QUESTION 101
You are the administrator of a Windows 2003 domain Certkiller .com. The domain contains 20 Windows 2000 Professional computers and two Windows 2003 Server computers. For the domain, you want to set an account policy that locks any user's account after three consecutive failed logon attempts. You also want to ensure that only administrators will be able to unlock the account.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Set the Account lockout duration value to 0.
B. Set the Account lockout duration value to 3.
C. Set the Account lockout threshold value to 0.
D. Set the Account lockout threshold value to 3.
E. Set the Reset account lockout counter after value to 0.
F. Set the Reset account lockout counter after value to 3.

Answer: A, D

Explanation: The Account lockout duration security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it.
The Account lockout threshold determines the number of failed logon attempts that will cause a user account to be locked out. A locked out account cannot be used until it is reset by an administrator or the account lockout duration has expired.
Incorrect Answers:
B: Setting the Account lockout duration value to 3 would cause a locked account to become unlocked after 3 minutes.
C: Setting the Account lockout threshold value to 0 would cause the accounts to never be locked out.
E: Setting the Reset account lockout counter after value to 0 determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. A setting of 0 is not possible.
F: Setting the Reset account lockout counter after value to 3 determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts.
References:
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 317

QUESTION 102
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. For security reasons, management decides that a particular user must not be able to log on to the domain after 5:00 P.M. If the user is logged on to the domain at 5:00 P.M., he must be logged off automatically.
You configure the Logon Hours setting for the appropriate user account. That night, you verify that the user cannot log on to the domain after 5:00 P.M. The next day, you notice that the user is still accessing domain resources at 6:00 P.M. You verify that the time on the user's computer and on the domain controller are correct.

You need to ensure that the user is logged off automatically if he is still working on the domain after 5:00 P.M.
What should you do?

A. In Active Directory Users and Computers, on the Sessions tab, configure the End Session setting for the user account. Instruct the user to log off from the domain and log on again.
B. Modify the Default Domain Policy GPO to enforce logoff when logon hours expire.
Ensure that the user's computer has the latest Group Policy settings applied.
C. Remove the user's domain account from the local Administrators group on the user's client computer.
Instruct the user to log off from the domain and log on again.
D. Use Computer Management on the domain controller. Restart the Net Logon service.

Answer: B

Explanation: When you restrict logon hours, you might also want to force users to log off after a certain point. If you apply this policy, users cannot log on to a new computer, but they can stay logged on even during restricted logon hours. To force users to log off when logon hours expire for their account, apply the Network security: Force logoff when logon hours expire policy.
You can assign logon hours as a means to ensure that employees are using computers only during specified hours. This setting applies both to interactive logon, in which a user unlocks a computer and has access to the local computer, and network logon, in which a user obtains credentials that allow him or her to access resources on the network.
Incorrect answers:
A: Option A suggests instructing the user to log off and then on again. This is not what is required.
C: Option C suggests instructing the user to log off and then on again. However, when removing the user's domain account from the local Administrator's group on the user's client computer, you will only be fulfilling half of what is required. You need to ensure that the user is logged off automatically if he is still working on the domain after 5:00 P.M.
D: Restarting the Net Logon service is not what is required in this scenario.
References:
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 582
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 58, 442.

QUESTION 103
Exhibit

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

Directory domain named Certkiller .com. All seven servers are configured as domain controllers and run Windows Server 2003, and all client computers run Windows XP Professional.
Certkiller .com frequently hires temporary employees. You specify account expiration dates when you configure user accounts for temporary employees.
A former temporary employee named Jack King is hired full-time. When Jack tries to log on, she receives the logon message shown in the exhibit.
You need to modify the properties of Jack user account to correct this problem.
What action should you take?

A. Select the Account is locked out option
B. Select the Password never expires option.
C. Set the Account expires option to never.
D. Clear the Account is disabled option.

Answer: C

Explanation: Setting an account expires option is a good feature if you have contract or temporary employees working for you. If you know they are on a six-month contract, go ahead and set their accounts to expire in six months. Some companies set all temporary employee user accounts to expire monthly as a security precaution. If the temporary user leaves the company without notifying the IT department, the account can only be used (or abused) for 30 days. However, in this scenario Jack is made one of the permanent staff and thus you have to set the Account expires option to never.
Incorrect Answers:
A: Selecting the Account is locked out option will not allow Jack to log on.
B: With this option the user's password will not expire. This option overrides the account policy configured for the domain (in the default domain policy GPO). This is not desired as it poses a security risk.
D: Disabling an account does not change any permissions assigned to or settings configured for the user account. It just disables logging on with the account.
References:
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 282-283

QUESTION 104
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named ad. Certkiller ,com. Certkiller also uses a DNS namespace named Certkiller .com for its external Internet communications.
Users in the sales department log on by using their e-mail addresses. A user named Ben Smith works for the sales department. He reports that when he attempts to log by using bsmith@ Certkiller .com, he receives the error message shown in the Error Message exhibit.

The details of Ben's user account are shown in the User Account exhibit.

You need to ensure that Ben can log on by using a user ID that matches his e-mail address.
What should you do?

A. Configure Ben's user account to be trusted for delegation.
B. Configure Ben's user account to require a smart card for interactive logon.

C. In User logon name options, change the user principal name (UPN) for Ben's account.
D. Change the Log On To options for Ben's account.

Answer: C

Explanation: As you can see in the User Account exhibit, his UPN is bsmith@ad. Certkiller .com. We must change this to bsmith@ Certkiller .com. After that he can logon to the domain.
Typing the User logon name automatically fills in the User logon name (pre-Windows 2000) field as well. When you have filled in all necessary information, click Next to continue.
• [/USER:[domainname\]username]
• [/USER:[dotted domain name\]username]
• [/USER:[username@dotted domain name]
The first one [/USER:[domainname\]username] tells you to specify the username in the format of domain name followed by the username. This format uses the one-word NetBIOS-compatible domain name. The second one tells you to specify the username in the format of fully qualified domain name followed by the username. This is the hierarchical Active Directory domain name. The third one tells you to specify the username by using the user principal name (UPN). This format uses the @ sign between the user account name and the domain name, like an Internet e-mail address. The Account tab is where most of the action takes place. This is where you change a user's logon name, the user principal name (UPN), or a user's UPN suffix.
-u <UserName> Connects as <UserName>. Default: the logged-on user. Username can be: username, domain\username, or user principal name (UPN).
Incorrect answers:
A: Delegation trust will not solve the problem that Ben is experiencing. This tab should be left unchecked most of the time. Selecting it could weaken your network security. Setting an account to be trusted for delegation enables a service running as this account to impersonate a client to get access to resources on another machine running the same service.
B: A smart card for interactive logon will not solve Ben problem. This configuration disables logging on without a smart card. The user's password is randomly changed and set to never expire. Active Directory manages the password for the account. This is good for security, but it can be a problem if a user forgets his or her smart card or needs to log on to a machine that does not have a smart card reader.
D: Changing the Log On To options for Ben's account will not solve the problem. Ben needs the UPN to be changed to enable him to log on.
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. 264, 282-284, 334

QUESTION 105
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003. Some user accounts have expiring passwords and some do not.
You need to identify all user accounts that do not have expiring passwords. You need to modify the password property to allow the passwords on these accounts to expire. You must complete this task by using the minimum amount of administrative effort.
First, you create a saved query to obtain a list of all user accounts that do not have expiring

passwords.
What should you do next?

A. Export the query results to a comma-delimited file.
Use a CSVDE script to modify the password property of each user account.
B. From the Results pane of the query, select all user accounts and modify their password properties simultaneously.
C. Export the query results to a comma-delimited file.
Use an LDIFDE script to modify the password property of each user account.
D. From the Results pane of the query, select each user account and modify the password property, one by one.
Answers: B

Explanation: You have created a saved query to obtain a list of all user accounts that do not have expiring passwords. A new feature of Windows 2003 is that you can make changes to the properties of multiple user accounts simultaneously. You can do this by displaying the resultant set of user accounts from the query, selecting them all and accessing the properties of the accounts. Here you can make a change that will apply to all user accounts. To get the desired effect you need to select all users and modify their passwords simultaneously after the query has been run.
Incorrect Answers:
A: A script is not necessary because it is not the quickest way to make the same change to multiple accounts. The csvde (CSV Directory Exchange) command can be used to import and export Active Directory information using files formatted in the Microsoft comma-separated value (CSV), or comma delimited, format. The csvde command can also support batch operations. The csvde command only allows you to add new objects. It does not allow you to modify existing objects.
C: A script is not necessary because it is not the quickest way to make the same change to multiple accounts. The ldifde (LDIF Directory Exchange) command can be used to create, modify, and delete directory objects on Windows Server 2000, Windows Server 2003 and Windows XP Professional. You can also use ldifde to extend the schema, export Active Directory user and group information to other LDAP (Lightweight Directory Access Protocol) applications or services, and populate Active Directory with data from other directory services. The ldifde command, however, uses the LDAP Data Interchange Format (LDIF) file format, which is a draft Internet standard for a file format that may be used to perform batch operations against directories that conform to the LDAP standards.
D: A new feature of Windows 2003 is that you can make changes to the properties of multiple user accounts simultaneously. You don't need to do it one at a time. This option will take much longer than option B though it will achieve the same result after much more administrative effort.
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. 3: 16, 20, 4: 13, 13: 6.

QUESTION 106
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. Half of the client computers run Windows XP Professional and the other half run Windows NT 4.0 Workstation. You install Terminal Server on five member servers named Certkiller SrvC through Certkiller SrvG. You place all five servers in an organizational unit (OU) named Terminal Server. You link a group

Policy object (GPO) to the Terminal Server OU.
Two days later, users notify you, that the performance of Certkiller SrvF is unacceptable slow. You discover that Certkiller SrvF has 75 disconnected Terminal Server sessions.
You need to configure all five terminal servers to end disconnected sessions after 15 minutes of inactivity. You must achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Log on the console of each terminal server. In the RDP-Tcp connection properties, set the End a disconnected session option to 15 minutes.
B. Edit the GPO to set the time limit for disconnected sessions to 15 minutes.
C. On Certkiller SrvC, run the tsdiscon] command to disconnect all 75 users from Certkiller SrvF
D. In Active Directory Users and Computers, set the End a disconnected session option for all domain user accounts to 15 minutes.

Answer: B

Explanation: We can configure a group policy to configure the Terminal Servers to set the time limit for disconnected sessions to 15 minutes.
Note: We are applying this policy to the Terminal Servers, not the users or the client computers.
The Sessions tab enables you to control how long a user may remain actively connected to a session and how long a disconnected session should be allowed to remain on the Terminal Services computer. Even though they are not active, disconnected sessions can use substantial resources on the Terminal Services computer because applications are still running on them. Depending on your environment, it may be advisable to terminate them after a specific period of time.
By default, most of the settings on this page are configured to use the user account property settings and several settings are grayed out. This can be overridden by selecting the check box next to Override user settings.
Incorrect Answers:
A: Using a group policy requires less administrative effort.
C: Ending the current disconnected sessions won't help. We also need to end future disconnected sessions after 15 minutes to prevent the problem reoccurring.
D: This would work for current users, but not future users.
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. 442, 551.

QUESTION 107
Your company network consists of a single Windows 2003 Active Directory domain. You are a member of the Domain Admins group. The network includes 10 member servers running Windows Server 2003 and 4 domain controllers running Windows Server 2003. The 200 client computers all run Windows XP Professional.
The user accounts for employees in the Finance department are located in an Organisational Unit (OU) named Finance. The Finance OU also contains a Global Security group named FinanceUsers. All Finance employees are members of FinanceUsers.
An employee named Alice works in the Finance department. Alice reports that she cannot log in the domain. She receives the error message shown in the exhibit:

You need to enable Alice to log in to the domain.
What should you do?

A. Use the dsmod user command line tool to enable Alice's user account.
B. Use Active Directory Users and Computers to add Alice's user account to the Domain Users group.
C. Use Active Directory Users and Computers to add Alice's user account to the Guests group.
D. Use the net accounts command line tool to enable Alice's user account.
E. Perform an authoritative restore of Alice's user account.

Answer: A

Explanation:
dsmod user UserDN -disabled {yes|no}
UserDN Specifies the distinguished name of the user object to be disabled or enabled.
{yes|no} Specifies whether the user account is disabled for log on (yes) or not (no).
Incorrect answers:
B: Domain users cannot make changes to their computer systems nor can they install application or utility programs. But the question states that Alice gets the account disables message which means that her account should be enabled first.
C: Guest accounts members can log on, run applications, and even shut down the system on computers that are not DCs. However, in this scenario Alice needs to be able to log into a domain.
D: Making use of the net accounts toll will not enable Alice to log in to the domain.
E: Performing an authoritative restore of Alice's user account will not enable her to log into the domain. The account has to be enabled first.
Reference:
http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/windowsxp/home/using/productdoc/en/dsmod_user.asp
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 85, 106, 194

QUESTION 108
You are the network administrator for your company. The network consists of a single Active Directory domain named Certkiller .com. All domain controllers run Windows Server 2003, and all client computers run Windows XP Professional.
All client computer accounts are stored in the Computer container.
A user named Peter reports that he cannot log on to the domain from his computer. Peter receives the logon message shown in the exhibit.
Exhibit:
Logon Message
Your account is configured to prevent you from using this computer. Please try another computer.

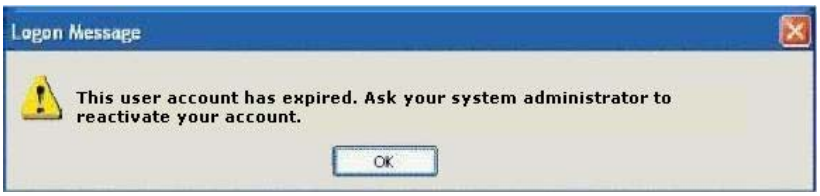
You need to enable Peter to log on.
What should you do?

A. Create an account for Peter's computer in the Computers container.
B. Grant the Log on locally user right to Peter's user account.
C. Enable Peter's user account.
D. Change the properties of Peter's user account so he can log on to any computer.

Answer: D

Explanation:
This issue occurs if the user account is configured to log on from specific workstations. Change the setting in LogOn To option in the User Properties dialog box.
Incorrect answers:
A: Although the Computers container is the default container for computer objects, it is not the ideal container for computer objects. Unlike OUs, containers such as Computers, Users and Builtin cannot be linked to policies, limiting the possible scope of computer-focused group policy. Thus placing Peter's computer in the Computers container is not the answer.
B: The Deny logon locally user right will override your capability as an administrator to log on to the console. You need to remove this group assignment to be able to log on to the console again. Thus the same will happen when you grant this right to the Users group. Thus this option will not ensure that all users be authenticated when they log on to the domain controller.
C: Peter's account is already enabled; he only needs to be able to log on meaning that all you need to do is to change the properties of his user account.
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. 146, 174, 209, 915
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 109
You are the network administrator for Certkiller GmBh. 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.
Certkiller 's main office is located in Berlin, which is also the location of all domain controllers. The Berlin office contains 200 client computers.
A branch office is located in Helsinki. This office contains 60 client computers. All user accounts for permanent employees in Helsinki are contained in an organizational unit (OU) named HelUsers. All user accounts for temporary employees in Helsinki are contained in an OU named TempUsers.
A temporary employee named King is hired in the Helsinki office. The business hours in his office are 9:00 A.M. to 5:00 P.M. at 9:05 A.M. on his first Monday at work, King tries to log on to the domain from his client computer. However, he receives the message shown in the exhibit.



You need to ensure that King can log on to the domain.
What should you do?

A. Move King's account to HelUsers.
Create a Group Policy object (GPO) and link it to HelUsers.
In the GPO, decrease the account lockout duration.
B. Make TempUsers a child of HelUsers.
Create a Group Policy object (GPO) and link it to HelUsers.
In the GPO, decrease the account lockout threshold.
C. Modify the properties of King's user account to the Logon Hours setting is the same as the business hours for the Helsinki office.
D. Modify the properties for King's user account to extend the dates during which his account can be used.

Answer: D

Explanation: The user account has expired. This means that the user account was created with an expiry date set. We need to modify the user account to extend the dates during which his account can be used. In other words, we need to set the account to expire at a later date.
Incorrect Answers:
A: The accounts in HelUsers are for permanent users and have no expiry date. King is a temporary user so we should set an expiry date on his account. The account lockout duration is the time an account is locked out after failed log on attempts due to incorrect username or passwords. It is not related to this question.
B: We don't need to rearrange the OU structure. The account lockout threshold is related to logon failures due to incorrect username or passwords. It is not related to this question.
C: The logon hours setting is not the cause of the problem. The account has expired. If you tried to log on 'out of hours', you would get a different error message.
References:
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 282, 318

QUESTION 110
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. All domain controllers run Windows Server 2003.
A user named King is responsible for managing groups in the domain. In Active Directory, you delegate the permissions to create, delete, and manage groups to him.
When King tries to log on to a domain controller, he receives the error message shown in the exhibit.

You need to ensure that King can immediately manage groups.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Modify the default security policy for the domain.
Refresh the policy by using Secedit.exe.
B. Modify the default security policy for the domain.
Refresh the policy by using Gpupdate.exe.
C. Modify the default security policy for the Domain Controllers organizational unit (OU).
Refresh the policy by using Secedit.exe.
D. Modify the default security policy for the Domain Controllers organizational unit (OU).
Refresh the policy by using Gpupdate.exe.
E. Install the Windows Server 2003 administrative tools on King's computer.
Instruct him to run Dsa.msc from his computer.
F. Share Dsa.msc from a computer running Windows Server 2003.
Instruct King to run Dsa.msc from his computer.

Answer: D, E

Explanation: Normal users are not able to log on to a domain by default. Thus, to enable King to manage accounts from his computer, his user account has to be granted these permissions. To apply the new policy immediately, we need to refresh the policy. The secedit tool to refresh policies has changed from 2000 server to 2003 server; the new tool is gpupdate.
Incorrect Answers:
A: Using a group policy is a quicker way of applying a setting to all the domain controllers.
B: King needs to log on to the domain controllers only, so we should apply the policy to the domain controllers OU.
C: Secedit.exe is no longer used in Windows 2003. It has been replaced by gpupdate.exe.
F: You cannot share a single file. You can only share folders containing files.
References:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapters 4 & 5

QUESTION 111
Exhibit

You are the network administrator for Certkiller .com. You manage a Windows Server 2003 computer named Certkiller 2. Certkiller 2 is a stand-alone server in your workgroup, which also contains five client computers.
All client computers on the network run Windows XP Professional. No time synchronization mechanism is currently in place.
A user named Sandra is given management responsibilities on Certkiller 2. However, when Sandra tries to log on to Certkiller 2, she receives the error message shown in the exhibit.
You need to ensure that Sandra can log on to Certkiller 2 to perform her management responsibilities.
What should you do?

A. Synchronize the clocks on all computers in your workgroup.
B. Install Active Directory on Certkiller 2.
C. Configure Sandra's account password so it never expires.
D. Modify the security policy on Certkiller 2 to assign the appropriate rights to Sandra.

Answer: D

Explanation: User right assignment is done in the Security settings in the local Policies. The default security settings do not allow regular users to log on interactively at a server. You can change this setting through Start _ Administrative Tools _ Security Policy. Expand Local Policies, then User Rights Assignment. Doubleclick Allow Log On Locally and click the Add User Or Group button. In the Add User Or Group dialog box, type in Sandra and click the OK button. In the Security Policy Setting dialog box, click the OK button. Close any open dialog boxes. In the exhibit is shows clearly that it is a local security policy violation when Sandra attempts to logon. What is thus necessary is to modify the security policy and assign Sandra the appropriate rights to carry out her tasks.
Incorrect answers:
A: It is not a matter if synhronizing clocks on the computers in the workgroup, as the problem are located at the local security policy.
B: You do not need to install Active Directory. This will not solve the problem of loging on interactively.
C: Following the exhibit, you will see that it is not a matter of altering Sandra's password so it never expires. Rather it is a matter of chaing the local security policy to allow Sandra to logon interactively.
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. 142

QUESTION 112
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 Default Domain Policy GPO is configured to prompt users to change their password 14 days before it expires.
A user who returns from a two-week vacation reportes that she cannot log on to the domain. You discover that when she last logged on, she was prompted to change her password. She reports that she did not change her password before leaving on vacation.
You need to ensure that the user can log on to the domain.
What should you do?

A. Enable the user account.

B. Reset the password for the user account.
C. Use Active Directory Users and Computers to select the Password never expires option.
D. Configure the Prompt user to change password before expiration security policy option to 21 days.

Answer: B

Explanation:
In the question it is mentioned that the default domain GPO is set to have users change their passwords 14 days before expiry which the user neglected to do. What is thus needed is to reset the password for the user account to enable to user to log on.
Incorrect answers:
A: The user account has worked before and thus it is not a matter of enabling the user account.
C: This is contradictory to the default domain GPO.
D: CHaning the policy option to 21 days will not ensure that the user can log on to the domain, the account is already not able to log on.
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. 149

QUESTION 113
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 3,500 user accounts are located in the default Users container.
All user accounts have their Department attribute values set to the appropriate employee department.
The network engineer creates an OU structure for the domain, based on the Certkiller 's departments.
You need to place all user accounts that have the Departmetn attribute set to Sales in the Sales OU.
Because of time constraints, you need to automate this process.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Run the dsmod command with the appropriate parameters.
B. Run the dsget command with the appropriate parameters.
C. Run the dsquery command with the appropriate parameters.
D. Run the dsmove command with the appropriate parameters.
E. Run the dsrm command with the appropriate parameters.
F. Run the find command with the appropriate parameters.

Answer: C, D

Explanation: The Dsmove command-line utility is used to rename or move a single object within the Active Directory. When you use the Dsmove command-line utility, you specify the object's distinguished name, then the new name of the object (if you are changing the object's name) and the new location of the object. You use the Dsquery command-line utility to query the Active Directory for objects that meet specified criteria.
Incorrect answers:

A: You can modify existing Active Directory objects through the Dsmod command-line utility.
B: The Dsget command-line utility is used to display the selected properties of a specified object within the Active Directory.
E: This is not what is needed in this case.
F: Find is usually used to find and locate. This is not what is required.
Reference:
Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, pp. 190-194

QUESTION 114
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.
The finance deparment uses a specific naming process to audit users and their computers. The process requires that each user's client computer has an account in Active Directory and that each client computer name corresponds to a specific user account.
A user name Marie is a member of only the Domain Users security group. She reports that the hardware on her computer fails. She receives a new computer.
You need to add Marie's new computer to the domain. You need to comply with the finance department naming process.
What should you do?

A. Instruct Marie to run the ipconfig /flushdns command on her new computer and to add the new computer to the domain by using the same computer name as her failed computer.
B. Assign Marie permissions for adding computer accounts to the default container named Computers. Instruct Marie to add her new computer to the domain.
C. Reset the computer account for Marie's failed computer. Instruct Marie to add her new computer to the domain by using the same name as her failed computer.
D. Configure the IP address of Marie's new computer to be the same as the failed computer. Instruct Marie to add the new computer to the domain.

Answer: C

Explanation: Active Directory is a directory service that is available with the Windows 2000 Server and Server 2003 platforms. It stores information in a central database that allows users to have a single user account for access to resources across the enterprise network. The users and groups that are stored in Active Directory's central database are called Active Directory users or domain users. Since Marie's hardware failed and she will be receiving a new computer, it will be a matter of just substituting the old computer account for the new one is you are to comply with the finance department's naming process. She will then still be using her own name.
Incorrect answers:
A: The ipconfig /flushdns command flushes and resets the DNS resolver cache. This is not what is required here.
B: It is not a matter of assigning permissions in this case.
D: This option will not solve the problem and comply with the finance departments requirements.
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, pp. 99, 311

QUESTION 115
Exhibit:

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.
A user named TessKing regularly accesses a folder named Certkiller Docs on a server named Certkiller 1. You instruct another administrator to audit and modify share permissions and NTFS permissions on Certkiller 1. Now, TessKing reports that she cannot access the shared folder from the network.
You verify that no changes were made to group memberships in the domain. On Certkiller 1, you view the effective permissions for the Certkiller Docs folder, as shown in the exhibit,
You need to ensure that TessKing can access the data in the shared folder.
What should you do?

A. Add TessKing's user account to the ACL on the Sharing tab.
B. Instruct TessKing to log off and log on to the computer.
C. Delete TessKing's user account and re-create the user account.
D. Add TessKing's user account to the local Power Users group.

Answer: A

Explanation: Since Jack could previously access that particular folder, and the question states that group memberships were not changed and that it is only a matter of share permissions and NTFS permissions that was modified, it stands to reason that Jack user account should be added to the Access Control List on the Sharing tab of the Certkiller Docs folder, because the shared folder has enough effective permissions for Tess to be able to access it.
Incorrect answers:

B: Merely logging on and logging off to the computer will not ensure access to the folder especially if you do not have access to the folder.
C: Recreating the user account will not solve the problem.
D: Adding that particular user account to the local Power Users group will not address the problem. It has been stated that the group memberships have not been altered and that there was previous access to this 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. 214, 291

QUESTION 116
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 .com purchases a new server to test applications in a stand-alone environment. The company's written security policy states that if a user attempts to log on by using an incorrect password three times in 30 minutes, the account is locked out. An administrator must unlock the account.
You discover that users of the new server who have accounts that are locked out can log on again after 30 minutes.
You need to ensure that the new server meets the requirements of the written security policy.
What should you do?

A. Set the Reset account lockout counter after policy to 1.
B. Set the Reset account lockout counter after policy to 99999.
C. Set the Account lockout duration policy to 0.
D. Set the Account lockout duration policy to 99999.

