on all Windows 2000 Server computers.
F. Upgrade all client computers to Windows XP Professional. Install SUS on all Windows Server 2003 computers.

Answer: A, B

Explanation: SUS server requirements include that you should be running Windows 2000 Server with Service Pack 2 or higher or Windows Server 2003
A: For SUS to work you should also install Automatic Updates client on the Windows XP Professinal computers.
B: SUS supports Windows XP Home Edition (with Service Pack 1 or higher) and Windows XP Professional (with Service Pack 1 or higher) as client platforms.
Incorrect answers:
C & D: Configuring the Internet browser is not how SUS is installed.
E: Active Directory (AD) is a directory service available with the Windows Server 2003 platform. The Active Directory stores information in a central database and allows users to have a single user account (called a domain user account or Active Directory user account) for the network. However, this option is not the solution.
F: SUS is already installed on Certkiller 1. You would need to to install Automatic Updates client on the Windows XP Professional computers.
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. 138

QUESTION 231
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 company has offices in Berlin, Dortmund, and Frankfurt. Each office is configured as a separate IP subnet. DNS is the only method of name resolution on the network.
You need to implement a software update infrastructure on the network. You install Software Update Services (SUS) on a computer named Certkiller 3 in the Berlin office. You install on Certkiller 3 with all default settings. You have no plans to install additional SUS servers. You configure all client computers appropriately.
You must ensure that client computers can successfully connect to the SUS server.

What should you do?

A. Configure the Internet browser home page on all client computers to point to http://windowsupdate.microsoft.com.
B. In the SUS Administrator, configure the Server Name property to be the server's fully qualified domain name (FQDN).
C. Open IIS Manager and enable HTTP over SSL.
D. Enable communication over port 135 between all client computers and the SUS server.

Answer: B

Explanation: It is generally a good idea to enter FQDNs so you can control what name is submitted to the server. With the Server Name property to be the server's fully qualified domain name configured in the SUS Administrator you should be assured that client computers will successfully connect to the SUS server.
Incorrect answers:
A: This option will not ensure that client computers will connect successfully to the SUS server.
C: Enabling HTTP over SSL will not work as you would need SSL need HTTPS to access the desired client.
D: This option does not necessarily means that client computers will successfully connect to the SUS server.
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. 308

QUESTION 232
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 2000 Professional with Service Pack 4 or Windows XP Professional.
You install Software Update Services (SUS) on a computer named Certkiller 1. You create a GPO that configures all client computers to receive their software update from Certkiller 1.
One week later, you run Microsoft Baseline Security Analyzer (MBSA) on all client computers to find out whether all updates are being applied. You discover that all the Windows 2000 Professional client computer received updates, but the Windows XP Professional client computers do not receive updates.
You verify that the GPO setting was applied on all Windows XP Professional computers.
You need to ensure that the Windows XP Professional client computers receive their updates from Certkiller 1.
What should you do?

A. Make all users of the Windows XP Professional client computers members of the Administrators local group.
B. On all Windows XP Professional client computers, install Service Pack 1.
C. On all Windows XP Professional client computers, restart Automatic Updates.
D. On all Windows XP Professional client computers, delete the NoAutoUpdate value under HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU.

Answer: B

QUESTION 233

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.

Certkiller .com has 16 sales representatives, who are mobile users. All 16 mobile users are member of the Power Users local group on their computers. From 5:00 P.M. until 9:00 A.M., the sales representatives' portable computers are usually turned off and disconnected from the corporate network.

Certkiller .com's written security policy states that all portable computers that are used by the mobile sales representivatives must receive software updates from the Windows Update servers every day. User interaction with the update process must be minimized.

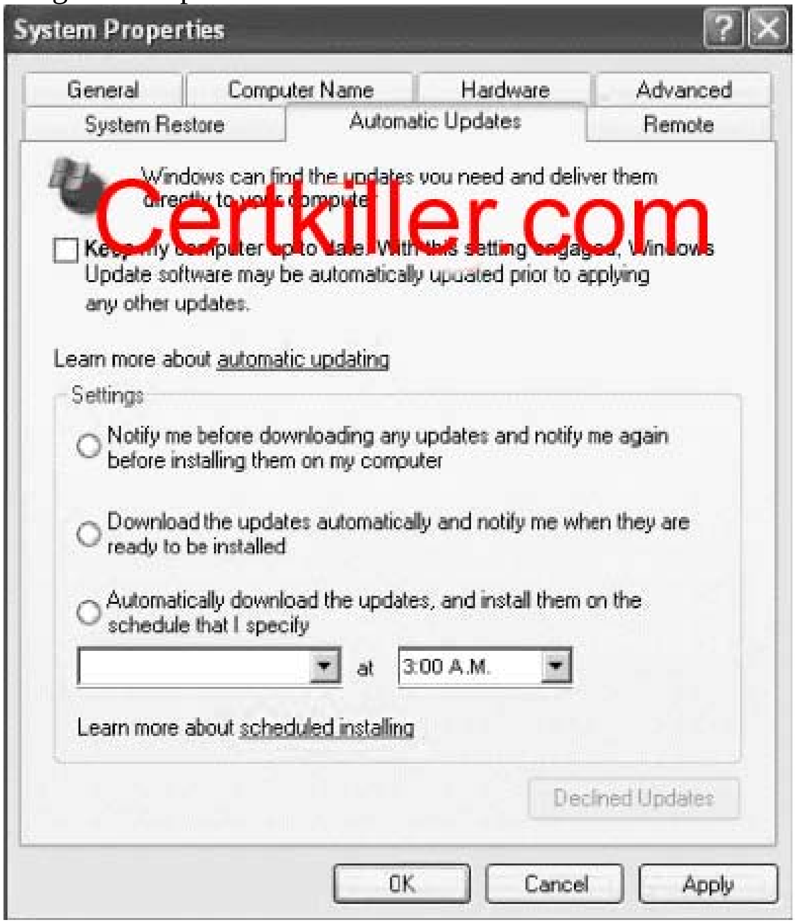
On a portable computer named Certkiller 2, you verify the recent updates and notice that updates from the Windows Update servers were not applied.

You need to ensure that software updates are applied to Certkiller 2 in compliance with the company policy.

What should you do?

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

Drag and Drop



Windows can find the updates you need and deliver them directly to your computer.

□ Keep my computer up to date. With this setting engaged, Windows Update software may be automatically updated prior to applying any other updates.

Learn more about automatic updating

Settings

○ Notify me before downloading any updates and notify me again before installing them on my computer

○ Download the updates automatically and notify me when they are ready to be installed

○ Automatically download the updates, and install them on the schedule that I specify

at 3:00 A.M.

Learn more about scheduled installing

Certkiller.com

Answer:

Select the "Keep my computer up to date. When this setting enabled windows update software may be

automatically updated prior to applying any other updates" checkbox.
Then select "Automatically download the updates and install them on the schedule that I specify".
The time should be specified every day between 9am and 5pm.

Explanation: You enable Automatic Updates by checking the option Keep My Computer Up To Date. With This Setting Enabled, Windows Update Software May Be Automatically Updated Prior To Applying Any Other Updates.
The settings that can be applied to Automatic Updates include the: Automatically Download The Updates, And Install Them On The Schedule That I Specify." Which allows you to specify the days and times you want Windows to search for updates, e.g. during non-business hours. You still have to verify that you want the updates installed prior to the updates being applied to your server.
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. 55

QUESTION 234
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains 35 Windows Server 2003 computers; 3,000 Windows XP Professional computers; and 2,000 Windows 2000 Professional computers.
You install and configure Software Update Services (SUS) on a server named Certkiller 3. You need to scan all computers in the domain to find out whether they have received all approved updates that are located on the SUS server.
What should you do?

A. On a server, install and run the mbsacli.exe command with the appropriate configuration switches.
B. On a server that runs IIS, install and configure urlscan.exe.
C. Edit and configure the Default Domain Policy to enable the Configure Automatic Updates policy.
D. From a command prompt on Certkiller 3, run the netsh.exe command to scan all computers in the domain.

Answer: D

Explanation: Netsh command is the updated version of the Ipsecpol.exe command of Windows 2000 Professional. With the Netsh.exe tool, you can direct the context commands you enter to the appropriate helper, and the helper then carries out the command. A helper is a Dynamic Link Library (.dll) file that extends the functionality of the Netsh.exe tool by providing configuration, monitoring, and support for one or more. Since Persistent policies are applied by making use of the netsh.exe command, you can use it to scan the computers in the domain to verify whether they all received the approved updates.
Incorrect answers:
A: Checking whether computers in the domain received all approved updates that were located on the SUS server is not a purpose of mbsacli.exe.
B: This is not the solution.
C: This option is not suggesting a way to check whether approved updates haver been received or not.
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.

173
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, pp. 871-874

QUESTION 235
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 and have the latest service pack installed. There are 500 client computers.
You manage a server that has Software Update Services (SUS) installed. The latest updates were synchronized and approved for installation on the client computers.
You need to configure the client computers to download the approved updates.
What should you do?

A. Create a text file named Auto-Update.ini. Configure the correct Automatic Updates settings in the file. Copy and paste the file into the Systemroot folder on all client computers.
B. Create a GPO that has the appropriate Automatic Updates settings configured.
Apply the GPO to the client computers that you to need to configure.
C. In Active Directory Users and Computers, modify the settings for the client computer accounts.
Configure the Managed By property to specify the SUS server account.
D. Create a local group on the SUS server. Assign the group the Allow - Read and the Allow - Write permissions for the AutoUpdate folder on the SUS server. Add all the users of the client computers to the local group.

Answer: B

Explanation: The advantages of SUS includes amongst others that Administrators have selective control over what updates are posted and deployed from the public Windows Update site. No updates are deployed to client computers unless they are first approved by an administrator. And that Administrators can control the synchronization of updates from the public Windows Update site to the SUS server either manually or automatically. Thus if you create an appropriate GPO and apply it to the client computers that need to be configured, thenyou will be able to ensure that client computers ony download approved updates.
Incorrect answers:
A: This option is not the solution.
C: There is no need to modify the settings for the client computers accounts in the Active Directory Users and Computers.
D: This option is not to ensure that only apprpoved updates are downloaded by the client computers. SUS has two major components: the SUS server and Automatic Updates, both which has to be installed before you can even think of downloading updates.
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. 56

QUESTION 236
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.
You are required to accommodate for five new support engineers.
The five support engineers will have have the following responsibilities:
• Stop and start printers, clear print jobs from the printer queues, and set permissions on printers.
• Back up and restore all files on the servers.
• Make changes to TCP/IP settings.
• Create and delete shared resources
You need to assign the support engineers the appropriate permissions to perform the required tasks on the 20 member servers.
Of which group should you make the Support Engineers group a member?

A. the Administrators local group on one of the domain controllers.
B. the Administrators local group on each of the servers.
C. the Server Operators local group on one of the domain controllers.
D. the Power Users local group on one of the servers.
E. the Backup Operators local group on one of the domain controllers.
F. the Backup Operators local group on each of the servers.

Answer: B

Explanation: 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.) Because of the permissions associated with this group, you should add users to this group with caution. If you want the Support Engineers to complete their tasks then you should make the Support Engineers group members of the Administrators local group on each of the servers.
Incorrect answers:
A: Making the Support Engineers members Administratores local on only one of the domain conmtreollers will be too restrictive for them to carry out their tasks.
C: 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. This is not enough.
D: Being members of the Power Users group on one of the servers will not be enough for this scenario.
E & F: Whether on one of the domain controllers or on each of the servers, 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, this is not enough to enable them to carry out all their tasks.
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. 167-170
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering(tm)Windows(r)
Server 2003, Sybex Inc., Alameda, 2003, p. 721

QUESTION 237

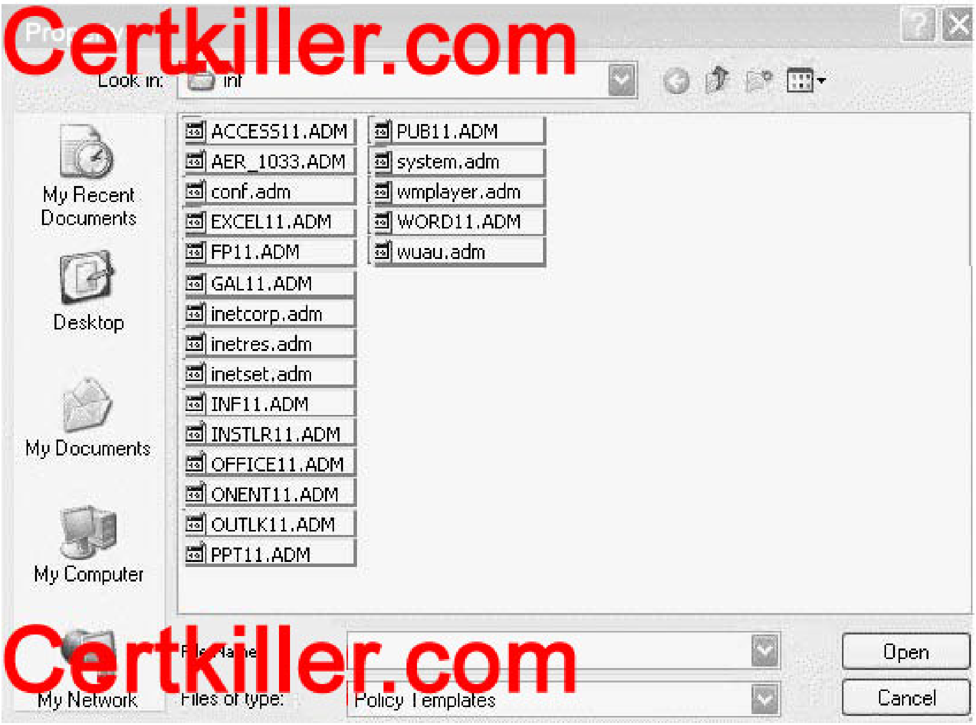
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

You install Software Update Services (SUS) on a Windows Server 2003 computer named Certkiller 6. You want all client computer on the network to use Certkiller 6 to receive their software updates. You decide to modify the Default Domain Policy GPO to set Certkiller 6 as the SUS server for all computers in the domain.

When you open the Default Domain Policy GPO, you notice that there are no settings for Windows Update. You realize that you need to load an administrative template into the Group Policy Objectg Editor.

Which template should you load?

To answer, select the appropriate template in the dialog box.



Answer:

QUESTION 238

You are the network administrator for Certkiller .com Active Directory.

Another system administrator installs Software Update Services (SUS) on a production Windows Server 2003 computer. You are assigned to manage the SUS computer. You need to ensure that you can recover SUS if the server fails.

You need to back up all components that are required to restore SUS to its current configuration. Because of limited space, you must not back up unnecessary data.

What action or actions should you perform? Select all that apply.

A. Back up the SUS folder that contains synchronized content.

B. Back up the folder in which the SYSAdmin site was created.
C. Back up the System State data from the Windows Server 2003 computer.
D. Back up the IIS metabase

Answer: A, B, D

Explanation: To get the current SUS comfiguration without backing up unnecessary data due to limited space, then you should back up IIS metabase which is necessary for SUS since it provides a wide range of options for configuring the content, performance, and access controls for your websites, the SUS folder that has the synchronized content and the folder in which the SYSAdmin was creates.
Incorrect answers:
C: System State data is a set of data that is critical to the operating system booting and includes the Registry, the COM+ registration database, and the system boot files. Thus to back up the required files to restore SUS to its current configuration and due to limited space it is not necessary to back up the System State data freom the Windows Server 2003 computer.
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. 310

QUESTION 239
You are the network administrator for Certkiller , which employs 500 users. 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 Terminal Services on three servers Certkiller 1, Certkiller 2, and Certkiller 3. Initially, users can successfully connect to all three terminal servers by using Remote Desktop connections.
Months later, users begin reporting that they can no longer connect to any of the terminal servers by using Remote Desktop connections.
How should you solve this problem?

A. On each terminal server, change the licensing mode form Per Server to Per Seat.
B. Add additional Microsoft Windows licenses to the Site License server for the domain.
C. Configure and activate an Enterprise license server.
D. On each terminal server, change the licensing mode from Per Device to Per User.

Answer: C

Explanation: The reason the users can no longer connect is that the time period to use Terminal Services in application mode has expired. A terminal server allows clients to connect without license tokens for 120 days before it requires communicating with a license server. The license server grace period ends after 120 days, or when a license server issues a permanent license token through the terminal server, whichever occurs first. Therefore, if the license server and terminal server are deployed at the same time, the terminal server grace period will immediately expire after the first permanent license token has been issued.
Terminal server running Windows Server 2003 must be licensed with one of the following:
- Windows Server 2003 Terminal Server Device Client Access License.
- Windows Server 2003 Terminal Server User Client Access License.
- Windows Server 2003 Terminal Server External Connector.

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. 9

QUESTION 240
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 offices in London, Paris, and Amsterdam. Each office is configured as a separate Active Directory site. Each office has a file server for local users.
ChiFile is the file server in London. It hosts a shared folder. Users report that they can no longer connect to the shared folder. A help desk technician who is a member of the Power Users group reports that he cannot connect to ChiFile.
However, you are able to make a successful connection with ChiFile by using Terminal Services.
How should you solve this problem?

A. Add Windows Server 2003 licenses to the Site License server for London.
B. Change the licensing mode on ChiFile from Per Device or User to Per Server.
C. Change the licensing mode on ChiFile from Per Server to Per Device or User.
D. Install a Terminal Services Enterprise license server on the London domain controller.

