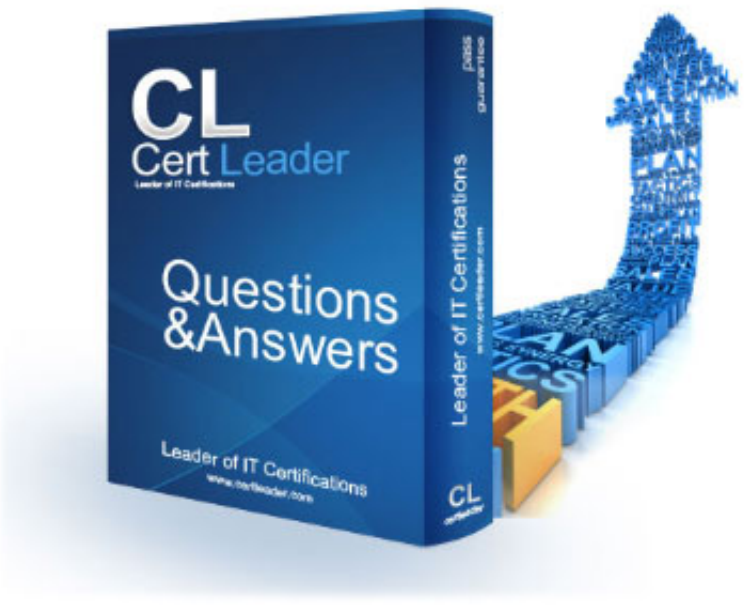
70-680 Dumps

TS:Windows 7,Configuring

https://www.certleader.com/70-680-dumps.html

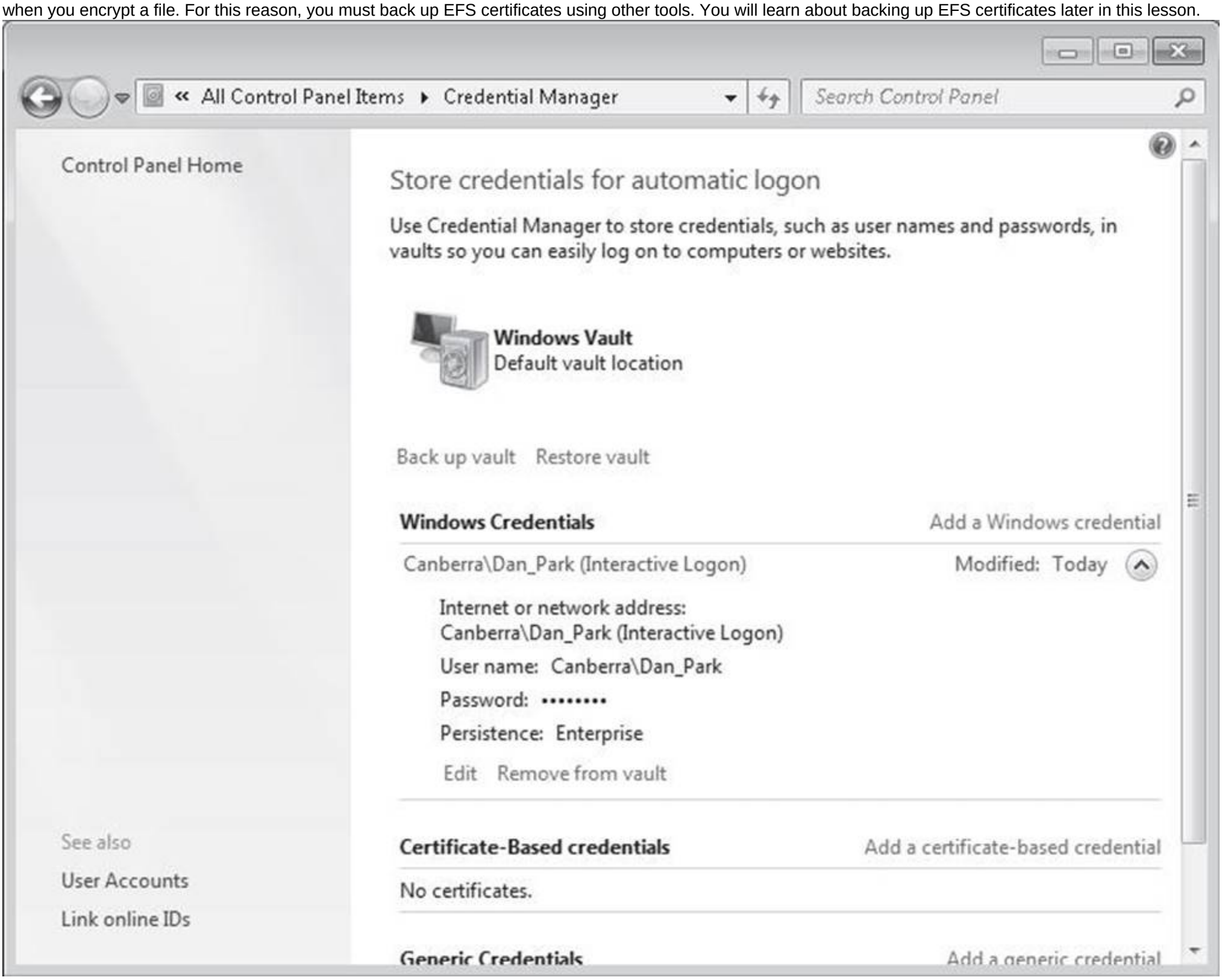


NEW QUESTION 1
You have a computer named Computer1 that runs Windows 7. The computer is a member of an Active Directory domain. The network contains a file server named Server1 that runs Windows Server 2008.
You log on to the computer by using an account named User1.
You need to ensure that when you connect to Server1, you authenticate by using an account named Admin1.
What should you do on Computer1?

A. From User Accounts, select Link online ID
B. From Windows CardSpace, select Add a car
C. From Credential Manager, select Add a Windows credentia
D. From Local Security Policy, modify the Access this computer from the network user righ

Answer: C

Explanation:
Credential Manager Credential Manager stores logon user name and passwords for network resources, including file servers, Web sites, and terminal services servers. Credential Manager stores user name and password data in the Windows Vault. You can back up the Windows Vault and restore it on other computers running Windows 7 as a method of transferring saved credentials from one computer to another. Although Credential Manager can be used to back up some forms of digital certificates, it cannot be used to back up and restore the self-signed Encrypting File System (EFS) certificates that Windows 7 generates automatically when you encrypt a file. For this reason, you must back up EFS certificates using other tools. You will learn about backing up EFS certificates later in this lesson.



NEW QUESTION 2
Your network consists of a single IPv4 subnet. The subnet contains 20 computers that run Windows 7.
You add a new computer named Computer1 to the subnet.
You discover that Computer1 has an IP address of 169.254.34.12.
You cannot connect to other computers on the network. Other computers on the network can connect to each other.
You need to ensure that you can connect to all computers on the network. What should you do?

A. Turn off Windows Firewal
B. Run Ipconfig.exe /rene
C. Configure a static TCP/IP addres
D. Run Netsh.exe interface ipv4 instal