Answer: C

Explanation: The account lockout policies are used to specify how many invalid logon attempts should be permitted. You configure the account lockout policies so that after x number of unsuccessful logon attempts within y number of minutes, the account will be locked for a specified amount of time or until the administrator unlocks it.
Account Lockout Duration specifies how long account will remain locked if Account Lockout Threshold is exceeded. Thus setting the account lockout duration policy to 0 will have the desired effect and comply with the written security policy.
Incorrect answers:
A & B: This counter specifies how long counter will remember unsuccessful logon attempts. Clearly this counter whether set to 1 or 99999 will not have the desired effect.
D: Setting the account lockout duration to 99999 will result in the new server being uinable to comply with written security policy.
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. 112

QUESTION 117
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.
Tess, a user in the Sales staff, reports that she has attempted to log on six times unsuccessfully. Tess reports that she logged on successfully yesterday. You discover that Jack reset her password three days ago to comply with a new security policy that requires strong passwords.
The account policies that are applied in the Domain Security GPO are shown in the following table.

Policy setting	**Value**
MinimumPasswordAge	1
MaximumPasswordAge	42
MinimumPasswordLength	7
PasswordComplexity	1
PasswordHistorySize	24
LockoutBadCount	5
ResetLockoutCount	30
LockoutDuration	30

You need to ensure that the user can log on to the domain.
What should you do?

A. Reset the password for the computer account.
B. Unlock the user account.
C. In the user account properties, select the Password never expires check box the user account.
D. In the user account properties, select the User must change password on next login check box the user account.

Answer: B

Explanation: Jack account got locked out since she made six unsuccessful attempts to log on to the domain and the table in the question clearly shows that the LockoutBadCount is set to 5.
The most common problems with user accounts are due to group membership, password problems, or account lockouts. Group membership problems manifest themselves by users not being able to access resources that are assigned through group membership. This can easily be verified and corrected via Active Directory Users and Computers or from the command line using the dsget.exe and dsmod.exe commands. Password problems are usually due to users forgetting their password and needing it reset. This can be accomplished via Active Directory Users and Computers or via the dsmod.exe command. Lastly: users often lockout their accounts due to them entering their password incorrectly. This is usually due to them forgetting their password because they just changed it recently, in which case you would need to unlock their account and reset their password. Sometimes they just cannot type or CAPS LOCK is on and they enter in their password incorrectly too many times and lock their account. User accounts can be unlocked by using Active Directory Users and Computers or by using the dsmod.exe command. The user said she attempted to log on six times, but failed. As a result the account is locked out. Therefore we can simply unlock the user account, and she can logon again.
Incorrect answers:

A: Resetting the password for the user account does not necessarily grant log on rights to the domain. You need to unlock the account first.
C: Modifying the properties of the account to password never expires will not affect the situation. The account must first be unlocked. Whether the password expires or not, she will still need to use a strong password once the account has been unlocked. She obviously went over the account lockout count threshold.
D: The user's problems stems from going over the account lockout threshold too many times. Her account has to be unlocked first to be able to log on to the domain. The User must change password on next logon check box in her user account properties will not help in this case as her account has been locked out.
References:
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 317-318.

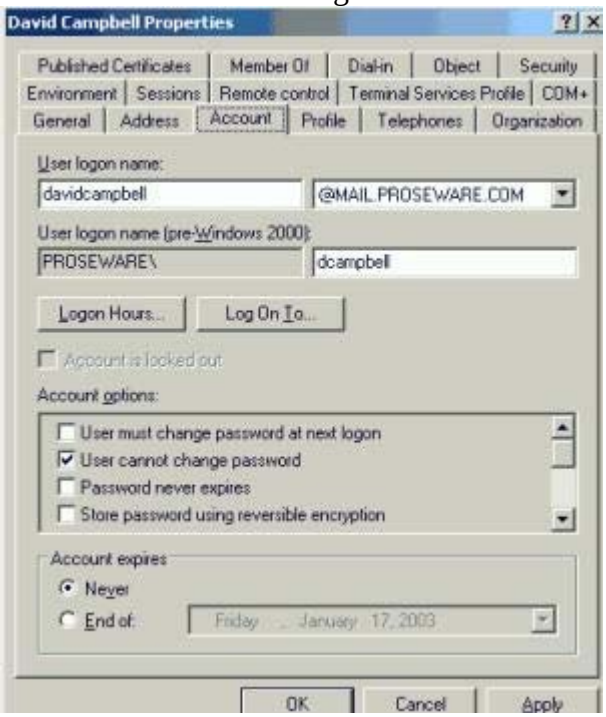
QUESTION 118
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003
You install a new server named Certkiller 6. You install an application on Certkiller 6. The application fails to start because of the NTFS permission on Certkiller 6 are too restrictive. You use a security template from the manufacturer of the application to modify the NTFS permissions on Certkiller 6 to allow the application work.
A new update to the application is released. The application no longer requires the modified NTFS permissions.
You need to restore the default permissions on Certkiller 6 to restore the original level of system security.
Which security template should you import into the local security policy of Certkiller 6?

A. The Syssetup.inf template.
B. The Profsec.inf template.
C. The Defltsv.inf template.
D. The Netserv.inf template.

Answer: C

Explanation: The default permissions are saved in the Defltsv.inf security template. This would thus be the template to import into the local security policy of Certkiller 6 if you need to restore default permissions in stead of the modified permissions. The other templates will not have the default permissions.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 202, 655
Diana Huggins, Windows(r) Server(tm) 2003 Network Infrastructure Exam Cram(tm) 2 (Exam 70-291), Chapter
4

QUESTION 119
You are the network administrator for Proseware, Inc. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
The network consists of two Active Directory forests: proseware.com and Certkiller .com. External trust relationships exist between the two forests.
You create an additional user principal name (UPN) suffix for proseware.com. The new UPN suffix is mail.proseware.com.
David Campbell a user from proseware.com, reports that he cannot log on to proseware.com from Certkiller .com. The configuration of David Campbell's user account is shown in the exhibit.



You need to ensure that David Campbell can log on to his domain from Certkiller .com.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Change David Campbell's user logon name to match his pre-Windows 2000 user logon name.
B. Clear the User cannot change password option in the David Campbell Properties dialog box.
C. Instruct David Campbell to log on by using his pre-Windows 2000 user logon name.
D. Change David Campbell's UPN suffix to proseware.com.
E. Create a computer account for David Campbell's computer in Certkiller .com.
F. Delete David Campbell's user account and recreate it in Certkiller .com.

Answer: A, C

Explanation: The user cannot log on because it is only possible to use an explicit UPN-Name to log on when there is forest trust. As stated in the question there is an external trust relationship between the two forests, not forest trust. In this case you can only use an implicit UPN-Name to log on. Alternatively, you can use the pre-Windows 2000 user logon name to log on.
A user principal name (UPN) is a variation of a user account name that looks like an e-mail name but can be

used to log on to a domain. The syntax is <user name>@<string>. UPNs allow you to use the same logon name across different domains in the same forest or in different forests.
The following two types of UPNs exist:
• Implicit: Always takes the form userID@DNSDomainName. For example, johns@corp.contoso.com is the UPN for the account of John Smith, whose user ID is johns and whose account is a member of the corp.contoso.com forest. The implicit UPN is always associated with the user's account, regardless of whether an explicit UPN is defined.
• Explicit: Always takes the form string@Anystring, where both string and Anystring are explicitly defined by the administrator. For example, John Smith might have the UPN ITJS@coneast. Explicit UPNs are useful for situations when the organization does not want to publicize the name of domains or the forest structure.
Incorrect Answers:
B: This is not a password problem. Thus clearing the option User cannot change password will not solve the problem.
D: David Campbell's user account already has the correct UPN suffix; all he needs to be able to log on is an implicit UPN name.
E: It is unnecessary to create a computer account for David Campbell's computer in Certkiller .com; there is an external trust relationship between the forests, not a forest trust. All that is needed to grant David Campbell logon abilities is to use an implicit UPN-name.
F: Deleting David Campbell's user account and recreating it in Certkiller .com is not the solution. There is already an external trust relationship between the two forests.
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. 264, 282-284, 334
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/plan/mtfstwp.asp

---

QUESTION 120
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 6. Certkiller 6 is a member of a workgroup. You configure Certkiller 6 as the Web server for Certkiller 's intranet Web site.
Certkiller 's written security policy states the following requirements:
• Smart cards are required to log on to all servers.
• Membership to the Remote Desktop Users group should remain empty.
• Users should not be able to log on through Terminal Server by using a blank password.
• Third-party applications should not be installed on network servers.
When you attempt to log on to Certkiller 6 by using your smart card, you receive an error message. You verify that your user account is a member of the Domain Admins global group in your domain.
You need to be able to log on to Certkiller 6 by using your smart card.
What should you do?

A. Join Certkiller 6 to the domain.
B. In Computer Management, add your user account to the Administrators local group.
C. Restart Certkiller 6 in safe mode.

From a command prompt, run the runas.exe /smartcard command.
D. In the local security policy, assign your user account the Allow log on locally user right.

Answer: A

Explanation: Smart cards are small credit-card-sized cards that usually store encryption keys, public key certificates, and other types of account information. The card is inserted into a card reader attached to the computer, which reads the information stored on the card. Typically, a password or Personal Identification Number (PIN) is required to release the account information for authentication within a network. This means that, in order to authenticate, a user must both have physical possession of the card and have knowledge of the PIN. This is commonly used with EAP-TLS authentication. What should also be kept in mind is that for you to be able to log on to Certkiller 6 using the smart card is that Certkiller 6 should also be joined to the domain.
Incorrect Answers:
B: Adding your user account to the Administrators local group will not work when you want to make use of smart cards to log on to Certkiller 6. Since you user account is already a member of the Domain Admins global group, you need to join Certkiller 6 to the domain.
C: Restarting Certkiller 6 and running the runas.exe/smartcard command is not enough, Certkiller 6 has to be part of the domain as well.
D: Allow logging on locally will make the use of smart cards obsolete and the question states pertinently that you want to log on by means of the smart card so as to comply with company policy.
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. 637-638

QUESTION 121
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. All client computers run Windows XP Professional with default settings. Some users have portable computers, and the rest have desktop computers.
You need to ensure that all users are authenticated by a domain controller when they log on.
How should you modify the local security policy?

A. Require authentication by a domain controller to unlock the client computer.
B. Cache zero interactive logons.
C. Cache 50 interactive logons.
D. Grant the Log on locally user right to the Users group.

Answer: B

Explanation: A cache is a local store of data commonly used. To ensure that all users are authenticated by a domain controller when they log on, you need to set the cache to zero for interactive logons. System cache holds data that was processed previously. It is faster to obtain data from cache, rather than repeating the transaction. But this also reduces the need to authenticate users and for security purposes you need to purge the cache and set it to not cache log on information so as to compel all users to be authenticated each time

they log on. GPO Setting -> Interactive logon: Number of previous logons to cache (in case domain controller is not available)
By default 10 logons. This setting would prevent logon using cached credentials if the network was down or domain controllers otherwise unavailable. Certainly a non viable setting for mobile laptop users!
If we use the zero setting, then every user MUST be authenticated by a domain controller.
Incorrect answers:
A: Unlocking the client computer will not serve the purpose of authentication by the domain controller upon log on.
C: If you cache 50 interactive logons then users will be able to bypass being authentication by the domain controller.
D: Users with this right will be able to log on to the console interactively as if they were sitting down at the actual server itself, and the question states pertinently that you want all users to be domain controller authenticated when they log on.
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. 439-441

QUESTION 122
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
All client computer accounts for the sales department are located in an organizational unit (OU) named Sales.
A user named Marie, in the sales department, uses a client computer named Certkiller 1. Her computer is a member of the domain. However, Marie reports that she cannot log on to the domain.
You verify that a computer account for Certkiller 1 exists in the Sales OU. Then you log on to Certkiller 1 as a local Administrator and use Event Viewer to view the contents of the event log, as shown in the exhibit.

You need to ensure that Marie can log on to the domain.
What should you do?

A. Move the Certkiller 1 account to the Computers OU.
B. Reset the password for Marie's user account.
C. Reset the Certkiller 1 account.
D. Configure the properties for the Certkiller 1 account so Certkiller 1 is managed by Marie's user account.

Answer: C

Explanation: The secure channel's password is stored along with the computer account on all domain controllers. For Windows 2000 or Windows XP, the default computer account password change period is every 30 days. If, for some reason, the computer account's password and the LSA secret are not synchronized, the Netlogon service logs one or both of the following errors messages:
The session setup from the computer DOMAINMEMBER failed to authenticate.
The name of the account referenced in the security database is DOMAINMEMBER$.
The following error occurred: Access is denied.
NETLOGON Event ID 3210
Failed to authenticate with \\DOMAINDC, a Windows NT domain controller for domain DOMAIN.
The Netlogon service on the domain controller logs the following error message when the password is not synchronized:
In the Active Directory Users and Computers MMC (DSA), you can right-click the computer object in the Computers or appropriate container and then click Reset Account.
This resets the machine account. Resetting the password for domain controllers using this method is not allowed. Resetting a computer account breaks that computer's connection to the domain and requires it to rejoin the domain, which will allow Marie to log on to the domain.
Incorrect answers:
A: Moving the Certkiller 1 account to the Computers OU will not help because Marie is part of the Sales OU as well as Certkiller 1. For Marie to be able to log on to the domain she needs to make use of Certkiller 1.
B: Resetting Marie's user account password will not ensure her logging on to the domain. What needs to be done is that the computer account that is used in the connection should be reset, in other words resetting the machine, so as to allow Marie to log on to the domain.
D: Option D will not ensure that Marie will be able to log on to the domain. It is the Certkiller 1 account that is problematic.
Reference:
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 771

QUESTION 123
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, and all client computers run Windows XP Professional.
A user named Lilli receives a new computer named Client223. She successfully logs on to the domain. The next day, she tries to log on again. The domain name appears in the domain dropdown list in the dialog box. However, Lilli cannot log on.
You try to log on by using Client223, but you are also unsuccessful. Then you use a local

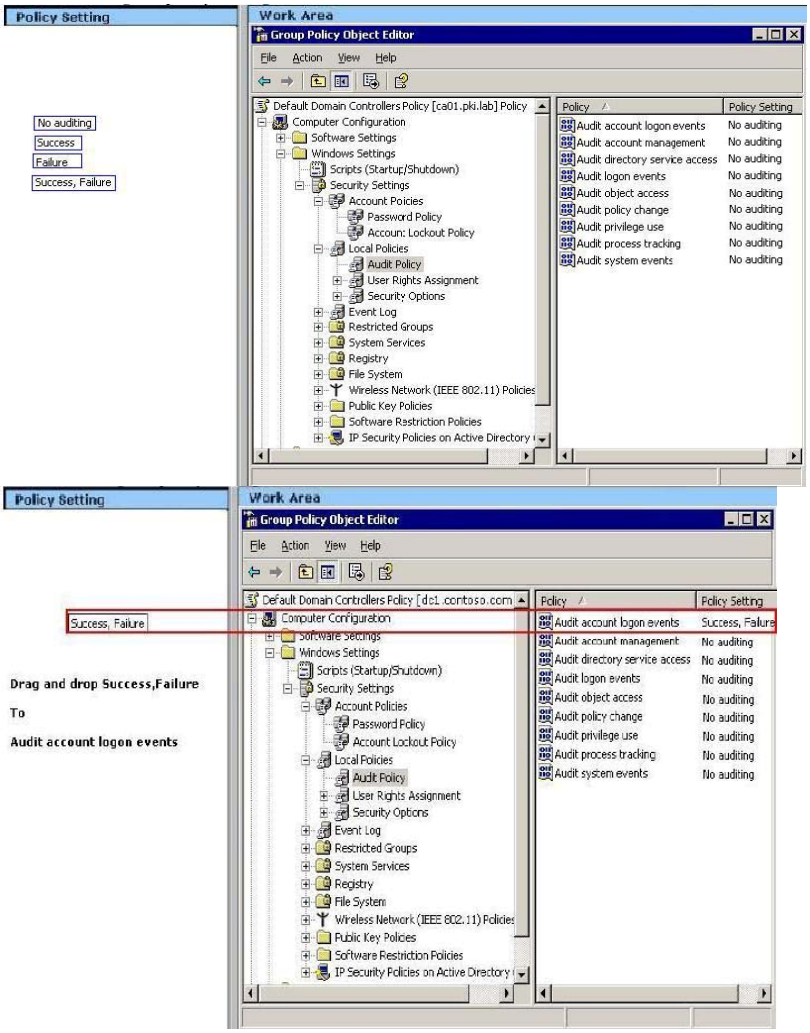
Administrator account to log on. You read the following error message in the system event log.
"NETLOGON Event ID 3210: Failed to authenticate with \\Server5, a Windows NT domain controller for domain Certkiller ".
You search the computer account for Client223 in Active Directory Users and Computers, but the account does not appear.
You need to ensure that Lilli can log on to the domain successfully.
What should you do?

A. Recreate the user account for Lilli and add her to all appropriate security groups.
B. Run the netdom reset 'Client223' /domain:' Certkiller ' command and then restart Client223.
C. Add Client223 to a workgroup.
Then join Client223 to the domain.
D. Reset the computer account for Server5 in Active Directory Users and Computers.

Answer: C

Explanation: For a user to be able to log on successfully to a domain, it has to be part of a work group that has the ability to log on to the domain.
Global groups can include other groups and user/computer accounts from only the domain in which the group is defined. Permissions for any domain in the forest can be assigned to global groups.
It looks like the computer account for Client223 has been deleted. Therefore we need to recreate the account. However, we cannot just create an account named Client223 as this account will have a different SID (Security Identifier) to the original account. Therefore, we need to disjoin Client223 from the domain by adding Client223 to a workgroup. Now we can rejoin Client223 to the domain and create a new computer account in the process.
Incorrect Answers:
A: Lilli's user account itself is not problematic. The problem is that the computer account is missing.
B: This command is used to reset the secure channel between a workstation and the domain. If the workstation and computer account passwords are out of sync, the secure channel will not work. However, this is not the problem in this question. The problem is that the computer account is missing (probably deleted).
D: With the computer account missing you will be unable to reset the computer account.
Reference:
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 771

QUESTION 124
You are the network administrator for Contoso, Ltd. Your network consists of a single Active Directory domain Certkiller .com. All network servers run Windows Server 2003.
You need to audit all logon attempts by domain users. You must ensure that the minimum amount of necessary information is audited. To achieve this goal, you will edit the Default Domain Controller Group Policy object (GPO).
What should you do?
To answer, drag the policy setting to the correct location or locations in the work area.



Explanation: This setting will audit all logon events that use domain user accounts.
The Audit Logon Events policy is for auditing log on attempts using local user accounts.
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. 321

QUESTION 125
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All domain controllers run Windows Server 2003, and all client computers run Windows XP Professional.
A user named King reports that she cannot log on to the domain from his computer. King receives the logon message shown in the exhibit.

You need to enable King to log on.
What should you do?

A. Run the net user command with the appropriate switches.
B. Run the net accounts command with the appropriate switches.
C. Run the dsmod user command with the appropriate switches.
D. Add King to the Users group.
E. Remove King from the Guests group.

Answer: C

Explanation: To enable King to log on to the domain you would need to run
dsmod user UserDN -disabled {yes|no}
where UserDN specifies the distinguished name of the user object to be disabled or enabled and {yes|no} specifies whether the user account is disabled for log on (yes) or not (no).
Incorrect answers:
A: The net user command is used mainly to find out which domain groups that a user is a member of, as well as view other pertinent information about a user.
B: This command will not enable King to log on to the domain.
D: The error message states that King's account has been disabled; this means that the account should first be enabled for King to have the ability to log on.
E: Removing King from the Guests group is irrelevant in this scenario.
Reference:
http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/windowsxp/home/using/productdoc/en/dsmod_user.asp
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 4

QUESTION 126
You are the network administrator for Certkiller .com. The network consists of a single Activev Directory domain named Certkiller .com. The company's main office is in Tokyo, and it has a branch office in Osaka. Each office is configured as an Active Directory site. The two offices are connected by a 128-Kbps connection. All domain controllers run Windows Server 2003. All client computers run Windows XP Professional. All network administrators are located in Tokyo. Universal group membership caching is enabled.
The server roles and IP addresses for each site are shown in the following table.

Site	Server role	IP address
Tokyo	DNS, global catalog, WINS, DHCP	10.10.10.200
Osaka	DNS, domain controller, DHCP	10.10.20.200

The network connection between Tokyo and Osaka intermittently fails. Only the client computers in Tokyo have NetBIOS enabled. All client computers are configured to use DHCP.
The significant DHCP scope options for Tokyo are shown in the following table

Scope option	Setting

WINS/NBNS Servers	10.10.20.200
DNS Servers	10.10.10.200, 10.10.20.200
Router	10.10.20.1

You create a user account for a new employee in Osaka. The user report that she cannot log on to the domain. You confirm that you can log on by using your account and then by using the user's account. You also confirm that all other users in Osaka can log on.
You need to ensure that the user can authenticate to the domain.
What should you do?

A. Configure the user's user account to store passwords by using reversible encryption.
B. Configure the user's computer account to be trusted for delegation.
C. Force Active Directory replication to occur between Tokyo and Osaka.
D. Change the Router setting in the DHCP scope options to 10.10.10.1.

Answer: C

Explanation:
Sites are primarily used for directory replication purposes. Consider what happens when you have two physically separate locations that share a common directory. Without frequent replication, the two directories would become horribly disjointed and practically useless. Thus if you force replication between Tokyo and Osaka, then you will enable the user to be authenticated to the domain sincew the user's account is in Osaka and only client computers in Tokyo have NetBIOS enabled.
Incorrect answers:
A: Storing password by means of reversible encryption is not going to solve the problem.
B: This is not a delegatory matter.
D: There is no need to change the router settings as it is only one user that is experiencing the problem.
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.104

QUESTION 127
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. The NetBIOS name of your domain is Certkiller .
Tess King, a user in a the branch office in Los Angeles, reports that she cannot log on to the domain from a client computer named Certkiller 172. She receives the following error message:
"The system cannot log you on to this domain because the system's computer account in its primary domain is missing or the password on that account is incorrect."
You verify that the user's computer is connected to the network. All other users can log on to the domain successfully.
You need to ensure that the user can log on to the domain.
What should you do?

A. In the DHCP snap-in, ensure that the correct DNS server settings are provided to client computers.
B. In Active Directory Users and Computers, ensure that a computer account exists for Certkiller 172.
C. In Active Directory Users and Computers, reset the user's user account password.
D. In the DNS snap-in, verify that the host (A) resource record exists for Certkiller 172.

Answer: B

Explanation: Active Directory Users and Computers on Windows Server 2003 domain controllers, is the main tool used for managing the Active Directory users, groups, and computers. To set up and manage domain user accounts, you use the Active Directory Users And Computers utility. This tool is the tool to use so that the user can log on to the domain.
Incorrect answers:
A: This is not a problem that can be solved with the DHCP snap-in. besides the other users can log on to the domain successfully.
C: Though you can use this tool to reset the user's account password, this will not solve the problem of the user being unble to log on.
D: This is not a DNS problem since the other users are all able to log on and that the user's computer is connected to the network.
Reference:
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r)Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, p. 227

QUESTION 128
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
You create a shared folder named Client Docs on a member server named Certkiller 13. Client Docs will store project documents. You configure shadow copies for the volume containing Client Docs.
You need to enable client computers to access previous version of the documents in Client Docs.
What should you do?

A. Create a Group Policy object (GPO) to enable Offline Files on all client computers.
B. On each client computer, customize the view for Client Docs to use the Documents (for any file type) folder template.
C. Create a Group Policy object (GPO) that installs the Previous Versions client software on all client computers.
D. Assign the Allow - Full Control permission on Client Docs to all users.
E. On each client computer, install the Backup utility and schedule a daily backup.

Answer: C

Explanation: To enable users to access previous versions of the files, you must install the Previous Versions client software on all client computers. The easiest way to do this is to deploy the software using a Group Policy Object.

Incorrect Answers:
A: Offline Files are irrelevant to this scenario.
B: This is irrelevant to this scenario.
D: The users do not need Full Control access to the files. This will not enable users to access previous versions of the files.
E: The files do not need to be backed up on each client computers. The Shadow Copy service creates backups of previous versions of the files on the server.
Reference:
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft Press, pp. 285-288

QUESTION 129
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.
Each of the 14 departments at Certkiller has an exclusive shared folder on a server named Certkiller 5.
You need to ensure that the managers can reset file permissions for any file and folder on Certkiller 5.
You want to achieve this goal by using the minimum amount of administrative effort.
What are two possible ways to achieve this goal? (Each correct answer is a complete solution. Select two.)

A. Assign the managers the Allow - Full Control NTFS permission for each folder.
B. Assign the managers the Take ownership of files or other objects user right.
C. Assign the managers the Bypass traverse checking user right.
D. Assign the managers the Act as part of the operating system user right.

Answer: A, B

Explanation: The Allow Full Control permission's access level is as follows: View and list folders and files; view the contents of files; write data to files; add folders and files; delete folders, files, and file contents; view and set attributes and extended attributes; change permissions for folders and files; take ownership of folders and files.
The special permission Take Ownership can be granted to any user or group. A user with Allow Take Ownership permission can take ownership of the resource. These two options will ensure that managers will have the ability to reset file permissions for a file or folder on Certkiller 5 with the least amount of administrative effort.
Incorrect answers:
C: Bypassing traverse checking permission will allow the users to navigate through the folder, but this is not what is required. The Managers need to be able to reset file permissions.
D: This option involves too much administrative effort.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 5

QUESTION 130
You are the network administrator for Certkiller .com. The network consists of a single Active

Directory forest containing two domains, ch. Certkiller .com and de. Certkiller .com. The functional level of both domains is Windows 2000 mixed.
ch. Certkiller .com contains two domain controllers running Windows 2003 and three domain controllers running Windows 2000 server. A member server named Certkiller 9 hosts applications and files that all company users need to access.
You need to enable all users in de. Certkiller .com to access the applications and files on Certkiller 9.
Which three actions should you perform? (Each correct answer is a part of a complete solution. Select three.)