Answer: A

Explanation: No more connections can be made to a server product because the number of user's connections has reached the maximum that the server can accept.
The server product might be configured with Per Server licensing and the number of licenses might be exhausted.
Check license usage for the product on the server.
The user can wait until others stop accessing the product.
You can purchase more licenses for the product in an effort to eliminate the problem.
Incorrect answers:
B: Per Device or Per User mode (formerly called "Per Seat" mode) requires that each device or user have its own Windows CAL. Furthermore this will have no effect on the situation.
C: Per Server mode requires a Windows CAL for each connection. These are assigned to each server and cannot be shared between servers. And you are only allowed one CAL
D: This would be obsolete as you can already make a successful connection through using Terminal Services.
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. 46-47

QUESTION 241
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 member server named Certkiller 17 hosts several shared folders.
Users report that they receive an error message when they try to connect to the shared folders. The error message states:

"No more connections can be made to this remote computer at this time because there are already as many connections as the computer can accept."
How should you solve the problem?

A. Add an additional network adapter to Certkiller 17. Configure a network bridge between the new network adapter and the original network adapter.
B. Purchase additional per-seat licenses for Certkiller 17. In Control Panel on Certkiller 17, run the Licensing application. Add the additional licenses to Certkiller 17.
C. Disable quota management on Certkiller 17.
D. In Active Directory Sites and Services, select the site that contains Certkiller 17. Add an additional Active Directory connection object to the domain controller for the site.

Answer: B

Explanation: No more connections can be made to a server product because the number of user's connections has reached the maximum that the server can accept.
Cause: The server product might be configured with Per Server licensing and the number of licenses might be exhausted.
Solution: Check license usage for the product on the server.
The user can wait until others stop accessing the product.
To eliminate the problem, you can purchase more licenses for the product.
Incorrect answers:
A: Adding in an additional network adapter and configuring a bridge between the new adapter and the original adapter means that it is still connected to Certkiller 17 which is already saturated and cannot grant more connections.
C: Disabling quota management will not suffice as you can apply a quota on a per-user, per-volume basis only.
D: By adding an additional connection object to the domain controller for the site still means that Certkiller 17 is saturated and this option will thus not allow more connections.
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. 373-380, 443

QUESTION 242
You are the network administrator for Certkiller .com. All servers run Windows Server 2003.
You manage a server named Certkiller 2. IIS is installed on Certkiller 2. Certkiller 2 hosts Certkiller 's public Web site.
You need to configure Certkiller 2 to allow remote administration of all Web sites. In addition, you must be able to view the system and application event logs remotely. The remote administration must be done by using a Web browser. The procedure for remote administration must be encrypted.
What should you do?

A. Enable Remote Desktop.
B. Install the Remote Administration (HTML) Windows component.
C. Install the Remote Desktop Web Connection Windows component.
D. Configure the startup type of the Telnet service to Automatic and start the Telnet service.

Answer: C

Explanation: The Remote Desktop Web Connection ActiveX control allows you to access your computer through Remote Desktop via the Internet, from another computer using Internet Explorer. You must be using Internet Information Services (IIS) to host a Web site to use this feature. Remote Desktop Web Connection provides most of the same functionality as the Remote Desktop Connection software.
Users of Windows Server 2003 do not need to download this package. They can manually add this package from Add/Remove in the Control Panel. This package is offered as a convenience to Microsoft customers.
Incorrect Answers:
A: To administrate, view the system and application event logs remotely, enabling Remote Desktop is not sufficient given the circumstances.
B: You need to install Remote Desktop Web Connection Windows component and not just the Remote Administration (HTML) Windows component.
D: This option will not work because configuring the startup type of the Telnet service to Automatic is more a dependency or recovery option.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5

QUESTION 243
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, and all client computers run Windows XP Professional.
XML Web services for the internal network run on a member server named Certkiller Srv1, which is configured with default settings. You are a member of the local Administrators group on Certkiller Srv1.
You need the ability to remotely manage Certkiller Srv1. You have no budget to purchase any additional licensing for your network until the next fiscal year.
How should you reconfigure Certkiller Srv1?

A. In the System Properties dialog box, enable Remote Desktop.
B. Add your user account to the Remote Desktop Users local group.
C. In the System Properties dialog box, enable Remote Assistance.
D. Install Terminal Services by using Add or Remove Programs.

Answer: A

Explanation: Enabling users to connect remotely to the server for Remote Desktop for Administration purposes, you must have the appropriate permissions. By default, members of the Administrator group can connect remotely to the server. But Remote Desktop Users group population does not happen by default. You must decide which users and groups should have permission to log on remotely, and then manually add them to the group.
Incorrect Answers:
B: Adding you user account to the Remote Desktop Users local group does not give you administrative rights which is needed to reconfigure the server, Certkiller Srv1.
C: Remote Desktop should be enabled not Remote Assistance.

D: Installing Terminal Services is not the way to remotely manage Certkiller Srv1.
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, pp. 472-474
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5

QUESTION 244
You are a network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The domain contains Windows Server 2003 domain controllers, Windows Server 2003 member servers, and Windows XP Professional computers.
All company network administrators need to have the remote administrative tools available on any computer that they log on to. All network administrators are members of the domain Administrators group. The network administrator accounts are located in multiple organizational units (OUs).
You need to ensure that the administrative tools are available to network administrators. You also need to ensure that the administrative tools are always installed on computers that have 100 MB or more free disks space.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

A. Create a Group Policy object (GPO) that will apply adminpak.msi at the domain level.
B. Create a Group Policy object (GPO) that will link adminpak.msi to the Domain Controllers OU.
C. Ensure that only the domain Administrators group is assigned the Allow - Read permission and the Allow - Apply Group Policy permission for the new Group Policy object (GPO).
D. Assign the domain Users group the Deny - Read permission on the Deny - Apply Group Policy permission for the new Group Policy object (GPO).
E. Create a WMI filter that queries the Win32_LogicalDisk object for more than 100 MB of free space.
F. Create a WMI filter that queries the Win32_LogicalDisk object for less than 100 MB of free space.

Answer: A, C, E

Explanation:
A: You can assign the administrative tools (contained in adminpak.msi) to the administrators using a group policy.
C: Ensuring that only the domain Administrators group is assigned the Allow - Read permission and the Allow - Apply Group Policy permission for the new Group Policy object (GPO) will ensure that only the domain administrators receive the administrative tools.
E: Creating a WMI filter that queries the Win32_LogicalDisk object for more than 100 MB of free space will ensure that the tools are only installed if there is more than 100MB of free disk space.
Incorrect Answers:
B: This would only install the tools on the domain controllers if a domain administrator logged in locally. The GPO needs to be assigned at domain level. Therefore, the tools are installed on any machine an administrator logs in to.
D: The domain admins are members of the domain users group. This would prevent the GPO applying to all users including the domain admins.
F: The software should be installed if there is more than 100MB of free disk space, not less than 100MB.

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, p. 401

QUESTION 245
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 member server named Certkiller 1 functions as a file and print server. Certkiller 1 is configured with default operating system settings.
A user named Jack is a member of the local Backup Operators group on Certkiller 1. She is responsible for performing backups on this computer.
You need to ensure that Jack can create Remote Assistance invitations from Certkiller 1.
What are two possible ways for you to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Log on to Certkiller 1 with administrative privileges.
Use the System Properties dialog box to enable Remote Assistance.
B. Direct Jack to use the System Properties dialog box to enable Remote Assistance on Certkiller 1.
C. In your Default Domain Policy, enable the Solicit Remote Assistance setting.
D. In your Default Domain Policy, enable the Offer Remote Assistance setting.
E. Log on to Certkiller 1 with administrative privileges.
Use GPedit.msc to enable the Offer Remote Assistance setting.

Answer: A, C.

Explanation: Remote Assistance is installed with the operating system by default but is disabled. Thus, it must be enabled before it can be used. Remote Assistance allows a user at one computer to ask for assistance from a user at another computer, on the network or across the Internet. This request for assistance can be made through Windows Messenger, e-mail, or through a transferred file. The assistant can also offer remote assistance without receiving an explicit request if Group Policy settings are configured to enable offering of remote assistance and the assistant is listed in the Offer Remote Assistance policy, or is a local administrator. However, the user requiring assistance must grant the assistant permission to take over the user's computer. The Solicit Remote Assistance setting determines whether remote assistance may be solicited from the Windows XP computers in your environment. Enabling this setting allows user to solicit remote assistance to their workstations from an IT "expert" administrator.
To enable RA, go to Control Panel and select the Remote tab in the System properties. Select the check box next to Turn on Remote Assistance and allow invitations to be sent from this computer, located in the Remote Assistance section of the tab.
Incorrect answers:
B: This will not work as Jack does not have administrator privileges. Furthermore she would have to be logged on to Certkiller 1.
D: The Offer Remote Assistance GPO setting determines whether another user, referred to as the "expert," is allowed to offer RA to the computer without the user requesting RA first. The expert user still cannot connect to the computer needing assistance without the user's permission, even if this GPO setting is

enabled. Therefore this option will not work.
E: You need to enable the Solicit Remote Assistance setting, not the Offer Remote Assistance setting.
References:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 246
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 are members of the domain. All client computers run Windows XP Professional.
Five Web servers host the content for the internal network. Each one runs IIS and has Remote Desktop connections enabled. Web developers are frequently required to update content on the Web servers.
You need to ensue that the Web developers can use Remote Desktop Connection to transfer Web documents from their client computers to the five Web servers.
What should you do?

A. Install the Terminal Server option on all five Web servers.
Use Terminal Services Configuration Manager to modify the session directory setting.
B. Install the Terminal Server option on all five Web servers.
Use Terminal Services Configuration Manager to create a new Microsoft RDP 5.2 connection.
C. On each Web developer's client computer, select the Disk Drives check box in the properties of Remote Desktop Connection.
D. On each Web developer's client computer, select the Allow users to connect remotely to this computer check box in the System Properties dialog box.

Answer: C

Explanation: When this option is enabled, you can open My Computer on the remote server, and view the disk drives from the client computer listed alongside the disk drives from the server. Also a connection to a Web Client Network is attempted only when the first two providers fail to respond. The "Disk Drives" option will make the Web Developer's local disk drives available to them when they connect to the web servers using a remote desktop connection.
Incorrect Answers:
A: Using the Terminal Services Configuration Manager to modify the session directory setting will not work
B: Terminal Services provides remote control capabilities but using the Terminal Services Configuration Manager to create a new RDP connection will not work. There is already a connection.
D: To select the Allow users to connect remotely to this computer check box in the System Properties dialog box will not ensure that Web developers will be able to make use of Remote Desktop Connections to transfer Web documents from their client computers to the five Web servers.
Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, p. 8:34
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, pp. 36, 574, 583

QUESTION 247

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

XML Web services for the internal network run on a member server named CK1 , which is configured with default settings. You are a member of the local Administrators group on CK1 .

You need the ability to remotely manage CK1 . You have no budget to purchase any additional licensing for your network until the next fiscal year.

How should you reconfigure CK1 ?

A. In the System Properties dialog box, enable Remote Desktop.
B. Add your user account to the Remote Desktop Users local group.
C. In the System Properties dialog box, enable Remote Assistance.
D. Install Terminal Services by using Add or Remove Programs.

Answer: A

Explanation: To configure Remote Desktop for Administration, select Start | Control Panel | System and click the Remote tab. To enable the feature, simply check the box next to Allow users to connect remotely to this computer located in the Remote Desktop section of the tab. Enabling the Remote Desktop will allow you to remotely manage the server whilst not necessitating an additional license.

Incorrect answers:

B: This will enable you to connect to Terminal Servers in the domain. It won't enable you to connect to CK1 .

C: Remote Assistance for x86-based computers allows you to invite a trusted person (a friend or computer expert) to remotely and interactively assist you with a problem. You can also use Remote Assistance to remotely assist a user who trusts you. This feature is useful in situations where detailed or lengthy instructions are required to reproduce or resolve problems.

D: Installing Terminal Services will require additional licensing.

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. 497

QUESTION 248

You are the network administrator for Certkiller .com. The company operates a main office and two branch offices. 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 server named Certkiller SrvA is located in one of the branch offices, where it is a member of a workgroup. Certkiller SrvA is configured with default operating system settings. Remote Desktop and Remote Assistance are enabled, and Windows Messenger is installed. The company intranet site is hosted on this server.

Mr King is the local administrator who manages the intranet site. He requests your assistance in installing an application on Certkiller SrvA.

You need the ability to view Mr King's desktop during the installation process.
What should you do?

A. From your computer, open a Remote Desktop connection with Certkiller SrvA.
B. Direct Mr King to create and send an invitation for Remote Assistance from Certkiller SrvA.
C. From your computer, offer Remote Assistance to Certkiller SrvA.
D. Direct Mr King to start Application Sharing from Windows Messenger.

Answer: B

Explanation: Certkiller SrvA is not a member of the domain; therefore, you do not have permission to connect to Certkiller SrvA using Remote Desktop. However, the administrator of Certkiller SrvA can temporarily give you permission to connect to the server using Remote Desktop, by sending you a Remote Assistance invitation. When you receive and accept the invitation, you will be able to connect to Certkiller SrvA to observe and/or control the administrators session.
Incorrect Answers:
A: You do not have permission to connect to Certkiller SrvA using Remote Desktop. You need an invitation.
C: You can only offer remote assistance to computers in the same domain. Certkiller SrvA is not a member of the domain. Thus you cannot offer Remote Assistance.
D: This will not enable you to connect to Certkiller SrvA using Remote Desktop.
Reference:
http://www.jsiinc.com/SUBI/tip4100/rh4138.htm
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 249
You are the network administrator for Certkiller , which employs 1,500 users. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003. Most client computers run Windows XP Professional, and the rest run Windows NT 4.0 Workstation. Two terminal servers are available to network users. You install a new application on both terminal servers. Everyone who uses the new application to create data must save the data directly to a folder on the local hard disk.
You need to ensure that client disk drives are always available when employees connect to the terminal servers.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Create a client connection object with default settings and deploy the object to each terminal server.
B. Edit the RDP-Tcp properties by selecting the Connect client drives at logon options.
C. Install NetMeeting on all client computers. Configure Remote Desktop Sharing.
D. Install the default Windows 2000 Terminal Server Client software on the Windows NT 4.0 workstations.
E. Install Remote Desktop Connections on the Windows NT 4.0 workstations.

Answer: B, E

Explanation: A listener connection (also called the RDP-Tcp connection) must be configured and exist on the server for clients to successfully establish Terminal Services sessions to that server.
Connect client drives at logon makes your mapped local client's drives accessible from within Windows Explorer, Save As, and Open windows in the session. Note that this option is available for clients running any edition of Windows Server 2003; it is not supported for other clients.
Incorrect answers:
A: You cannot override the RDP-Tcp settings by creating a client connection with default settings to a terminal server.
C: NetMeeting and Remote Desktop Sharing is conferencing software for Windows 98 SE machines.
D: Installing the default Windows 2000 Terminal Server Client software will not necessarily ensure that client disk drives are always available when employees connect to the terminal servers.
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. 7, 547-555

QUESTION 250
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.
Another system administrator, Jack King, needs your help in configuring the volume shadow copy settings on a member server. Jack is logged on to the server console. The settings are configured to allow the proper use of all available remote tools.
You need to provide remote help to Jack by using a remote administration tool. You also need to ensure that Jack can observe your actions from the console.
What should you do?

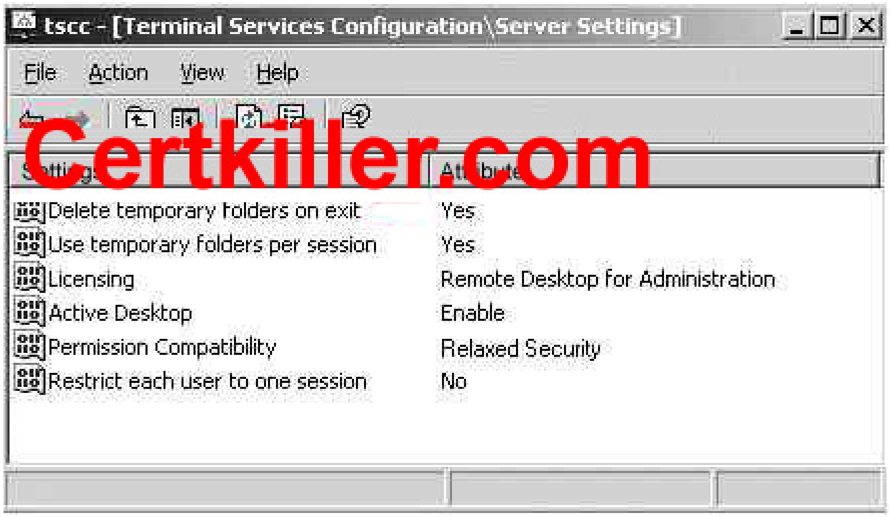
A. Use Remote Desktop in Windows XP Professional to establish a Remote Desktop connection to the member server.
B. Use Help and Support in Windows XP Professional to offer Remote Assistance to the member server.
C. Use Computer Management to connect remotely to the member server.
D. Use the Remote Registry tool to connect to the server.

Answer: B

Explanation: Remote Assistance allows for a novice user to use Windows Messenger to request personal, interactive help from an expert user. When the help request is accepted and the remote session negotiated, the expert is able to view and, if allowed by the novice, control the desktop. In that time Jack should be able observe your actions provided that you make use of Help and Support in Windows XP Professional.
Incorrect answers:
A: Remote Desktop is a different concept to Remote Assistance. With Remote Desktop for Administration or the terminal server role, a user can connect from a wide range of client systems without permission, provided the user has a valid username and password. However this is not what is required in this case.
C: To connect remotely to the member server will not be providing Jack with remote help and allow her to observe your actions.
D: The Remote Registry service is needed to determine whether sufficient privileges exist for remote connection. This is not what the question requires.