Answer: C

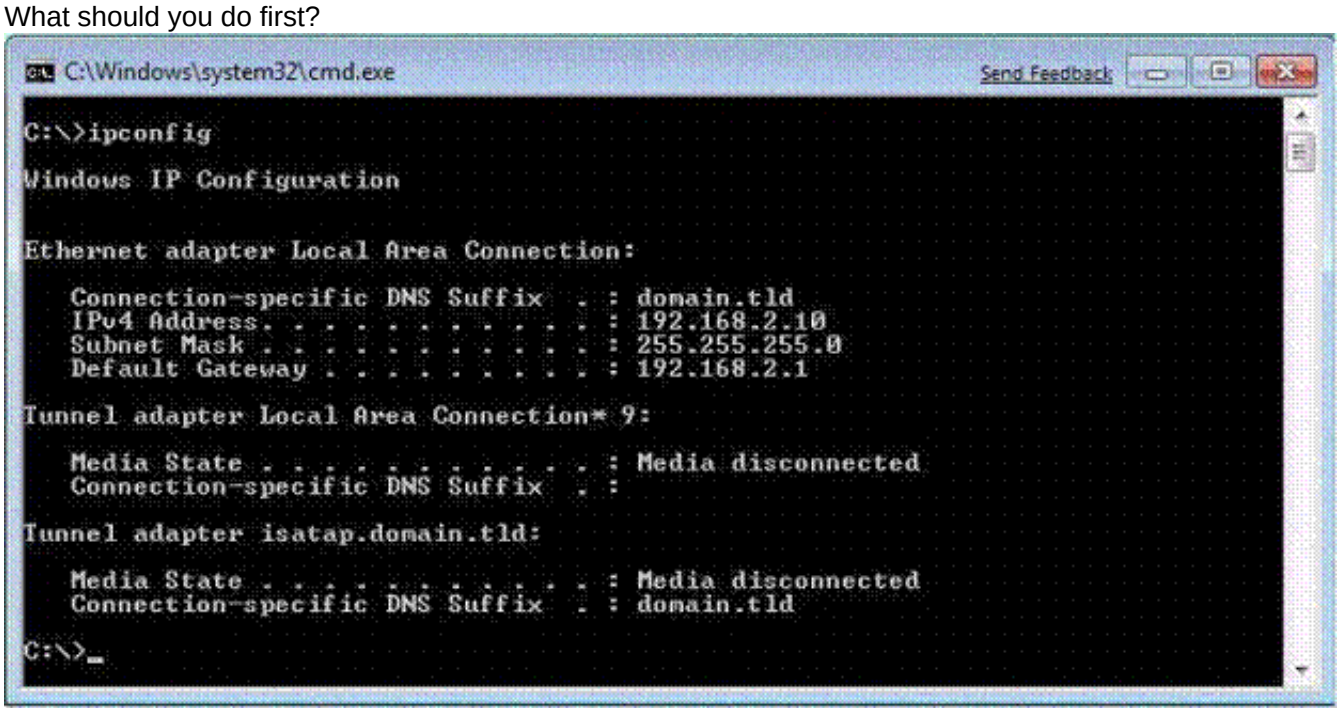
Explanation:
[Need better justification] Configuring static IP addresses When you assign a static IP address, you need to tell the computer the IP address you want to use, the subnet mask for this IP address, and, if necessary, the default gateway to use for internetwork communications. An IP address is a numeric identifier for a computer. Ip addressing schemes vary according to how your network is configured, but they're normally assigned based on a particular network segment.

NEW QUESTION 3
In Windows 7 you can control when users such as kids can login to Windows 7.
Which of the following best describes where to configure this option?

A. You cannot choose this feature unless you are connected to a domai
B. Go to the Start, Control Panel, User Accounts and Family Safety, Setup Parental Controls, and then choose Time Restriction
C. Go to Start, Control Pane
D. User Profiles, and then Time Restriction Setting
E. Go to the Homegroup settings and choose Offline Time Setting

Answer: B

NEW QUESTION 4
You have a computer that runs Windows 7.
You run Ipconfig as shown in the exhibit. (Click the Exhibit button.)
You need to ensure that you can establish a DirectAccess connection to the network.
What should you do first?



A. Create a new VPN connectio
B. Configure a static IPv4 addres
C. Enable IPv6 on the network adapte
D. Add an additional default gateway addres

Answer: C

NEW QUESTION 5
In which of the following scenarios must you perform a migration rather than an upgrade? Choose three.