A. Create a domain local group named DeutschUsers in ch. Certkiller .com.
B. Create a domain local group named DeutschUsers in de. Certkiller .com.
C. Add the Users group from ch. Certkiller .com to DeutschUsers.
D. Add the Users group from de. Certkiller .com to DeutschUsers.
E. On Certkiller 9, grant the appropriate permissions to the Users group from ch. Certkiller .com.
F. On Certkiller 9, grant the appropriate permissions to DeutschUsers.

Answer: A, D, F.

Explanation: Domain local groups can contain user accounts, universal groups, and global groups from any domain in the tree or forest. A domain local group can also contain other domain local groups from its own local domain. To enable the all users to connect to the applications and files on Certkiller 9, a member server that resides on sc. Certkiller .com; you need to create a domain local group in ch. Certkiller .com. Then you should add the de. Certkiller .com users to this group and then grant the appropriate permissions to the "united" group. This should enable that all users have access to applications and files on Certkiller 9.
Incorrect answers:
B: The domain local group should be created in ch. Certkiller .com since this is where Certkiller 9 resides.
C: It follows logically that the de. Certkiller .com users group should be added to the domain local group that was created and not the users of ch. Certkiller .com
E: Permissions should be granted to the DeutchUsers not to the ch. Certkiller .com Users.
References:
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 319-320

QUESTION 131
You are a 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.
A server named Certkiller 32 contains a folder that is shared as ManagerData$. A global group named AllManagers has permission to access the shared folder.
A user reports that he needs access to the ManagerData$ shared folder. You add his user account to the AllManagers global group. When the user attempts to connect to the shared folder by typing \\ Certkiller 32\ManagerData$\ , he receives the following error message: "\\ Certkiller 32\ManagerData$\ is not accessible. You might not have permissions to use the network resource. Contact the administrator of this server to find out if you have access permissions. Access is denied.
You need to ensure that the user can access the ManagerData$ shared folder on t Certkiller 32.
What should you do?

A. Instruct the user to type \\ Certkiller 32\ManagerData\ when he attempts to access the folder.
B. Add the Anonymous Logon group to the ACL for the ManagerData$ shared folder.
C. Select the Replace permission entries on all child object with entries shown here that apply to child objects check box.
D. Instruct the user to log off and log on again before he accesses the folder.

Answer: D

Explanation: When a user logs on to the network, an access token is created that lists the users' group memberships. This access token is used when the user tries to access a resource. If you change a user's group membership, the change will not be reflected in the access token until the user logs off and logs on again. Instructing the use to log off and then on again will ensure that all the connections will be made. It could have been that the user tried to access the folder before he was granted access. And to effect those changes of adding that particular user to gain access needs to be enabled. This action should enable access to the shared folder.
Incorrect answers:
A: The user account has already been added to the AllManagers global group and there is thus no need to type \\ Certkiller 32\ManagerData\ when attempting to gain access.
B: It will be a huge security breach if Anonymous access is enabled.
C: By following option C, you will not be granting access to the user.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 5

QUESTION 132
You are a 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.
The user accounts for all managers are in a global group named Managers. A manager named Roger creates a folder named ManagerData on a computer named Certkiller 1. He shares the folder to enable other managers to review employee documents. Other managers need to be able to browse and read the documents in the ManagerData folder. Managers must not have other permissions to the shared folder.
You add the Managers group to the ACL on the Security tab for the folder.
You need to configure permissions for the shared folder. You need to ensure that you do not grant any unnecessary permissions.
What should you do?
To answer, configure the appropriate option or options in the dialog box in the work area.


ManagerData Properties
General
Sharing
Security
Web Sharing
Customize
Group or user names:
Managers (Certkiller\Managers)
Certkiller.com
Add...
Remove
Permission for Everyone
Allow
Deny
Full Control
Modify
Read & Execute
List Folder Contents
Read
Write
For special permissions or for advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

Answer:

Explanation: For managers to be able to browse, read, and edit documents that are in the shared folder, you should assign the allow Read & Execute, List Folder Contents, Read and Write permissions.
NTFS Folder Permissions are as follows:
• Read -Enables objects to read the contents of a folder, including file attributes and permissions.
• Write - Enables objects to create new files and folders within a folder, write attributes and extended attributes on files and folders, and can read permissions and attributes on files and folders.
• List Folder - Gives objects the same rights as the Read permission, but also Contents enables the object to traverse the folder path beneath the folder where this permission is applied.
• Read & Execute - Gives objects the same rights as the List Folder Contents permission, but also enables the object to execute program files stored in the folder.
• Modify - Gives the object the same permissions as the Read, Write, List Folder Contents, and Read & Execute permissions, but also enables the object to delete files and folders within the designated folder.
• Full Control - Gives objects full access to the entire contents, including the capability to take ownership of files and change permissions on files and folders.
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. 414

QUESTION 133
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 Certkiller data is stored in shared folders on network file servers. The data for each department is stored in a departmental shared folder. Users in each department are members of the departmental global group. Each departmental global group is assigned the Allow - Full Control permission for the corresponding departmental shared folder.
Certkiller requirements state that all access to shared folders must be configured by using global groups.
A user named Dr King works in the sales department. Dr King needs to be able to modify files in the Marketing shared folder.
You need to ensure that Dr King has the minimum permissions for the Marketing shared folder that he needs to do his job. You need to achieve this goal while meeting Certkiller requirements and without granting unnecessary permissions.
What should you do?

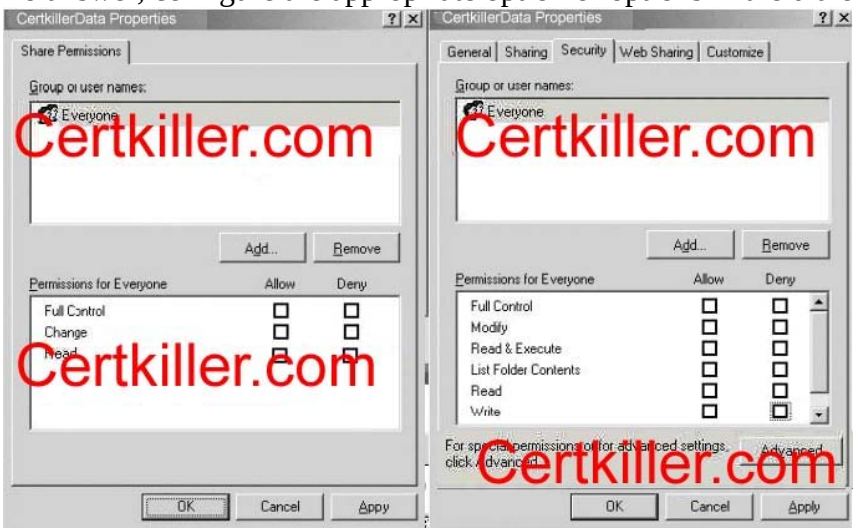
A. Add Dr King's user account to the Marketing global group.
B. Assign the Sales global group the Allow - Change permission for the Marketing shared folder.
C. Create a new global group. Add Dr King' user account to the group.
Assign the new global group the Allow - Change permission for the Marketing shared folder.
D. Assign Dr King's user account the Allow - Change permission for the Marketing shared folder.

Answer: C

Explanation: The best way to accomplish this task is to create a new global group. You need to add Dr King' user account to the group and assign the new global group the Allow - Change permission for the Marketing shared folder. Global groups can include other groups and user/computer accounts from only the domain in which the group is defined. Permissions for any domain in the forest can be assigned to global groups.
Incorrect Answers:
A: This would mean that Dr. King would have permissions on other folders as well. We need to ensure that Dr King has the minimum permissions for the Marketing shared folder that he needs to do his job.
B: This would mean that the whole SALES group would have permissions on Marketing. We need to ensure that Dr King has the minimum permissions for the Marketing shared folder that he needs to do his job.
D: Microsoft does NOT want you to give user account permissions to files. We must do this through making use of groups.
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. 320.

QUESTION 134
You are a 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.
Another administrator shares a folder as Certkiller Data. He wants users to be able to create files in

the folder. He does not want users to able to open files in the folder. When users attempt to connect to the Certkiller Data folder, they receive an error message.
You need to configure the permission for the folder so that users can place their files in the shared folder. You need to achieve this goal without granting unnecessary permissions.
What should you do?
To answer, configure the appropriate option or options in the dialog boxes in the work area.



Answer: Allow List Folder Contents and Write

Explanation: Allowing the List Folder Contents and Write permissions will allow users to place their files in the shared folder.
• List Folder - Gives objects the same rights as the Read permission, but also Contents enables the object to traverse the folder path beneath the folder where this permission is applied.
• Write - Enables objects to create new files and folders within a folder, write attributes and extended attributes on files and folders, and can read permissions and attributes on files and folders.
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. 414

QUESTION 135
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 hosts a folder named Public, which stores files for all users in Certkiller . Public is located on an NTFS partition. Existing permissions for Public are configured as shown in the exhibit.

You need to share Public on the network. All network users, including members of the Administrators group, should have read-only permissions on the contents of the folder.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Share Public with default share permissions.
B. Share Public by assigning the Allow - Full Control permission to the Everyone group.
C. Share Public by assigning the Allow - Full Control permission to the Authenticated Users group.
D. On the Security tab, add the Authenticated Users group and assign the Allow - Read permission to this group.
E. On the Security tab, add the Interactive group and assign the Allow - Read permission to this group.
F. On the Security tab, assign the Deny - Full Control permission to the Administrators group.

Answer: A, D

Explanation: By default, the Everyone group has only Read and Execute permissions on the root of each drive. These permissions are not inherited by subfolders; the Everyone group has no permissions by default to a newly created folder or file.
Similarly, when you create a shared drive or folder, the Everyone group now has only Read permission by default, rather than full control. This is quite a change from earlier versions of Windows, where every new folder gave everyone full control via both NTFS and share permissions.
So every user that is trying to access the files by using the SHARE will have read permissions.
However if an admin is trying to access the files by NOT going through the SHARE, he/she can still change

the contents. Therefore we add the Authenticated Users group and assign the Allow - Read permission to this group.
The file that needs to be shared with everybody having read-only permissions on the contents should have the default share permissions. That should ensure that only administrators will have full-control permissions on it and not the other users as well. However, the question states that all users including network administrators should have read-only permission, thus you should add the Authenticated Users group to the Allow-Read permission group.
Incorrect answers:
B: The Allow-Full Control will also allow more permissions than are required. The file that needs to be shared with everybody having read-only permissions on the contents should have the default share permissions.
C: The Allow-Full Control will also allow authenticated users more permissions than are required because the file that needs to be shared with everybody having read-only permissions on the contents should have the default share permissions.
E: The authenticated users and not the interactive group should be granted permissions.
F: Assigning the Deny - Full Control permission to the Administrators group on the Security tab will not have the file that needs to be shared with everybody having read-only permissions on the contents.
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. 414-428

QUESTION 136
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
You create and share a folder named Sales on a member server. You apply the default share permission and NTFS permissions to Sales. Then you create a folder named SalesForecast in Sales. You apply the default NTFS permissions to SalesForecast.
Managers in the sales department are members of a domain user group named SalesManagers. When members of SalesManagers try to add files to SalesForecast, they receive the "Access is denied" error message.
You need to configure permissions on these folders to fulfil the following requirements:
• Members of SalesManagers must be able to create, modify, and delete files in both folders.
• All other domain users must only be able to read files in both folders.
What should you do?

A. Configure the share permissions on Sales to assign the Allow - Change permission to the Everyone group.
Configure the NTSF permissions on SalesForecast to assign the Allow - Write permission to the SalesManagers group.
B. Configure the share permissions on Sales to assign the Allow - Change permissions to the SalesManagers group.
Configure the NTSF permissions on Sales to assign the Allow - Write permissions to the SalesManagers group.
C. Configure the share permissions on Sales to assign the Allow - Change permissions to the Everyone group.

Configure the NTFS permissions on Sales to assign the Allow - Modify permission to the SalesManagers group.
D. Configure the share permissions on Sales to assign the Allow - Change permission to the SalesManagers group.
Configure the NTFS permissions on Sales to assign the Allow - Modify permission to the SalesManagers group.

Answer: D

Explanation: By default, the Everyone group has only Read and Execute permissions on the root of each drive. These permissions are not inherited by subfolders; the Everyone group has no permissions by default to a newly created folder or file.
Similarly, when you create a shared drive or folder, the Everyone group now has only Read permission by default, rather than full control. This is quite a change from earlier versions of Windows, where every new folder gave everyone full control via both NTFS and share permissions.
The following configurations should be carried out when configuring the correct permissions:
• Share Permissions - Sales Folder - Everyone group - Allow Read Permissions.
• Share Permissions - Sales Folder - SalesManagers group - Allow Change Permissions.
• NTFS Permissions - Sales Folder - Everyone group - Allow Read Permissions.
• NTFS Permissions - Sales Folder - SalesManagers group - Allow modify Permissions.
Incorrect Answers:
A: This would prevent the SalesManagers group being able to delete files in the SalesForecast folder.
B: This would prevent the SalesManagers group being able to delete files in the SalesForecast and Sales folder.
C: This option would work, however answer D would be a better and more secure solution.
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. 423-425

QUESTION 137
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional. All file and print services are hosted by a member server named CK1 .
You create a folder named Data on CK1 .
You need to configure the initial permissions settings for Data. You must ensure that only local access is prevented. You must also ensure that users who are logged on to CK1 cannot modify any access permissions for Data.
What should you do?
To answer, configure the appropriate options in the dialog box. Drag the appropriate group to the correct location.

Groups

Network Group

Interactive Group

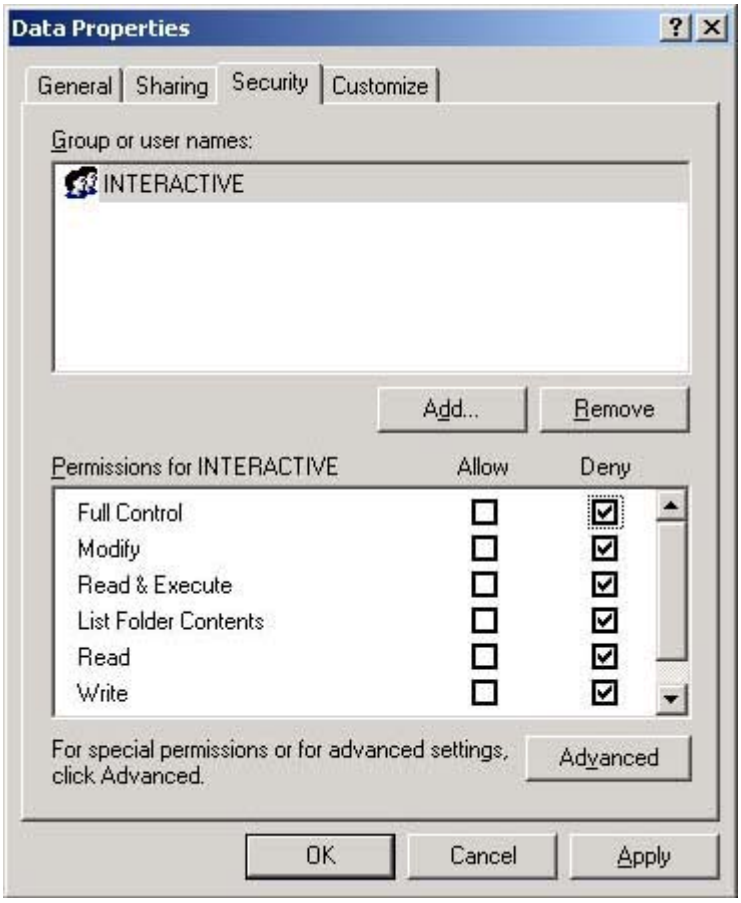
System Group

Authenticated Users Group

Digest Authentication Group

Dialog Box

Answer:



Explanation: To prevent local access we must Deny the interactive group.
Setting User Rights and Privileges
• User rights can override NTFS permissions in certain cases (a user with the Backup files and directories right is able to read all files on the volume, regardless of the NTFS permissions assigned, but only for the purpose of backing up and restoring data).
• Assign user rights to groups whenever possible. Assigning user rights to individual user accounts is difficult to manage.
• User rights are set using Group Policy.
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. 475

QUESTION 138
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. Some client computers run Windows NT 4.0 Workstation. Others run Windows 2000 Professional, and the rest run Windows XP Professional.
Users in the accounting department require a shared folder for their own use only. The accounting users must be able to read, edit, and delete files in the shared folder.
You create the shared folder and use default share permissions. You assign the Allow - Full Control NTFS permission to members of the Administrators group. You assign the Allow - Modify NTFS

permission to the accounting users.
However, accounting users report that they cannot access the shared folder.
How should you solve this problem?

A. Change the type of setting on the folder to Documents (for any file types).
B. Change the NTFS permissions on the folder to assign the Allow - Delete Sub-Folders and Files permission to the accounting users.
C. Add the accounting users as owners of the folder.
D. Change the share permissions to assign the Allow - Full Control permission to the accounting users.

Answer: D

Explanation: By default, the Everyone group has only Read and Execute permissions on the root of each drive. These permissions are not inherited by subfolders; the Everyone group has no permissions by default to a newly created folder or file. Similarly, when you create a shared drive or folder, the Everyone group now has only Read permission by default, rather than full control. This is quite a change from earlier versions of Windows, where every new folder gave everyone full control via both NTFS and share permissions.
To grant the accounting users access to the shared folder so that that can read, write, edit and delete files, they need the Allow-Full control permission.
Incorrect answers:
A: Changing the file type to whatever type will not solve the problem of access to the shared folder. It is a permissions issue not a file type issue.
B: Assigning the Allow-Delete Subfolders and Files permission to the accounting users enables the object to delete a file or subfolder, even if the Delete permission has not been granted to the object. Though, this does not solve the access problem.
C: Taking Ownership enables the object to change the owner of a file or folder to the object's user ownership. But what is needed in this scenario is to have Allow-Full Control permission. Changing ownership of the file effectively removes the user that created the file from the CREATOR OWNER group for that file, and that user's access to the file reverts to the default access he or she has based on the folder permissions.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 420 - 421, 423

QUESTION 139
You are the network administrator for Certkiller .com. All network servers run Windows Server 2003.
A file server named Certkiller SrvA has shadow copies enabled. One shared folder on Certkiller SrvA has the configuration shown in the following table.

Folder	Location	Contents
CertkillerDocs	D:\CertkillerDocs	D:\CertkillerDocs\AccountingData.xls, Financials.xls

While viewing a previous version of Certkiller Docs, you open and edit Financials.xls. However, when you try to save the edited file, you receive the following error message:

You need to save your changes to the previous version of Financials.xls. You must ensure that other users can continue to access current data on Certkiller SrvA without interruption.
What should you do?

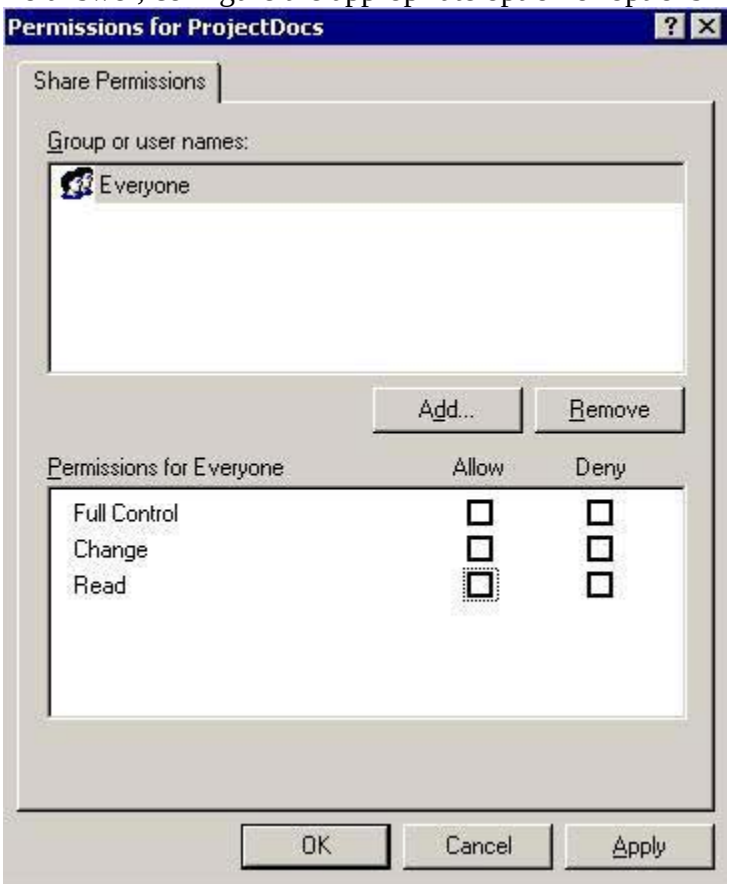
A. Copy the previous version of Certkiller Docs to a separate location.
B. Restore the previous version of Certkiller Docs to the default location.
C. Save Financials.xls in a separate location by using Microsoft Excel.
D. In the security properties of Financials.xls, assign the Allow - Modify permissions to the Everyone group.

Answer: C

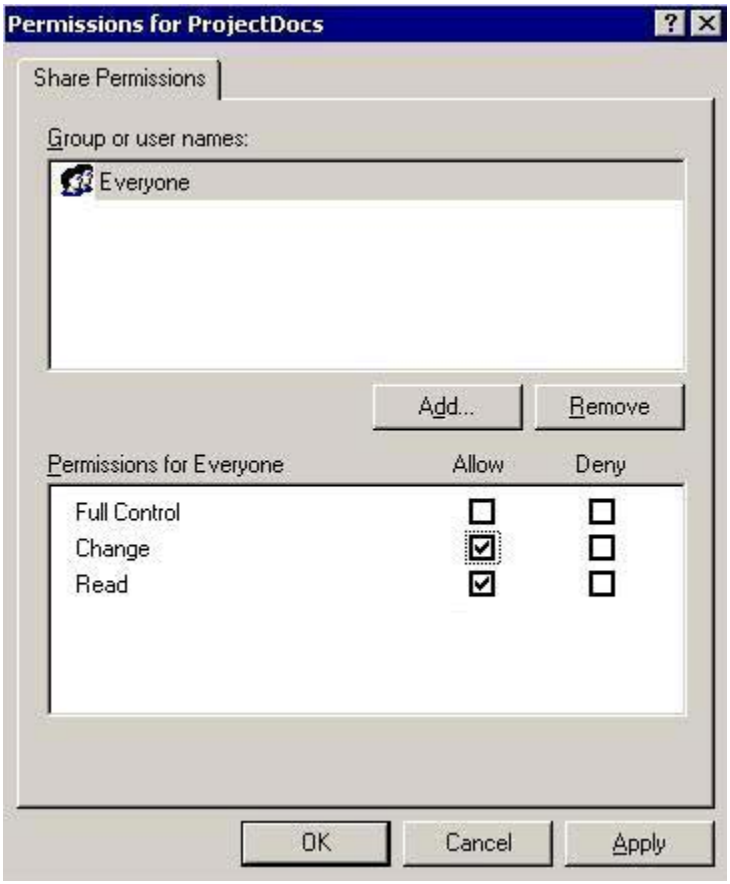
Explanation: When you view a 'previous version' of a file, the file is opened as Read Only. You can make changes to the file, but you cannot save the file in its current location. You need to save the file to an alternate location or else you will interrupt the other users.
Incorrect Answers:
A: If you copy a shared folder to a new location, the original folder will continue to have the original share pointing to it. You have made changes to the file. You cannot copy the file to another location without losing your changes. This is why you must save the file to another location.
B: You have made changes to the file by editing it. You will be unable to restore the previous version of the file to the default location without losing your changes.
D: You cannot modify the permissions of previous versions of files; you must save or copy the file to another location first (or restore it to its default location). In this scenario, the file must be saved to an alternate location because you don't want to lose your changes to the file.
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. 426-428

QUESTION 140
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. Most client computers run Windows XP Professional, and the rest run Windows 2000 Professional.
You create and share a folder named ProjectDocs on a member server. The current state of permissions for the folder is shown in the dialog box.
Users report that they receive an 'Access is denied' error message when they try to add or create files and folders in ProjectDocs.
You need to configure the permissions on ProjectsDocs to fulfill the following requirements:
• Domain users must be able to create or add files and folder.
• Domain users must not be able to change NTFS permissions on the files or folders that they create or add.
• Domain users must receive the minimum level of required permissions.
What should you do?

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



Answer:



Explanation: The default share permission is Everyone - Read. To be able to write to the shared folder, the users require "Change" permission. The Change permission allows users to Read, Write, Execute and Delete files in the shared folder. Note: the exhibit shows the everyone group. In the exam, if you have the option to select the groups, then selecting Domain users - Change would be a better option.
Share permissions can be set only at the folder level, not at the file level. Also note that shared-folder permissions apply only when accessing the resources across the network. These are the two most important ways in which NTFS permissions differ from shared-folder permissions.
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. 414

QUESTION 141
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. The functional level of the domain is Windows 2000 native. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
The network includes a shared folder named Certkiller Info. Your boss Dr. King reports that he is often unable to access this folder. You discover that the problem occurs whenever more than 10 users try to connect to the folder.
You need to ensure that all appropriate users can access Certkiller Info.
What should you do?

A. Decrease the default user quota limit.

B. Raise the functional level of the domain to Windows Server 2003.
C. Purchase additional client access licenses.
D. Move Certkiller Info to one of the servers.