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. 493

QUESTION 251
Exhibit



Certkiller.com

Settings	Attribute
Delete temporary folders on exit	Yes
Use temporary folders per session	Yes
Licensing	Remote Desktop for Administration
Active Desktop	Enable
Permission Compatibility	Relaxed Security
Restrict each user to one session	No

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.
A member server named Certkiller 8 hosts all file and print services for the network. Certkiller 8 is accessible only by Remote Desktop Connection. On Certkiller 8, you configure the Terminal Services configuration settings shown in the exhibit.
Shortly afterward, you discover that several different members of the local Administrators group on Certkiller 8 periodically make critical modifications to the configuration settings.
You need to modify Certkiller 8 to ensure that multiple administrators cannot modify the same configuration setting simultaneously.
What should you do?

A. Select Yes as the attribute for the Restrict each user to one session setting.
B. Enable only a single RDP-Tcp connection at one time.
C. Add only the Administrator account to the Remote Desktop Users local group.
D. Select Full Security as the permissions compatibility setting.

Answer: B

Explanation: A terminal server has one RDP-Tcp connection by default, and can have only one connection object per network adapter, but if a terminal server has multiple adapters, you can create connections for those adapters. Each connection maintains properties that affect all user sessions connected to that server connection. Thus if you want to ensure that multiple administrators is not able to modify the same configuration setting on Certkiller 8 simultaneously, then you should enable only a single RDP-Tcp connection at one time.
Incorrect answers:
A: The restricting each user to one session will only affect the user individually as it means that a particular

user will be restricted to a single session at a time. This has no bearing on the problem that you want to avoid.
C: Adding the Administrator account to the Remote Desktop Users local group will not address your concern.
D: The permissions compatibility setting, Full Security, is the default and protects certain operating system files and shared program files only. This is not what is needed.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 252
You are the network administrator for Certkiller . The network consists of a single Active Directory domain Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
Certkiller includes a main office and several branch offices. You work in the main office. A DNS server named Certkiller 1 is located in one of the branch offices.
You need to perform DNS management on Certkiller 1.
First, you log on to a client computer. However, the computer does not have the DNS snap-in installed.
What should you do next?

A. Install the Windows Support Tools on the client computer.
B. From a command prompt, start Nslookup.exe.
At the prompt, type install.
C. Use Windows Explorer to open the c$ share on Certkiller 1.
Select \windows\system32 and install Adminpak.msi.
D. Use Windows Explorer to copy C:\windows\system32\dnsmgmt.msc from Certkiller 1 to C:\windows\system32 on the client computer.

Answer: C

Explanation: Adminpak.msi installs the administrative tools including the DNS management console. Answer D would work, but it wouldn't place a shortcut to the DNS snap-in in the start menu (or anywhere else), so the user would have to open the snap-in using a command prompt. The Windows Server 2003 Administration Tools Pack provides tools that an administrator can use to manage Windows Server 2003 computers remotely from Windows XP Professional with Service Pack 1 client computers. These tools are packaged as adminpak.msi in the i386 folder on the Windows Server 2003 CD-ROM. The Windows Server 2003 Administration Tools Pack includes the DNS snap-in. This would thus make the DNS snap-in available on the client computer.
Incorrect Answers:
A: The Windows Support Tools are located in the Support/Tools folder on the Windows Server 2003 CDROM. However, the Support Tools does not include the DNS snap-in. Thus installing the Windows Support Tools will not give us access to the DNS snap-in.
B: The Nslookup.exe command-line utility displays information that we can use to diagnose the DNS infrastructure. In cannot be used to install the DNS snap-in on a client computer. Indeed, the Nslookup.exe utility does not support an install subcommand. This will not install the DNS management

snap-in.
D: Copying the dnsmgmt.msc from DNS1 to C:\windows\system32 on the client computer. Would make the DNS snap-in available on the client computer. However, we would need to use the command prompt to open the snap-in. It would be easier to use the Windows graphical user interface (GUI) than the command prompt. This is thus not the best option. Thus option D could work because the Adminpak.msi installs the administrative tools
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 594-5.

QUESTION 253
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.
Your new assistant, Tess, will perform basic administrative tasks on a member server named Certkiller SrvC. Jack is not a member of the local Administrators group on Certkiller SrvC, but she can log on to the server console.
Tess reports that she receives an error message when she tries to use Remote Desktop. The error message states: "The local policy of this system does not permit you to log on interactively".
You need to ensure that Jack can use Remote Desktop to log on to Certkiller SrvC.
What should you do?

A. Add Jack's user account to the Remote Desktop Users domain local group.
B. Add Jack's user account to the Remote Desktop Users local group on Certkiller SrvC.
C. On the Remote Control tab of Jack's domain account, select the Enable remote control option.
D. On the Security tab of Jack's domain account, add the Remote Desktop Users domain local group. Assign the Allow - Full Control permissions to this group.

Answer: B

Explanation: The Remote Desktop Users local group on Certkiller SrvC has the necessary permissions to connect to Certkiller SrvC using a remote desktop connection. We can enable Jack to connect using a remote desktop connection by simply adding her domain user account to this local group.
Incorrect Answers:
A: This would permit her to log on to any computer using a remote desktop connection.
C: This allows an administrator to remotely control her session. It doesn't enable her to connect to Certkiller SrvC using a remote desktop connection.
D: This tab doesn't exist.

QUESTION 254
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.
Another system administrator, Jack King, needs your help in configuring the volume shadow copy settings on a member server. Jack is logged on to the server console. The settings are configured to allow the proper use of all available remote tools.
You need to provide remote help to Jack by using a remote administration tool. You also need to ensure that Jack can observe your actions from the console.

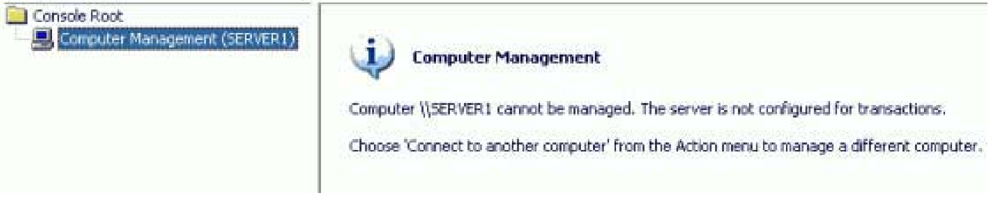
What should you do?

A. Use Remote Desktop in Windows XP Professional to establish a Remote Desktop connection to the member server.
B. Use Help and Support in Windows XP Professional to offer Remote Assistance to the member server.
C. Use Computer Management to connect remotely to the member server.
D. Use the Remote Registry tool to connect to the server.

Answer: B

Explanation: Remote Assistance allows for a novice user to use Windows Messenger to request personal, interactive help from an expert user. When the help request is accepted and the remote session negotiated, the expert is able to view and, if allowed by the novice, control the desktop. In that time Jack should be able observe your actions provided that you make use of Help and Support in Windows XP Professional.
Incorrect answers:
A: Remote Desktop is a different concept to Remote Assistance. With Remote Desktop for Administration or the terminal server role, a user can connect from a wide range of client systems without permission, provided the user has a valid username and password. However this is not what is required in this case.
C: To connect remotely to the member server will not be providing Jack with remote help and allow her to observe your actions.
D: The Remote Registry service is needed to determine whether sufficient privileges exist for remote connection. This is not what the question requires.
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. 493

QUESTION 255
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All client computers run Windows XP Professional.
You manage a member server named Server1, which runs Windows Server 2003. Server1 is also managed by other network administrators at Certkiller .
From your client computer, you open Computer Management and connect to Server1. However, you receive the error message shown in the exhibit.

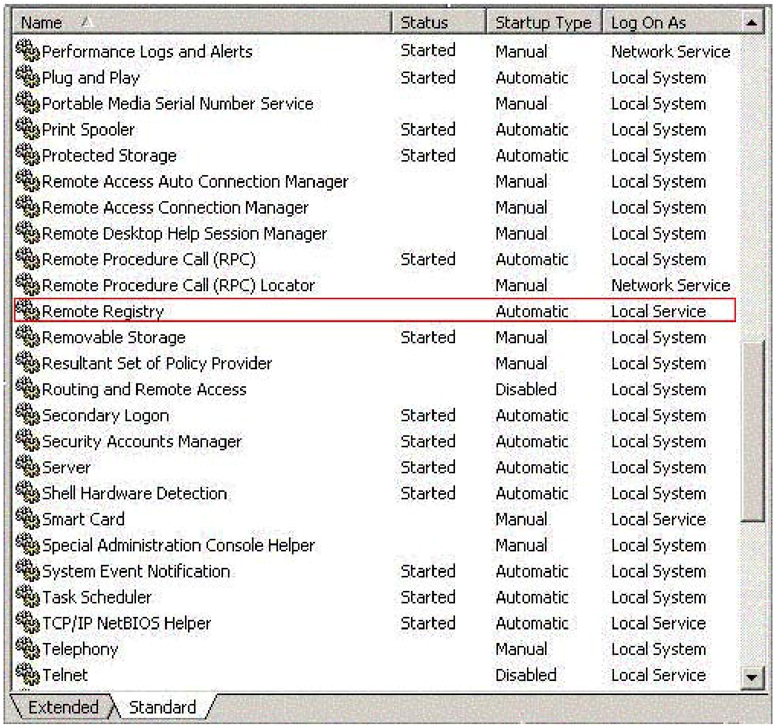


Computer Management

Computer \\SERVER1 cannot be managed. The server is not configured for transactions.

Choose 'Connect to another computer' from the Action menu to manage a different computer.

You need to solve this problem.
First, you log on locally to Server1 and open the Services snap-in, as shown in the work area.
Which service should be modified?
To answer, select the appropriate service in the work area.



Name	Status	Startup Type	Log On As
Performance Logs and Alerts	Started	Manual	Network Service
Plug and Play	Started	Automatic	Local System
Portable Media Serial Number Service		Manual	Local System
Print Spooler	Started	Automatic	Local System
Protected Storage	Started	Automatic	Local System
Remote Access Auto Connection Manager		Manual	Local System
Remote Access Connection Manager		Manual	Local System
Remote Desktop Help Session Manager		Manual	Local System
Remote Procedure Call (RPC)	Started	Automatic	Local System
Remote Procedure Call (RPC) Locator		Manual	Network Service
Remote Registry		Automatic	Local Service
Removable Storage	Started	Manual	Local System
Resultant Set of Policy Provider		Manual	Local System
Routing and Remote Access		Disabled	Local System
Secondary Logon	Started	Automatic	Local System
Security Accounts Manager	Started	Automatic	Local System
Server	Started	Automatic	Local System
Shell Hardware Detection	Started	Automatic	Local System
Smart Card		Manual	Local Service
Special Administration Console Helper		Manual	Local System
System Event Notification	Started	Automatic	Local System
Task Scheduler	Started	Automatic	Local System
TCP/IP NetBIOS Helper	Started	Automatic	Local Service
Telephony		Manual	Local System
Telnet		Disabled	Local Service

Explanation: The Remote Registry service has to be started.
Windows Server 2003 relies on a number of services to work in concert for a computer to be managed remotely using Computer Management, such as the Server service and Windows Management Instrumentation (WMI) services. Of the services displayed in the work area, the Remote Registry service is not started and must be running on the remote computer for the computer to be managed remotely.
Objective: Managing and Maintaining a Server Environment
Sub-Objective: Manage servers remotely
References:
Windows Server 2003 Online Help - Computer Management
Windows Server 2003 Online Help - Performance Logs and Alerts
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. 768

QUESTION 256
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All 40 network servers run Windows Server 2003, and all 1,500 client computers run Windows XP Professional.
The servers are located in seven different buildings. All are configured to allow Remote Desktop connections.
A new administrator named Jack King is hired to help you configure applications and perform disk defragmentation on all 40 servers.
You need to enable Jack King to manage the servers remotely by using Remote Desktop for Administration.
What should you do?

A. Add Jack King to the Administrators group.

B. Add Jack King to the Power Users group.
C. Add Jack King to the Remote Desktop Users group.
D. Delegate control of the Domain Controllers organizational unit (OU) to Jack King.
E. Delegate control of the Computers organizational unit (OU) to Jack King.

Answer: A

Explanation: Enabling users to connect remotely to the server: Before you can create a remote connection to Remote Desktop for Administration you must have the appropriate permissions. By default, members of the Administrators group and the Remote Desktop Users group can connect remotely to the server. However, the Remote Desktop Users group is not populated by default.
You must decide which users and groups should have permission to log on remotely, and then manually add them to the appropriate group. To be able to use the Remote Desktop for Administration for the purpose of configuring applications and disk defragmentation, you need to make Jack part of the Administrator's group.
Incorrect answers:
B: Being part of the Power Users group will not grant Jack the ability to manage servers remotely.
C: Remote Desktop Users group; with the exception of administrators, users must be authorized to connect using Remote Desktop for Administration. This is accomplished by adding a user's account to the Remote Desktop Users group. Though, this is just connecting to the remote desktop not to manage servers.
D: Delegating control of the Domain Controllers organizational unit to Jack King will not grant her the ability to fulfill her task.
E: Delegate control of the Computers organizational unit (OU) will not suffice; she needs administrator's rights to manage the server.
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. 440-441
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4

QUESTION 257
You are a network administrator for Certkiller .com. A Windows Server 2003 computer named Certkiller 1 functions as a print server on the network. Certkiller 1 contains a single printer named SalesPrinter12.
Several users submit large print jobs to SalesPrinter12. A user reports that the print jobs fails to complete. You examine the print queue on SalesPrinter12, and you discover that one of the print jobs is showing an error. You attempt to delete the job, but you are unsuccessful.
You need to ensure that print jobs submitted to SalesPrinter12 complete successfully.
What should you do?

A. Configure SalesPrinter12 to use a TCP/IP port.
B. Increase the priority of SalesPrinter12.
C. Delete all files from the C:\Windows\System32\Spool folder.
D. Restart the spooler service on Certkiller 1.

Answer: D

Explanation: The Print Spooler service loads files to memory for printing. Sometimes we need to stop and restart the service to delete the queues. We can do this by using the net stop spooler command to stop the service. We can delete the print objects from the queue in C:\WINDOWS\System32\spool\PRINTERS, and then start the service with the net start spooler command. After deleting the queues the users will need to resubmit their print jobs.

All printing is managed by the spooler service. If this service is not running, users cannot print. The spooler has a number of configuration options. To change these, open the Printers and Faxes folder and select Server Properties from the File pull-down menu. This opens the Print Server Properties dialog box containing four tabs: Forms, Ports, Drivers, and Advanced, which are used as follows:

- Use the Forms tab to define custom paper sizes.
- Use the Ports tab to define new ports (especially TCP/IP ports) and to configure properties of existing ports.
- Use the Drivers tab to add new drivers or configure existing drivers.
- Use the Advanced tab to modify the behavior of the spooler service.

In particular, note the Spool Folder under the Advanced tab. This location is where print jobs are stored until they are printed. Thus restarting the spooler service will reset it.

Incorrect answers:

A: If the printer is connected directly to the network, you need to use a TCP/IP port and specify the IP address of the printer. Usually, if you connect a printer to a USB port, Windows uses Plug and Play to automatically install the printer for you.

B: You can use priorities to control the order in which print jobs are processed. Normally, jobs are printed in the order in which they are received. The priority of a print job will be increased to make it print next despite its position in the queue. But his has no bearing on the situation in the question because the jobs do print, but not completely.

C: Deleting all files from the spooler will result in no jobs being printed.

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. 602, 607, 610.

QUESTION 258

Your company network consists of a single Active Directory domain named Certkiller .com. The network has a print server running Windows 2003 Server. A single printer is installed on the print server. Technicians in the IT Support department have the necessary permissions to manage printers on the print server. You are a member of the Domain Admins group.

A user in the Accounts department reports that his documents are not printing. A technician named John examines the print queue and finds a list of documents waiting to be printed. John tries to delete the documents from the queue but is unsuccessful.

You need to enable users to successfully print.

What should you do?

A. Install a new print device. Reconfigure the printer to send print jobs to the new print device.

B. Stop and restart the Print Spooler service on the print server. Instruct users to resubmit their print jobs.

C. Install a second instance of the printer. Configure the print queue to hold mismatched documents. Redirect the original printer to the new printer.

D. Install a second instance of the printer. Delete the original printer. Instruct users to resubmit their print jobs.

Answer: B

Explanation: The Print Spooler service loads files to memory for printing. Sometimes we need to stop and restart the service to delete the queues.
We can do this by using the net stop spooler command to stop the service.
We can delete the printer objects from the queue in C:\WINDOWS\System32\spool\PRINTERS, and then start the service with the net start spooler command. After deleting the queues the users will need to resubmit their print jobs.
Incorrect Answers:
A: It is likely that the print jobs in the print queue have become corrupted. They should be deleted. Redirecting them to a new printer will not work.
C: This will not work. The jobs have already been submitted.
D: The users need to resubmit their documents for printing, not John.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6

QUESTION 259
You are the network administrator for Certkiller .com. The network includes three office locations. Each office has one Windows Server 2003 computer that functions as a file and print server. This server hosts home folders for network users.
In each office, a single printer is installed on the file and print server. The local help desk technicians have the necessary permissions to manage printers.
A user named King notifies the local help desk that his documents are not printing. A help desk technician finds a list of documents waiting in the print queue. No user can successfully print. The technician cannot delete documents from the queue.
You need to restore printing capabilities.
What should you do?

A. Install a second instance of the printer.
Redirect the original printer to the new printer.
B. Stop and restart the Print Spooler service.
Ask users to resubmit the documents for printing.
C. Pause the printer.
Reconfigure the print queue to hold mismatched documents.
Unpause the printer.
D. Install a second instance of the printer.
Delete the original printer.
Direct King to resubmit the documents for printing.