A. Windows XP Professional (x64) to Windows 7 Professional (x64)
B. Windows Vista Business (x86) to Windows 7 Professional (x64)
C. Windows Vista Enterprise (x64) to Windows 7 Enterprise (x64)
D. Windows Vista Home Premium (x64) to Windows 7 Home Premium (x86)

Answer: ABD

NEW QUESTION 6
You manage a computer that runs Windows 7.
You are tasked to identify which applications were installed during the last week.
What Windows component would you use to find this information? Choose two.

A. Check the Windows System Change Log in the Control Pane
B. View the events in the Applications Log under Windows Logs in the System and Security component section of the Control Pane
C. The informational events should be reviewed from Reliability Monito
D. Check the Windows System Diagnostics Report under the Performance Monitor MM

Answer: BC

NEW QUESTION 7
You have a Virtual Hard Disk (VHD) and a computer that runs Windows 7. The VHD has Windows 7 installed.

You need to start the computer from the VHD.
What should you do?

A. From Diskpart.exe, run Select vdis
B. From Disk Management, modify the active partitio
C. Run Bootcfg.exe and specify the /default paramete
D. Run Bcdedit.exe and modify the Windows Boot Manager setting

Answer: D

Explanation:
When you have created a VHD and installed a system image on it, you can use the BCDEdit tool Bcdedit.exe to add a boot entry for the VHD file in your computer running Windows 7.

NEW QUESTION 8
You have a computer that runs Windows 7.
Multiple users log on to the computer.
You need to deny one user access to removable devices on the computer. All other users must have access to the removable drives.
What should you do?

A. From the local Group Policy, modify an application control polic
B. From Control Panel, modify the BitLocker Drive Encryption setting
C. From Device Manager, modify the settings of all removable device
D. From the local Group Policy, modify a removable storage access polic

Answer: D

NEW QUESTION 9
A user named User1 uses a shared computer that runs Windows 7. User1 is a member of group named Group1.
The computer contains a folder named Folder1.
You need to configure the permissions on Folder1 to meet the following requirements:
User1 must be allowed to delete all files in Folder1
Members of Group1 must be able to create files in Folder1
All other members of Group1 must be prevented from deleting files they did not create in Folder1
All users must be prevented from modifying the permissions on Folder1
What should you do?

A. Assign Group1 the Write permissio
B. Assign User1 the Modify permissio
C. Assign Group1 the Modify permissio
D. Assign User1 the Write permissio
E. Deny Group1 the Write permissio
F. Assign User1 the Modify permissio
G. Deny Group1 the Modify permissio
H. Assign User1 the Write permissio

Answer: A

Explanation:
File and Folder Permissions ReadFolders: Permits viewing and listing of files and subfoldersFiles: Permits viewing or accessing of the file's contentsWriteFolders: Permits adding of files and subfoldersFiles: Permits writing to a fileRead & ExecuteFolders: Permits viewing and listing of files and subfolders as well as executing of files; inherited by files and folders Files: Permits viewing and accessing of the file's contents as well as executing of the fileList Folder ContentsFolders: Permits viewing and listing of files and subfolders as well as executing of files; inherited by folders onlyFiles: N/AModifyFolders: Permits reading and writing of files and subfolders; allows deletion of the folderFiles: Permits reading and writing of the file; allows deletion of the fileFull ControlFolders: Permits reading, writing, changing, and deleting of files and subfoldersFiles: Permits reading, writing, changing and deleting of the file