Answer: D

Explanation: It is likely that the share exists on a Windows XP client. That would lead to a situation where the Windows XP client computer only allows up to 10 connections at the same time resulting in users being unable to access Certkiller Info when the 10 connections are full. Moving the shared folder to a server computer will allow more concurrent connections.
Incorrect Answers:
A: The quota limit is irrelevant to network connections. It only comes into play when considering disk space.
B: The functional level of the domain is not the cause of the problem. The problem stems from connectivity difficulties when multiple users access the folder. Windows 2000 Native- this level supports Windows 2000 DCs and Windows Server 2003 DCs only. Windows 2000 DCs in native mode move to Windows 2000 native functional level when upgraded to Windows Server 2003.
C: This is not a CAL problem.
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. 47-50, 141

QUESTION 142
You are the administrator of Certkiller 's network. Your accounting department has a Windows Server 2003 computer named Certkiller Srv
A. This computer hosts a secured application that is shared
among several users in the accounting department. All users of the application must log on locally to Certkiller SrvA.
You decide to create desktop shortcuts that point to the application. These shortcuts must be available only to new users of Certkiller SrvA.
Which folder or folders should you modify on Server? (Choose all that apply)
To answer, select the appropriate folder or folders in the work area.

Answer: Default User

Explanation: When a new user logs on to a machine for the first time, a new profile is created for that user. The "Default User" profile is copied and given the same name as the username. Any settings in the Default User profile will be applied to any new users.
Incorrect Answers:
All Users: Settings in this profile apply to all users of the machine, including current users. This is contrary to the requirements set out in the question.
Administrator, MZimmerman, RHunter, User: These are all user profiles. i.e. Profiles belonging to users who have logged in to the computer.
References:
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 286-292

QUESTION 143
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.
Terminal services is installed on a server named Certkiller 6. This server also stores user profiles.
Certkiller 6 has limited processor resources, limited memory resources, and limited disk space.
Remote users connect to Certkiller 6 to read e-mail, review documents, and access a front-end SQL query tool. All remote users have sufficient permissions to edit their registries. All client computers are licensed to use the query tool.
Tess King, another administrator at Certkiller , accidentally changes the server settings on Certkiller 6.
You are required to restore the server settings to comply with company standards. You also need to ensure that no unnecessary files are stored on Certkiller 6.
What action should you? (Use the dialog box)

Answer:
Delete temporary folders on exit = Yes.
Use temporary folders per session = Yes.
Licensing = Per Device.
Active Desktop = Disable.
Permission Compatibility = Full Security.
Restrict Users to one session = Yes.

Explanation: Delete a session's temporary folder when the user logs off. This setting is configured to Yes by default. Thus the Delete temporary folders on exit enabled is necessary as Certkiller 6's disk space is limited.
Licensing - Allows for the administrator to configure the server as a terminal server or Remote Desktop for Administration computer. This setting is configured to Remote Desktop for Administration if the terminal server role has not been installed. If it has, this setting reflects the licensing choice made when you installed the terminal server role (per Device or per User) and can be changed here.
Active Desktop - Enables the use of Active Desktop technologies in Terminal Services sessions. These desktops can use considerably more bandwidth than traditional desktops. This setting is configured to be enabled by default.
Permission Compatibility Full security is the only choice available for Remote Desktop for Administration. A second mode, Relaxed Security, is added when the terminal server role is installed on the server, which loosens security to accommodate older Windows computers and legacy applications. This is configured as Full Security by default.
Restrict each user to one session - Can be used to ensure that users do not establish more than one session to a Terminal Services system. Savvy users may be able to work around this setting by specifying a different program to start upon connection for each different session.
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. 559

QUESTION 144
You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains two domains. You have not modified the default Active Directory site configurations. The functional level of both domains is Windows 2000 native. Servers run either Windows Server 2003 or Windows 2000 Server.
Certkiller 's internal domain is named Certkiller .local. Certkiller 's external domain is named

extranet. Certkiller .com. The external domain is accessed only by Certkiller 's business partners.
You install a Windows Server 2003 computer named Certkiller 7 in the extranet. Certkiller .com domain. You install and configure Terminal Services on Certkiller 7. Certkiller 7 is configured as a member server in the domain. You install a secure database application on Certkiller 7 that will be accessed by Certkiller 's business partners.
A few months later, users report that they can no longer establish Terminal Services session to Certkiller 7. You verify that only the default ports for HTTP, HTTPS, and Terminal Services on your firewall are open to the Internet.
You need to ensure that Certkiller 's business partners can establish Terminal Services sessions to Certkiller 7.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Install Terminal Services Licensing on a Windows 2000 Server computer in Certkiller .local. Configure the computer as an Enterprise License Server.
B. Install Terminal Services Licensing on a Windows 2000 Server computer in extranet. Certkiller .com. Configure the computer as an Enterprise License Server.
C. Install Terminal Services Licensing on a Windows Server 2003 computer in extranet. Certkiller .com. Configure the computer as an Enterprise License Server.
D. Install Terminal Services Licensing on a Windows Server 2003 computer in Certkiller .local. Configure the computer as an Enterprise License Server.
E. Instruct Certkiller 's business partners to connect by using the Terminal Services Advanced Client (TSAC) over HTTPS.

Answer: B, C

Explanation: Clients connecting to a Windows 2000 terminal server from a Windows 2000 Professional computer are not required to purchase a license, as Windows 2000 Pro includes a Terminal Services CAL. However, you still must set up a licensing server. In Windows Server 2003, Remote Administration mode has been renamed to Remote Desktop for Administration and it is installed by default. This works like the Remote Desktop feature in Windows XP. As in Windows 2000, you are still limited to two simultaneous remote desktops at a time. However, there is one improvement: you can now take over the local console session.
Incorrect answers:
A: Installing Terminal Services on Certkiller .local will not enable Certkiller 's business partners to establish terminal service sessions on Certkiller 7.
D: Installing Terminal Services on Certkiller .local even if it is a Windows Server 2003 machine, will not enable Certkiller 's business partners to establish Terminal Service sessions.
E: With the release of the Terminal Services Advanced Client (TSAC) as a ValueAdd component on Microsoft Windows 2000 Server, Service Pack 1, the Terminal Services solution is now extended to the Web. For example, organizations needing to deploy line of business applications to remote offices can do so by means of a Terminal server and a Web server running ASP pages, such as the sample pages supplied with the TSAC. On the client side, all that is needed is Internet Explorer, a connection to the World Wide Web, and appropriate access rights, however this is not applicable 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, p. 39.

QUESTION 145
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
You install Terminal Server on three member servers named Certkiller 1, Certkiller 2, and Certkiller 3.
You add a domain group named HR to the Remote Desktop Users group on all three terminal servers.
One week later, you discover that files on Certkiller 1 and Certkiller 2 were deleted by a user named Tess, who is a member of the HR group.
You need to prevent Jack from connecting to any of the terminal servers.
What should you do?

A. On all three terminal servers, modify the RDP-Tcp connection permissions to assign the Deny - Users Access and the Deny - Guest Access permissions to the HR group.
B. On all three terminal servers, modify the RDP-Tcp connection permissions to assign the Allow - Guest Access permission to Jack's user account.
C. In the properties of Jack's user account, disable the Allow logon to a terminal server option.
D. On all three terminal servers, modify the RDP-Tcp connection permissions to assign the Deny - User Access and the Deny -Guest Access permissions to the Remote Desktop Users group.
E. In the properties of Jack's user account, enable the End session option.

Answer: C

Explanation: Jack is a member of the HR group which is a member of the Remote Desktop Users group on the member servers. As such she has permission to log in to the member servers. We can deny that permission by disabling the "Allow logon to a terminal server" option on the Terminal Services Profile tab in the properties of her user account. This setting will override the permissions given to her by way of group membership.
Incorrect Answers:
A: The Deny - Users access permission will deny all users access to the terminal servers.
B: We need to prevent Jack from connecting to the terminal servers. Allowing Guest - access will still enable her to connect.
D: This will prevent anyone from connecting to the terminal servers.
E: The End Session option will only limit the time Jack can connect to the servers for; it will not prevent her connecting to the servers.
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. 547-548

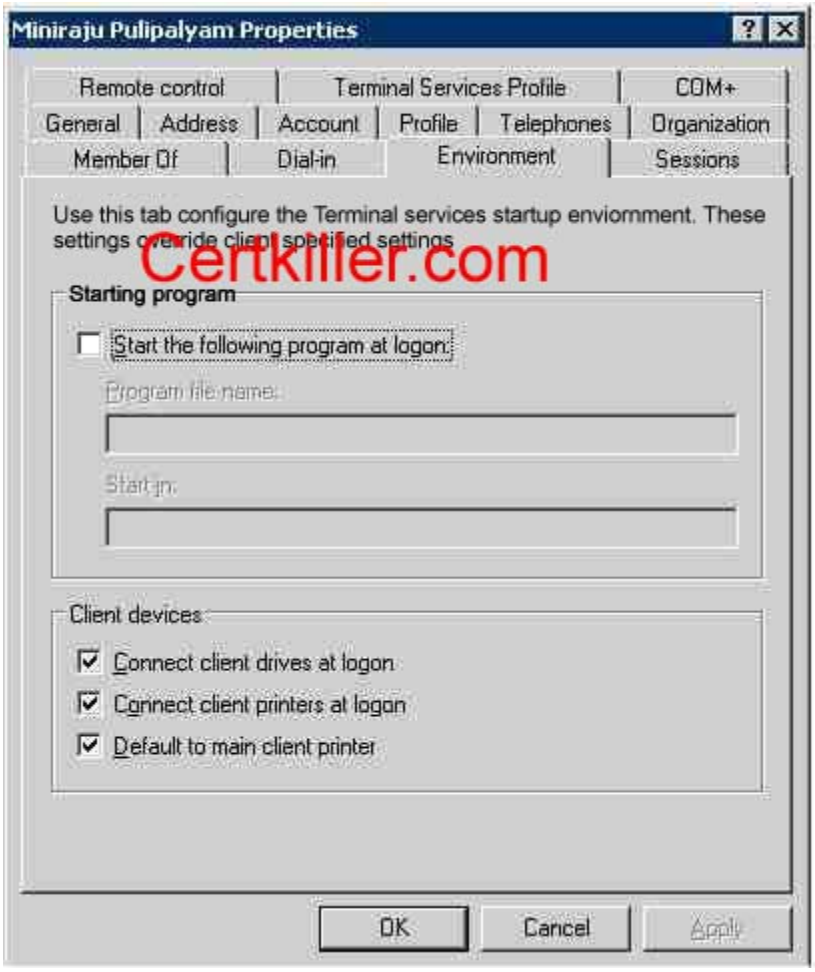
QUESTION 146
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.
Three member servers are configured as terminal servers. All three host confidential data. Currently, all network users are full-time employees, and all network users are allowed to log on to the terminal

servers.
Certkiller hires 25 temporary employees. You create a user account for each one.
You need to ensure that only full-time employees are allowed to log on to the terminal servers.
What should you do?

A. Modify the Default Domain Group Policy object (GPO).
Configure a computer-level policy to prevent the temporary employees from connecting to the terminal servers.
B. Modify the Default Domain Group Policy object (GPO).
Enable the user-level Terminal Server setting Sets rules for remote control of Terminal Services user sessions.
C. On the Terminal Services Profile tab of the user properties for each account, disable the option to log on to terminal servers.
D. In the security policy for domain controllers, disable the computer-level Terminal Server setting Allow users to connect remotely using the terminal server.
Answers: C

Explanation: Terminal Services is the underlying technology that enables Remote Desktop for Administration, Remote Assistance, and Terminal Server. By disabling the logon option in the Profile tab will effectively prevent workers other than full time workers from logging on. Since all network users are full time employees are the as such the only users allowed in the network The Allow Logon to Terminal Server check box controls whether the person is permitted to log in to the terminal server at all. By default, anyone with an account on the domain or server may do so. Therefore we need to disable this for the temporary users.
Incorrect Answers:
A: This would affect all users; we only need to configure the temporary users. You should not affect the network users.
B: This would affect all users; we only need to configure the temporary users.
D: Disabling the computer-level Terminal Server is bound to affect all users; we only need to configure the temporary users without interfering with the full-time personnel.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 147
You are the administrator for Certkiller .com's Active Directory domain. All client computers run Windows XP Professional.
A Windows Server 2003 computer named Certkiller 8 has Terminal Services installed. Users in the finance department access a custom application that is installed on Certkiller 8.
A finance department user reports that he cannot copy files from his Terminal Services session to his local computer. You view his user account properties, which are shown in the exhibit.



Other finance department users are not experiencing this problem.
You need to ensure that the user can access his local drives through his Terminal Services session.
What should you do?

A. In the environment properties of the user account, enable the Start the following program at logon option.
Specify net use z: \\Localhost\C$ as the program file name.
B. Instruct the user to enable the Disk Drives option in the properties of his remote desktop connection.
C. Instruct the user to log off, and then to select Log on using dial-up connection from the Log On to Windows dialog box.
D. Instruct the user to run the mstsc /console command.
E. Instruct the user to run the mstsc /edit command.

Answer: B

Explanation: When you initially launch the Remote Desktop Connection utility, most of its configuration information is hidden. To display it before you use it to establish a connection, click the Options button. This will reveal a series of tabs and many additional settings that have be configured. Local Resources tab enables you to control whether or not client resources are accessible in your remote session. By instructing the user to enable the disk drives will ensure his/her access through his terminal sessions.

Incorrect answers:
A: This option will not solve the user's problem. The user's disk drives should be enabled in the properties of his remote desktop connection.
C: To solve this user's problem a new connection must be added using the Remote Desktops snap-in and accept all default settings. Not logging on and using the dial-up connection.
D: The mstsc /console command can be used to connect to the console session of a Terminal Services computer. However, an administrator actually sitting at the server and using the console session can request help by using the Remote Assistance functionality in Terminal Services.
E: This command does allow editing it displays the Remote Desktop Connection to establish a connection with a terminal server. But this is not going to help this user.
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. 525-526
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 148
You are a network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com.
The domain contains two Windows Server 2003 terminal servers that host applications that are used by company employees. An organization unit (OU) named TerminalServers contains only the computer accounts for these two Terminal servers. A Group Policy object (GPO) named TSPolicy is linked to the TerminalServers OU, and you have been granted the right to modify the GPO.
Users should use the terminal servers to run only authorized applications. A custom financial application suite is currently the only allowed application. The financial application suite is installed in the folder C:\Program Files\MT Apps. The financial application suite contains many executable files.
Users must also be able to use Internet Explorer to access a browser-based application on the company intranet. The browser-based application makes extensive use of unsigned ActiveX components.
The financial application suite and the browser-based application are frequently updates with patches or new versions.
You need to configure the terminal servers to prevent users from running unauthorized applications.
You plan to configure software restriction policies in the TSPolicy GPO. To reduce administrative overhead, you want to create a solution that can be implemented once, without requiring constant reconfiguration.
Which three actions should you perform to configure software restriction polices? (Each correct answer presents part of the solution. Choose three)

A. Set the default security level to Disallowed.
B. Set the default security level to Unrestricted.
C. Create a new certificate rule.
D. Create a new hash rule.
E. Create a new Internet zone rule.
F. Create a new path rule.

Answer: A, E, F

Explanation: We need to prevent unauthorized applications from running. We should set the default security level to Disallowed. This will prevent the users running any applications; we can then make exceptions to this rule.
An Internet zone rule would allow the users to run the intranet application.
A path rule would allow the users to run the application in a certain path; in this case C:\Program Files\MT Apps. The question states that the application is regularly updated with patches etc. Therefore, we cannot use a hash rule or a certificate rule, because we would have to recreate the hash or the certificate every time the application was updated.
The purpose of a rule is to identify one or more software applications, and specify whether or not they are allowed to run. Creating rules largely consists of identifying software that is an exception to the default rule. Each rule can include descriptive text to help communicate why the rule was created.
A software restriction policy supports the following four ways to identify software. Following are two of them:
• Path Rule - Path is the local or universal naming convention (UNC) path of where the file is stored. A path rule can specify a folder or fully qualified path to a program. When a path rule specifies a folder, it matches any program contained in that folder and any programs contained in subfolders. Both local and UNC paths are supported.
• Zone Rule - A rule can identify software from the Internet Explorer zone from which it is downloaded.
Incorrect answers:
B: The unrestricted security level will not restrict the users from running unauthorized applications.
C: Certificate Rule: A certificate rule specifies a code-signing, software publisher certificate. For example, a company can require that all scripts and ActiveX controls be signed with a particular set of publisher certificates. Certificates used in a certificate rule can be issued from a commercial certificate authority (CA) such as VeriSign, a Windows 2000/Windows Server 2003 PKI, or a self-signed certificate. A certificate rule is a strong way to identify software because it uses signed hashes contained in the signature of the signed file to match files regardless of name or location. If you wish to make exceptions to a certificate rule, you can use a hash rule to identify the exceptions.
D: Hash is a cryptographic fingerprint of the file.
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. 657 -659

QUESTION 149
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003. You install Terminal Services on all domain controllers. However, your technical support specialists report that they cannot use Terminal Services to access any domain controllers.
Which action or actions should you perform to solve this problem? (Choose all that apply)

A. Install Remote Desktop for Administration.
B. Require the support specialists to use a console session to connect to the terminal servers.
C. Add the Remote Administrators group to the Account Operators group.
D. Add the support specialists to the Remote Desktop group.

E. Modify the Default Domain Controller Group Policy object (GPO) to grant the Log on locally user right to the support specialists.

Answer: D, E

Explanation: The Remote Desktop group has the necessary permissions to connect to the servers using Terminal Services. Terminal Services is a built-in service that enables you to use the Remote Desktop Connection software to connect to a session that is running on a remote computer while you are sitting at another computer in a different location. This process is extremely useful for employees who want to work from home but need to access their computers at work. Terminal Server mode, deployed traditionally, allows multiple remote clients to simultaneously access Windows-based applications that run on the server. Remote Desktop for Administration is used to remotely manage Windows Server 2003 servers.
We need to add the support specialists to the Remote Desktop group. As the servers are domain controllers, we must to grant the Log on locally user right to the support specialists.
Incorrect Answers:
A: Remote Desktop for Administration is installed by default in Windows Server 2003.
For security reasons it is disabled by default. It can be enabled through the System control panel. There is thus no need to install it.
B: They do not require a console session.
C: The Account Operators do not have permission to connect using Terminal Services.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapters 5 & 7

QUESTION 150
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. A Windows Server 2003 computer named Certkiller 3 is configured as a member server in your domain.
You install Terminal Services on Certkiller 3. You also install several legacy applications on Certkiller 3. Users report that they cannot run many of the legacy applications on Certkiller 3 through their Terminal Services sessions. You establish a Terminal Services session by using the Administrator account, and you verify that you can run the legacy applications.
You need to ensure that users can run the legacy applications on Certkiller 3 while they are connected through Terminal Services.
What should you do?

A. Add all Terminal Services users to the domain Server Operators group.
B. Share the C:\Program Files folders on Certkiller 2. Assign the Domain Users group the Allow - Full Control share permissions.
C. Install Terminal Server Licensing Server on Certkiller 3.
D. Use Terminal Services Configuration to change the Permissions Compatibility setting.

Answer: D

Explanation: Permission Compatibility can be set to either Full Security or Relaxed Security. It specifies whether you are using Full Security or Relaxed Security for clients accessing the Terminal Services server.

Some applications may not work properly with Full Security.
Thus in this case you need to change the Permissions Compatibility setting to ensure that users will be able to run the legacy applications on Certkiller 3 when connected through Terminal Services.
Incorrect answers:
A: This option will not ensure that all Terminal Services users will be bale to run the legacy applications on Certkiller 3.
B: Even though Certkiller 3 is a member server in the domain, assigning Domain Users the Allow-Full Control share permission will not ensure that they can run the legacy application when connected through Terminal Services.
C: It is not a Licensing matter.
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. 410

QUESTION 151
You are the network administrator for Certkiller . Your network consists of two Active Directory domains. Each department has its own organizational unit (OU) for departmental user accounts. Each OU has a separate Group Policy object (GPO)
A single terminal server named Certkiller Term1 is reserved for remote users. In addition, several departments have their own terminal servers for departmental use.
Your help desk reports that user sessions on Certkiller Term1 remain connected even if the sessions are inactive for days. Users in the accounting department report slow response times on their terminal server.
You need to ensure that users of Certkiller Term1 are automatically logged off when their sessions are inactive for more than two hours. Your solution must not affect users of any other terminal servers.
What should you do?

A. For all accounting users, change the session limit settings.
B. On Certkiller Term1, use the Terminal Services configuration tool to change the session limit settings.
C. Modify the GPO linked to the Accounting OU by changing the session limit settings in user-level group polices.
D. Modify the GPO linked to the Accounting OU by changing the session limit settings in computerlevel group polices.

Answer: B

Explanation: The question states that you need to ensure that users of Certkiller Term1 are automatically logged off when their sessions are inactive for more than two hours. Therefore, you need to configure Certkiller Term1 by changing the session limit settings.
You can limit the amount of time that active, disconnected, and idle (without client activity) sessions remain on the server. This is effective since sessions which remain running indefinitely on the server, typically consume valuable system resources. When a session limit is reached for active or idle sessions, you can select to either disconnect the user from the session or end the session. A user who is disconnected from a session can reconnect to the same session later. When a session ends, it is permanently deleted from the server, and any running applications are forced to shut down. This can result in data loss at the client. When a session limit is reached for a disconnected session, the session ends. This permanently deletes it from the

server.
Sessions can also be allowed to continue indefinitely.
Incorrect Answers:
A: You need to change the session limit for all users of Certkiller Term1, not only for the Finance users.
C: You need to configure Certkiller Term1 to change the session limit settings.
D: You need to configure Certkiller Term1 to change the session limit settings.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, p. 665

QUESTION 152
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. Half of the client computers run Windows XP Professional, and the other half run Windows NT 4.0 Workstation.
You install Terminal Server on three member servers named Certkiller 1, Certkiller 2, and Certkiller 3. Each server has a single Pentium III 600-Mhz CPU with 512 MB of RAM and a single-channel EIDE disk subsystem. You place all three terminal servers in an organizational unit (OU) named Terminal Server. You link a Group Policy Object (GPO) to the Terminal Server OU.
Several days after the installation, users report that the performance of all three terminal servers is unacceptably slow. You discover that each server has at least 50 active sessions at once.
You need to improve performance of all three terminal servers. You must achieve this goal by using the minimum amount of administrative effort, without upgrading any hardware.
What should you do?

A. Log on to the console of each terminal server. In the RDP-Tcp connection properties, set the Maximum connections option to 35.
B. Edit the GPO to set the Limit number of connections policy to 35.
C. Modify all domain user accounts to set the When a session limit is reached or broken user property to End session.
D. Edit the GPO to enable the Remove Disconnect option from shutdown dialog policy.

Answer: B

Explanation: By setting the Limit number of connections policy in the group policy object to 35, you will be able to prevent a situation where there is more than the necessary amount of simultaneous connections at any one time. Then you will not get a situation where there is more than 50 simultaneous connections that would probably be idle sessions and thus cause the performance of the servers to be poor. This option will not require the upgrading of any hardware or unnecessary administrative effort.
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. 47-51, 682
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6

QUESTION 153
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. A single server running Terminal Server is available to remote users.
Your help desk staff is responsible for monitoring user activity on the terminal server. The staff is also responsible for sending messages to users about new programs and about modifications to the terminal server. A company developer writes a script that will log the relevant user information in a file and provide pop-up messages as needed.
You need to ensure that the script runs every time a user logs on to the terminal server.
What should you do?

A. Deploy a client connection object for remote users.
Configure the client connection object to run the script.
B. On the terminal server, configure the RDP-tcp properties with the name of the script.
Override other settings.
C. In the Default Domain Group Policy object (GPO), select the Start a program on startup option and specify the name of the script.
D. On the terminal server, configure the RDP client properties with the name of the script.
Answers: B

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.
You should keep in mind that every property you set will affect all users who connect through the listener connection. Thus by configuring RDP-Tcp properties with the name of the script on the terminal server and overriding all the settings will ensure that the script runs every time a user logs on to the terminal server.
Incorrect answers:
A: Configuring the client connection object to run the script will not run the script when a user logs on to the terminal server.
C: Selecting the Start a program on startup option and specifying the name of the script in the Default Domain Group Policy object will not make a scrip run every time a user logs on to the terminal server.
D: The most important thing to remember is that every property you set affects all users who connect through the listener connection. But configuring the RDP client properties will not ensure that the script runs every time a user logs on to the terminal 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. 547-549.

QUESTION 154
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003. Some client computers run Windows XP Professional, and the rest run Windows NT 4.0 Workstation.
Certkiller includes departments for accounting, design, marketing, and sales. Each department has a corresponding organizational unit (OU).
A member server named Certkiller 1 can be accessed only by user accounts in the Accounting, Design, Marketing, and Sales OUs. You install Terminal Server on Certkiller 1. Then you install four new applications on Certkiller 1. Each application is intended for users in only one of the four departments.
You need to ensure that each application can be accessed only by users in the appropriate department. You need to achieve this goal by using the minimum amount of administrative effort.

What should you do?