Answer: B

Explanation: The Print Spooler service loads files to memory for printing. Sometimes we need to stop and

restart the service to delete the queues.
We can do this by using the net stop spooler command to stop the service.
We can delete the printer objects from the queue in C:\WINDOWS\System32\spool\PRINTERS, and then start the service with the net start spooler command. After deleting the queues the users will need to resubmit their print jobs.
Incorrect Answers:
A: It is likely that the print jobs in the print queue have become corrupted. They should be deleted. Redirecting them to a new printer will not work.
C: This will not work. The jobs have already been submitted.
D: The users need to resubmit their documents for printing, not King.
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. 111

QUESTION 260
You are the network administrator for Certkiller .com. All network servers run Windows Server 2003.
A server named Print CK1 contains a print queue that is shared for use by all users in your office.
Marie is the office manager. She reports that users frequently submit large print jobs just before they leave for lunch. These print jobs require long printing times. They often prevent users from printing other important documents.
You need to enable Marie to delete print jobs that are submitted to the printer by anyone in the office.
What should you do?

A. Configure the printer permission to assign the Allow - Manage Printers permission to Marie.
B. Configure the printer permission to assign the Allow - Manage Documents permission to Marie.
C. On Marie's client computer, create a new print queue that prints to the same print device.
Configure the permission on the print queue to assign the Allow - Manage Printers permission to Marie.
D. On Marie's client computer, create a new print queue that prints to the same print device.
Configure the permission on the print queue to assign the Allow - Manage Documents permission to Marie.
Answers: B

Explanation: Windows Server 2003 provides three levels of printer permissions: Print, Manage Printers, and Manage Documents. Print permission is assigned to the Everyone group. Choosing this permission allows all users to send documents to the printer. To restrict printer usage, remove this permission and assign Allow Print permission to other groups or individual users. Alternatively, you can deny Print permission to groups or users. As with file system ACLs, denied permissions override allowed permissions.
The Manage Documents permission provides the ability to cancel, pause, resume, or restart a print job.
When multiple permissions are granted to a group of users, the least restrictive permission applies. However, when a Deny permission is applied, it takes precedence over any permission. Thus you need to grant Marie the Allow-Manage Documents permission because it will enable her to complete her tasks.
Incorrect answers:
A: The Allow Manage Printers permission will enable Marie to modify printer settings and configuration, including the ACL itself. It will not enable her to complete her tasks. Not even when configured on the printer permission.

C: The Allow Manage Printers permission will enable Marie to modify printer settings and configuration, including the ACL itself. It will not enable her to complete her tasks.
D: The Allow - Manage Documents permission will enable Marie to complete her tasks, but not when applied to the print queue. It should be configured on the printer permission.
Reference:
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 8: 17, 319

QUESTION 261
You are the network administrator for Certkiller .com. All network servers run Windows Server 2003.
A server named Print CK1 has a print device directly connected to the parallel port. The print device is shared for use by all users.
Peter is the IT manager. Peter reports that his documents are often printed after documents submitted by other users.
You need to ensure that Peter's documents take precedence over documents submitted for printing by other users. However, if a document is already printing, the printing must not be interrupted.
What should you do?

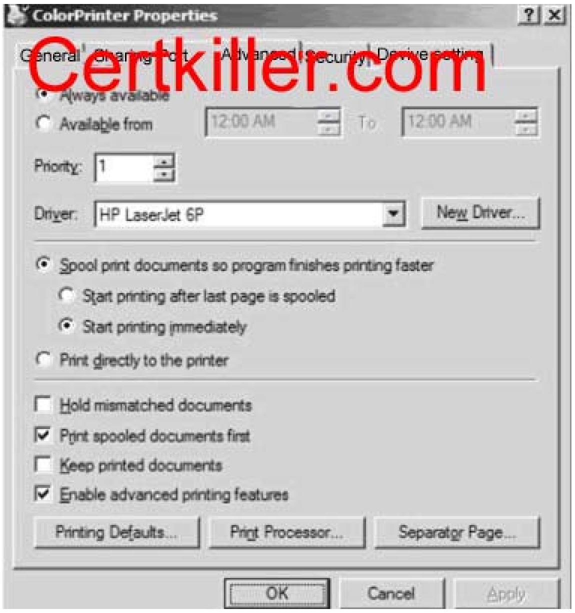
A. Configure the printer permissions to assign the Allow - Take Ownership permission to Peter. Restart the Print Spooler service on Print CK1 .
B. Make Peter's user account the owner of the printer. Restart the Print Spooler service on Print CK1 .
C. Create a new printer on Print CK1 and configure it to print to the print device. In the Advanced tab of the new printer properties, select the Print directly to the printer option. Configure Peter's computer to print to the new printer.
D. Create a new printer Print CK1 and configure it to print to the print device. Modify the priority of the new printer. Configure Peter's computer to print to the new printer.

Answer: D

Explanation: You may want to configure printer priorities for two printers that print to the same print device. This configuration guarantees that the printer with the highest priority prints to the print device before the printer with the lower priority.
This is a good strategy if the printer with the lower priority is only available to print during non-business hours and has many documents waiting to print. If you must print to the print device, you can select the printer with the higher print priority, and your print job will move to the top of the print queue.
To set priorities between printers, perform the following tasks:
* Point two or more printers to the same print device (the same port). The port can be either a physical port on the print server or a port that points to a network-interface print device.
* Set a different priority for each printer that is connected to the print device, and then have different groups of users print to different printers. You can also have users send high-priority documents to the printer with higher priority and low-priority documents to the printer with lower priority.
If Peter's computer is configured to print to the print server, Print1, after it has been recreated, then you can set the priority of the printer to suit the situation.
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. 607

QUESTION 262

Exhibit



Certkiller.com

● Always available
○ Available from 12:00 AM To 12:00 AM

Priority: 1

Driver: HP LaserJet 6P

● Spool print documents so program finishes printing faster
○ Start printing after last page is spooled
● Start printing immediately
○ Print directly to the printer

□ Hold mismatched documents
☑ Print spooled documents first
□ Keep printed documents
☑ Enable advanced printing features

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 1 functions as a print server on the network.

A high-speed color print device is attached to Certkiller 1. You configure a printer named ColorPrinter on Certkiller 1. Several other printers are also configured on Certkiller 1. The configuration of ColorPrinter is shown in the exhibit.

Users in the marketing department report that when they print large files that contain multiple graphics, the documents print very slowly, pausing for several seconds between each page.

You need to minimize the impact that large print jobs have on the performance of the printer. You need to achieve this goal by using the least administrative effort.

What should you do?

A. Create a printer pool that includes an additional printer of the same type as ColorPrinter.

B. Add a second printer to Certkiller 1 that prints to the same print device as ColorPrinter. Instruct marketing users to submit large print jobs to one device and smaller print jobs to the other.

C. Configure ColorPrinter to start printing after the last page is spooled.

D. Increase the priority of ColorPrinter so that it is higher than all other printers.

Answer: C

Explanation: When you configure spooling options, you specify whether print jobs are spooled or sent directly to the printer. Spooling means that print jobs are saved to disk in a queue before they are sent to the printer. Consider spooling as the traffic controller of printing-it keeps all of the print jobs from trying to print at the same time. In the Advanced tab, you can leave the Start Printing Immediately option selected, or you can choose the Start Printing After Last Page Is Spooled option. If you choose the latter option, a smaller print job that finishes spooling first will print before your print job, even if your job started spooling before it did. This option should minimize the impact large print jobs have on the performance of the printer.

Incorrect answers:
A: This option will not have the desired effect.
B: This option suggests too much administrative effort than is necessary.
D: Increasing the piority of ColorPrinter so that it is higher than all other printers will the opposite of the desired effect.
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. 354-355

QUESTION 263
You are the network administrator for Certkiller .com. The network contains a Windows Server 2003 computer named Print1 that functions as a print server.
Print1 contains a printer named MarketingPrinter. Users report that print jobs they submit to the MarketingPrinter take a long time to print. You immediately examine Print1 and conclude that the server is performing at acceptable levels.
You need to identify the problem.
What should your next step be?

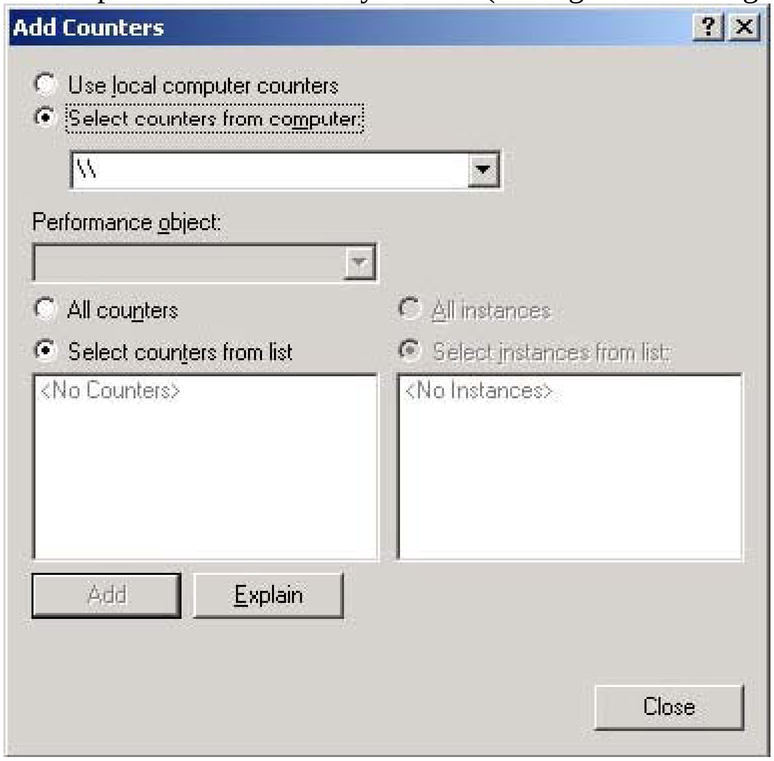
A. Use Task Manager to monitor processor and memory performance.
B. Use Windows Explorer to monitor the size of the Windows\System32\Spool\prtprocs folder.
C. Use System Monitor to view the Print Queue\Jobs counter.
D. Use System Monitor to view the Print Queue\Enumerate Network Printer Calls counter.

Answer: C

Explanation: the Print Queue\Jobs counter specifies the current number of print jobs that are pending in the print queue.
Incorrect answers:
A: Task Manager is a Windows Server 2003 utility that can be used to start, end, or prioritize applications. The Task Manager shows the applications and processes that are currently running on the computer, as well as CPU and memory usage information. You can also view network utilization and manage network users. However this is not the information needed in this case.
B: Monitoring the size of that particular folder will not yield the relevant information.
D: The Enumerate NetworkPrinter Calls counter specifies how many browser requests have been made to the print server from network browse lists. The number is cumulative from when the server was last started. This is not the counter to be using in these circumstances.
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. 375-376

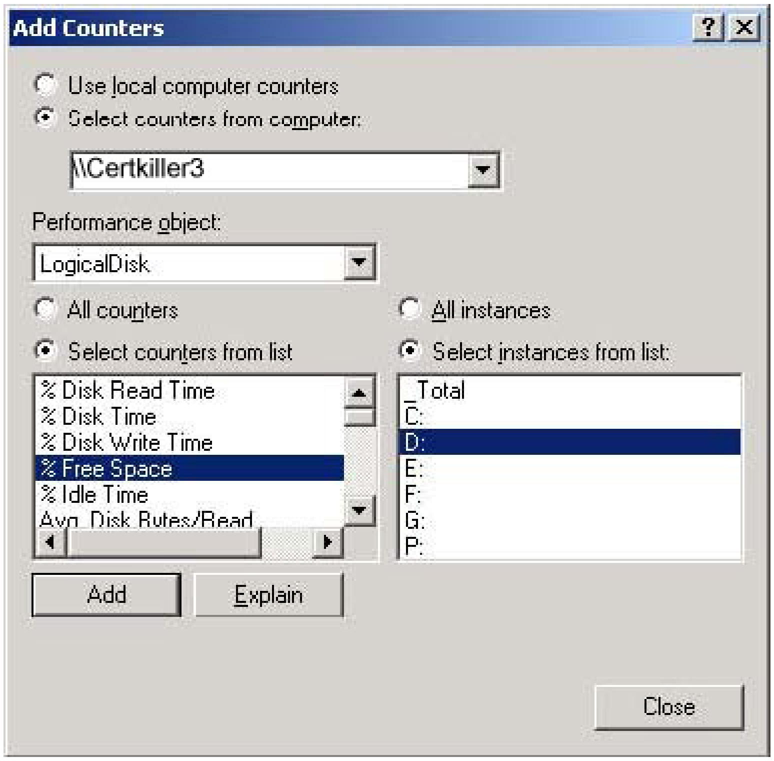
QUESTION 264
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
Your FTP Server is named Certkiller 3. Files uploaded to Certkiller 3 are stored on D:\. Business rules require you to set an alert that will inform you when D:\ reaches 80 percent of capacity.

You open the Performance console and create a new alert.
New you need to add a performance counter to the alert.
Which performance should you add? (Configure the fitting option or options in the dialog box)



○ Use local computer counters
● Select counters from computer:
\\
Performance object:
○ All counters
● Select counters from list
<No Counters>
○ All instances
● Select instances from list:
<No Instances>

Answer:



○ Use local computer counters
● Select counters from computer:
\\Certkiller3
Performance object:
LogicalDisk
○ All counters
● Select counters from list
% Disk Read Time
% Disk Time
% Disk Write Time
% Free Space
% Idle Time
Avg. Disk Bytes/Read
○ All instances
● Select instances from list:
_Total
C:
D:
E:
F:
G:
P:

Explanation: This 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.
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. 461

QUESTION 265
You are a domain administrator for Certkiller . The network contains three Windows 2003 Server domain controllers and one Windows 2003 Server member server.
The member server contains three hard disks, which use software RAID-5. The member server also contains an ISA card that has 12 modems attached for Routing and Remote Access dial-up access.
Usage of the member server's disk subsystem is occasionally as much as 80 percent. This level of usage results in slow response times for dial-in users.
You run System Monitor on the member server. The System Monitor results are shown in the following table.

Object	**Counter**	**Average value**
System	Processor Queue Length	1
Processor	%Processor Time	56
Processor	Interrupts/sec	320
PhysicalDisk	Disk Queue Length	1
PhysicalDisk	Disk Bytes/sec	1900 KB
PhysicalDisk	%Disk Time	74
Memory	Page Faults/sec	10
Memory	Page Reads/sec	9
Memory	Pages/sec	50

You want to maximize the performance of the member server. What should you do?

A. Increase the number of hard disks in the RAID-5 system.
B. Upgrade the RAM.
C. Upgrade the processor.
D. Upgrade the ISA card to PCI.

Answer: B

Explanation: The Memory: Pages/sec counter is too high. A value of no more than 20 is recommended. This counter shows that the paging file is being used too much. We can fix this by upgrading the RAM. The question states that the usage of the member server's disk subsystem is occasionally as much as 80 percent. This is due to the excessive paging file usage.
Incorrect Answers:
A: Increasing the number of hard disks won't reduce the page file usage.
C: The Processor counters are within acceptable limits.
D: The ISA card would not cause excessive disk usage.
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, p. 540

QUESTION 266
You are one of the network administrators for Certkiller . All network servers run Windows Server 2003. Certkiller operates a total of four offices.
The office where you work has 15 servers. You are responsible for supporting and maintaining all of these servers.
You need to design a monitoring plan that will achieve the following goals:
• Track all performance changes on the servers.
• Record performance data to anticipate the need for future upgrades.
What should you do?

A. On each server in your office, use Performance Logs and Alerts to create a baseline log.
Configure the log to collect data every five minutes for one day.
Use the same counters for each server to create a log file.
Schedule the log to run weekly.
B. From a monitoring computer, use Performance Logs and Alerts to create a baseline log for each server in your office.
Configure the log to collect data every five minutes for one day.
Use the same counters for each server to create a log file.
Schedule the log to run weekly.
C. On each server in your office, use Performance Logs and Alerts to create threshold-based alerts.
Configure the alerts to send a message to your monitoring computer when they are triggered.
Set each alert to start a new scan when the alert finishes.
D. From a monitoring computer use Performance Logs and Alerts to create a new counter set in System Monitor.
Configure the counters to run continuously.
Answers: B

Explanation: Performance Logs and Alerts provide logging and alert capabilities for both local and remote computers. You use logging for detailed analysis and recordkeeping. Retaining and analyzing log data that is collected over time can be helpful for capacity and upgrade planning. To perform this procedure, you must be a member of the Administrators group, or you must have been delegated the appropriate authority. If the computer is connected to a domain, members of the Domain Admins group might be able to perform this procedure.
Performance Monitor Users - Members of this group can monitor performance counters on the server locally and from remote clients without being a member of the Administrators or Performance Log Users groups.
Performance Log Users - Members of this group can manage performance counters, logs and alerts on the server locally and from remote clients without being a member of the Administrators group.
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.
The Performance Logs And Alerts snap-in is designed to write data to a file (log) and report counter values

that breach a threshold (alert). Logs written by Performance Logs And Alerts can be loaded into System Monitor for analysis, and exported to various file types (such as CSV and HTML) for reporting purposes.
Incorrect answers:
A: You need to create the baseline log for each server from a monitoring computer because members of the Performance Monitor users group can monitor performance counters on the server locally and from remote clients without being a member of the Administrators or Performance Log Users groups
C: Creating threshold-based alerts will not be sufficient for the purposes of tracking all performance changes. Also starting a new scan after each alert will not work efficiently.
D: Creating a new counter set in the System Monitor will not provide you with the necessary data. You need to create a baseline log.
Reference:
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 12: 11-33.

