Part-7

QUESTION 426
Exhibit, Table

```
-------------------------------------------------------------------------------
        POLICY                            POLICY SETTINGS
-------------------------------------------------------------------------------
Access this computer from the network    Administrators,Backup Operators, Everyone, Power Users, Users
-------------------------------------------------------------------------------
Allow log on locally                     Administrators
-------------------------------------------------------------------------------
Allow log on through Terminal Services   Remote Desktp Users
-------------------------------------------------------------------------------
Deny log on locally                      Domain Users
-------------------------------------------------------------------------------
Perform volume maintenance tasks         Administrators
-------------------------------------------------------------------------------
```

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 user accounts are members of the
Domain Users group.
You manage a server that is a member of the domain. Some administration tasks must be performed
while you are logged on to the server. A new written security policy states that only specified users must
be able to access the server by using Terminal Services. The written security policy also states that only
administrators on the local server must be able to log on locally to the server.
The settings for the server are shown in the table exhibit.
You are a member of the Domain Admins global group. You attempt to perform maintenance tasks on
the server, but you receive an error message stating that the local policy of the computer is preventing
you from logging on locally.
You need to ensure that you can perform the maintenance tasks that are required for the serer. You also
need to meet the requirements of the written security policy.
What should you do?

A. Remove the Everyone group from the Access this computer from the network policy. Add the Domain
Admins group to the Allow log on locally policy.
B. Remove the Domain Users group from the Deny log on locally policy.
C. Add the Administrators group to the Allow log on through Terminal Services policy.
D. Add the Domain Admins group to the Allow log on through Terminal Services policy.

Answer: B

QUESTION 427
You are the administrator of a Windows Server 2003 computer named Certkiller 3. Certkiller 3 has
Terminal Services installed. Certkiller 3 connects to the Internet through a proxy server on the company
network.
Help desk employees periodically access custom web applications on the company network. You install
IIS on Certkiller 3 with all the default settings.
You need to ensure that help desk employees can access Terminal Services on Certkiller 3 from Internet
Explorer 6.0.
What should you do?

A. Uninstall IIS and Terminal Services. Reinstall IIS, and then reinstall Terminal Services.
B. Configure the Internet Connection Firewall (ICF) to allow incoming ports 80 and 3389.

C. Create a new virtual directory named Tsweb.
D. Create a new web site named Tsweb.
E. Install Remote Desktop Web Connection.

Answer: E

QUESTION 428
You are the network administrator for Certkiller .com. You manage a server that runs Windows Server 2003. You use a client computer that runs Windows XP Professional to perform administrative tasks. The network was attacked recently, which prompts you to change the security settings on the server. After you change the settings, you attempt to manage the server by using Remote Desktop. You attempt to connect to the server by using its IP address, but you cannot connect. The Remote Desktop client worked properly before you changed the security settings.
You verify that the server has network access and that you are a member of the local administrators group. You also confirm that Remote Desktop is enabled. You suspect that the Internet Connection Firewall is not configured correctly.
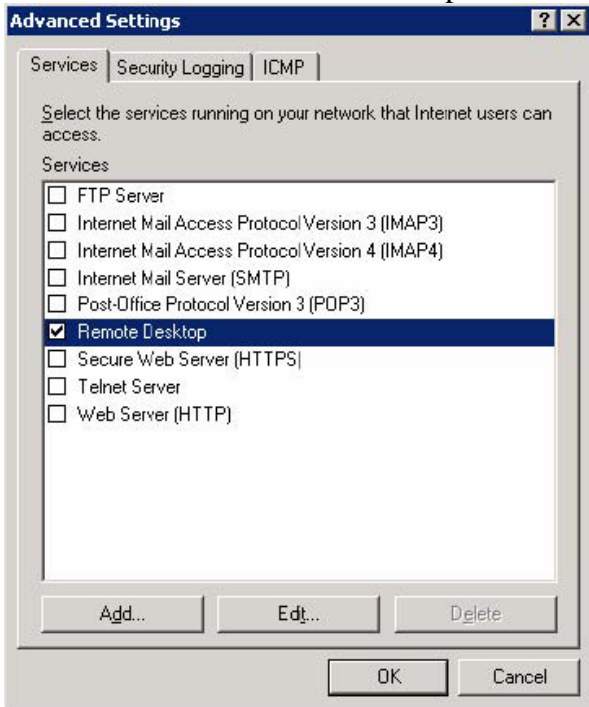You need to maintain the highest possible level of security for the server. You also need ensure that Remote Desktop functions properly.
What should you do?
To answer, configure the appropriate option or options in the dialog box in the work area.
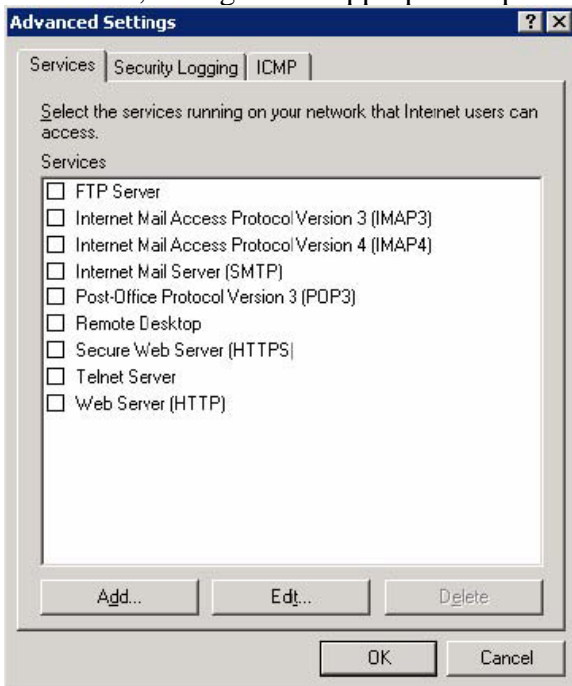
Answer: Tick the "Remote Desktop" checkbox.