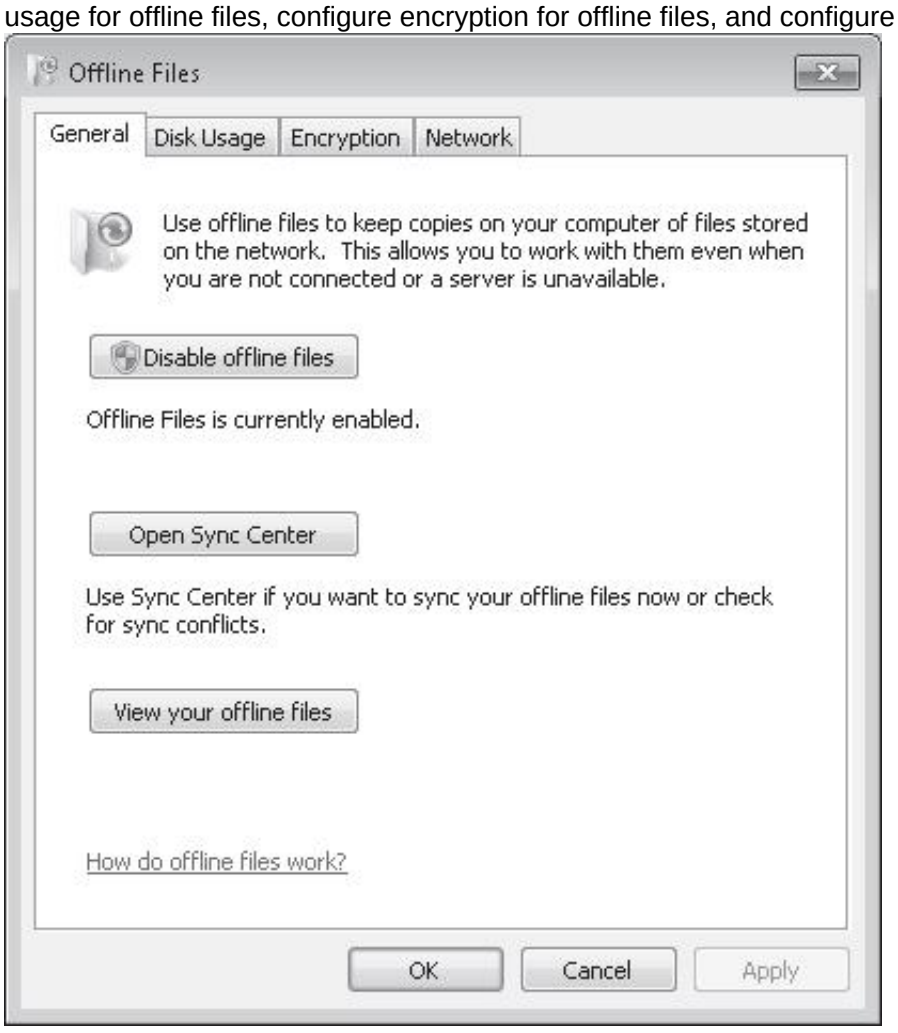
NEW QUESTION 10
You have a portable computer named Computer1 that runs Windows 7.
You have a file server named Server1 that runs Windows Server 2008. Server1 contains a shared folder named Share1.
You need to configure Computer1 to meet the following requirements:
. Ensure that cached files from Share1 are encrypted.
. Ensure that files located in Share1 are available when Server1 is disconnected from the network.
What should you do?

A. On Server1, encrypt the files in Share1. On Computer1, make Share1 available offlin
B. On Server1, configure BitLocker Drive Encryptio
C. On Computer1, make Share1 available offlin
D. On Computer1, make Share1 available offline and enable encryption of offline file
E. On Computer1, copy the files from Share1 to the Documents library and configure BitLocker Drive Encryptio

Answer: C

Explanation:
Offline FilesThe Offline Files feature of Windows 7 allows a client to locally cache files
hosted in shared folders so that they are accessible when the computer is unable to connect directly to the network resource. The Offline Files feature is available to users of the Professional, Enterprise, and Ultimate editions of Windows 7. You can use the Offline Files feature to ensure access when a client computer is out of the office or when a temporary disruption, such as a wide area network (WAN) link failing between a branch office and a head office, blocks access to specially configured shared folders.

Using Sync CenterYou can use Sync Center to synchronize files, manage offline files, and resolve synchronization conflicts manually. Sync Center is located within the Control Panel or by typing Sync Center into the Search Programs and Files text box on the Start menu. Clicking Manage Offline Files opens the Offline Files. This dialog box is also available using the Offline Files control panel. Using this dialog box, you can disable offline files, view offline files, configure disk usage for offline files, configure encryption for offline files, and configure how often Windows 7 should check for slow network conditions.