QUESTION 267
You are the network administrator for Certkiller .com. Your network contains a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.
One of your application servers runs proprietary software. This server stops responding. After help desk technicians restart the server, it appears to run normally.
Two weeks later, the same server stops responding again. You need to gather and store data to diagnose the problem.
What should you do?

A. Open Event Viewer and review the security logs on the server.
B. Create a System Monitor log that uses memory counters and gather data over time.
C. Open Task Manager and gather memory usage statistics.
D. Modify Boot.ini to use /maxmem:1536.

Answer: B

Explanation: The System Monitor is the primary tool for monitoring system performance. Since the question states that the problem occurred and then; after a restart performed normally. After two weeks the same server stops responding again. Thus a memory counter that gathers data over time will help in troubleshooting the problem.
Incorrect answers:
A: Event viewer is more appropriate to use when doing security auditing. It is used to view information, warnings, and error events raised by various components of the system, including device drivers and the device management services. As you navigate Event Viewer, you might see events that are generated by various devices.
C: Task Manager is a utility program that displays the current application programs and processes that are running on the computer. It also monitors the system's recent processor usage, recent memory usage, current network utilization, and currently logged-on users. Though, this is only useful for shorter period monitoring as it monitors recent processor and memory usage.
D: This option is more suited to check the startup environment rather than gathering and storing data as is needed in this scenario.
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. 219, 725-735.

QUESTION 268

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.
Your network includes domain controllers, file and print servers, and application servers. The application servers run a variety of programs, including Microsoft SQL Server 2000 and Microsoft Exchange Server 2003.
Your staff are responsible for monitoring current system performance on all servers.
You need to enable your staff to use System Monitor to gather performance data for each unique server type. The data will be used for trend analysis and forecasting.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

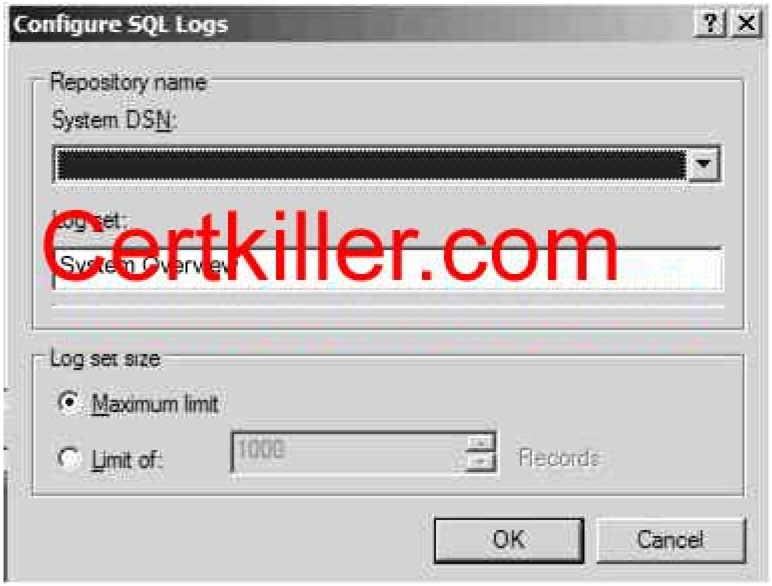
A. For each server, add the most common performance counters and save them as an HTML file.
B. For each server, add the most common performance counters and save them as a counter report file.
C. Create trace logs based on the file and schedule and trace logs to gather data.
D. Create alerts on the file and schedule the alerts to gather data.
E. Create counter logs based on the file and schedule the counter logs to gather data.

Answer: A, E

Explanation: With System Monitor, you can measure the performance of your own computer or other computers on a network.
Performance Counters are data items direct System Monitor about which areas of performance to track and display. Each performance object has several performance counters associated with it. E.g. Pages/sec, Available Bytes, and %Committed Bytes in Use are all examples of counters for the Memory performance object.
Incorrect answers:
B: Adding the most common performance counters into a counter report file will not suffice as you need to take into account that there are several different types of servers in the network.
C: The trace logs enable you to trace applications and processes. You need to gather performance data.
D: Creating alerts on the file is not the same as the counter logs which is actually what is necessary.
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. 227, 726, 729, 733-735.

QUESTION 269

Exhibit



Repository name

System DSN: [redacted]

Log set: System Overview

Log set size

● Maximum limit

○ Limit of: 1000 Records

Certkiller.com

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

You manage a file server named Certkiller 1. You need to create a performance baseline for Certkiller 1 by using Performance Logs and Alerts. You need to store the performance data in an existing Microsoft SQL Server database on another computer.

You create a new counter log, and select SQL Database as the log file format. When you attempt to save your changes, you receive an error message that you must select a data source name. You examine the configuration of the SQL logs, as shown in the exhibit.

You need to configure the counter log to use a SQL database.

What should you do?

A. Use the relog command-line utility to configure a connection to your SQL database.

B. Use Add or Remove programs to install Connection Point Services. Configure a connection to your SQL database.

C. Use the logman command-line utility with the create switch to configure a connection to your SQL database.

D. Use Data Sources (ODBC) to configure a connection to your SQL database.

Answer: D

Explanation: Your problem will be best addressed by making use of Data Sources to configure a connection to the SQL database in order to create a new counter log that makes use of the SQL database as its file format. Only then will you not encounter the error message stating that you must select a data source name when you want to save your changes.

Incorrect answers:

A: Making use of the relog command will not ensure that the log file format will be in a SQL database form.

B: This option will not work.

C: Creating a switch to the SQL database by means of the logman command-line utility does not ensure that your counter log will make use of a SQL database.

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. 731

QUESTION 270

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.

A server named Certkiller 2 functions as an application server. Users in the Certkiller marketing department use an application on Certkiller 2 to analyze data. The application produces a high volume of disk activity.

You give access to 15 new users for the application on Certkiller 2. Users in the Certkiller marketing department report unacceptable delays when they use the application during periods of peak activity.

You use System Monitor to analyze the performance of Certkiller 2.

You need to ensure that Certkiller 2 can support the new users.

Which counter should you monitor?

A. The % Disk Time counter for the PhysicalDisk performance object
B. The Current Disk Queue Length counter for the PhysicalDisk performance object
C. The Free Megabytes counter for the LogicalDisk performance object
D. The Disk Transfers/sec counter for the LogicalDisk performance object

Answer: A

Explanation: PhysicalDisk: % Disk Time and % Idle Time - These two counters indicate the percentage of time the disk was used and the percentage of time the disk has been idle. If the disk usage time is high, you should consider moving some applications to other servers.

Incorrect answers:

B: This indicates the length of the queue involved in writing or reading from the disk in number of requests that are waiting when the counter is measured, including requests in service. This is not what you want if you want to ensure that Certkiller 2 has the capacity to support the new users.

C: This gives you the throughput of the disk activity. You need to monitor % Disk Time counter for the PhysicalDisk performance object.

D: This counter describes how long the disk is taking to fulfill the requests. The more time it spends on fulfilling the requests, the slower the disk controller is. Though this has nothing to do with wanting to ensure that Certkiller 2 can support the new users or not.

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. 748

QUESTION 271

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 member server named CK1 contains a large number of files that are frequently accessed by network users. Users report unacceptable response times on CK1 .

You compare the current performance of CK1 to a system performance baseline that you created several weeks ago. You decide that CK1 needs a higher-performance network adapter. After you add the appropriate network adapter, users report satisfactory performance.

You need to gather new server performance data so you can establish a new performance baseline for CK1 .
You open the Performance console.
What should you do next?

A. Add all counters for the Network Interface object to the System Monitor object.
B. Create a new trace log object.
Under Events logged by system provider in the new object, select the Network TCP/IP setting.
Start the trace log.
C. Create a new counter log object.
Add all counters for the Network Interface object to the new object.
Start the counter.
D. Create a new alert object.
Add all counters for the Network Interface object to the new object.
Start the alert.

Answer: C

Explanation: Creating and maintaining a performance baseline is a good practice. Monitoring devices on a regular basis is important to maintaining a healthy system. Consider capturing a baseline of key performance metrics on your system during an "average" timeframe using the Performance Logs feature of the Performance console. When it comes to troubleshooting issues or doing capacity planning, this data will go a long way toward helping you make informed decisions.
The Performance Monitor application contains the System Monitor ActiveX control, counter logs, trace logs, and alerts.
Incorrect answers:
A: System Monitor can be used to view real-time metric data in a graphical fashion, or logged data resulting from Performance Logs and Alerts.
B: The trace logs enable you to trace applications and processes and you want to establish a new performance baseline.
D: You need to start the counter not the alert. A Counter log object is what is needed for establish a performance baseline.
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. 230, 735, 785

QUESTION 272
You are the network administrator for Certkiller .com. A Windows Server 2003 computer named Certkiller 6 functions as a file server. Drive C on Certkiller 6 is running low on free disk space.
You need to ensure that an event is written to the application log on Drive C when 10 percent of the available free space on the server remains.
What should you do?

A. Open Event Viewer and expand the application log. Select New Log View.
B. Open Computer Management and expand Storage. Right-click Disk Management, and then select Rescan Disks.

C. Open Performance and expand Performance Logs and Alerts. Right-click Counter Logs, and then select New Log Settings.
D. Open Performance and expand Performance Logs and Alerts. Right-click Alerts, and then select New Alert Settings.

Answer: D

Explanation: The Performance Logs And Alerts utility is used to create reports, which can then be viewed with the System Monitor utility. The New Alert Settings is used to create an alert.
Incorrect answers:
A: This is not the solution.
B: Scanning the disks will not influence where the event is written to.
C: This setting is used to create a new baseline report. This is not what is required in this question.
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. 463

QUESTION 273
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.
A server named Certkiller 4 hosts all shared documents for the legal and human resources departments. Certkiller 4 is frequently accessed and updated throughout the business day.
Users report extremely slow response times when they try to open the shared documents.
You log on to Certkiller 4 and observe real-time data indicating that the processor is operating at 100 percent of capacity.
Now you need to gather additional data to diagnose the cause of the problem.
What should you do?

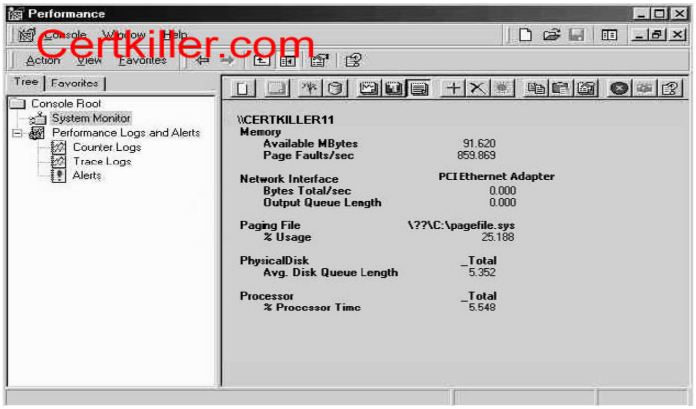
A. In System Monitor, create an alert that will be triggered when processor usage exceeds 80 percent for more than five minutes.
B. In Event Viewer, open and review the application log for the System Monitor events.
C. In Task Manager, review the Processes tab to see the percentage of processor capacity used by each application.
D. In the Performance console, create a counter log to track processor usage.

Answer: C

Explanation: Task Manager is a Windows Server 2003 utility that can be used to start, end, or prioritize applications. The Task Manager shows the applications and processes that are currently running on the computer, as well as CPU and memory usage information. You can also view network utilization and manage network users. All this is can be viewed in real time. The Processes tab of Task Manager can be used to manage process priorities. To change the priority of a process that is already running, right-click the process you want to manage and select Set Priority. You can select from Realtime, High, AboveNormal, Normal, BelowNormal, and Low priorities.
Incorrect answers:
A: System Monitor is a Windows Server 2003 utility used to monitor real-time system activity or view data

from a log file. An alert is a system-monitoring feature that is generated when a specific counter exceeds or falls below a specified value. Through the Performance Logs and Alerts utility, administrators can configure alerts so that a message is sent, a program is run, or a more detailed log file is generated. This is not necessary.
B: Application log is a log that tracks events that are related to applications running on the computer. The Application log can be viewed in the Event Viewer utility. However, this is not what is needed.
D: Counter logs record data about hardware usage and the activity of system services. This is not he 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. 446, 483

QUESTION 274
Exhibit:



```
\\CERTKILLER11
Memory
     Available MBytes                    91.620
     Page Faults/sec                    859.869

Network Interface                 PCI Ethernet Adapter
     Bytes Total/sec                          0.000
     Output Queue Length                      0.000

Paging File                    \??\C:\pagefile.sys
     % Usage                                 25.188

PhysicalDisk                          _Total
     Avg. Disk Queue Length            5.352

Processor                             _Total
     % Processor Time                  5.548
```

You are the network administrator for Certkiller . All network servers run Windows Server 2003.
System Monitor logs are created weekly for each server.
Certkiller 2, one of your servers, runs Microsoft SQL Server 2000 and hosts several databases.
Certkiller 2 is frequently updated throughout the day. Users report extremely slow response times when they try to access the databases.
Using the System Monitor logs, you create the chart shown in the exhibit.
What is the cause of the slow response times?

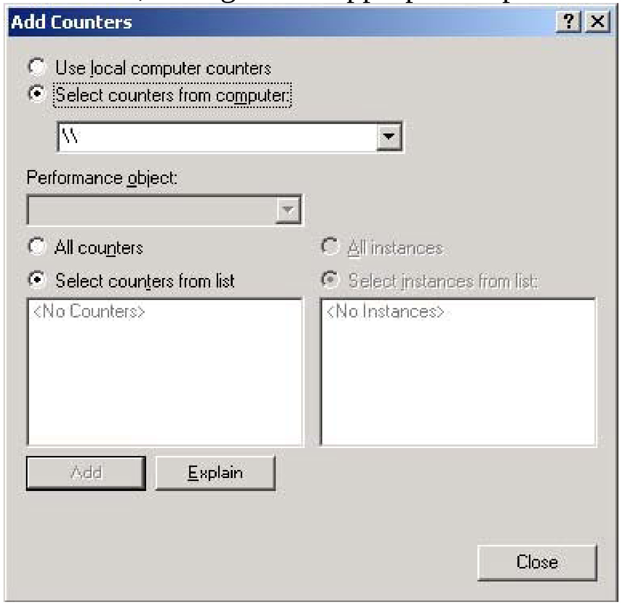
A. insufficient memory
B. insufficient processor speed
C. excess network traffic
D. insufficient disk subsystem

Answer: D

Explanation: The main subsystems that should be monitored on a Windows Server 2003 computer are memory, processor, processes, disk subsystem, and the network subsystem. Disk access is the amount of time it takes your disk subsystem to retrieve data that is requested by the operating system. The two factors that determine how quickly your disk subsystem will respond to system requests are the average disk access time on your hard drive and the speed of your disk controller. On writes, the OS writes only to the controller. Therefore, high-speed writes mandate a very fast controller. On reads, the data is accessed from the disk to the controller. Therefore, on reads the disk access speed is critical. Using high-speed disk

controllers and drives in a stripe set, you can attain a disk access time of approximately 5.1 to 6.4 milliseconds.
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. 459-460

QUESTION 275
You are the network administrator for Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
Your FTP server is named Certkiller 3. File uploaded to Certkiller 3 are stored on D:\. Business rules require you to set an alert that will inform you when D:\ reaches 80 percent of capacity.
You open the Performance console and create a new alert.
Now you need to add a performance counter to the alert.
Which performance counter should you add?
To answer, configure the appropriate option or options in the dialog box.



Add Counters

○ Use local computer counters
● Select counters from computer:

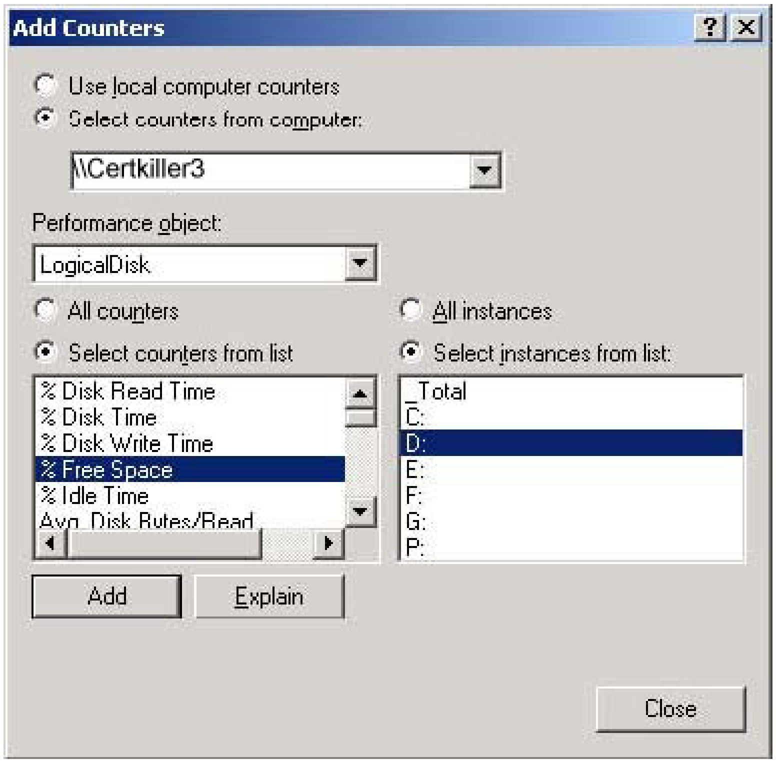
\\

Performance object:

○ All counters
● Select counters from list
○ All instances
● Select instances from list:

<No Counters>
<No Instances>

Answer:



○ Use local computer counters
● Select counters from computer:

\\Certkiller3

Performance object:

LogicalDisk

○ All counters
● Select counters from list

% Disk Read Time
% Disk Time
% Disk Write Time
% Free Space
% Idle Time
Avg. Disk Bytes/Read

○ All instances
● Select instances from list:

_Total
C:
D:
E:
F:
G:
P:

Explanation: Server3 the FTP server is stored on drive D, thus you have to check D: by running the performance counter on D. The specific counter in this scenario would be the amount of free space available.
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. 229-230

QUESTION 276
You are the network administrator for Certkiller .com. The network is distributed across five countries in Europe, namely Spain, Italy, Hungary, Austria, and Germany. All network servers run Windows Server 2003. Each location has three print servers.
You need to monitor usage of print queues on all print servers on the network. You plan to enable monitoring for each print server in the same way. Monitoring data must be stored in a central location and archived for five years to enable data comparison.
What should you do?