A. In the Default Policy Group Policy object (GPO), configure the Start program on connection policy to be the program path and file name of the application to start when the user logs on.
B. In each OU, set the Environment property for each user to the program path and file name of the application that corresponds to the OU.
C. On Certkiller 1, select the RDP-Tcp connection properties.
Set the program path and file name of the application to start when the user logs on.
D. Create one Group Policy object (GPO) for each department.
Link each GPO to the corresponding OU.
For each GPO, configure the Start program on connection policy to run the application that corresponds to the appropriate department.
Answers: D

Explanation: Group policies cannot be applied to groups, only sites, domains, and organizational units. An organizational unit (OU) is a container object in Active Directory used to separate computers, users, and other resources into logical units. An organizational unit is the smallest entity to which Group Policy can be linked. It is also the smallest scope to which administration authority can be delegated. At the client level, a user can specify that a program be launched when they connect to a server instead of receiving a desktop. Likewise, an administrator can specify this at the connection level for all users that connect to a specific listener connection. Finally, this can also be set in Group Policy. However, the client may receive a message stating, "This initial program cannot be started"
This error may be caused by an input error or incorrect path and executable file name. If you have entered the incorrect path and executable file name, they will be pointing to a file that does not exist.
Another possible cause is that the correct permissions are not set on the executable file. If Windows Server 2003 cannot access the file, it will not be able to launch the program. You should verify that the appropriate read and execute permissions are applied to both the file and the working folder. If neither of these two possible solutions resolves the issue, the application itself may have become corrupt. Try to launch the application at the server. If it will not open, you may need to uninstall and reinstall the application.
Incorrect Answers:
A: All users would start the same application; this is not what we need.
B: All users would start the same application; this is not what we need.
C: The question states: minimum amount of administrative effort, therefore we need to use a GPO. This would work though.
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. 17: 20
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 155
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.
Terminal Services is installed on a member server named Terminal1 with default settings.
Users in the editing department are members of a group named Editors. When these users try to

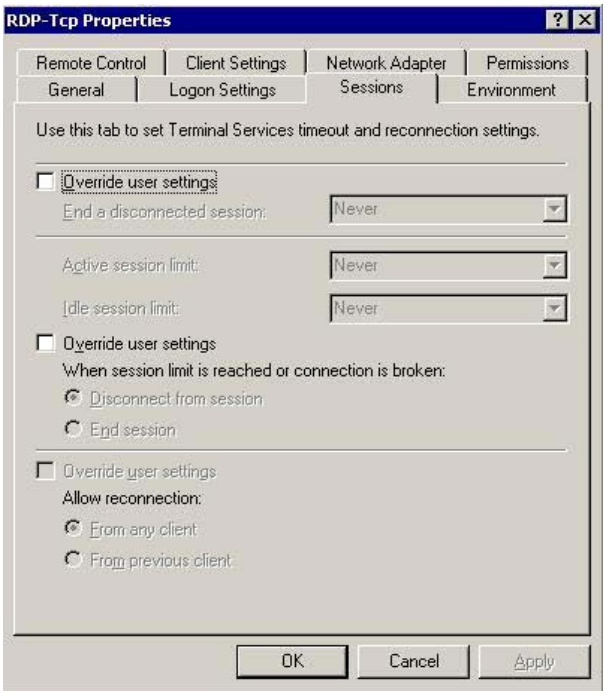
make a Terminal Services connection to Terminal1, they receive the following error message: "The local policy of this system does not permit you to logon interactively".
You need to enable members of the Editors group to establish Terminal Services sessions on Terminal1.
What should you do?

A. Enable the Allow users to connect remotely to this computer option on Terminal1.
B. Add the Editors group to the Remote Desktop Users group on Terminal1.
C. Configure the RDP-Tcp connection properties on Terminal1 to assign the Allow - Full Control permission to the Editors group.
D. Add the Editors group to the Remote Desktop Users group in Active Directory.

Answer: B

Explanation: The Remote Desktop Users group on Terminal1 have the necessary permission to connect to Terminal1 using a remote desktop connection. By simply adding the Editors group to the Remote Desktop Users group on Terminal1 we can give the Editors the required permission. The Remote Desktop Services on Terminal1 is not configured to allow Editors access. This group should be added to the Remote Desktop Users group on Terminal1 to enable them to establish Terminal Services sessions.
Incorrect Answers:
A: The Allow users to connect remotely to this computer option are for Remote Desktop For Administration, not Terminal Services.
C: The Editors group do not need Full Control access to the server. The problem is that they don't have the necessary permission to connect to Terminal1 using a remote desktop connection.
D: If you add the Editors group to the remote Desktop Users group in Active Directory you would allow the Editors group to connect to any Terminal server in the domain.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 156
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. All servers run Windows Server 2003, and all client computers run Windows XP Professional.
You install Terminal Server on a member server named Certkiller 4. Several days later, users report that server performance is unacceptably slow.
On Server1, you discover 75 disconnected sessions and 25 sessions that have been idle for at least three hours.
You need to configure Certkiller 4 to fulfill the following requirements:
• Disconnected sessions remain on the server for a maximum of 1 minute.
• Idle sessions remain on the server for a maximum of 30 minutes.
• Sessions idle for more than 30 minutes are automatically reset.
• Active sessions are not affected.
What should you do?
To answer, configure the appropriate option or options in the dialog box.



Answer:

Explanation: By default, most of the settings in the sessions tab are configured to use the user account property settings and several settings are grayed out. This can be overridden by selecting the check box next to Override user settings. When user settings are overridden, several settings are no longer grayed out; these include:
• End a disconnected session Used to specify the amount of time a disconnected session can remain running on the Terminal Services computer.
• Active session limit Used to specify the amount of time an actively used session can remain connected and in use.
• Idle session limit Used to specify the amount of time an idle session can remain connected to the Terminal Services computer.
The first 'Override user settings' checkbox specifies that a session is ended when the session limit is reached or the connection is broken. That will ensure that disconnected sessions remain on the server for a maximum of one minute. You can specify the maximum time limit for a disconnected session to remain on the server by configuring the 'End a disconnected session' option; the maximum time limit that a user session can remain active on the server by configuring the 'Active session limit' option; and the maximum time limit for a session to remain idle by configuring the 'Idle session limit' option. This should keep idle sessions on the server for a maximum of 30 minutes and reset them automatically.
The second 'Override user settings' checkbox specifies the type of action to be taken when the session limit is reached.
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. 551

QUESTION 157
You are the network administrator for Certkiller .com. All client computers run Windows 2000

Professional.
You recently deployed 10 new servers that run Windows Server 2003. You placed the servers in a new OU named W2K3Servers.
Tess is another network administrator.
You need to configure the appropriate permissions to allow Jack to manage the new servers by using Terminal Services from her client computer. You need to assign Jack only the permissions she needs to perform her job.
What should you do?

A. Add Jack's users account to the local Power Users group on each server that runs Windows Server 2003.
B. Add Jack's users account to the Remote Desktop Users group on each server that runs Windows Server 2003.
C. Assign Jack's user account the Allow - Read and the Allow - Write permissions for the W2K3Servers OU.
D. Configure the Managed By property for the W2K2Servers Out to Jack's user account.

Answer: B

Explanation: The Remote Desktop Users group is a special group that allows its members to log on to the server remotely. This is what is needed by Jack if she is to perform her job.
Incorrect answers:
A: Adding Jack account to the local Power Users group will not enable her to make use of Terminal Services.
C: Having the Allow-Read and the Allow-Write permissions will not ensure that Jack can do her job via Terminal Services.
D: This will not work for Jack as she will not be able to use Terminal Services to carry out her 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. 169

QUESTION 158
You are the network administrator for Certkiller . 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 domain contains a group named SalesAdmin. Members of the SalesAdmin group need the permission to add Group Policy links and create Group Policy objects (GPOs) for only the Sales organizational unit (OU).
You need to configure the domain to provide the SalesAdmin group with the minimum permissions necessary to meet these requirements.
What should you do?

A. Add the SalesAdmins group to the Group Policy Creator Owners group.
B. Configure the discretionary access control list (DACL) on all of the Group Policy links for the Sales OU to assign the SalesAdmins group the Allow - Apply Group Policy permission.
C. Run the Delegation of Control wizard on the domain to assign the SalesAdmin group the Manage

Group Policy links task.
D. Run the Delegation of Control wizard on the Sales OU to assign the SalesAdmins group the Manage Group Policy links task.

Answer: D

Explanation: To specify which Group Policy objects are linked to a given site, domain, or OU, use the Group Policy tab in the Properties page for a site, domain, or OU. This property page stores the user's choices in two Active Directory properties called gPLink and gPOptions. The gPLink property contains the prioritized list of Group Policy objects, and the gPOptions property contains the Block Policy Inheritance setting.
To manage GPO links to a site, domain, or OU, you must have Read and Write access to the gPLink and gPOptions properties. By default, Domain Administrators have this permission for domains and OUs. Enterprise Administrators and Domain Administrators of the forest root domain can manage links to sites. You can delegate rights to additional groups and users by using the Delegation Wizard and selecting the Manage Group Policy links predefined task.
Incorrect Answers:
A: The Creator Owner group permissions should be applied at the root of the volume. The Creator Owner group e.g. is a special group that determines the access that a user has to files and folders he or she has created. By default, the Full Control special permissions assigned to this group automatically apply to every folder created on the volume. Thus the default permissions of being Creator Owner would grant the SalesAdmins group too many permissions than is necessary.
B: The DACL is the part of the security descriptor that grants or denies access to individuals or groups for the object. These permissions can be assigned by anyone with "change permissions" credentials. Hence, it is under the discretion of the owner to assign access rights. This should work; however, they only need to apply their group policy links and objects to their own group. This type of permission will allow them to apply their work to all on the domain.
C: You should be running the Delegation of Control Wizard on the Sales OU and not on the domain.
Reference: Designing a Group Policy Infrastructure Windows Resource Kits
Delegating Group Policy-Related Permissions on Sites, Domains, and OUs
Managing GPO links

QUESTION 159
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All domain controllers run Windows Server 2003, and all client computers run Windows XP Professional.
A manager named Jack King creates a new folder named Certkiller Data. Jack shares this folder on a server so that Certkiller employees can create, edit, and delete documents. Jack wants users to have only these permissions.
You add the Authenticated Users group to the ACL on the Sharing tab and the ACL on the Security tab for the Certkiller Data folder.
You need to configure the appropriate permissions.
What should you do?
To answer, drag the appropriate share permissions and NTFS permissions to the correct location or locations in the work area.

Answer: Share permission: Change
NTFS permission: Modify

Explanation: One has to keep in mind that (1) Both NTFS and share permissions are cumulative. If a user belongs to more than one group, and two or more of these groups are assigned permissions on a file or folder, the user's effective permissions (NTFS or share) on the file or folder is the sum of all the groups' permissions. (2) When determining the effective permissions on a file or folder access through a share, the more restrictive permissions (that is, the cumulative effective NTFS permissions or the cumulative effective share permissions) are the ones applied. And (3) Assign user rights to groups whenever possible, assigning user rights to individual user accounts is difficult to manage.
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. 475-476

QUESTION 160
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
You create a network share named AppShare. This Share resides on a NTFS partition on a server named Certkiller SrvC. You set NTFS permissions on AppShare as shown in the following table.

Users	**NTFS permissions**	**Share permissions**
TessKing	Read	Read
Certkiller Group3	Read	Change
Certkiller Group4	Read/Write	Full Control
All Users	Read and Execute	Read

Tess belongs only to the All User Groups.
You need to enable Jack to delete files from AppShare.
What should you do?

A. Assign the Allow - Full Control share permissions to the All Users group.
B. Add Jack's User account to Certkiller Group4. Assign the Allow - Read and Execute NTFS permission to Certkiller Group4.
C. Add Jack's user Account to Certkiller Group3. Assign the Allow - Modify NTFS permissions to Certkiller Group3.
D. Assign the Allow - Full Control NTFS permissions to the All Users group.
E. Assign the Allow - Full Control share permissions to Jack's user account.

Answer: C

Explanation: Jack only belongs to the ALL USERS group, so her effective NTFS permissions are: Read/Execute + Read = Read/Execute permissions.
Tess only belongs to the ALL USERS group, so her effective SHARE permissions are: Read + Read = Read permissions. THUS her Total effective permissions are: Read/Execute + Read = READ Permissions.
Changing Jack status by adding her to the Usergroup3 will enable Jack with the rights to delete files from the AppShare.
If we add Jack to the Certkiller Group3, and we add - modify NTFS permissions to that group:
Then her effective NTFS permissions are: Read/Execute + Read + Modify = Modify permissions.
Then her effective SHARE permissions are: Read + Read + Full Control = Full Control permissions.
Her total effective permissions will be: Modify + Full Control = MODIFY Permissions.
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. 475 - 480

QUESTION 161
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
All summer interns in the company are members of the Interns global group. All users in the engineering department are members of the Engineering global group.
A member server named CK1 contains a folder that is shared as Blueprints. Permissions on Blueprints are shown in the following table.

Share permissions	**NTFS permissions**
Everyone: Change	Administrators: Full Control
	Engineers: Modify

User accounts in Interns and Engineers do not have the Log on locally user right on CK1 .
A user named Mark is a member of both Interns and Engineers. You discover that data in Blueprints was modified by Mark.
You need to reconfigure the permissions on Blueprints to ensure that Mark cannot access the folder. You must not affect the access of any other users. You must ensure that Mark remains in Engineers so he can access other appropriate resources.
What should you do?

A. Configure the share permissions to assign the Allow - Read permission to Mark.
B. Configure the NTFS permissions to assign the Deny - Read permission to Engineers.
C. Configure the NTFS permissions to assign the Deny - Read and Deny - Execute permissions to Mark.
D. Configure the NTFS permissions to assign the Allow - Read permission to Interns.

Answer: C

Explanation: We can prevent Mark from accessing the Blueprints folder by assigning the Deny - Read and Deny - Execute permissions to Mark. The Deny permissions will overwrite any other permissions that give Mark access to the folder. To accommodate Mark's needs, since he forms part of both Interns and Engineers, you should configure the NTFS permissions to assign the Allow-Read permission to Interns which would be the appropriate setting so as not to affect other users while allowing Mark to remain and operate in Engineers. Also keep in mind that when a Deny permission is applied, it takes precedence over any permission.
Incorrect answers:
A: Mark has dual membership and is thus also a member of the Everyone group. So he has change share permissions already. This will not prevent Mark from accessing the Blueprints folder.
B: Assigning the Deny - Read permission to the Engineers group will prevent the Engineers group accessing the folder. The Engineers group require access to the folder so this answer is incorrect.
D: Assigning the Allow - Read permission to the Interns group will not affect Marks access to the folder because of his membership to the two groups.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter &
Will Schmied, Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 423-425

QUESTION 162
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 2003 Server, and all client computers run Windows XP Professional.
A file server named CK1 has two hard drives. You format D:\ and use the default file permissions. Then you copy a directory named Data from another file server to D:\ on CK1 .
Now you need to create a network share and configure NTFS permissions settings for D:\Data. You must fulfil the following requirements:
• All domain users need read access to D:\Data.
• Members of the Sales group need the ability to add and delete files in a directory named

D:\Data\Sales.
• Members of the Engineering group need the ability to read and modify files in a directory named D:\Data\Enginering.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

A. Assign the Allow - Modify NTFS permission on D:\Data\Sales to the Sales group.
B. Assign the Allow - Write NTFS permission on D:\Data\Engineering to the Engineering group.
C. Share D:\Data as Data and use the default share permissions.
D. Share D:\Data as Data and assign the Allow - Change share permission to the Everyone group.
E. Assign the Allow - Full Control NTFS permission on D:\Data to the Administrators group.
F. Change the share permission on D:\Data to assign the Allow - Modify permission to the Everyone group.
G. Assign the Allow - Read NTFS permission on D:\Data to the Users group.
H. Assign the Allow - Write NTFS permission on D:\Data\Sales and D:\Data\Engineering to the Creator Owner group.

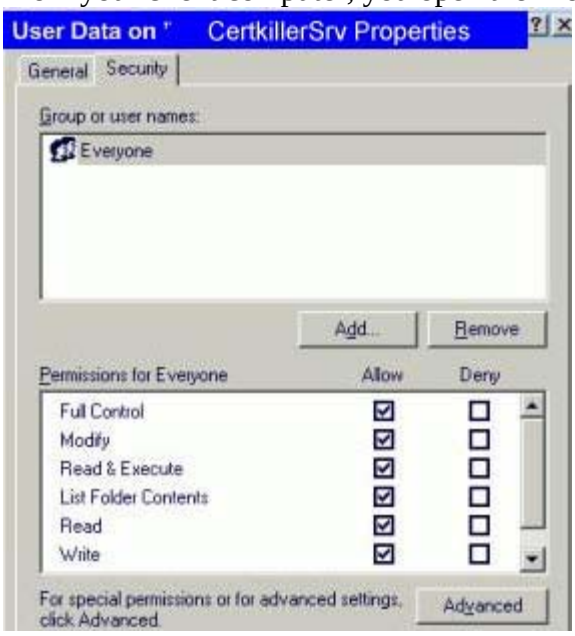
Answer: A, B, D

Explanation: By default, the Everyone group has only Read and Execute permissions on the root of each drive. These permissions are not inherited by subfolders; the Everyone group has no permissions by default to a newly created folder or file.
Similarly, when you create a shared drive or folder, the Everyone group now has only Read permission by default, rather than full control. This is quite a change from earlier versions of Windows, where every new folder gave everyone full control via both NTFS and share permissions.
One big difference between Everyone and Users is that you can add and delete members of the Users group. By default, any new user you create will belong to the Users group but this can be changed. The Everyone group is a built-in group with set membership (that is, you cannot add and delete members as you can with most other security groups).
Incorrect answers:
C: Share permissions, be it default permissions or not can only be set at folder level.
E: Although the Everyone group has no NTFS permissions to a newly created folder or file, the Users group does have the following permissions: Read & Execute, Read, and List Folder Contents.
F: As mentioned in the previous option, Share permissions can only be set at folder level.
G: The engineering group must not only be able to read, they also need to modify. Thus this option will not allow then to fulfil their tasks. This option will only allow the users group to have read access and nothing more.
H: The Modify permission gives the object the same permissions as the Read, Write, List Folder Contents, and Read & Execute permissions, but also enables the object to delete files and folders within the designated folder. Assigning the Allow - Write permission will not be sufficient.
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. 414-417

QUESTION 163
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 file server named Certkiller FileSrv is configured as a stand-alone Distributed File System (DFS) root. The disk configuration of Certkiller FileSrv is shown in the following table.

Disk	Volume	Contents
Disk0	MAIN	System files
Disk1	DATA	Database files
Disk1	USERS	Files and data for users

USERS hosts a shared folder named User Data.
You use Group Policy to deploy the Previous Versions client software to all client computers.
However, users report that they cannot access any previous version of any of the files in User Data.
From your client computer, you open the Properties dialog box of User Data, as shown in the exhibit.'



You need to enable all users to access previous versions of the file in User Data. To achieve this goal, you will modify Certkiller FileSrv.
What should you do?

A. Start the Distributed Link Tracking Client service.
B. Create a DFS link to User Data.
C. Enable shadow copies of USERS.
D. Disable quota management on USERS.

Answer: C

Explanation: Enabling users to access previous versions of their files is a two step process. The clients need the 'previous versions' client software installed and the volume hosting the shared folder must have

Shadow Copies enabled.
Incorrect Answers:
A: The Distributed Link Tracking Client service is not related to shadow copies.
B: Creating a DFS link to User Data is not necessary to enable shadow copies. DFS allows you to create a single logical tree view for multiple servers, so that all directories appear to be on the same server.
D: Quota management is not enabled by default. The question doesn't state that quota management is enabled. Either way, quota management is not related to shadow copies.
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. 29, 140

QUESTION 164
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. You manage a Windows Server 2003 computer named Certkiller 3. This server hosts all file and print services for the network on NTFS volumes.
Tess King is a technical support specialist for Certkiller . She belongs only to default groups in Active Directory. She needs the ability to change permissions for files stored in a folder named Data on Certkiller 3.
You share Data and configure the folder permissions shown in the following table.

Users	NTFS permissions	Share permissions
Certkiller	Read	Full Control
Group 1	Modify	Change
Group 2	Read/Write	Change
Group 3	Full Control	Deny – Read

Tess logs on to Certkiller 3, but she cannot change permissions for any files in Data.
How should you solve this problem?

A. Remove the Allow - Read NTFS permissions from Jack's user account.
Add Jack's user account to Group 1.
B. Add Jack's user account to Group 3.
C. Assign the Allow - Full Control share permissions to Group 2.
Add Jack's user account to Group 2.
D. Assign the Allow -Modify NTFS permission to Jack's user account.

Answer: B

Explanation: Group 3 has the Full Control NTFS permission and this is thus the only permission listed that will enable Jack the change the file permissions. However, this answer will prevent Jack from reading the files over the network due to the Deny - Read Share permission. Since her task is to change permissions for files this is the appropriate answer.
Incorrect answers:
A: Adding Jack to Group1 will result in Jack being able to give the object the same permissions as the Read, Write, List Folder Contents, and Read & Execute permissions, but also enables the object to delete files and folders within the designated folder.

C: Assigning the allow full control share permissions to Group 2 will not resolve the problem
D: The more restrictive permission (of the cumulative total of each type of permission) is the one that takes precedence in determining access. Look first at the permissions defined on the share before you look at the NTFS permissions defined. If the user only has Read permissions on the share, he or she will only have read access to the contents. If the user has Full Control permissions on the share, then look to the NTFS permissions defined to determine the level of access the user has.
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. 414-415, 425-426

QUESTION 165
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com.
The company has a main office in Cairo and a branch office in Dubai. The Dubai branch office has three servers that are described in the following table.

	Server name	*Operating System*	*Server Role*
2.	Certkiller 1	Windows Server 2003	Domain Controller
3.	Certkiller 2	Windows Server 2003	File server
4.	Certkiller 3	Windows Server 2003	Print server

Every server that functions as a file server or as a print server contains a shared folder named Certkiller Logs that contain log files. Members of a global group named ITSecurity must not be able to change the log files on any file or print server that is located in Dubai.
You need to create the appropriate group or groups and grant the necessary permissions to the ITSecurity group to allow them to read the server logs on all file or print servers.
What should you do?

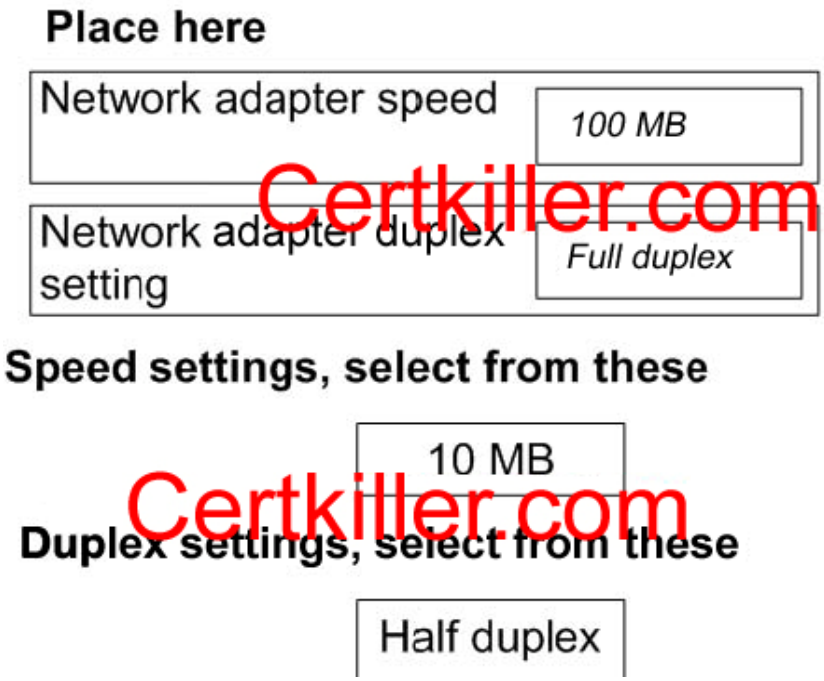
A. Create a domain local group named DubaiLogAccess and add the ITSecurity global group to it.
Assign the DubaiLogAcces group the Allow - Read permission for the Certkiller Logs shared folder on Certkiller 2.
Assign the DubaiLogAcces group the Allow - Read permission for the Certkiller Logs shared folder on Certkiller 3.
B. Create a domain local group named DubaiLogAccess and add the ITSecurity global group to it.
Assign the DubaiLogAcces group the Deny - Full Control permission for the Certkiller Logs shared folder on Certkiller 2.
Assign the DubaiLogAcces group the Deny - Full Control permission for the Certkiller Logs shared folder on Certkiller 3.
C. Create a local group named Certkiller 2LogAccess and add the ITSecurity global group to it.
Create a local group named Certkiller 3LogAccess and add the ITSecurity global group to it.
Assign the DubaiLogAcces group the Allow - Read permission for the Certkiller Logs shared folder on Certkiller 2.

Assign the DubaiLogAcces group the Allow - Read permission for the Certkiller Logs shared folder on Certkiller 3.
D. Create a local group named Certkiller 2LogAccess and add the ITSecurity global group to it.
Create a local group named Certkiller 3LogAccess and add the ITSecurity global group to it.
Assign the DubaiLogAcces group the Deny - Full Control permission for the Certkiller Logs shared folder on Certkiller 2.
Assign the DubaiLogAcces group the Deny - Full Control permission for the Certkiller Logs shared folder on Certkiller 3.

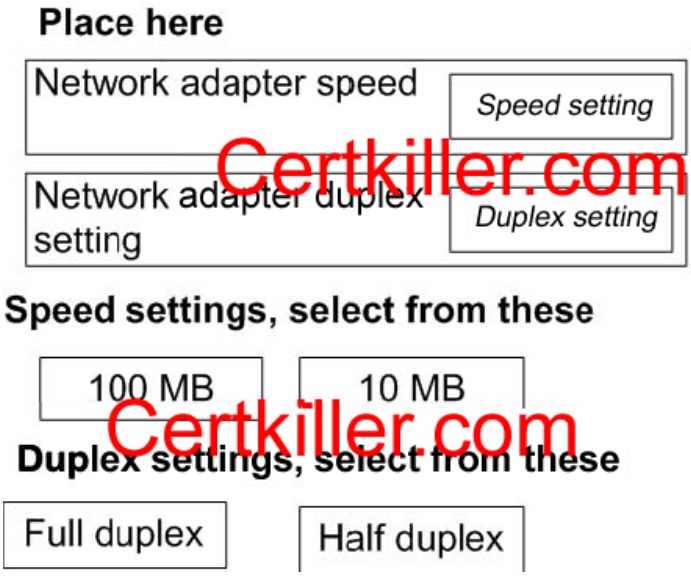
Answer: A

Explanation: Domain local groups are a type of group used to assign permissions to resources. Domain local groups can contain user accounts, universal groups, and global groups from any domain in the tree or forest. A domain local group can also contain other domain local groups from its own local domain.
The share-level permission only represents the maximum level of access you will get on the inside. If you get read permissions at the share, the best you can do once you've connected remotely to the share is read. Thus option A would be the solution to this problem.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering(tm)Windows(r)
Server 2003, Sybex Inc., Alameda, 2003, p. 920

QUESTION 166
You are the network administrator for Certkiller .com. You install a new Windows Server 2003 computer in an existing subnet for server computers. The switch that manages this subnet uses full duplex Fast Ethernet connections. The Windows Server 2003 computers functions as a file server.
Users have only intermittent network access to the file server.
You need to ensure that users maintain a consistent connection to the file server.
What should you do?
To answer, drag the appropriate setting or settings to the correct location in the work area.
Drag and Drop.