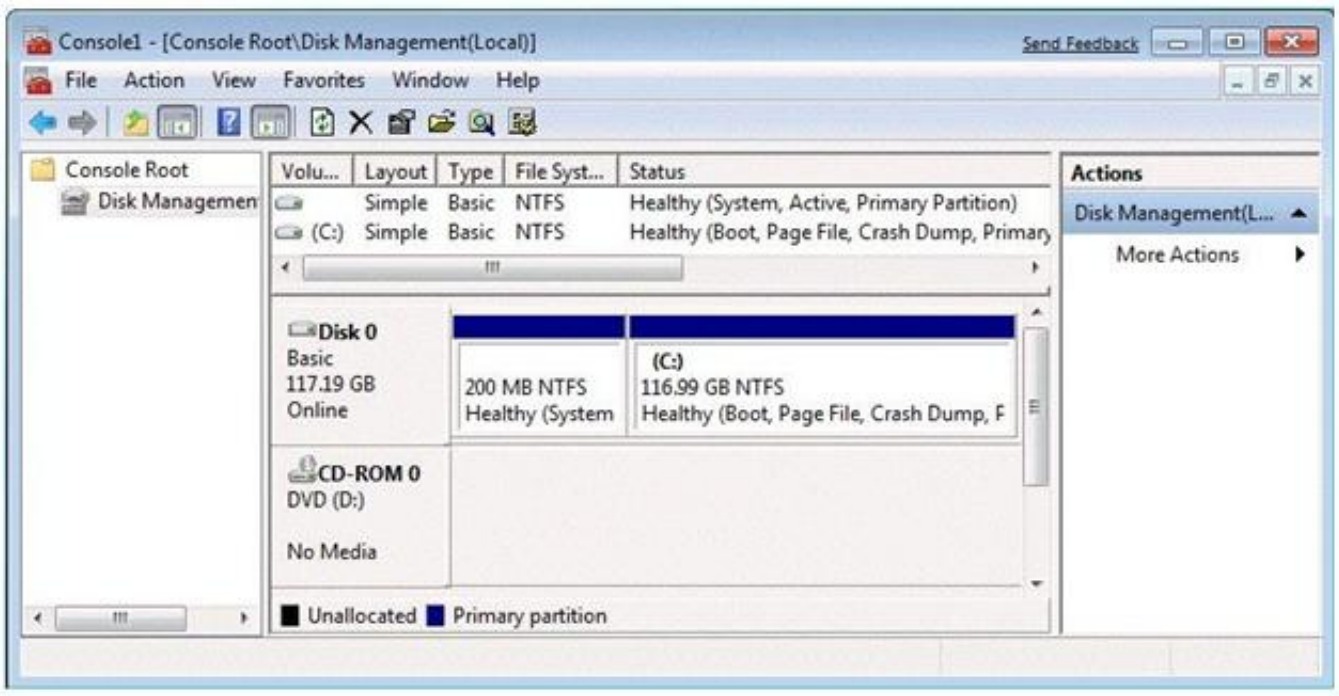
NEW QUESTION 10
You have a computer that runs Windows Vista. The computer contains a custom application.
You need to export the user state and the settings of the custom application.
What should you do?