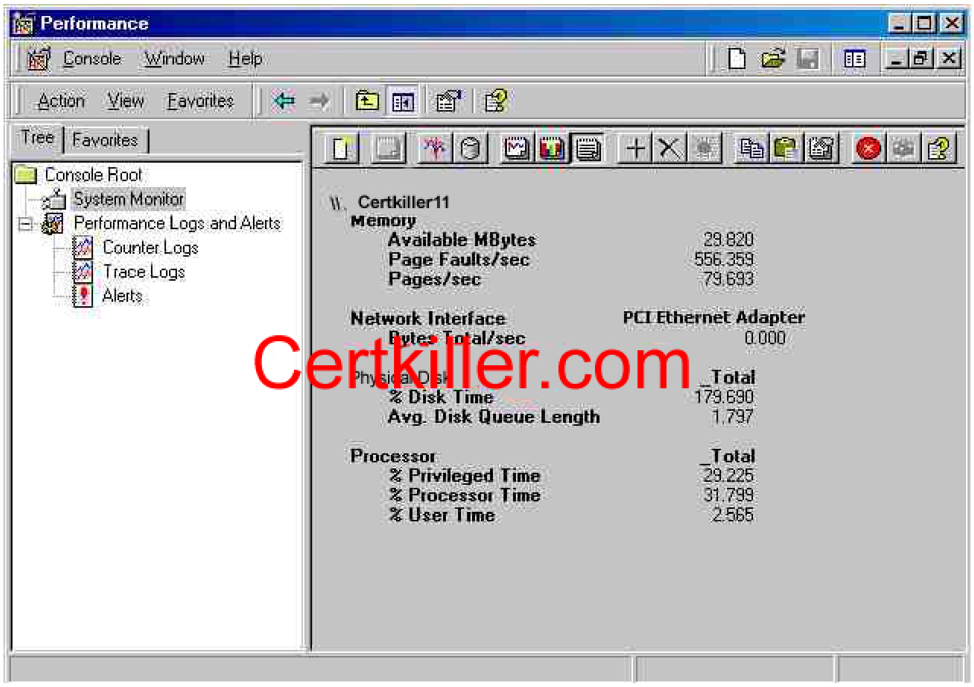
A. Create a counter log and specify SQL Database as the log file type.
B. Create a trace log and specify Circular Trace File as the log file type.
C. Create a counter log and specify Binary Circular File as the log file type.
D. Create a trace log and specify Sequential Trace File as the log file type.

Answer: A

Explanation: Logging to a relational database instead of a standard text file has the advantage that relationships between data tables enable the flexible creation of dynamic data views by using queries and

reports. Counter logs record data about hardware usage, of which the print queue is an example, as well as the activity of system services. We should therefore create a counter log to monitor print queue usage. Furthermore, we want to store the data generated by the counter log in a central location. Counter logs can be created in a number for file types. These are: comma-delimited (.csv) text files, tab-delimited (.tsv) text files, binary-format (.blg) log files, circular, binary-format (.blg) log files, to a SQL database. Of these only the SQL database is stored in a central location (on the SQL Server); all the others are stored on the local computer. We should thus use SQL database as the file type.
Incorrect Options:
B: Trace logs track applications and processes. The print queue usage is not applications and processes and thus cannot be tracked using a trace log. Counter logs on the other hand record data about hardware usage, of which the print queue is an example. We should therefore create a counter log rather than a trace log to monitor print queue usage. Furthermore, a circular trace log - file records data continuously to the same log file, overwriting previous records with new data when the file reaches its maximum size. This thus does not allow us to archive the data for 5 years. In addition, a circular trace log file can only be written to the local computer. We must store the data in a central location. We therefore cannot use a circular trace log file.
C: The counter logs record data about hardware usage, of which the print queue is an example, as well as the activity of system services. We should therefore create a counter log to monitor print queue usage. However, a circular, binary-format trace log file also records data continuously to the same log file, overwriting previous records with new data when the file reaches its maximum size. This thus does not allow us to archive the data for 5 years. Furthermore, a circular, binary-format trace log file can only be written to the local computer. We must store the data in a central location. We therefore cannot use a circular, binary-format trace log file.
D: Trace logs track applications and processes. The print queue usage is not applications and processes and thus cannot be tracked using a trace log. Counter logs on the other hand record data about hardware usage, of which the print queue is an example. We should therefore create a counter log rather than a trace log to monitor print queue usage. Furthermore, a sequential trace log file collects data until it reaches its maximum size and then closes and starts a new file. However, sequential trace log file can only be written to the local computer. We must store the data in a central location. We therefore cannot use a sequential trace log 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 733-6.
Lisa Donald with Suzan Sage London and James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, pp 374-9, 446-51

QUESTION 277
You are the network administrator for Certkiller , which operates five branch offices. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.
The network includes a member server that runs Microsoft SQL Server and hosts an inventory database. The database is continually updated during business hours by users from all branch offices. Users report extremely slow response times when they query the database. You investigate the problem and use System Monitor to create the chart shown in the exhibit.



```
\\Certkiller11
 Memory
     Available MBytes                 29.820
     Page Faults/sec                 556.359
     Pages/sec                        79.693

 Network Interface          PCI Ethernet Adapter
     Bytes Total/sec                        0.000

 PhysicalDisk                         _Total
     % Disk Time                     179.690
     Avg. Disk Queue Length            1.797

 Processor                            _Total
     % Privileged Time                29.225
     % Processor Time                 31.799
     % User Time                       2.565
```

Certkiller.com

You need to bring response times within acceptable limits.
What should you do?

A. Add additional RAM.
B. Add a second processor.
C. Add an additional network adapter.
D. Upgrade the disk subsystem.
Answers: A

Explanation: The output as illustrated by the System Monitor shows that there is too little memory available. By adding RAM you can bring the response time within acceptable limits. Excessive swapping as well as updating of data degrades the performance of the computer insofar as response time is concerned. This can be addressed either by reducing the demands on the computer or increasing the amount of physical RAM. In this case it is a matter of additional RAM that is needed.
Incorrect answers:
B: Adding a second processor will not necessarily speed up querying performance. It will probably only increase the cache.
C: Due to the database being updated continually you will not solve the problem by adding in an additional network adapter.
D: Upgrading the disk subsystem will not address the problem of slow response times when querying the database because the database is not stagnant. It is updated continually.
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. 68

QUESTION 278
You are the network administrator for your company. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.

Terminal Server is installed on a member server named Server1, which is located in an organization unit (OU) named Servers.
User of Server1 report unacceptable response times.
To investigate, you start Task Manager on Server1. You discover that the average CPU usage is 80 percent. However, when you select the Processes tab, none of the processes show significant CPU usage.
You need to identify the process that is responsible for the CPU usage.
What should you do?

A. In Task Manager, select the Show processes from all users option.
B. From a command prompt, run the query process command.
C. Open the Terminal Services Manager. Select Server1 from the list of servers, and then select the Processes tab.
D. Edit the Group policy object (GPO) for the Servers OU by adding your user account to the Profile a single process policy. Then use Task Manager to re-examine Server1.

Answer: A

Explanation: You know something eats up most of your CPU, but you are unable to see it through Task Manager. By default, Window Task Manager only displays tasks which are owned by you. Since the system is running Terminal services, that means the system is used by more than one user. You need to view Processes from all users.
Incorrect
Answer:
B: Running the query process is wrong, because "query process" command only displays something like: process, ID, PID, image.
C: Opening the Terminal Services Manager. Selecting Server1 from the list of servers, and then selecting the Processes tab will not suffice, because it only displays: user, session, ID, PID, image.
D: Editing the Group policy object (GPO) for the Servers OU by adding your user account to the Profile a single process policy. Then using Task Manager to re-examine Server1 would be obsolete.
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. 576-580

QUESTION 279
You are the network administrator for Certkiller . All network servers run Windows Server 2003. A server named Certkiller Srv hosts applications for network users.
Certkiller Srv contains a motherboard that can support two CPUs. One CPU is currently installed.
Certkiller Srv has 512 MB of RAM and a single 36 - GB integrated device electronics (IDE) hard disk.
It has a 10 MB Ethernet card connected to a 10/100 Mb switch.
After Certkiller Srv is in use for five months, network users report unacceptable response times on their applications.
You open System Monitor on Certkiller Srv and see the information shown in the following table.

Counter	**Minimum**	**Maximum**	**Average**
Memory – Pages/sec	0.00	31.97	1.22

Logical Disk – Avg. Disk Queue Length	.69	20.61	9.73
Processor - % Processor Time	3.00	100.00	5.15
Network Interface – Bytes/sec	189.72	2927.84	379.46

You need to improve the performance of Server 1.
What should you do?

A. Add an additional CPU.
B. Add an additional 512 MB of RAM.
C. Replace the existing hard disk with a faster one.
D. Replace the 10-Mb Ethernet card with a 100-Mb Ethernet card.

Answer: C

Explanation: The average disk queue length should not exceed two. According to the table all the other counters are within an acceptable range.
Incorrect answers:
A: According to the System Monitor table the CPU figures does not indicate a problem.
B: Additional RAM will not enhance the performance time for the users who connect to Certkiller Srv. It will at best improve only the performance of the server itself and not that of the client computers.
D: Most Ethernet-based networks run at 100Mbps or below.
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. 745

QUESTION 280
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.
Certkiller .com purchases a host-connectivity gateway application developed by an independent software vendor. You need to install the application on a Windows Server 2003 computer named Certkiller 2.
A support technician named Marie is assigned to install the application. Marie's user account is not a member of the Administrator's group on Certkiller 2. The installation fails and displays an error message stating the user account used for installing the application needs to be a member of the local Administrators group.
Your user account is a member of the Domain Admins group. You want to enable Marie to install applications, but you do not want her to be able to make other changes on Certkiller 2.
What should you do?

A. Log on locally on Certkiller 2 as the local administrator. On Certkiller 2, in Control Panel, start Add or Remove Programs. Instruct Marie to install the application.
B. Use the Run as option to start the Add or Remove Programs Control Panel item on Certkiller 2. Provide the credentials of the local Administrator account. Instruct Marie to install the application.

C. Make Marie's user account a member of the local Administrators group on Certkiller 2. Instruct him to log on locally by using his user account and to install the application.
D. Instruct Marie to log on locally and to send a Remote Assistance request to you. Accept the request, and take remote control of the session. On Certkiller 2, in Control Panel, start Add or Remove Programs. Instruct Marie to install the application.

Answer: B

Explanation: The Run As option allows you to use a secondary logon process to log on to a computer using administrative credentials in order to perform a specific task. For security purposes, it is recommended that you use the Run As option when performing administrative tasks as opposed to logging into a computer or domain with an administrative account. You can use the Run As option through most Windows programs, some Control Panel items, and the Microsoft Management Console (MMC). You can also use the Run As option with command-line utilities.
The Domain Admins group has complete administrative rights over the domain. By default, the Administrator user account is a member of this group.
Since Marie is not a member of the Administrator's group on Certkiller 2, you should follow option B to enable Marie to install the application from her user account.
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. 165

QUESTION 281
You are a network administrator for Certkiller .com. All servers run Windows Server 2003.
A server named Certkiller 6 runs an application named App1. Certkiller 6 has one network adapter installed. App1 uses a large amount of network bandwidth per client connection. You suspect the network connection on Certkiller 6 is running out of available network capacity.
You need to view how much total network bandwidth is being used on Certkiller 6.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Use System Monitor to configure the Network Interface object.
B. Run the netstat command.
C. In Task Manager, monitor the Networking tab.
D. Use Network Monitor to configure a capture filter for the local area connection.

Answer: A, C

Explanation: It is important to monitor the network usage of your servers so that you can detect network bottlenecks. You will be able to monitor network usage by using either the Performance console or Task Manager.
The Networking tab displays network activity. This tab is displayed only if one or more network adapters are present. This tab provides information on the availability and the quality of network resources. A graph indicates the amount of associated traffic when you select each network resource.
• You should be using the Network Monitor tool to manage large network traffic situations. (This is not installed by default in the Windows Server 2003 installation. You might need to install it via

Add/Remove Programs in Control Panel in order to use it.)
Incorrect answers:
B: Making use of the netstat command will not yield the proper results for you with which to see how much bandwidth is being used on Certkiller 6.
D: Configuring a capture filter for the local area connection through the Network Monitor will not suffice as you should be using Event Viewer instead.
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. 725, 746.

QUESTION 282
You are the network administrator for your company. All network servers run Windows Server 2003. Business hours are 8 A.M. to 5 P.M. You provide network assistance during business hours only.
A server named Server1 stores personal files for all network users. Mobile users access Server1 by using the company's VPN. They must have 24-hour access to the files on Server1.
You need to be able to identify the source of the recurring slowdowns in VPN access.
First, you log on to Server1.
What should you do next?

A. Use Task Manager to review network utilization of the VPN adapter.
B. Use the Performance console to create a log of network utilization outside of business hours.
C. Use System Monitor to review network utilization of the VPN connection.
D. Use Task Manager to select Bytes Sent as the Network Adapter History setting.

Answer: C

Explanation: We are required to monitor the network utilization of the VPN connection over a period of time (at least 24 hours). This can be done by making use of System Monitor.
Incorrect Answers:
A: Task Manager doesn't log performance. It only displays a real time set of values, thus you cannot view network utilization of the VPN adapter.
B: We need to log network utilization throughout the whole day, not just out of business hours.
D: Task Manager only displays a real time set of values is does not log performance.
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. 624-628

QUESTION 283
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.
Terminal Services is installed on three servers running Windows 2000 Server. Remote users use the terminal servers to access the company intranet so they can read e-mail and submit time sheets. To make a connection, users choose a terminal server from a list. This process generates help desk requests.
Over time, the remote user load increases. The existing terminal server cannot support the number of

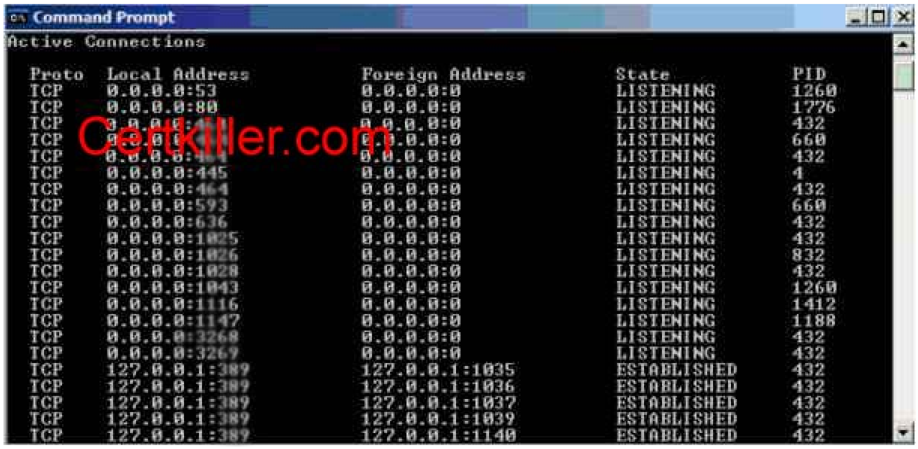
concurrent connections.
You need to create a new terminal server to assist in handling the load. However, you must not add any new server names to the list of terminal servers.
First, you upgrade all three servers to Windows Server 2003 with Terminal Server installed.
What should you do next?

A. Create a Session Directory terminal server farm.
B. Configure the Windows Cluster Services on each terminal server.
C. Install and configure Network Load Balancing.
D. Install and configure round robin DNS.