Answer:



Explanation: In the question it is mentioned that the swith that manages the subnet where the new server has been introduced, makes use of full duplex Fast Ethernet connections. For the users to get consistent connection to the file server, the network adapter speed and duplex setting has to match that at which the switch operates.

QUESTION 167

You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. Users in the human resources (HR) department print to a printer named Certkiller Pr1. Certkiller Pr1 is configured on a Windows Server 2003 computer named Certkiller A.

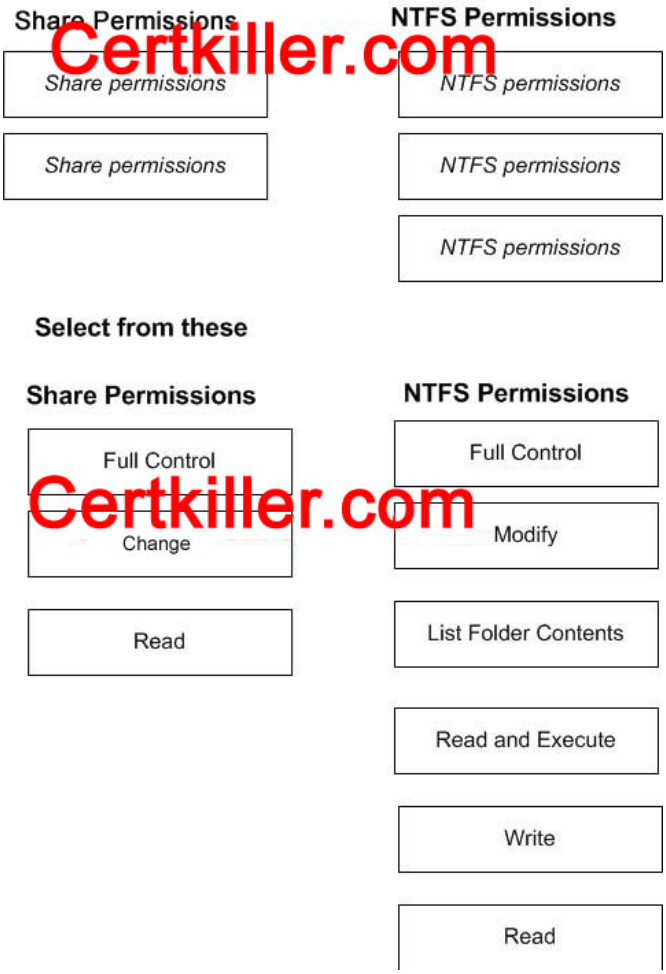
A user named Jack King is in the HR department. Jack is responsible for pausing documents that are submitted to Certkiller Pr1 when required. Jack reports that she cannot pause documents that are submitted by other users.
You need to ensure that Jack can pause documents when required, but cannot pause the entire printer.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Assign Jack the Allow - Manage Documents permission for Certkiller Pr1.
B. Remote the Allow - Manage Printers permission assigned to Tess.
C. Assign Jack the Allow - Modify permission for the C:\Windows\System32\Spool\Printers folder.
D. Assign Jack the Deny - Full Control permission for the C:\Windows\System32\Spool\Printers folder.

Answer: A, B

Explanation: The Manage Documents permission allows a user to control document-specific settings and pause, resume, restart, and delete spooled print jobs. And the Manage Printers permission allows a user to change printer properties and permissions. Thus options A and B will allow Jack to pause documents when required to do so without pausing the entire printer.
Incorrect answers:
C & D: These options will not result in the desired effect.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C. A. Callahan & Lisa Justice, Mastering(tm)Windows(r) Server 2003, Sybex Inc., Alameda, 2003, p. 1104

QUESTION 168
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003. All client computers run Windows XP Professional.
The user accounts for all managers are in global group named Managers. You create a new shared folder that managers will use to run an application. The application supports files are stored locally on the client computers. Only application's executable files are stored in the shared folder. You need to ensure that the managers have only the permissions that are required to run the application from the shared folder.
You add the Managers group to the ACL on the Sharing tab and the ACL on the Security tab for the folder.
You need to configure the appropriate permissions.
What should you do?
Drag the appropriate share permissions and NTFS permissions to the correct location or locations in the work area.



Answer:

QUESTION 169

You are a 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.

Another administrator shares a folder as Certkiller Data. He wants users to be able to create and modify documents in the folder. When users attempt to connect to open a document in the Certkiller Data folder, they receive an error message.

You need to configure the permission for the folder so that users can only create and modify documents.

What should you do?

To answer, configure the appropriate option or options in the dialog boxes in the work area.

Answer: Allow Modify

Explanation: The Modify permission simply put, Modify permissions are the combination of Read and Execute and Write, but give you the added luxury of Delete. Even when you could change a file, you never really could delete the file. You'll notice that, when you select permissions for files and folders, if you select Modify only, then Read, Read and Execute, and Write are automatically checked for you. In full, the Modify permission also includes the right to Write Attributes, Write Extended Attributes, and Delete files and folders.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering(tm)Windows(r)
Server 2003, Sybex Inc., Alameda, 2003, p. 940

QUESTION 170
You are the administrator of some of Certkiller 's file servers. Peter is hired as an intern in the human resources department. Peter needs access to some HR files. He also needs to be able to read the file named Handbook.doc, but he must not be able to make changes to it.
Handbook.doc exists in a folder named HRResources. Peter needs to have Read and Modify permissions for the other files in the HRResources folder.

Peter is a member of the Domain Users group and the HR group. The permissions on the HRResources folder are shown in the following table.

Group	Permission	Type of permission
Domain Users	Read	Share
HR	Change	Share
Domain Users	Read	NTFS
HR	Modify	NTFS

You need to ensure that Peter can access the appropriate files and that he cannot make changes to Handbook.doc. What should you do?

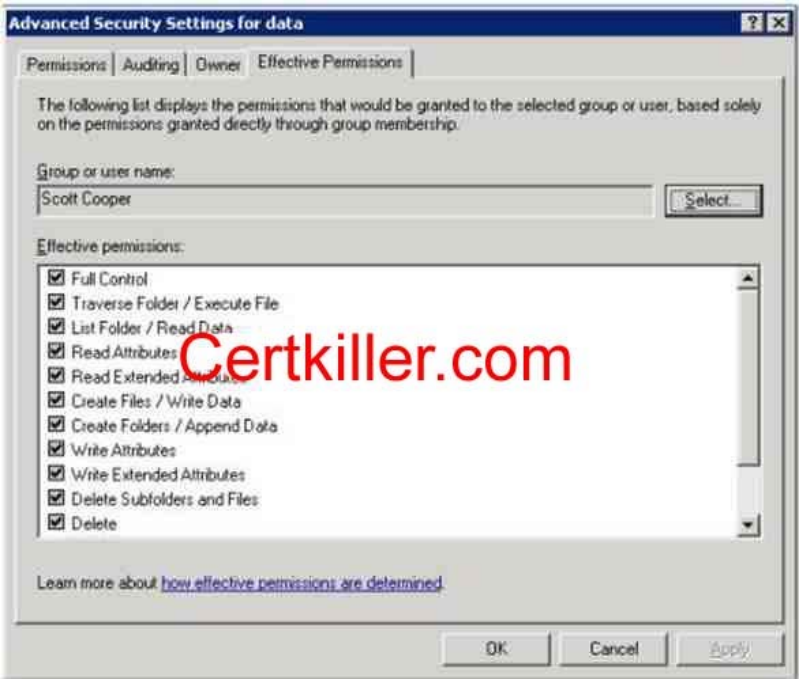
A. Set the hidden and system attributes on Handbook.Doc.
B. Disable permissions inheritance on Handbook.doc.
C. Assign Peter the Allow-Read permission for Handbook.doc.
D. Assign Peter the Deny-Write NTFS permission for Handbook.doc.

Answer: D

Explanation: Peter has Change/Modify permission on the Handbook.doc file by way of his membership of the HR group. We need to ensure that Peter cannot make changes to the Handbook.doc file. To make changes, Peter needs the 'write' permission. We can prevent Peter making changes to the file by denying him the write permission on the file.
Incorrect Answers:
A: This would hide the file. It wouldn't stop Peter editing the file if he opens it by entering the correct path to the file.
B: If you disabled the permission inheritance, you would have to manually configure the permissions to give Peter (and everyone else) the appropriate permissions. This would work, but it is unnecessary and impractical.
C: Peter already has Change/Modify permission on the file. Adding the Allow-Read permission wouldn't make any difference to his existing permissions.
Reference:
Server Help
http://www.seagate.com/support/kb/tape/4062.html
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. 822-823.
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 9
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, pp. 280-286

QUESTION 171
You are the network administrator for Certkiller .com. All network servers run Windows Server 2003.
A folder named Data resides on a network server. You share Data with default share permissions.
A user named Scott Cooper reports that he can access Data, but he cannot create new files in the

folder. You review Scott Cooper's effective permissions for Data, which are shown in the exhibit.



You need to ensure that Scoot Cooper can create files in Data.
What should you do?

A. On the Sharing tab of Data, assign the Allow - Full Control permission to the Interactive group.
B. On the Sharing tab of Data, assign the Allow - Change permission to Scott Cooper's user account.
C. On the Security tab of Data, assign the Allow - Full Control permission to the Authenticated users.
D. On the Security tab of Data, assign the Allow - Modify permission to the Network group.

Answer: B

Explanation: The default Share permissions are usually Allow-Read on the root of each drive. These permissions are not inherited by subfolders; the Everyone group has no permissions by default to a newly created folder or file.
Similarly, when you create a shared drive or folder, the Everyone group now has only Read permission by default, rather than full control. This is quite a change from earlier versions of Windows, where every new folder gave everyone full control via both NTFS and share permissions.
The effective permissions tabs show effective NTFS permissions, not shares.
Scott only has read permissions because READ is the default share permission. To enable Scott to write to the share, we need to change the share permissions. We can set the permissions to Allow-Change.
To enable Scott Cooper to use and create new files in this particular folder, he needs to be assigned the Allow-Change permissions. This should be done on the Sharing tab of Data.
Incorrect answers:
A: The Allow-Full Control will also allow Scott Cooper to create files in the Data folder, but this would give him more permissions than are required.
C: The Allow-Full Control on the Security tab is not the same as the Sharing tab of data and will thus not have the desired effect. Besides, as mentioned in option A, it will only lead to Scot Cooper having more permissions than is necessary

D: The assigning of the Allow- Modify permission on the security tab will not have the desired effect.
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. 414-428

QUESTION 172
You are the network administrator for Certkiller .com. Your network consists of two Active Directory domains in a single forest. All network servers run Windows Server 2003. Currently, you use more than 1,000 security groups.
A member server named CK1 contains a folder named Testing. This folder contains resources required by users in the engineering department.
A written security policy states that engineering users must have the approval of the management group before they can be assigned the Full Control NTFS permission on Testing.
You need to discover whether any engineering users currently have the Full Control NTFS permission on Testing. You must complete this task by using the minimum amount of administrative effort.
What should you do?

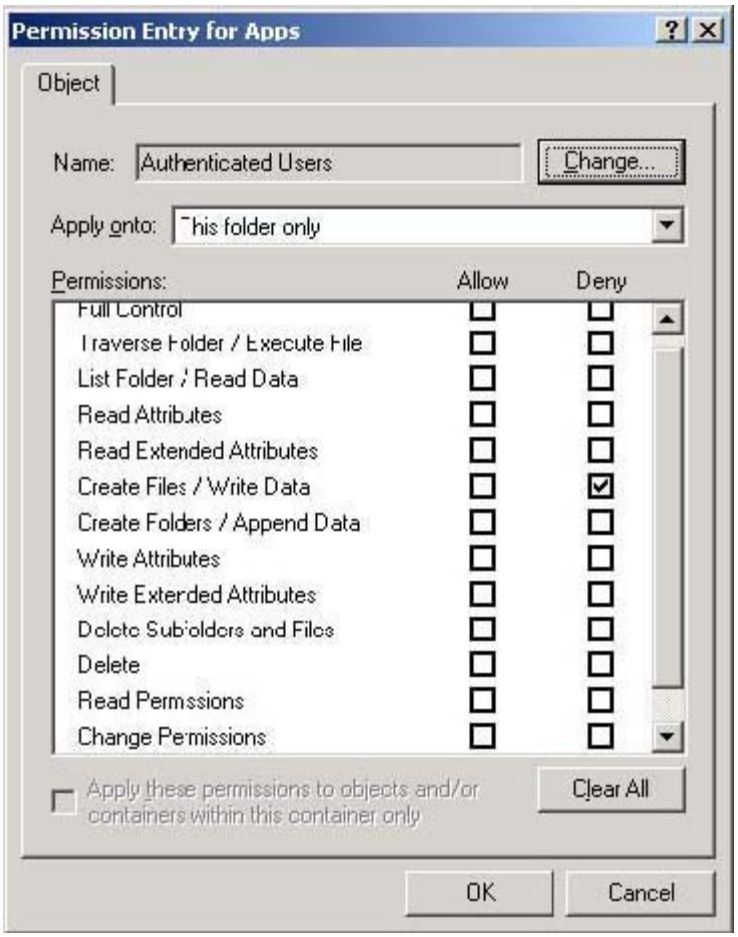
A. Use Active Directory Users and Computers to view the access level available to engineering users.
B. Use the Find Users, Contacts, and Groups utility to view the membership of each group that has access to Testing.
C. In the properties of Testing, view the Effective Permissions tab.
D. Write an ADSI script to search for members of all groups that have access to testing.

Answer: C

Explanation: Effective Permissions are the permissions that result from the evaluation of group and user permissions allowed, denied, inherited, and explicitly defined on a resource. The effective permissions determine the actual access for a security principal. Windows 2003 offers an easy way to view which permissions are effectively granted to any specified user or group for the current object. You can view this information in the Effective Permissions dialog box. Effective permissions reflect the work of combining permissions, both allowed and denied, from all matching entries, whether explicit or inherited. Matching entries name either the user or group directly, or a group in which the specified user or group is a member. The effective permissions tab of Testing is what you need to view to check whether any of the engineering users have Full Control NTFS permission. The properties of Testing will reveal the information that you need, i.e., which users currently have which permissions.
Incorrect answers:
A: The Active Directory Users and Computers console allows you to configure a Terminal Services User Profile, logon permissions, Remote Control permissions, session settings, and TS startup and redirection settings for domain users. Not to view who has which permissions.
B: Viewing memberships does not mean viewing permissions.
D: This option will result in unnecessary administrative effort, since you first have to write a script and then run it whereas all you need to do is to view the Effective Permissions in the properties of Testing.
References:
Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, p. 759

QUESTION 173
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 users log on to the domain to access resources.
All files and folders are stored on a member server named Server CK1 .
You need to configure permissions for a folder named Apps. You must ensure that authenticated users cannot create new files directly in Apps. This restriction must not affect any other permissions set on Apps, on the contents of its subfolders, or on its existing files. Users must still be able to modify files in Apps.
What should you do?
To answer, configure the appropriate option or options in the dialog box.

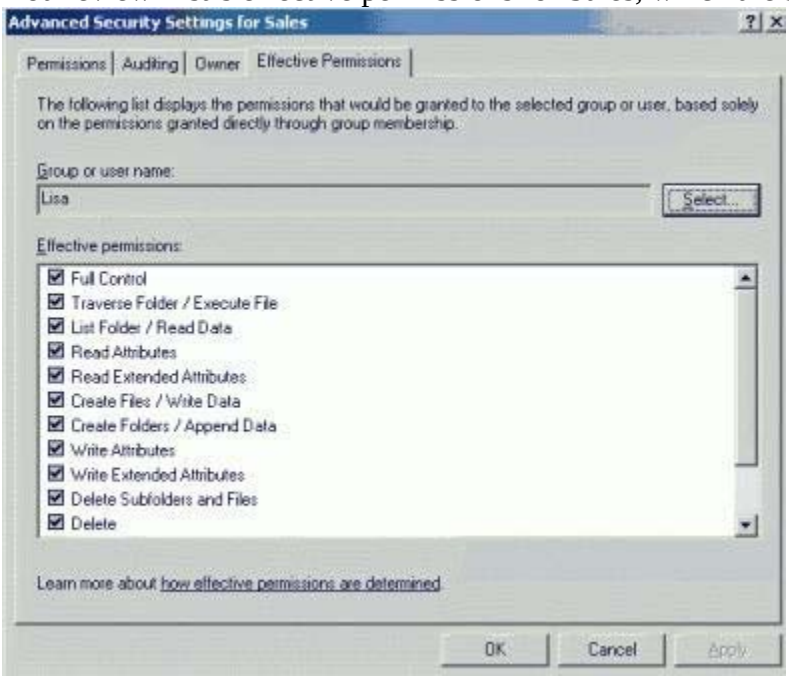
Answer:



Explanation: The Create Files/Write Data permission for folders, enables the object to create new files within the folder. While for files it enables the object to change or replace the contents of an existing file. The Create Folders/Append Data permission for folders create Folders allows or denies creating folders within the folder. In files it the Append Data allows or denies making changes to the end of the file but not changing, deleting, or overwriting existing data. Denying the right to create files and write data will not affect other permissions that were set on Apps, on the contents of its subfolders, or on its existing files. It will however deny authenticated users the right to create new files directly in Apps.
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. 420

QUESTION 174
You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
Disk drive D on a server named Certkiller A is formatted with default NTFS file permissions. You create a folder named D:\ Certkiller Data on Certkiller
A. You share D:\ Certkiller Data as Certkiller Data
with default share permissions. Then you create a subfolder named Sales in D:\ Certkiller Data.

A user named Lisa works in the sales department. Her user account is a member of 34 security groups. Lisa reports that she cannot add files to \\ Certkiller A\ Certkiller Data\Sales.
You review Lisa's effective permissions for Sales, which are shown in the exhibit:

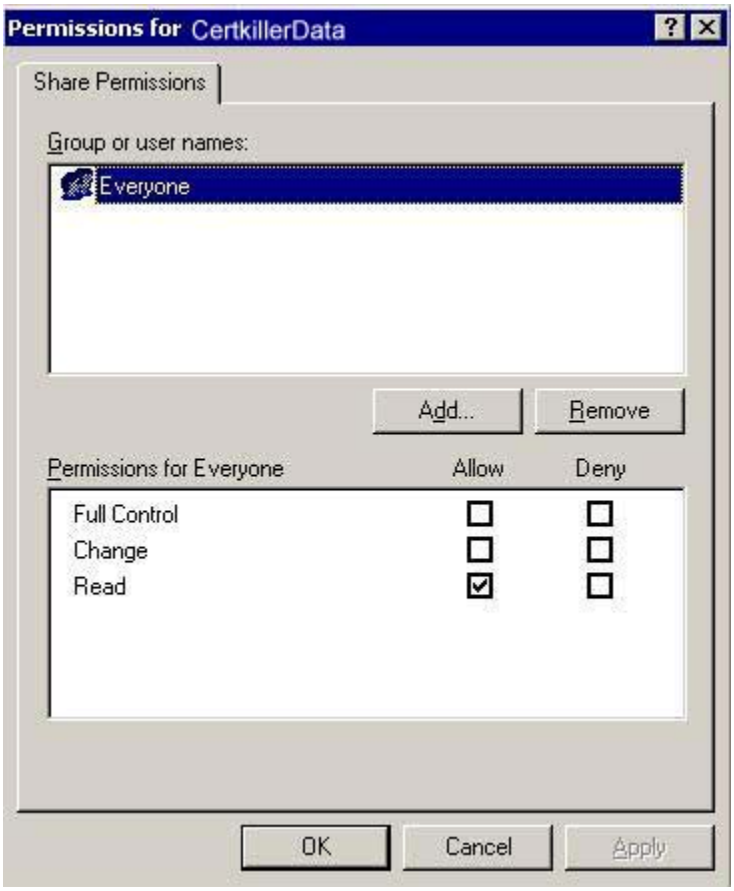


You need to ensure that Lisa can add files to \\ Certkiller A\ Certkiller Data\Sales.
What should you do?

A. Modify the NTFS permissions so Lisa inherits permissions on Sales from \\ Certkiller A\ Certkiller Data.
B. Remove Lisa from the Users group.
C. Assign the Allow - Modify NTFS permissions to the Creator Owner group.
D. Modify the share permissions for \\ Certkiller A\ Certkiller Data to assign the Allow - Change permissions to the Everyone group.

Answer: D

Explanation: The exhibit shows that Lisa has enough permissions to be able to write to the directory. The problem must therefore be with the share permissions. The default share permission is Everyone - Allow Read. This needs to be changed to Everyone - Allow Change.



Incorrect Answers:
A: The exhibit shows that Lisa has enough permissions to be able to write to the directory. The problem must therefore be with the share permissions. When permissions are applied to a folder, those permissions apply to the files within the folder as well.
B: The exhibit shows that Lisa has enough permissions to be able to write to the directory. The problem must therefore be with the share permissions. Removing Lisa from the Users group will be to her detriment.
C: The exhibit shows that Lisa has enough permissions to be able to write to the directory. The problem must therefore be with the share permissions. To assign the Allow-Modify permission to the Creator Owner group will not solve Lisa's problem.
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. 415-416

QUESTION 175
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
All users in the sales department are members of a group names Sales. Tess, a member of Sales, creates a custom document named Salescustom.doc. She is responsible for making all required changes to this file. Jack places the file in a shared folder named TessDocs on a member server named Certkiller
A. Then she goes on vacation.

When users from the sales department try to open Salescustom.doc, they receive the following error message:
'Access is denied'.
You log on to the console of Certkiller A and try to open Salescustom.doc. You receive the same error message.
You need to ensure that members of Sales have read-only access to Salescustom.doc. You must not affect Jack's permissions on Salescustom.doc or on any other files in TessDocs. You must not grant access to Salescustom.doc to any other users.
First, you log on to Certkiller A as an administrator.
What should you do next?

A. Take ownership of TessDocs and select the Replace owner on subcontainers and objects check box.
Configure the NTFS permissions to assign the Allow - Modify permissions on the folder to Sales.
B. Take ownership of Salescustom.doc.
Configure the NTFS permissions to assign the Allow - Create Files/Write Data permissions on the file to Sales.
C. Take ownership of Salescustom.doc.
Configure the NTFS permissions to assign the Allow - Read permissions on the file to Sales.
D. Take ownership of TessDocs and select the Replace owner on subcontainers and Object check box.
Configure the NTFS permissions to assign the Allow - Read permissions on the folder to Sales.

Answer: C

Explanation: Ownership can be transferred in the following ways:
• The current owner can grant the Take ownership permission to another user, allowing that user to take ownership at any time.
• The user must actually take ownership to complete the transfer.
• An administrator can take ownership.
• A user who has the Restore files and directories privilege can double-click
• Other users and groups and choose any user or group to assign ownership to.
• We must change the permissions on the Salescustom.doc file only.
Every object has an owner, whether in an NTFS volume or Active Directory. And it is the owner that controls how permissions are set on that specific object as well as to whom permissions are granted. We must change the permissions on the Salescustom.doc file only.
Incorrect Answers:
A: Granting the Sales group Allow - Modify permissions to the TessDocs folder will allow members of that group to make changes to all files in the TessDocs folder, including the Salescustom.doc file.This will give Sales modify access to every file in the TessDocs folder.
B: We must only assign Read access. However, if we grant the Sales group Allow - Create Files/Write Data permissions to the Salescustom.doc file, we would allow members of that group to make changes to the file.
D: Grant permissions at the file level and not the folder level as permissions granted at the folder level will apply to all files and subfolders contained in the folder. This will give Sales read access to every file in the TessDocs folder.

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 6-13 to 6-24
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 419-23.

QUESTION 176
You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. All client computers run Windows XP Professional.
You create a folder on the network and share it as Certkiller Docs. You want users to be able to read, create, and modify documents that are stored in the shared folder. You also want users to be able to delete the folders and the files that they create.
A user reports that another used deleted a folder that she created. You discover that the Everyone group is assigned the Allow - Full Control NTFS permission for the folder. You remove all assigned permissions for the Everyone group.
You need to configure permission for the Certkiller Docs shared folder to meet your requirements. You also need to ensure that users cannot delete the folders and files that other users create.
Which two actions should you perform (Each correct answer presents part of the solution. Choose two.)

A. Assign the Authenticated Users group the Allow - Read & Execute permission.
B. Assign the Anonymous group the Allow - Modify permission.
C. Assign the Creator Owner group the Allow - Modify permission.
D. Assign the Creator Owner group the Allow - Full Control permission.