QUESTION 429

You are the network administrator for Certkiller .com. The network consists of a single Active
Directory domain named Certkiller .com. All domain controllers run Windows Server 2003.
A member server named Certkiller 3 has IIS installed. Certkiller 3 hosts all content for company web sites.
The server is backed up on magnetic tape once each month.
To replace the web functionality of Certkiller 3, the company acquires a new computer. You configure the
computer as a member server named Certkiller 4 and install IIS. You transfer all content from Certkiller 3
to Certkiller 4 and start the IIS service on Certkiller 4.
You discover that Certkiller 4 is not configured with the IIS settings that were defined on Certkiller 3.
You need to ensure that Certkiller 4 has the same IIS settings that were defined on Certkiller 3.
What should you do?

A. Use the most recent backup tape of Certkiller 3 to restore the System State data on Certkiller 4.
B. Use the most recent backup tape of Certkiller 3 to restore C:\windows\system32\inetsrv\History on
Certkiller 4.
C. Use IIS manager on Certkiller 3 to select the Save Configuration to Disk option. Edit the files to replace
system-specific information. Use the edited files to restore the IIS metabase on Certkiller 4.
D. Use IIS manager on Certkiller 3 to select the Backup/Restore Configuration option. Edit the files to
replace system-specific information. Use the edited files to restore the IIS metabase on Certkiller 4.

Answer: D

QUESTION 430

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

Another Systems Administrator recently installed Software Update Services (SUS) on a server on the
network. You need to troubleshoot a problem that involves SUS.
You need to view the SUS approval log to verify that the latest updates are available to client computers.
What should you do?

A. Open the most recent IIS log file on the SUS server. View the data in the log file.
B. Open the Hotfixes.txt file on the SUS server. View the data in the Hotfixes.txt file.
C. Run the wmic qfe > Approval.txt command on the SUS server. View the data in Approval.txt file
D. Open the file named History-Approve.xml on the SUS server. View the data in the log file.

Answer: D

QUESTION 431
You are the network administrator for Certkiller .com. The network consists of a single Active
Directory domain named Certkiller .com. All domain controllers run Windows Server 2003, and each one
has a locally attached tape device.
You need to back up each domain controller. Your backup process must fulfil the following
requirements:
System recovery must be possible in the event of server failure.
The system configuration and all current dynamic disk configurations must be backed up.
Other data partitions do not need to be backed up.
What should you do?

A. Use the Backup utility to back up the system files and to create an Automated System Recovery (ASR)
disk.
B. Use the Backup utility to back up the contents of all mounted drives.
C. Use the Backup utility to back up only the System State data.
D. Use the Copy command to copy C:\windows and its subfolders to a shared folder on the network.
E. Use the Xcopy command to copy C:\windows and its subfolders to a shared folder on the network.

Answer: A