Answer: C

Explanation: Network Load Balancing (NLB) is a technology that allows for efficient utilization of multiple network cards.
A cluster is a set of computers joined together in such a way that they behave as a single system. Clustering is used for network load balancing as well as fault tolerance. In data storage, a cluster is the smallest amount of disk space that can be allocated for a file.
Round Robin works by creating multiple host records in DNS for one machine. Each record points to a different IP address. As clients make requests, DNS rotates through its list of records.
In addition to the before mentioned, to configure a terminal server cluster, you need a load-balancing technology such as Network Load Balancing (NLB) or DNS round-robin. The load-balancing solution will distribute client connections to each of the terminal servers.
Now, keeping this in mind you will find that this is a rather tricky question: because Answer A is needed to run terminal services on multiple terminal servers in a Network Load Balancing Cluster.
Terminal Server Session Directory is a feature that allows users to easily and automatically reconnect to a disconnected session in a load balanced Terminal Server farm. The session directory keeps a list of sessions indexed by user name and server name. This enables a user, after disconnecting a session, to reconnect to the correct terminal server where the disconnected session resides to resume working in that session. This reconnection will work even if the user connects from a different client computer.
However, the question pertinently asks, "What should you do next?" The next step is to install and configure Network Load Balancing. NLB is a prerequisite for creating a Session Directory terminal server farm.
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. 750, 757, 766
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. 883

QUESTION 284
Exhibit



Certkiller.com

```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:53             0.0.0.0:0              LISTENING       1260
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       1776
  TCP    0.0.0.0:[illegible]    0.0.0.0:0              LISTENING       432
  TCP    [illegible]            0.0.0.0:0              LISTENING       660
  TCP    0.0.0.0:[illegible]    0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:464            0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:593            0.0.0.0:0              LISTENING       660
  TCP    0.0.0.0:636            0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING       832
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:1043           0.0.0.0:0              LISTENING       1260
  TCP    0.0.0.0:1116           0.0.0.0:0              LISTENING       1412
  TCP    0.0.0.0:1147           0.0.0.0:0              LISTENING       1188
  TCP    0.0.0.0:3268           0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:3269           0.0.0.0:0              LISTENING       432
  TCP    127.0.0.1:389          127.0.0.1:1035         ESTABLISHED     432
  TCP    127.0.0.1:389          127.0.0.1:1036         ESTABLISHED     432
  TCP    127.0.0.1:389          127.0.0.1:1037         ESTABLISHED     432
  TCP    127.0.0.1:389          127.0.0.1:1039         ESTABLISHED     432
  TCP    127.0.0.1:389          127.0.0.1:1140         ESTABLISHED     432
```

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. A server named Certkiller 1 runs an application named Certkiller App3.
Users report that Certkiller App3 is performing slowly. You suspect that an unauthorized application is installed on Certkiller 1. You run the netstat command and examine the output, as shown in the exhibit.
You need to identify the unauthorized application by using the output from the netstat command.
Which tool should you use to identify the application?

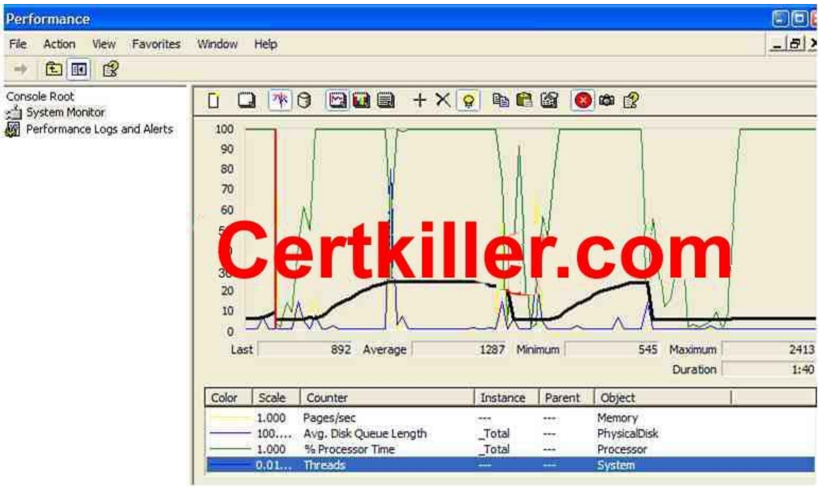
A. Performance console
B. System monitor
C. Network Monitor
D. Task manager

Answer: D

Explanation: Task Manager offers you a quick glimpse at the following items: Applications currently in use, Processes currently running, current processor usage, Current paging file usage, overall current memory usage, Current network utilization and currently logged-on users.
Incorrect answers:
A: Performance MMC snap-in is a utility for monitoring, tracking, and displaying a computer's performance statistics, both in real time and over an extended period for establishing a system baseline. This console includes the System Monitor node and the Performance Logs and Alerts node.
B: System Monitor is a node in the Performance MMC snap-in for monitoring and logging computer performance statistics using performance objects, counters, and instances.
C: You should be using the Network Monitor tool to manage large network traffic situations.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6

QUESTION 285
You are a network administrator for Certkiller .com. All servers run Windows Server 2003.
A server named Certkiller 1 functions as an application server. Certkiller 1 runs several applications.
Certkiller 1 is located on Certkiller 's perimeter network. You allow communication to Certkiller 1 only

over port 80.
Users report that applications on Certkiller 1 perform poorly during periods of peak activity. You monitor Certkiller 1. The results are shown in the exhibit.



Certkiller.com

Last 892 Average 1287 Minimum 545 Maximum 2413
Duration 1:40

Color	Scale	Counter	Instance	Parent	Object
—	1.000	Pages/sec	---	---	Memory
—	100....	Avg. Disk Queue Length	_Total	---	PhysicalDisk
—	1.000	% Processor Time	_Total	---	Processor
—	0.01...	Threads	---	---	System

You need to identify which process is causing Certkiller 1 to perform poorly.
Which two tools can you use to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Event Viewer
B. Task Manager
C. Network Monitor
D. System Monitor

Answer: B, D

Explanation: Administrators often must perform situational real-time monitoring to answer questions about server performance from users, management, other systems administrators, and systems engineers. Task Manager is valuable when you must quickly evaluate processor usage, page file usage, and network usage. Performance monitor provides you with additional counters that can you can use to analyze problems as you view interrupts per second, queue lengths, pages per second, and so on. The Task Manager displays all the applications and processes on the Windows Server 2003 computer. It also displays some common performance measures. The Task Manager can be invoked in many ways. The System Monitor is the primary tool for monitoring system performance.
Incorrect answers:
A: Event Viewer is a MMC snap-in that displays the Windows Server 2003 event logs for system, application, security, directory services, DNS server, and File Replication Service log files.
C: System Monitor is a node in the Performance MMC snap-in for monitoring and logging computer performance statistics using performance objects, counters, and instances.
References:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6

QUESTION 286
You are a network administrator for Certkiller .com. The network contains a Windows Server 2003

computer named Certkiller 4, which functions as a file server.
Certkiller 4 contains several applications. One application is named App1. Another application is named App2. Users report that App2 is performing poorly. You examine Certkiller 4 and discover that App1 was started by using the start app1 /realtime command.
You need to ensure that no other application was started by using the /realtime switch.
What should you do?

A. Use Performance Monitor to create a trace log.
Trace Process creations/deletions.
B. Use Performance Monitor to create a trace log.
Trace Thread creations/deletions.
C. Use Task Manager to view processes.
View the Base Priority column.
D. Use Task Manager to view performance.
On the View menu, select Show Kernel Times.

Answer: C

Explanation: If we want to check this we must use Task Manager to view processes. View the Base Priority column. The Task Manager provides a snapshot of the applications and the processes running on the system. You can view the CPU activity and the memory utilization using graphs. You can also view, start, and stop applications using the Task Manager. Some other benefits include manipulating processes, monitoring network traffic, and monitoring user activity. The Task Manager enables you to manage the applications and the processes of the system. You can monitor memory and CPU activity using graphs.
Incorrect answers:
A: You must view processes through the task Manager by checking the Base Priority column. Creating a trace log to trace creations/deletion will not work in this scenario.
B: In this particular case you are required to view processes through the task Manager by checking the Base Priority column. Creating a trace log to thread creations/deletion is not what is required.
D: You must view processes not performance.
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. 784 - 785.

QUESTION 287
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 member server named CK1 contains a single SCSI hard disk. Users report that server performance is slow.
You configure System Monitor to report performance values for CK1 at regular intervals. System Monitor reports the following values over six 30-second intervals.

Computer name	**Interval 1**	**Interval 2**	**Interval 3**	**Interval 4**	**Interval 5**	**Interval 6**
PhysicalDisk, & Disk Read Time	5	2	8	3	0	1
PhycialDisk, % Disk Write Time	20	30	5	15	35	30

You need to improve disk performance.
What should you do?

A. Replace the existing hard disk with a striped volume that uses disks with performance characteristics similar to those of the existing hard disk.
B. Replace the existing hard disk with a RAID-5 disk array that uses disks with performance characteristics similar to those of the existing hard disk.
C. Use Disk Management to clear the Compress drive to save disk space option on the dynamic volume.
D. Use Disk Management to disable write caching on the physical disk.

Answer: A

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.

Incorrect answers:
B: 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.
C: Compression is usually implemented in cases where space needs to be conserved. The question does not mention or ask for space to be used or saved.
D: Caching is process used to enhance performance by retaining previously-accessed information in a location that provides faster response than the original location.
Hard disk caching is used by the File and Print Sharing for Microsoft Networks service, which stores recently accessed disk information in memory for faster retrieval. Thus disabling caching on the physical disk will result in slower performance.
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 288

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 member server named Certkiller 1 runs IIS and hosts all content for company Web sites.
One Web site is redesigned. When you browse the redesigned site, you select a hyperlink and receive the following error message: "HTTP Error 404 - File or directory not found." You verify that a necessary content file is missing from Certkiller 1.
You need to discover whether the same error was generated by any other Web server requests.
What should you do?

A. Open the most recent file in C:\windows\system32\inetsrv\History.
Search for error entries of type 404.
B. Open the most recent file in C:\windows\system32\LogFiles\W3SVC1.
Search for error entries of type 404.
C. Open Event Viewer and connect to Certkiller 1.
Filter the system event log to display only events from the IISLOG event source with event ID 404.
D. Open Event Viewer and connect to Certkiller 1.
Filter the application event log to display only events from the WebClient event source with event ID 404.

Answer: B

Explanation: Not Found Objects generate the 404 Not Found error. IIS logs typically reside in %Windir%\System32\Logfiles\W3svc1. By searching for the error type 404 file in the most recent file would be the logical step to take in checking for the same error by other Web server requests.
The Web server cannot find the file or script you asked for. Please check the URL to ensure that the path is correct.
Contact the server's administrator if this problem persists.
By reviewing the IIS logs at a later time, you can identify these errors and take necessary actions to fix them.
These logs are stored by default in C:\windows\system32\LogFiles\W3SVC1.
Incorrect Answers:
A: The IIS logs are not stored in C:\windows\system32\inetsrv\History.
C: The errors are not stored in the system log.
D: The errors are not stored in the application log.
Reference:
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 9: 15.

QUESTION 289

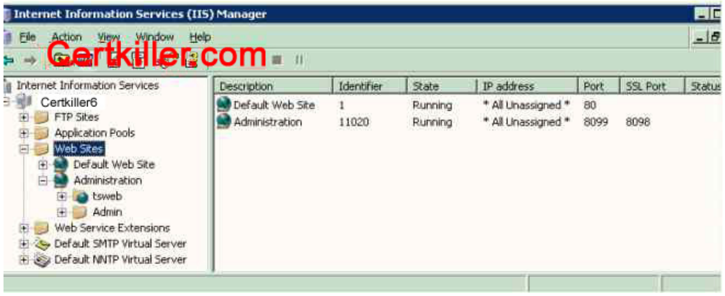
You are the network administrator for Certkiller .com. In particular you administer a Windows 2003 server named Certkiller 3. Certkiller 3 functions as an application server and runs IIS.
You discover that one of the IIS sites on Certkiller 3 is corrupted.
You need to recover the IIS site settings. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Restore the IIS configuration settings by running the iisweb.vbs /create command.
B. Open IIS Manager, and restore a previous version of the site.
C. Restore the IIS configuration settings by running the iisback.vbs /restore command.
D. Restore the IIS configuration settings by running the iisback.vbs /backup command.

Answer: C

Explanation: Making use of the iisback.vbs /restore command will recover your site settings with the least amount of administrative effort.
Incorrect answers:
A: You do not restore settings by creating new ones. This involves too much administrative effort.
B: You need to restore the IIS configuration settings and not a previous version of the site.
D: This option states the wrong parameter on the command, you need to restore not backup.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 290
Exhibit



Certkiller.com

- Internet Information Services
  - Certkiller6
    - FTP Sites
    - Application Pools
    - Web Sites
      - Default Web Site
      - Administration
        - tsweb
        - Admin
    - Web Service Extensions
    - Default SMTP Virtual Server
    - Default NNTP Virtual Server

Description	Identifier	State	IP address	Port	SSL Port	Status
Default Web Site	1	Running	* All Unassigned *	80		
Administration	11020	Running	* All Unassigned *	8099	8098	

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.
You install the Remote Administration tools on server named Certkiller 6, selecting all default settings.
In Internet Explorer, you type https:// Certkiller 6/admin. You receive the following error message:
"HTTP Error 404 - File or directory not found."
You open IIS Manager and see the configuration shown in the exhibit.
You need to ensure that you can use Internet Explorer to administer Certkiller 6.
What should you do?

A. In Internet Explorer, type http:// Certkiller 6:8099
B. In Internet Explorer, type http:// Certkiller 6
C. Install the Remote Desktop Connection subcomponent of the World Wide Web services.
D. In Internet Explorer, type https:// Certkiller 6:8098
E. In Internet Explorer, type https:// Certkiller 6

Answer: D

Explanation: You should type https:// Certkiller 6:8098 to make sure that you can make use of the Internet Explorer to administer Certkiller 6 since the SSL port is 8098 as shown in the exhibit. You must use a secure connection. The :8098 in the URL directs the browser to connect to port 8098 on the server instead of the

default port 80.You can change your server to work on a different port in Internet Information Services (IIS) Manager. After you've connected to the server, you'll see the Welcome page.
Incorrect answers:
A, B, E: These are incorrect URLs. These options will not ensure that you can use the Internet Explorer to administer Certkiller 6 since it is advisable to use a secure connection.
C: This option is irrelevant in this scenario.
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. 591-593,647

QUESTION 291
You are the network administrator for Certkiller .com. You manage a computer named Certkiller 3 that runs Windows Server 2003 with the default settings.
You install Terminal Services on Certkiller 3. You attempt to connect to Certkiller 3 by using the URL http:// Certkiller 3/ Certkiller web. You cannot connect to Certkiller 3.
You need to be able to access Terminal Services on Certkiller 3 by using Internet Explorer 6.0.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

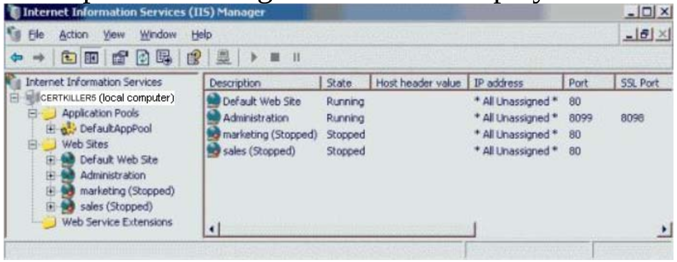
A. Create a new Web site named Certkiller web.
B. Create a new virtual directory named Certkiller web.
C. Install IIS.
D. Install the Remote Administration IIS subcomponent.
E. Install the Remote Desktop Web Connection IIS subcomponent.

Answer: C, E

Explanation: Internet Information Services (IIS) is a group of services that host Internet and intranet-related features on Windows Server 2003 computers such as File Transfer Protocol (FTP) and the World Wide Web (WWW) service under IIS version 6.0. Each of these services must be installed individually; none of these features are installed by default. On the other hand, Remote Desktop Connection is Client software that enables you to access a Terminal Services session that is running on a remote computer while you are sitting at another computer in a different location. Thus by installing IIS and the Remote Desktop Web Connection IIS subcomponent you will be able to access Terminal Services of Certkiller 3 by making use of Internet Explorer 6.0.
Incorrect answers:
A: Creating a new Web site will not address your concern.
B: A virtual directory is a folder that does not have to be located on the IIS server. Creating a virtual directory named Certkiller Web is not the same as being granted access to Terminal Services on Certkiller 3 which is what is required in this question.
D: Installing Remote Administration IIS subcomponent allows up to two remote connections to a server for remote administration purposes. This is not what is needed.
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. 6: 38-49

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

QUESTION 292
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 company Web sites are hosted on a server named Certkiller 5, which runs IIS. You create two new Web sites, Marketing and Sales. You create the appropriate host records on the DNS server. You test both Web sites offline and successfully access all content.
However, when you test the Web site online, you cannot access either site. You are directed to pages on the default Web site.
You open IIS Manager and see the display shown in the exhibit:



Description	State	Host header value	IP address	Port	SSL Port
Default Web Site	Running		* All Unassigned *	80	
Administration	Running		* All Unassigned *	8099	8098
marketing (Stopped)	Stopped		* All Unassigned *	80	
sales (Stopped)	Stopped		* All Unassigned *	80	

You need to ensure that you can start all Web sites on Certkiller 5.
What are three possible ways for you to achieve this goal? (Each correct answer presents a complete solution. Choose three)

A. Specify Marketing. Certkiller .com and Sales. Certkiller .com as the host header names for the two new Web sites.
B. For each new Web site, create a file named Default.htm in the directory path.
C. For each new Web site, specify a unique TCP port.
Ensure that all client computers use the appropriate port to connect to each site,
D. For all Web sites, create custom HTTP headers.
E. For all Web sites, specify unique IP addresses.
Modify the appropriate host records on the DNS server.
F. For all Web sites, enable anonymous access.

Answer: A, C, E

Explanation: To create and host multiple Web sites, you must first ensure that each site has a unique identification. There are three ways to do this:
• You can obtain multiple IP addresses and assign a different IP address to each site.
• You can assign different host header names to each site and use a single IP address. Host header names are the "friendly" names for Web sites, such as www.microsoft.com.
• You can use Nonstandard TCP port numbers, and assign a different port number to each site. This is generally not recommended. This method can be used for private Web site development and testing purposes but is rarely used on production Web servers, because this method requires clients to type in the name or IP address followed by a non standard port number to reach the site.
Incorrect Answers:
B: This can be used to set a default page for each site. However, this will not enable you to host multiple web sites.