Answer: A, C

Explanation: Read and Execute permissions are identical to Read, but give you the added atomic privilege of traversing a folder. Modify permissions are the combination of Read and Execute and Write, but give you the added luxury of Delete. Even when you could change a file, you never really could delete the file. You'll notice that, when you select permissions for files and folders, if you select Modify only, then Read, Read and Execute, and Write are automatically checked for you. These permissions applied as suggested by options A and C will have the desired effect.
Incorrect answers:
B: You cannot assign the Allow - modify permission to the Anonymous group as this will result in users being able to delete folders and files that others created.
D: Full Control is a combination of all a number of permissions, with the abilities to change permissions and take ownership of objects thrown in. Full Control also allows you to delete subfolders and files, even when the subfolders and files don't specifically allow you to delete them. This is not the appropriate permission for this group.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering(tm)Windows(r)
Server 2003, Sybex Inc., Alameda, 2003, p. 930

QUESTION 177
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.
Resources for the Certkiller Sales department are located on a network named Certkiller Files.
Members of a group named Sales are allowed to run applications from the network share.
You need to configure permissions on Certkiller Files for member of a group named Sales Managers.
Members of Sales Managers must be able to run the same applications that are run by members of Sales. However, member of Sales Managers must be assigned only the minimum level of required permissions.
Which permissions should you assign to Sales Managers?
To answer, configure the appropriate options in the dialog box.

Answer: Allow - Read

Explanation: Read permissions are your most basic rights. They allow you to view the contents, permissions, and attributes associated with an object. If that object is a file, you can view the file, which happens to include the ability to launch the file, should it be an executable program file. If the object in question is a folder, Read permissions let you view the contents of the folder.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering(tm)Windows(r)
Server 2003, Sybex Inc., Alameda, 2003, p. 929

QUESTION 178
You are the network administrator for Certkiller .com. The network contains a Windows Server 2003 computer named Certkiller 1. Certkiller 1 functions as a file server.
Six users in the accounting department use an accounting software application to open files that are stored in a shared folder on Certkiller 1. The users keep these files open for an extended period of time.
You need to restart Certkiller 1. You need to find out if any files on Certkiller 1 are open before you restart the computer.
What should you do?

A. Use Computer Management to view existing connections.
B. Use the netsend command to send a message to all domain members.
C. Use Task Manager to monitor processes started by all users.
D. Use System Monitor to monitor the Server object in Report view.

Answer: A

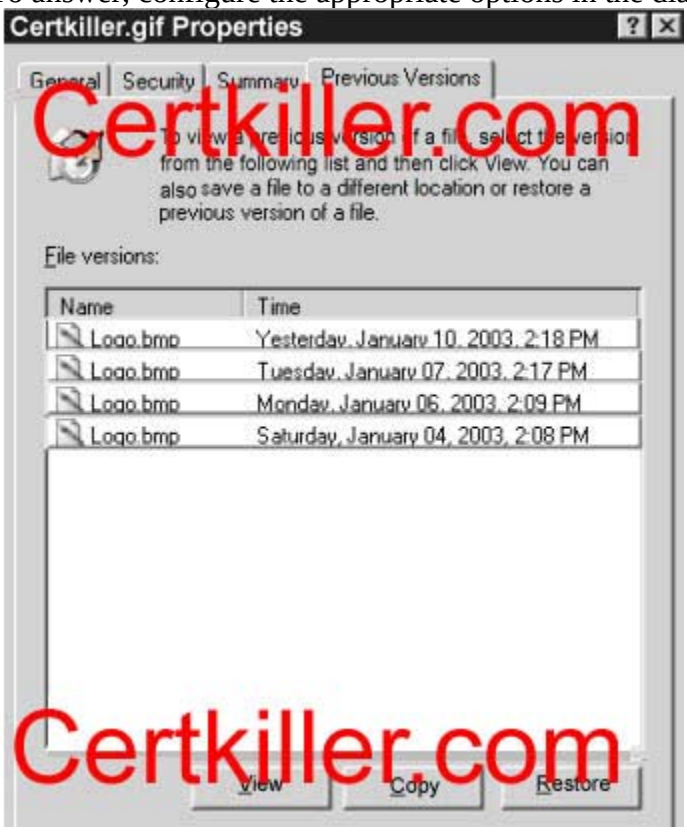
Explanation: Advanced user, group, and computer management, which is used to locate objects within the Active Directory, move objects within the Active Directory, create and manage users, groups, and computers through automation, and how to import user accounts from a Windows NT 4.0 domain or a Windows 2000 domain. If you want to find out if any files on Certkiller 1 are open before attempting to restart the computer you should make use of Computer Management to view the existing connections as Computer Management will also yield this information to you.
Incorrect answers:
B: Making use of the Netsend command to message all domain members is not her way to check existing connections to see if any files on Certkiller 1 are open.
C: 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 wil not shows if files are open. For that you need to make use of Computer Management.
D: System Monitor is a Windows Server 2003 utility used to monitor real-time system activity or view data from a log file.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering(tm)Windows(r)
Server 2003, Sybex Inc., Alameda, 2003, p. 53
Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 476

QUESTION 179
You are the network administrator for Certkiller .com. All network servers run Windows Server 2003. All file servers contain shared volumes that use shadow copies. All client computers run the Previous Versions client software.
A user named Marie creates a file named Certkiller .gif. Other users edit the file. The editing history of Logo.bmp is shown in the following table.

1. ***User***	1. ***Changes to Certkiller .gif***	1. ***Date***

2.	Marie	2.	Creates Certkiller .gif. The foreground color is green. The background color is yellow.	2.	January 4, 2003
3.	Ellen	3.	Changes the background color to blue.	3.	January 6, 2003
4.	Andy	4.	Change the foreground color to magenta.	4.	January 7, 2003
5.	Sandra	5.	Changes the foreground color to green. During the save, Certkiller .gif is corrupted and cannot be reopened.	5.	January 10, 2003

Certkiller .gif is corrupted and cannot be reopened.
5. January 10, 2003
You need to ensure that the foreground color of Certkiller .gif is green and the background color is blue. You also need to ensure that other users cannot access the corrupted version of Certkiller .gif. Your solution must require the minimum amount of user effort.
What should you do?
To answer, configure the appropriate options in the dialog box.



Answer:

QUESTION 180
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.
One manager's client computer has a single partition formatted as NTFS. The manager creates a file named Certkiller Data.doc on his client computer. He wants to share this file with other users in the company. He assigns the Domain Users security group the Allow - Read permission for the file. He then moves the Certkiller Data.doc file from the folder in which he created it to a shared folder named Certkiller Files on his computer. The permissions for the Certkiller Files folder are shown in the following table.

	Group		***Permission***
2.	Managers	2.	Modify
3.	Users	3.	Read

When another manager attempts to edit the document over the network, he receives an error message.
You need to ensure that managers have the appropriate permissions for the file when they access the file over the network.
What should you do?

A. Select the Replace permission entries on all child objects with entries shown here that apply to child objects option for the Certkiller Files folder.
B. Select the Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here option for the Certkiller Files folder.
C. Import the Rootsec.inf security template by using Secedit.exe.
D. Import the Hisecws.inf security template by using Secedit.exe.

Answer: A

Explanation: The options that can be configured for permission inheritance are:
1. Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.
2. Replace permission entries on all child objects with entries shown here that apply to child objects.
If an Allow or a Deny checkbox in the Permission list in the Security tab has a shaded check mark, this indicates that the permission was inherited from an upper-level folder. If the check mark is not shaded, it indicates that the permission was applied at the selected folder. This is known as an explicitly assigned permission. It is useful to see inherited permissions so that you can more easily troubleshoot permissions.
To minimize administration and simplify troubleshooting of folder permissions, you should assign permissions at higher-level folders within the directory structure and use inheritable permissions to

propagate the permissions to all child objects within the directory structure.
Incorrect answers:
B: Selecting this option for the Certkiller Files folder will not ensure that managers have the appropriate permissions.
C: The rootsec.inf security template is used to restore permissions on the root file system. This is not appropriate in this case.
D: The Highly Secure Workstation (hisecws.inf) template applies super-secure settings to workstations or non-DC servers. You'll want to read the documentation on this template carefully before applying it to your systems; it makes several changes to client-server authentication and encryption requirements. It also removes all members of the Power Users group and removes all members from the local Administrators group except Domain Admins and the local Administrator account. This is not the solution.
Reference:
Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 284

QUESTION 181
You are the network administrator for Certkiller .com. You administer a Windows Server 2003 computer named Certkiller 3. A user needs to share documents that are stored in a folder on Certkiller 3 with other users in his department. When she attempts to share the folder, she discovers that the Sharing tab is missing.
You need to ensure that the user can share the documents on Certkiller 3. You need to ensure that you grant the user the minimum amount of permissions required.
What should you do?

A. Instruct the user to move the documents to the Shared Folders folder.
B. Add the user's user account to the local Power Users group.
C. Add the user's user account to the Network Configuration Operators group.
D. Add the user's user account to the local Administrators group.

Answer: B

Explanation: Before you can create a shared folder, you must have appropriate rights to do so. This requires that you are either an Administrator or a Power User. Thus you should add the user's user account to the local Power Users group.
Incorrect answers:
A: Moving the folder will not enable sharing. It is a matter of adding the user to the appropriate group.
C: This is the wrong group to be adding the user to for the purposes of this case.
D: This option will result in granting the user more than the minimum appropriate rights.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering(tm)Windows(r)
Server 2003, Sybex Inc., Alameda, 2003, p. 913

QUESTION 182
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 includes a member server named Certkiller 4.
You need to create a shared folder on Certkiller 4 to store project documents. You must fulfill the following requirements:
• Users must be able to access previous versions of the documents in the shared folder.
• Copies of the documents must be retained every hour during business hours.
• A history of the last 10 versions of each document must be maintained.
• Documents that are not contained in the shared folder must not be retained.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Create the shared folder in the root of the system disk on Certkiller 4.
B. Create a new volume on Certkiller 4. Create the shared folder on the new volume.
C. Enable the Offline Files option to make the shared folder available offline.
D. Enable the Offline Files option to make the shared automatically folder available offline.
E. Use Disk Management to configure shadow copies of the volume that contains the shared folder.

Answer: B, E

Explanation: Shadow copies are used to create copies of shared folders and files at specified points in time. Shadow copies are copies of files taken at different points in time that can be restored in the event that a file is accidentally deleted or overwritten, or if you want to compare a current version of a file with a previous version of the same file. You can configure the Client for Shadow Copies on Windows XP and Window Server 2003 computers. In order to use shadow copies, the client must install the Shadow Copies of Shared Folders software. Windows Server 2003 computers have this software installed in the \\windir\system32\clients\twclient folder. You can distribute this software through group policy, or you can create a share to let the clients download and install the client software. Thus to comply with the requirement as stated in the question options B and E is the way to go.
Incorrect answers:
A: Creating a shared folder in the root of the system disk is not the solution to this problem.
C& D: These two options will not comply with the requirements.
Reference:
Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows(r)Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 272

QUESTION 183
Exhibit, Error message

Exhibit, Effective Permissions

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003. All client computers run Windows XP Professional.
An administrator named Sandra creates a shared folder named Certkiller sData on a server named Certkiller 5. The shared folder is a central location for users to store and share data. The shared folder is accessed only from the network.
When a user named Jack King attempts to copy a file named Certkiller Proj.doc to a shared folder, she receives the error message shown in the exhibit.
You view the effective permissions of the Users group group for the Certkiller Data folder, as shown in the Effective Permissions exhibit.
You need to ensure that users can modify documents in the Certkiller Data shared folder.
What should you do?

A. Assign the Anonymous group the Allow - Full Control NTFS permissions for the Certkiller Data folder.
B. Assign the Anonymous group the Allow - Change share permissions for the Certkiller Data shared folder.
C. Instruct Jack King to log off and then log on to her computer.
D. Enable File and Print Sharing on Jack King's computer.

Answer: B

Explanation: The Change share permission allows users to change data in a file or to delete files.
Incorrect answers:
A: The Allow - Change share permission will be sufficient. There is no need to assign this group the Allow - Full Control NTFS permission.
C: Logging on and off will not ensure that Jack King will habe permissions to modify documents in the Certkiller Data shared folder.
D: This is not a matter of enabling File and Print Sharing on Jack 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. 293

QUESTION 184
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003. All client computers run Windows XP Professional.
All users in the publishing department are members of a global group named Publishing. Interns in the publishing department are also member of a global group named of PublishingInterns.
A network file server contains a shared folder PubSalesData. Interns must not be able to view or modify any files in the PubsSalesData folder. All other employees in the publishing department must be able to view and modify the files in the PubsSalesData folder.
The NTFS permissions for all folders are configured the Allow - Full Control permissions to members of the Domain Users global group.
You need to configure the share permissions for the PubSalesData folder.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Assign the Allow - Read permission to the Publishing global group.
B. Assign the Allow - Change permission to the Publishing global group.
C. Assign the Deny - Change permission to the PublishingInterns global group.
D. Assign the Allow - Read permission to the PublishingInterns global group

Answer: B, C

Explanation: You can assign three types of share permissions: (1) The Full Control share permission allows full access to the shared folder. When the Full Control permission is assigned, the Change and Read permissions are checked as well. (2) The Change share permission allows users to change data in a file or to delete files. And (3) The Read share permission allows a user to view and execute files in the shared folder. Thus options B and C will represent the appropriate share permissions for the PubSalesData folder for the groups as indicated in these options.
Incorrect answers:
A & D: The Allow - Read permission will be inappropriate in both these cases..
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. 293

QUESTION 185
You are the network administrator for Certkiller . The network consists of an internal network and a perimeter network. The internal network is protected by a firewall. The perimeter network is exposed to the Internet.
You are deploying 10 Windows Server 2003 computers as Web servers. The servers will be located in the perimeter network. The servers will host only publicly available Web pages.
You want to reduce the possibility that users can gain unauthorized access to the servers. You are concerned that a user will probe the Web servers and find ports or services to attack.
What should you do?

A. Disable File and Printer Sharing on the servers.

B. Disable the IIS Admin service on the servers.
C. Enable Server Message Block (SMB) signing on the servers.
D. Assign the Secure Server (Require Security) IPSec policy to the servers.

Answer: A

Explanation: We can secure the web servers by disabling File and Printer sharing.
File and Printer Sharing for Microsoft Networks
The File and Printer Sharing for Microsoft Networks component allows other computers on a network to access resources on your computer by using a Microsoft network.
This component is installed and enabled by default for all VPN connections. However, this component needs to be enabled for PPPoE and dial-up connections. It is enabled per connection and is necessary to share local folders. The File and Printer Sharing for Microsoft Networks component is the equivalent of the Server service in Windows NT 4.0.
File and Printer sharing is not required on web servers because the web pages are accesses over web protocols such as http or https, and not over a Microsoft LAN.
Incorrect Answers:
B: This is needed to administer the web servers. Whilst it could be disabled, disabling File and Printer sharing will secure the servers more.
C: SMB signing is used to verify, that the data has not been changed during the transit through the network. It will not help in reducing the possibility that users can gain unauthorized access to the servers.
D: This will prevent computers on the internet accessing the web pages.

QUESTION 186
You are the administrator of the Certkiller .com company network. The network consists of a single active directory domain. The network includes 10 servers running Windows Server 2003 and 200 client computers running Windows XP Professional.
You install and configure a server named Certkiller Srv as a print server. The name of the print queue is \\ Certkiller Srv\laserprinter. You assign the Everyone group the Allow - Print permissions.
A user named Lisa in the Finance department reports that she is unable to print to \\ Certkiller Srv\laserprinter. Several other users report that they are unable to print to \\ Certkiller Srv\laserprinter. You log on to Lisa's computer and submit several print jobs, but none of them print and no error message is displayed.
In Printers and Faxes on Lisa's computer, you open \\ Certkiller Srv\laserprinter. You see the following status of the print queue: "laserprinter on Certkiller Srv is unable to connect". You are able to ping Certkiller Srv.
You need to ensure that print jobs submitted to \\ Certkiller Srv\laserprinter will be printed.
What should you do?

A. On a domain controller, create a shared printer object in Active Directory for \\ Certkiller Srv \laserprinter.
B. From a command prompt on Lisa's computer, run the Net Print \\ Certkiller Srv \lasterprinter command.
C. On Lisa's computer, open the Services console and restart the Print Spooler service.
D. On Lisa's computer, open the Services console and connect to Certkiller Srv.
Restart the Print Spooler service.

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 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: The printer is already shared. It does not have to be published in Active Directory.
B: This command is used to connect to a shared printer. This has already been done.
C: Other users are experiencing printing problems. The problem is therefore likely to be with the print server, not just Lisa's computer.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, p. 82

QUESTION 187
You are the administrator of a Windows 2003 print server named Server
A. ServerA is a member of a
Windows 2003 Domain. You install a high-speed laser print device on the network. You create and share a printer on ServerA named FastLsr with the default settings.
You want all of the users in Certkiller to be able to use to FastLsr. You want the users in the Payroll domain local group to have exclusive use of the print device between the hours of 10:00 A.M and 3:00 P.M and shared use of the print device during all other times.
What should you do?

A. Configure and share FastLsr to be available from 3:00 P.M to 10:00 A.M. For the print device, create a second printer that has default availability. For the second printer, assign the Everyone group the Deny-Print permission and assign the Payroll group the Allow-Print permission. Instruct users in the Payroll group to use the second printer.
B. Configure and share FastLsr to be available from 3:00 P.M to 10:00 A.M. For the print device, create a second printer that has default availability. For the second printer, remove permissions for the Everyone group and assign the Payroll group the Allow-Print permission. Instruct users in the Payroll group to use the second printer.
C. Create and share a second printer device and configure it to be available from 10:00 A.M to 3:00 P.M. For the second printer, assign the Everyone group the Deny-Print permission and assign the Payroll group the Allow-Print permission. Instruct users in the Payroll group to use the second printer.
D. Create and share a second printer for the print device and configure it to be available from 10:00 A.M to 3:00 P.M. For the second printer, remove permissions for the Everyone group and assign the Payroll group the Allow-Print permission. Instruct users in the Payroll group to use the second printer.

Answer: B

Explanation: We have a shared printer named FastLsr. The default permission for a shared printer is to allow everyone to print at any time. We need to change the availability of FastLsr so that it is available for anyone to print from 3:00 P.M to 10:00 A.M. This means that no one can print to it between 10:00 A.M and 3:00 P.M.
Only the Payroll group should be able to print between 10:00 A.M and 3:00 P.M. Therefore, we need to create a second shared printer and change the availability to be between 10:00 A.M and 3:00 P.M. Then we need to configure the permissions so that only the Payroll group can use the second shared printer.
Incorrect Answers:
A: We can't assign the Everyone group the Deny-Print permission, because no one (including the Payroll group) would be able to use the printer.
C: We can't assign the Everyone group the Deny-Print permission, because no one (including the Payroll group) would be able to use the printer.
D: This answer is close, but incomplete. The first shared printer (FastLsr) allows anyone to print at any time. We need to re-configure the availability of FastLsr.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 366-367

QUESTION 188
You are the network administrator for Certkiller .com. All network servers run Windows 2003 Server, and all client computers run Windows XP Professional.
A shared folder named Sales resides on an NTFS volume on one of your servers. Sales contains two subfolders named Certkiller 1 and Certkiller 2. Files and folders in these two subfolders were created by various users with varying NTFS permissions.
You need to move some of the files and folders from Certkiller 1 to Certkiller 2. You must retain the existing file permissions, and you must accomplish your goal by using the minimum amount of administrative effort.
Which action or actions should you perform? (Choose all that apply)

A. Move the files and folders from Certkiller 1 to Certkiller 2.
B. Copy the files and folders from Certkiller 1 to Certkiller 2.
C. Change the NTFS permissions on Certkiller 2 to match the NTFS permissions on Certkiller 1.
D. Back up the files and folders in Certkiller 1 and restore them, including permissions, to Certkiller 2.

Answer: A

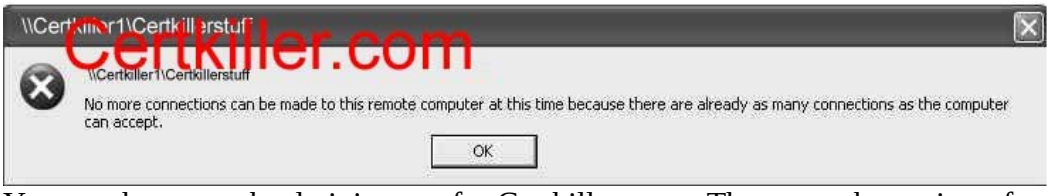
Explanation: A number of factors impact the security settings that will be placed on the file in its new location, including the following:
• Whether the file is copied or moved
• Whether the destination is an NTFS volume or not
• Whether the destination is on the same volume as the original location
Files and folders that are moved or copied to non-NTFS volumes lose all permissions. If the destination is on an NTFS volume, the security permissions the file will have after the transfer will depend on several

factors.
When copying files or folders to a location on an NTFS volume, the user must have permission to create files in the destination location. When the file or folder is copied, it is created as a new object in the destination, and the user object that copied the file or folder becomes the owner of the newly created item.

Destination	Permissions
Objects moved within the same NTFS volume	Objects retain their original NTFS permissions in the new location
Objects moved to a different NTFS volume	Objects inherit the permissions of the new location

The question states pertinently to move the files and folders from Srv1 to Srv2 which resides in the same NTFS volume. Not copy. Moving the files will ensure that the permissions as assigned to the various creators of these files and folders will not be modified. Copying it would result in modification. Since both Certkiller 1 and Certkiller 2 reside within the same volume, it will retain its original NTFS permissions in the new location.
Incorrect answers:
B: When copying files and folders from one volume to another albeit both NTFS volumes you are bound to lose the permissions that are on those files and folders. Copying files and folders will result in modifications.
C: There is no need to change any permissions since both Certkiller 1 and Certkiller 2 reside within the same NTFS volume and the questions only asks for moving files and folders which can be done without changing the original permissions. Changing the permissions will result in more than the minimum amount of administrative effort.
D: Backing up and restoring the files and folders into the desired locations will also accomplish the task, but it will result in more administrative effort than is necessary.
References:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 5
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. 423-424

QUESTION 189
Exhibit



You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains a Windows Server 2003 computer named Certkiller 1 that functions as a file server.
Certkiller 1 contains a shared folder named Certkiller Staff for the Certkiller Staff and a shared folder named Engineering for the engineering department.
Users in the Certkiller Staff report that when they attempt to connect to the Certkiller Staff shared

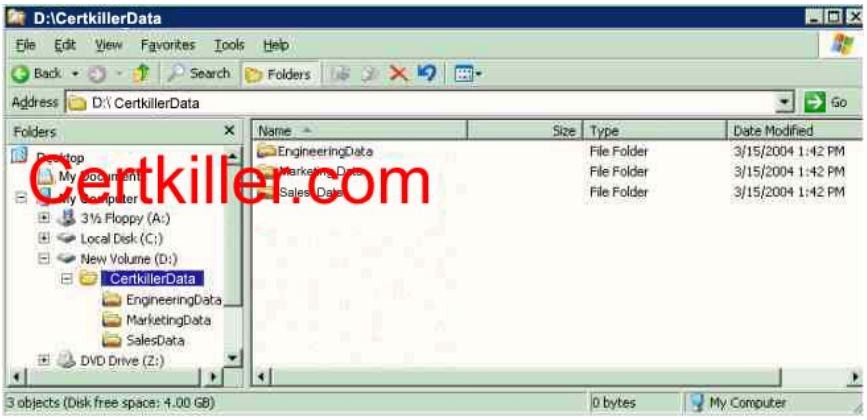
folder the connection occasionally fails. When the connection fails, users receive the error message in the exhibit.
Users in the engineering department do not receive the error message when they connect to the Engineering shared folder.
You need to ensure that users in the marketing department can consistently connect to the Certkiller Staff shared folder.
What should you do?

A. Increase the user limit value on the Certkiller Staff shared folder.
B. Purchase additional licenses and install them on the file server.
C. Change the server licensing mode from Per Server to Per Seat.
D. Replace the user limit value on the Engineering shared folder.

Answer: A

Explanation: To increase the user limit value on the Certkiller Staff shared folder should enable all the users to connect to the Certkiller Staff shared folder on a consistent basis.
Incorrect answers:
B: The problem is not licensing. Purchasing additional licenses would be unnecessary.
C: Per Device or Per User mode (formerly called "Per Seat" mode) requires that each device or user have its own Windows CAL. Changing server licensing from per server to per seat mode will have no effect on the situation.
D: The engineering department is not the department that is experiencing the problems of non-connectivity.
References:
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
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 5

QUESTION 190
Exhibit



You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. Certkiller F, a network file server, contains a folder named Certkiller Data. The file structure is shown in the exhibit.
All users are members of the Domain Users global group. Users in the sales department are members

of a global group named Sales. All users access shared folders only by using mapped drives.
Users in the engineering, marketing, and sales departments need to be able to view documents that are in any of the folders in Certkiller Data. Users in the sales department need to be able to modify only the documents in the SalesData folder.
The NTFS permissions for all folders are configured to assign the Allow- Full Control permission to the Domain Users global group.
You need to configure the appropriate share permissions. You need to achieve this goal by using the minimum amount of administrative effort.
Which two actions should you perform? (Each correct answer present part of the solution. Select two)

A. Assign the Sales global group the Allow - Read permission for both the EngineeringData share and the MarketingData share.
B. Share the Certkiller Data folder. Assign the Domain Users global group the Allow - Read permission for the Certkiller data share.
C. Share the Certkiller Data folder. Assign the Sales global group the Allow - Change permission for the Certkiller data share.
D. Assign the Sales global group the Allow - Change permission for the SalesData Share.

Answer: B, D

Explanation: One has to keep in mind that (1) Both NTFS and share permissions are cumulative. If a user belongs to more than one group, and two or more of these groups are assigned permissions on a file or folder, the user's effective permissions (NTFS or share) on the file or folder is the sum of all the groups' permissions. (2) When determining the effective permissions on a file or folder access through a share, the more restrictive permissions (that is, the cumulative effective NTFS permissions or the cumulative effective share permissions) are the ones applied. And (3) Assign user rights to groups whenever possible, assigning user rights to individual user accounts is difficult to manage. Thus in this scenario options B and D would be appropriate.
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. 475-476

QUESTION 191
All network servers run Windows Server 2003, and all client computers run Windows XP Professional.
Sandra, the manager of the human resources department, asks you to create a shared folder named HRDrop.
You create a HRDrop folder on a member server. You assign the Allow - Full Control share permission to the Everyone group.
Now you need to configure the NTFS permissions on HRDrop to fulfil the following requirements:
• Sandra must be able to read, modify, change permissions on, and delete all files and subfolders in HRDrop.
• All other domain users must only be able to add new files to HRDrop.
What should you do?