D: Custom HTTP headers can not be used to host multiple web sites.
F: Anonymous access will allow anyone to connect to a website. However, this will not enable you to host multiple web sites. It is also a security risk.
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. 646, 663

QUESTION 293
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 2000 Professional.
You install Windows Server 2003 with default settings on a new computer named Certkiller Srv1. You install and share several printers on Certkiller Srv1. You instruct all users to connect to these printers by using the address http:// Certkiller Srv1/Printers.
However, users report that they cannot connect to this address.
You need to ensure that all users can connect to the printers by using HTTP.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

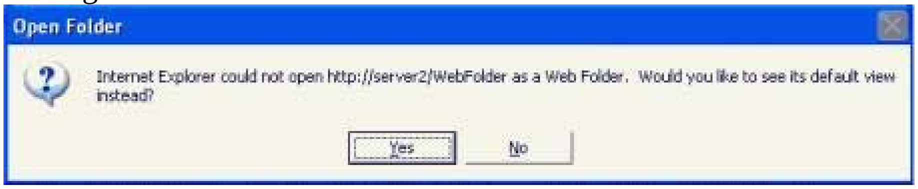
A. Publish all shared printers that are installed on Certkiller Srv1.
B. Create a virtual directory named Printers on Certkiller Srv1.
C. Install IIS with default settings on Certkiller Srv1.
D. Reshare all printers on Certkiller Srv1.
E. Install the Internet Printing component of IIS.
F. Type Net Stat W3SVC at a command prompt.

Answer: C, E

Explanation: The Windows Server 2003 family of operating systems and Windows XP can process print jobs sent to URLs. Windows Server 2003 must be running Microsoft Internet Information Services (IIS). Internet printing uses Internet Printing Protocol (IPP) as its low-level protocol which is encapsulated within HTTP, using it as a carrier. When accessing a printer through a browser, the system first attempts to connect using RPC (on Intranets and LANs), which is fast and efficient.
Incorrect Answers:
A: The printers do not have to be published in Active Directory.
B: Creating a virtual directory named printers will not work.
D: The printers do not need to be reshared.
F: This command will not enable internet printing.
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. 570

QUESTION 294
You are the network administrator for Certkiller .com. All network servers run either Windows 2000 Server or Windows Server 2003, and all client computers run Windows XP Professional.
A computer named Server2 runs Windows Server 2003 with IIS 6.0 installed. On Server2, you create

a virtual directory named WebFolder. You use IIS Manager to enable the following permissions on WebFolder: Read, Write, and Directory Browsing.
When users try to access WebFolder as a Web folder from Internet Explorer, they receive the error message shown in the exhibit.



Internet Explorer could not open http://server2/WebFolder as a Web Folder. Would you like to see its default view instead?

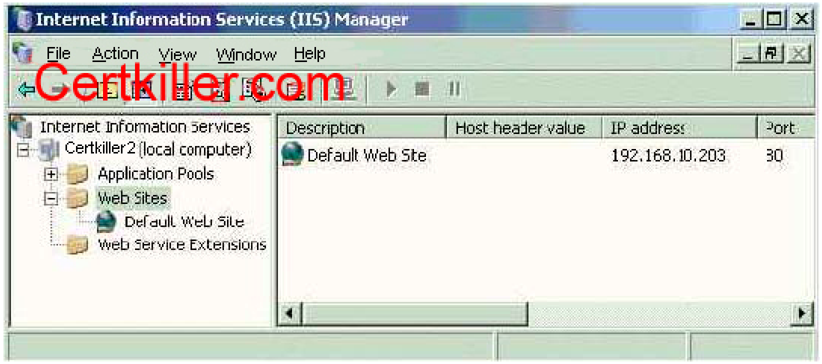
You need to ensure that all users can access WebFolder as a Web folder.
What should you do?

A. Restart the World Wide Web Publishing Service on Server2.
B. Enable anonymous access to WebFolder.
C. Modify the Execute permissions to allow scripts and executable files.
D. Enable the WebDAV Web service extension on Server2.

Answer: D

Explanation: "Web Folders" is Microsoft's implementation of WebDAV. WebDAV is disabled by default and so needs to be enabled.
Incorrect Answers:
A: This will not solve the problem. WebDAV needs to be enabled.
B: This is an unnecessary security risk and is not required.
C: It is not necessary to modify the permissions. We just need to enable WebDAV to ensure that all users can access WebFolder.
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. 658

QUESTION 295
Exhibit


Internet Information Services (IIS) Manager
File
Action
View
Window
Help
Internet Information Services
Certkiller2 (local computer)
Application Pools
Web Sites
Default Web Site
Web Service Extensions

Certkiller.com

Description	Host header value	IP address	Port
Default Web Site		192.168.10.203	30

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.
Your IIS server is named Certkiller 2. Its configuration is shown in the exhibit. Users access the internal network by connecting to http:// Certkiller 2. Certkiller .intra.
A folder Certkiller _Data stores the Web interface for Certkiller .com's client management tool.

Currently, users in the marketing can access this tool by connecting to
http:// Certkiller 2. Certkiller .intra/ Certkiller _Web.
You share Certkiller _Data on a server named Certkiller 6.
You need to modify Certkiller 2 to ensure that marketing users can access Certkiller _data through the internal network.
What should you do?

A. Create a new virtual directory named Certkiller _Web under the default Web site. Specify \\ Certkiller 6\ Certkiller _data as the Web site content directory.
B. Create a new Web site named Certkiller _Dta. Specify \\ Certkiller 6\ Certkiller _data as the Web site home directory.
C. Create a new Web site named Certkiller _Dta. Specify Certkiller _Data as the host head name of the Web site.
D. Redirect the default Web site home directory to http:// Certkiller 6/ Certkiller _Data. Specify Certkiller _Data as the host header name of the default Web site.

Answer: A

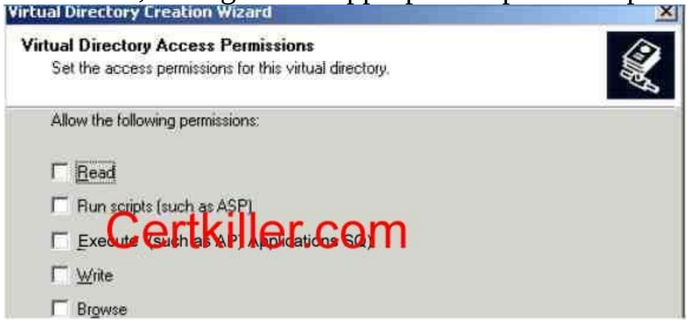
Explanation: The iisvdir.vbs command enables us to create virtual directories for a specific Web site. We can use create, delete, and query switches on this script. It is important to clarify that this command does not generate any new code or physical directories. This command will basically instruct the IIS configuration to point at existing directories and refer to it as a local directory of the Web site. Creating a new virtual directory named Certkiller _Web under the default Web site and then specifying Certkiller _data on Certkiller 6 as the web site content directory will ensure that the marketing users will be able to access Certkiller 2, the IIS server.
Incorrect answers:
B, C: There is no need to create a new Web site.
D: This is not necessary.
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. 696-699

QUESTION 296
You are the network administrator for Certkiller .com. A computer named Webserver CK1 runs Windows Server 2003. Webserver CK1 gives users access to Certkiller 's internal Web site.
A folder named D:\Webfolders\Sales on Webserver CK1 contains Certkiller 's sales reports. The NTFS permissions for the Sales Folder are set as shown in the following table.

Group Name	**Permissions**
Administrators	Full Control
Sales	Modify
Users	Read & Execute

You need to create a new virtual directory for the sales department on Webserver CK1 and configure it to meet the following requirements:
• The new virtual directory must be accessible as a Web folder.

• Members of the Sales group must be able to upload Microsoft Word documents and HTML files.
• No dynamic content is allowed to be run from the virtual directory.
What should you do?
To answer, configure the appropriate option or options in the dialog box in the work area.



Virtual Directory Creation Wizard

Virtual Directory Access Permissions
Set the access permissions for this virtual directory.

Allow the following permissions:

□ Read
□ Run scripts (such as ASP)
□ Execute (such as ISAPI applications or CGI)
□ Write
□ Browse

Certkiller.com

Answer:
Select the Read, Write and Browse checkboxes.

Explanation: Select the access permissions from the Virtual Directory Access Permissions window. The default is Read and Run Scripts. The options are very similar to Web site creation options. These options will allow members of the Sales Group to upload Microsoft Word documents and HTML files as well as not allowing any dynamic content to be run from the virtual directory.
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. 697

QUESTION 297
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 member server named CK1 has IIS installed.
You are directed to provide Internet-based users with a hierarchical list of files that they can download. You copy the list to C:\inetpub\wwwroot\data on CK1 . You create a new virtual directory named ListData, and you specify its path as C:\inetpub\wwwroot\data.
When users try to access ListData, they receive the following error message: "Directory Listing Denied". This Virtual Directory does not allow contents to be listed".
You need to ensure that users can successfully access ListData.
What should you do?

A. Assign the Allow - Read permission on C:\inetpub\wwwroot\data to the Anonymous user account.
B. Use IIS Manager to enable directory browsing.
C. Edit the properties of the Directory Listing Denial error code with CK1 .
Change the message type to File and specify the file name as index.htm.
D. Use IIS manager to allow anonymous access.

Answer: B

Explanation: Directory Browsing displays a list of files and subfolders in the home directory if a default web page is not defined or is absent. Enabling Web Service Extensions - Web Service Extensions is a new feature in IIS 6.0.This utility will give a Control Panel-like functionality on your IIS components. We will be able to allow, prohibit, or change IIS properties using this tool. This will also enable you to add new IIS extensions (ISAPI applications and third-party IIS tools) to the IIS 6.0 server. You can also enable or disable All Web Service Extensions by using this management console. Here is a list of components the Web service extensions can enable or disable.

- ASP.NET executions
- ASP executions
- CGI and ISAPI Applications
- Front Page Server Extensions 2000 and 2002
- WebDAV support for IIS directories

We can get to the Web Service Extensions by using Start | Administrative Tools | IIS Manager and clicking on Web Server Extensions node on a selected server name.

IIS Manager is the GUI interface for all IIS management functions. You can also perform these management functions by using command-line tools. All these command line tools are VBScript functions with *.VBS file extensions.

- The insweb.vbs utility is used to create and manage Web sites in IIS 6.0.
- The iisvdir.vbs command enables us to create virtual directories for a specific Web site. We can use create, delete, and query switches on this script. It is important to clarify that this command does not generate any new code or physical directories. This command will basically instruct the IIS configuration to point at existing directories and refer to it as a local directory of the Web site.

Incorrect answers:

A: Assigning the Allow - Read permission will not work because you need to make use of the insweb.vbs utility.

C: Editing the properties of the Directory Listing Denial error code with CK1 will not enable access to the directory.

D: This option will not work as users will have to authenticate to get access.

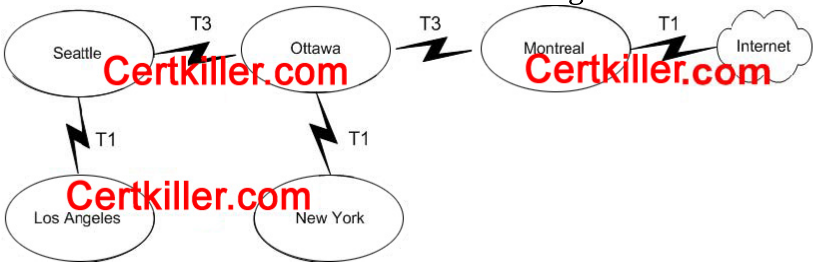
Reference:

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. 677, 692

QUESTION 298

You are the network administrator for Certkiller . All servers run Windows Server 2003.

Certkiller 's main office is located in New York City, and four branch offices are located in various North American cities. The network is configured as shown in the exhibit.



Access to the Internet is provided by a Network Address Translation (NAT) server locate din the Montreal office. The IP address of the NAT server is 192.168.10.254.

Users in the Los Angeles office report that they cannot connect to the Internet. Users in the New York

office report that they can successfully connect to the Internet. From a computer in the Los Angeles office, you cannot connect to servers located in the Montreal office by using their IP address.
You want to find out where the communication failure resides by running a command prompt on a computer in the Los Angeles office.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Run the pathping 192.168.10.254 command.
B. Run the net view \\192.168.10.254 command.
C. Run the tracert 192.168.10.254 command.
D. Run the nslookup 192.168.10.254 command.

Answer: A, C

Explanation: Ping is a command used to send an Internet Control Message Protocol (ICMP) echo request and echo reply to verify that a remote computer is available. Tracert is a tool used to map out the path that the packets are taking as they flow to a remote system.
The pathping tool provides the functionality of both ping and tracert and adds some of its own features into the mix as well. The first list in the output is the route that the packet takes to reach the destination. This is similar to the output of the tracert command. These two commands will enable you to find where the communication failure resides.
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. 81

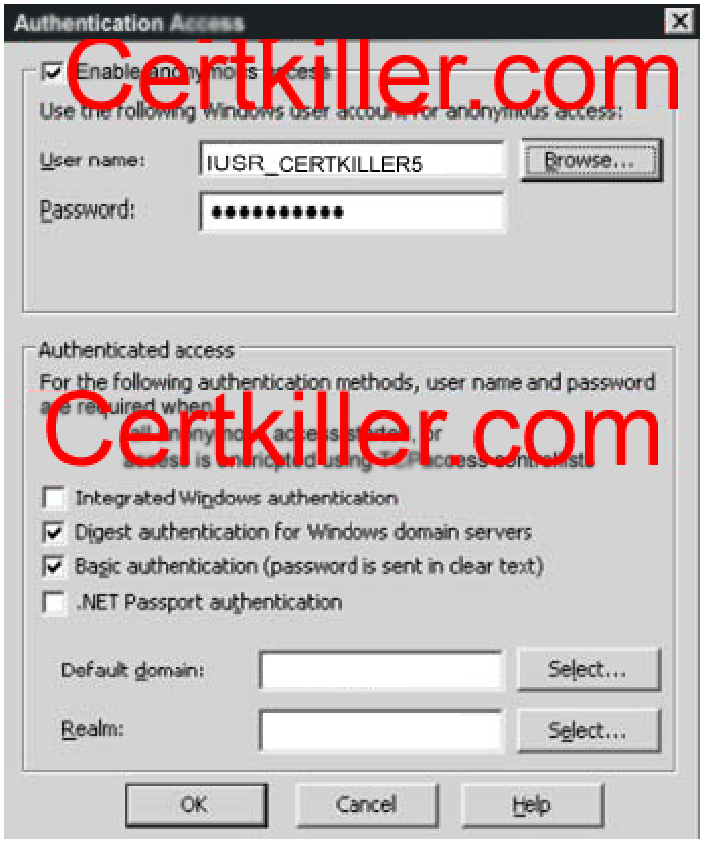
QUESTION 299
You are the network administrator for Certkiller . All servers run Windows Server 2003.
Twenty Certkiller employees connect to a terminal server named Certkiller 1 to run applications and to gain access to the Internet.
The 20 employees report that they receive security messages while browsing Internet Web sites. The employees report that they cannot modify the Internet Explorer security settings on their client computers while connected to Certkiller 2.
You need to allow these 20 employees to modify the Internet Explorer security settings in their client computers while connected to Certkiller 2.
What should you do?

A. Log on to Certkiller 2 as Administrator and add http:// to the list of trusted sites in Internet Explorer.
B. Instruct the 20 employees to add http:// to the list of trusted sites in Internet Explorer on their client computers.
C. Instruct the 20 employees to change the Internet Explorer privacy settings on their client computers to Low.
D. Uninstall Internet Explorer Enhanced Security Configuration on Certkiller 2.

Answer: D

QUESTION 300

Exhibit



Authentication Access

☑ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_CERTKILLER5

Password: ●●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Integrated Windows authentication

☑ Digest authentication for Windows domain servers

☑ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm:

Certkiller.com
Certkiller.com

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

You install Windows Server 2003 on a computer named Certkiller 5. Certkiller 5 has IIS installed and is a member of the Certkiller .com domain. You create a new Web site for the sales department on Certkiller 4. The home directory for the sales Web site is C:\Inetpub\Sales.

Users from the sales department report that they are prompted for credentials when they attempt to connect to the sales Web site. After they enter their login information, they are denied access to the Sales Web site. Users from other departments observe the same behavior when they attempt to access the Sales Web site.

You examine the directory security for the sales Web site, as shown in the exhibit.

You need to ensure that users from sales department can access the sales Web site. You also need to ensure that no other users can access the Sales Web site.

What should you do?

A. Clear the Enable anonymous access check box.

B. Select the Digest authentication for Windows domain servers check box.

C. Clear the Basic authentication check box.

D. Change the value of the Default domain to Certkiller .com.

E. Modify the NTFS permissions on the C:\Inetpub\Sales folder.

Answer: E

Explanation: When you apply NTFS permissions to a folder with subfolders, the default is to allow inheritable permissions to propagate from the parent to this object. This means that whatever permissions have been applied to the parent folder will be automatically applied to subfolders. If you want to make sure that Sales department users can access the website while assuring that other users cannot access the Sales Web site, then you should apply the appropriate NTFS permissions on the C:\Inetpub\Sales folder.
Incorrect answers:
A: Clearing the Enable Anonymous Access check box is not the solution in this case.
B: The Digest Authentication For Windows Domain Servers option works only with Active Directory accounts and sends a hash value rather than a clear-text password. It works across proxy servers and other firewalls. Digest authentication requires Windows 2000 or later client computers. This is not what is desired.
C: The Basic Authentication option requires a Windows 2000 or Windows Server 2003 user account. If anonymous access is disabled or the anonymous account tries to access data that the account does not have permission to access, the system will prompt the user for a valid user account. With this method, all passwords are sent as clear text. You should use this option with extreme caution since it poses a security risk. However this option is not the answer.
D: Changing the value of the Default domain to Certkiller .com will not ensure that other users will not be able to access the Sales Web site.
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. 307, 326-327