A. Assign the Allow - Modify permission to Sandra.

Assign the Allow - Read permission to the Users group.
B. Assign the Allow - Full Control permission to Sandra.
Assign the Allow - Write permission and the Deny - Read and Execute permission to the Users group.
C. Assign the Allow - Modify permission to Sandra.
Assign the Allow - List Folder permission to the Users group.
D. Assign the Allow - Full Control permission to Sandra.
Assign the Allow - Read permission to the Users group.
E. Assign the Allow - Full Control permission to Sandra.
Assign the Allow - Write permission to the Users group and remove the Read and Execute permissions to the Users group.

Answer: E

Explanation: Many access problems can arise from incorrectly configured Share and NTFS permissions, you can expect to see at least one exam question related to setting Share and NTFS permissions. Always remember that the more restrictive permission (of the cumulative total of each type of permission) is the one that takes precedence in determining access. Look first at the permissions defined on the share before you look at the NTFS permissions defined. If the user only has Read permissions on the share, he or she will only have read access to the contents. If the user has Full Control permissions on the share, then look to the NTFS permissions defined to determine the level of access the user has. A user's access to a file or folder is the most restrictive set of effective permissions between share permissions and NTFS permissions on that resource. If you want a group to have full control of a folder and have granted full control through NTFS permissions, but the share permission is the default (Everyone: Allow Read) or even if the share permission allows Change, that group's NTFS full control access will be limited by the share permission.
This dynamic means that share permissions add a layer of complexity to the management of resource access, and is one of several reasons that organizations cite for their directives to configure shares with open share permissions (Everyone: Allow Full Control), and to use only NTFS permissions to secure folders and files.
It is useful to remember:
• Permissions on shares are cumulative. If a user belongs to multiple groups, and two or more of those groups have permissions on a share, the user has all the permissions allowed by all the groups.
• Deny permissions override Allow permissions. If a user belongs to multiple groups, and one of those groups has Allow permissions on a share while another has Deny permissions, the user will be denied access to the share based on the Deny permission.
Incorrect answers:
A: The Allow- Read and Allow- Modify permissions will not be enough for Sandra and her job requirements.
B: The Deny - Read and Execute permission will take precedence over the other permissions. Thus this option will not suffice.
C: The Allow-Modify and Allow - List Folder permissions to Sandra and the Users group respectively will result not result in Sandra being granted the ability to fulfil her tasks.
D: The Read and Execute permission of the Users group should also be removed since this will prevent Sandra from carrying out her duties.
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. 6: 7

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. 426, 428

QUESTION 192
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.
Your network includes a shared folder named Certkiller Docs. This folder must not be visible in a browse list.
However, users report that they can see Certkiller Docs when they browse for shared folders.
How should you solve this problem?

A. Modify the share permissions to remove the All - Read permission on Certkiller Docs from the Users group.
B. Modify the NTFS permissions to remove the Allow - Read permissions on Certkiller Docs from the Users group.
C. Change the share name to Certkiller Docs#.
D. Change the share name to Certkiller Docs$.

Answer: D

Explanation: Appending a dollar sign ($) to a share name hides the share.
You can hide the shared resource from users by typing $ as the last character of the shared resource name (the $ then becomes part of the resource name).
Users can map a drive to this shared resource, but they cannot see the shared resource when they browse to it in Windows Explorer, or in My Computer on the remote computer, or when they use the net view command on the remote computer.
Incorrect Answers:
A: This will not hide the share.
B: This will not hide the share. Users will see the share, but get an "Access Denied" message.
C: The share will be visible with the name Certkiller Docs#.
Reference:
Server Help: To share a folder or drive
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. 478

QUESTION 193
Exhibit

Share permissions	**NTFS Permissions**
Certkiller HR: Change	Certkiller 4 Administrators: Full Control
	Certkiller HR: Full Control

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.
Users in the human resources department are members of a domain user group named Certkiller HR.

You create and share a folder named Certkiller HRFiles on a member server named Certkiller 4. You configure permissions on the Certkiller HRFiles as shown in the exhibit.
Marie, a user in the human resources department, create a file in Certkiller HRFiles. At Marie's request, you assign the Deny - Delete special permission on her file to the HR Group.
The next day, Veronika reports that her file is deleted.
You need to reconfigure the permissions on Certkiller HRFiles. You must fulfil the following requirements:
• Members of the Certkiller HR group must be able to read, create, and modify files.
• Members of the Certkiller HR group must not be able to delete files on which they have no access permission.
• Members of the Certkiller HR group must not be able to delete files that they do not have permission to delete.
What should you do?

A. In the share permissions, assign the Deny - Change permission to the Certkiller HR group.
B. In the NTFS permissions, assign the Allow - Read permission to the Certkiller HR group.
C. In the share permissions, assign the Allow - Read permission to the Certkiller HR group.
D. In the NTFS permissions, assign the Allow - Modify permission to the Certkiller HR group.

Answer: D

Explanation: One has to keep in mind that (1) Both NTFS and share permissions are cumulative. If a user belongs to more than one group, and two or more of these groups are assigned permissions on a file or folder, the user's effective permissions (NTFS or share) on the file or folder is the sum of all the groups' permissions. (2) When determining the effective permissions on a file or folder access through a share, the more restrictive permissions (that is, the cumulative effective NTFS permissions or the cumulative effective share permissions) are the ones applied. In this scenario the Allow - Modify NTFS permission would be the best option to fulfil the stated requirements.
Incorrect answers:
A: You need to assign NTFS, not share permissions in this scenario. Besides the Deny-Change permission would have been too restrictive to comply with the stated requirements.
B: Even if it is done in the NTFS permissions, the Allow - Read permission will not satisfy all the stated requirements.
C: You need to assign NTFS, not share permissions in this scenario. The Allow - Read permission also would not have complied with all of the stated requirements.
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. 475 - 47

QUESTION 194
You are the network administrator for Certkiller .com. Among other duties you administer a Windows 2003 server named Certkiller B.
You install Terminal Services on Certkiller B. You add users from the Certkiller support department to the Power Users group and to the Remote Desktop Users group on Certkiller B.
You notice that Certkiller B is periodically unavailable. You open Event Viewer on Certkiller B and

discover that the server was restarted accidentally by users in the Certkiller support department.
You need to ensure that users in the Certkiller support department can establish a Terminal Services session and can manage local user accounts on Certkiller B. However, they should not have the ability to restart Certkiller B.
Which action or actions should you perform? Select all that apply.

A. Remove the Certkiller Support department user accounts from the Power Users group.
B. Remove the Certkiller Support department user accounts from the Remote Desktop Users group.
C. Remove the Power Users group from the Shut down the system user right.
D. Add the Power Users group to the Deny log on locally user right.
E. Modify the permission on the RDP-Tcp connection by using Terminal Services Configuration. Assign the Power Users group the Deny - Full Control permission

Answer: C

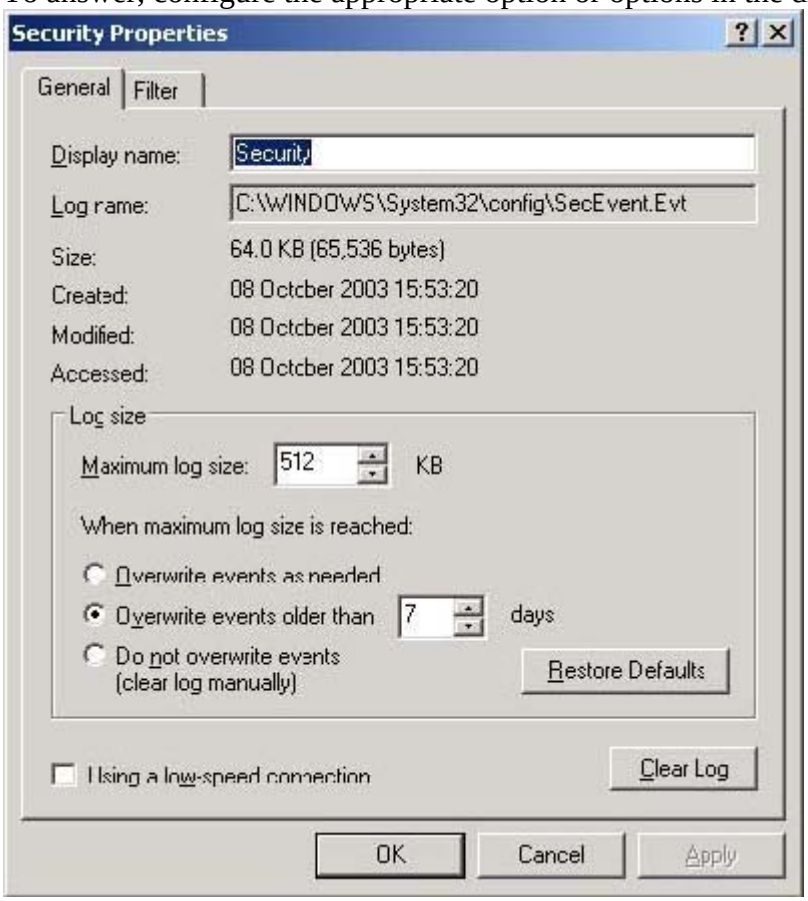
Explanation: If you want to ensure that Certkiller support department users have the ability to establish Terminal services and manage local user accounts on Certkiller B without being able to restart Certkiller B then you need to deny them the Shut down the system user right by removing them from the Power Users group.
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

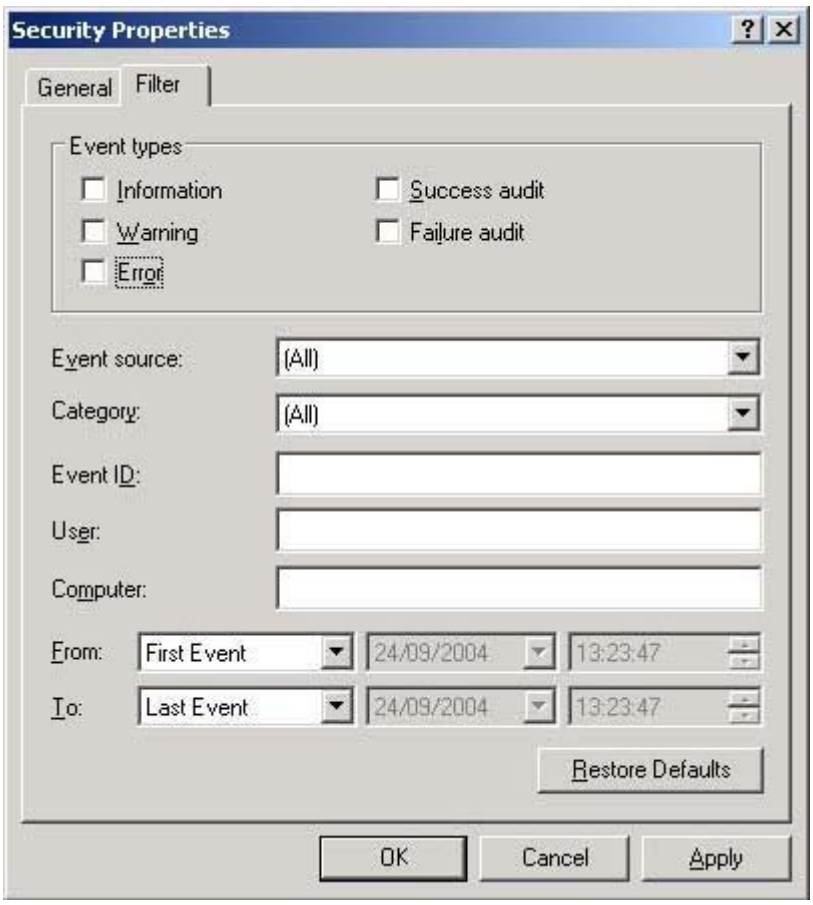
QUESTION 195
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003.
You open Event Viewer on a server named Certkiller 1. You see the view shown in the exhibit.

Type	Date	Time	Source	Category	Event	User	Computer
Failure Audit	1/17/2003	4:13:16 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:16 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:15 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:15 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:14 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:14 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:06 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:06 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:05 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:05 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:02 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:13:02 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:12:04 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:12:04 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:11:59 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:11:59 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:11:54 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:11:54 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:11:52 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:11:52 PM	Security	Account Logon	672	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:11:48 PM	Security	Account Logon	675	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:11:43 PM	Security	Account Logon	675	SYSTEM	Certkiller1
Failure Audit	1/17/2003	4:02:21 PM	Security	Account Logon	675	SYSTEM	Certkiller1

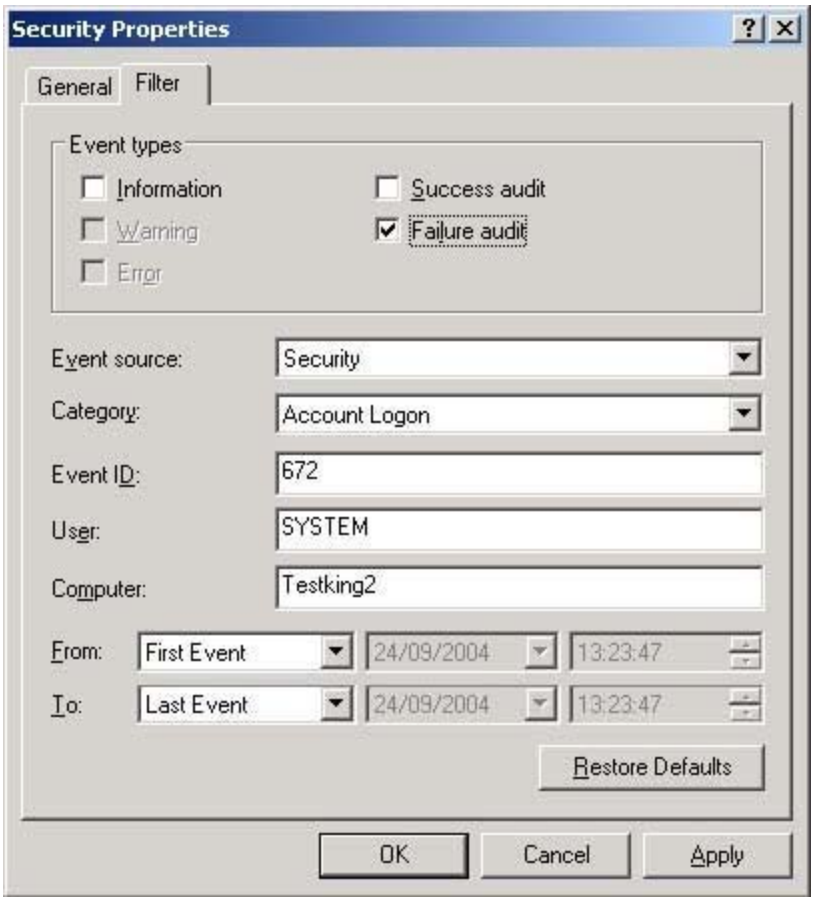
You need to configure a server named Certkiller 2 to fulfill the following requirements:
• Configure the security log to display only the events that are shown in the exhibit.
• Ensure that security information can be deleted only by user intervention.
What should you do?

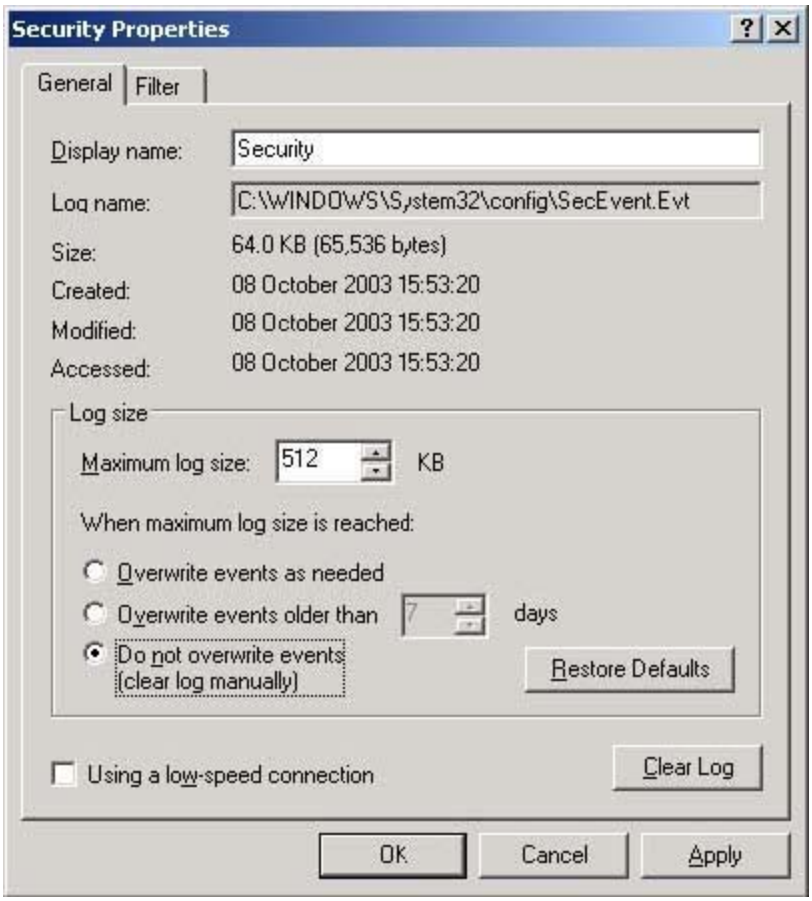
To answer, configure the appropriate option or options in the dialog boxes.




Security Properties
General
Filter
Event types
Information
Warning
Error
Success audit
Failure audit
Event source:
(All)
Category:
(All)
Event ID:
User:
Computer:
From:
First Event
24/09/2004
13:23:47
To:
Last Event
24/09/2004
13:23:47
Restore Defaults
OK
Cancel
Apply

Answers:


Security Properties
General
Filter
Event types
Information
Warning
Error
Success audit
Failure audit
Event source:
Security
Category:
Account Logon
Event ID:
672
User:
SYSTEM
Computer:
Testking2
From:
First Event
24/09/2004
13:23:47
To:
Last Event
24/09/2004
13:23:47
Restore Defaults
OK
Cancel
Apply



Explanation:
Server2 configuration should have a security property filter for failure auditing following the output from the event viewer. To ensure that the security information is not deleted automatically you should configure the security properties to the setting that states DO not overwrite events (clear log manually) to ensure that security information is deleted only through user intervention.
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. 767

QUESTION 196
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All domain controllers run Windows Server 2003, and all client computers run Windows XP Professional.
The audit policy for the domain ensures that all accounts logon events are audited.
Two client computers, CK1 and CK2 , are configured as kiosks in the lobby of the main office. Some users log on to the domain by using these two computers.
You need to use Event Viewer to review successful logon attempts on these two computers only. You do not want to view any other auditing details.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Configure a filter for the security log to list all successful account logon attempts.
B. Configure a filter for the security log to list all failed account attempts.
C. Create one new log view.
Configure a filter to show all account logon and account logoff events.
D. Create two new log views.
Configure a filter on one log view to show successful account logon events only.
Configure a filter on the other log view to show failed account logon events only.
E. Create two new log views.
Configure a filter on one log view to show account logon events for CK1 only.
Configure a filter on the other log to show account logon events for CK2 only.

Answer: A, E

Explanation: 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 users 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:
B: You need to log all successful account logon attempts and not the failed account attempts.
C: You will have to create two new log views and not only one.
D: You need to configure the views to show the account logon events for CK1 , and to show the account logon events for CK2 , respectively.
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. 620-623

QUESTION 197
You are the network administrator for Certkiller .com. The company contains of a main office and five branch offices. Network servers are installed in each office. All servers run 2003
The technical support stuff is located in the main office. Users in the branch office do not have the "Log on locally" right on local servers.

Servers in the branch office collect auditing information.
You need the ability to review the ability to review the auditing information located on each branch office server while you are working at the main office. You also need to save the auditing information on each branch office server on the local hard drive.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. From the Security Configuration and Analysis snap-in save the appropriate .inf file on the local hard drive.
B. Solicit Remote Assistance from each branch office server.
C. From Computer Management open Event Viewer, save the appropriate .evt file on the local hard drive
D. Run secedit.exe, specify the appropriate parameter
E. Establish a Remote Desktop client session with each branch office server

Answer: C, E.

Explanation: We can connect to the branch office servers using a Remote Desktop connection. We can then use Event Viewer to save the log files to the local hard disk.
Incorrect Answers:
A: Auditing information is not stored in .inf files. .inf files have to do with setup information.
B: We do not require remote assistance; we can use a Remote Desktop client session.
D: Secedit.exe is not used to save auditing information.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 198
You are the network administrator for the Berlin office of Certkiller . The company network consists of a single Active Directory domain named Certkiller .com.
The Berlin office contains 15 file servers that contain confidential files. All the file servers run either Windows Server 2003 or Windows 2000 Server. All the file servers are in the BerlinFilePrint organizational unit (OU).
Certkiller 's security department sets a rule that specifies the size and retention settings for the Security event log of all file servers. The rule also specified that local administrators on servers cannot override the changes you make to the settings for the Security event log.
You need to define a method to modify the Security event log settings on each file server in the Berlin office in order to meet the states requirements.
What should you do?

A. Modify the local security policy on each file server.
Define the size and retention settings for the Security event log.
B. Create a security template on one of the file servers by using the Security Configuration and Analysis tool.
Define the size and retention settings for the Security event log in the template.
Import the security template into the local security policy of the other 14 file servers.

C. Use Event Viewer to modify the event log properties on each file server.
Define the size and retention settings for the Security event log.
D. Create a new Group Policy object (GPO) and link it to the BerlinFilePrint OU.
In the GPO, define the size and retention settings for the Security event log.

Answer: D

Explanation: The servers are in OU BerlinFilePrint. Setting will apply to Windows 2000 Servers and Windows 2003 Servers. Consider implementing these Event Log settings at the site, domain, or organizational unit level, to take advantage of Group Policy settings.
Event Log - This security area defines attributes related to the Application, Security, and System event logs: maximum log size, access rights for each log, and retention settings and methods.
Event Log size and log wrapping should be defined to match the business and security requirements you determined when designing your Enterprise Security Plan.
Incorrect answers:
A: Modifying the local security policy on each file server will not suffice in this scenario.
B: Creating a security template on one of the servers and then importing it to the other servers will not work as you need to define the size and retention settings for the Security event log in a GPO.
C: Making use of Event Viewer to modify the event log properties on each file server will not work. Furthermore you need to define the size and retention settings for the Security event log in the GPO.
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. 761

QUESTION 199
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All five domain controllers run Windows Server 2003, and all client computers run Windows XP Professional.
The domain's audit policy ensures that all account logon events are audited.
A temporary employee named King uses a client computer named Certkiller 1. When King's temporary assignment concludes, his employment is terminated.
Now you need to learn the times and dates when King logged on to the domain. You need to accomplish this goal by reviewing the minimum amount of information.
What should you do?

A. Log on to Certkiller 1 as a local Administrator.
Use Event Viewer to view the local security log.
Use the Find option to list only the events for King's user account.
B. Log on to Certkiller 1 as a local Administrator.
Use Event Viewer to view the local security log.
Use the Find option to list only the events for the Certkiller 1 computer account.
C. Use Event Viewer to view the security log on each domain controller.
Use the Find option to list only the events for King's user account.
D. Use Event Viewer to view the security log on each domain controller.
Set a filter to list only the events for King's user account.
E. Use Event Viewer to view the security log on each domain controller.

Set a filter to list only the events for the Certkiller 1 computer account.

Answer: D

Explanation: 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 users' 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.
Incorrect Answers:
A: The logon events will be recorded in the logs on the domain controllers, not the client computer.
B: The logon events will be recorded in the logs on the domain controllers, not the client computer.
C: The Find option will move to the next event in the log according to the Find criteria. It will not filter the log to just show the relevant information.
E: This will show when someone logged on to Certkiller 1 using a domain account. This is not what we're looking for.
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. 786-789

QUESTION 200
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com.
The Certkiller Staff department has a Windows 2003 computer that functions as a file server. The computer contains a folder named Certkiller Data. Auditing is enabled on the Certkiller Data folder.
The Certkiller Staff department reports that confidential files were deleted from the folder.
You need to identify the user who deleted the confidential files.
What should you do?

A. In Event Viewer, create a new log view from the security log. Filter the log view to display only success audits.
B. In Event Viewer, create a new log view from the security log. Filter the log view to display only failure audits.
C. In Event Viewer, create a new log view from the system log. Filter the log view to display only success audits.
D. In Event Viewer, create a new log view from the system log. Filter the log view to display only failure audits.

Answer: A

Explanation: 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. Security log provides vital information for tracking successful and failed breaches of security.

Security events are logged in the security log, accessible by administrators via the Event Viewer. An audit entry can be either a Success or a Failure event in the security log. Filtering the log view to display only success audits will display audited security events that are completed successfully are logged in this category. (For example, a successful user logon when security auditing is enabled.) To be able to identify the user who deleted confidential files means that this user obviously had a successful logon, thus this option will help you identify the culprit.
Incorrect answers:
B: Failure Audit All audited security events that fail are logged here. Thus this option will not reveal who the user was that deleted the confidential files.
C, D: The System log contains events related to Windows system components. This includes entries regarding failure of drivers and other system components during startup and shutdown. This will not display security breaches.
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. 749, 760-762.
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 6