A. Run Loadstate.exe and specify the /config paramete
B. Run Scanstate.exe and specify the /genconfig paramete
C. Modify the miguser.xml fil
D. Run Loadstate.exe and specify the /ui paramete
E. Modify the migapp.xml fil
F. Run Scanstate.exe and specify the /i paramete

Answer: D

Explanation:
MigApp.xml This file contains rules about migrating application settings. These include Accessibility settings, dial-up connections, favorites, folder options, fonts, group membership, Open Database Connectivity (ODBC) settings, Microsoft Office Outlook Express mailbox files, mouse and keyboard settings, phone and modem options, Remote Access Service (RAS) connection phone book files, regional options, remote access, screensaver settings, taskbar settings, and wallpaper settings.(Include) /i:[Path\]FileName Specifies an .xml file that contains rules that define what user, application or system state to migrate. You can specify this option multiple times to include all of your .xml files (MigApp.xml, MigUser.xml and any custom .xml files that you create). Path can be either a relative or full path. If you do not specify the Path variable, then FileName must be located in the current directory.NOT MigUser.xmlMigUser.xml This file contains rules about user profiles and user data. The default settings for this file migrate all data in My Documents, My Video, My Music, My Pictures, desktop files, Start Menu, Quick Launch settings, favorites, Shared Documents, Shared Video, Shared Music, Shared desktop files, Shared Pictures, Shared Start menu, and Shared Favorites. This file also contains rules that ensure that all the following file types are migrated from fixed volumes: .qdf, .qsd, .qel, .qph, .doc, .dot, .rtf, .mcw, .wps, .scd, .wri, .wpd, .xl*, .csv, .iqy, . dqy, .oqy, .rqy, .wk*, .wq1, .slk, .dif, .ppt*, .pps*, .pot*, .sh3, .ch3, .pre, .ppa, .txt, .pst, .one*, .mpp, .vsd, .vl*, .or6, .accdb, .mdb, .pub, .xla, .xlb and .xls. The asterisk (*) represents zero or more characters.

NEW QUESTION 15
You have a computer that runs Windows 7. You open the Disk Management snap-in as shown in the exhibit. (Click the Exhibit button.)?



You need to ensure that you can create a new partition on Disk 0.
What should you do?

A. Shrink volume
B. Compress volume
C. Convert Disk 0 into a dynamic dis
D. Create and initialize a Virtual Hard Disk (VHD).

Answer: A

Explanation:
Needs to have sufficient space in order to create a new partition. Hence shrinking the C: partition will create additional space that can be used for a new partition.

NEW QUESTION 17
Your network has a main office and a branch office.
The branch office has five client computers that run Windows 7. All client computers are configured to use BranchCache.
At the branch office, a computer named Computer1 is experiencing performance issues.
You need to temporarily prevent all computers from retrieving cached content from Computer1.
What should you do on Computer1?

A. At the command prompt, run Netsh branchcache flus
B. At the command prompt, run Netsh branchcache dum
C. Modify the Configure BranchCache for network files Group Policy settin
D. Modify the Set percentage of disk space used for client computer cache Group Policy settin

Answer: A

Explanation:
Flush
Deletes the contents of the local BranchCache cache.

NEW QUESTION 19
Your network has a main office and a branch office. The branch office has computers that run Windows 7. A network administrator enables BranchCache in the main office. You run Netsh on your computer as shown in the exhibit. (Click the Exhibit button.)

```
C:\Users\administrator>netsh branchcache show status all

BranchCache Service Status:
----------------------------------------------------------------------
Service Mode                = Distributed Caching (Set By Group Policy)
Current Status              = Running
Service Start Type          = Manual

Local Cache Status:
----------------------------------------------------------------------
Maximum Cache Size          = 5% of hard disk
Active Current Cache Size   = 3425166 Bytes
Local Cache Location        = C:\Windows\ServiceProfiles\NetworkService\AppData\Lo
cal\PeerDistRepub (Default)
This machine is not configured as a hosted cache client.

Networking Status:
----------------------------------------------------------------------
Content Retrieval URL Reservation           = Configured     (Required)
Hosted Cache URL Reservation                = Configured     (Not Required)
SSL Certificate Bound To Hosted Cache Port  = Not Configured (Not Required)
Content Retrieval Firewall Rules            = Disabled       (Required)
Peer Discovery Firewall Rules               = Disabled       (Required)
Hosted Cache Server Firewall Rules          = Disabled       (Not Required)
Hosted Cache Client Firewall Rules          = Enabled        (Not Required)
```

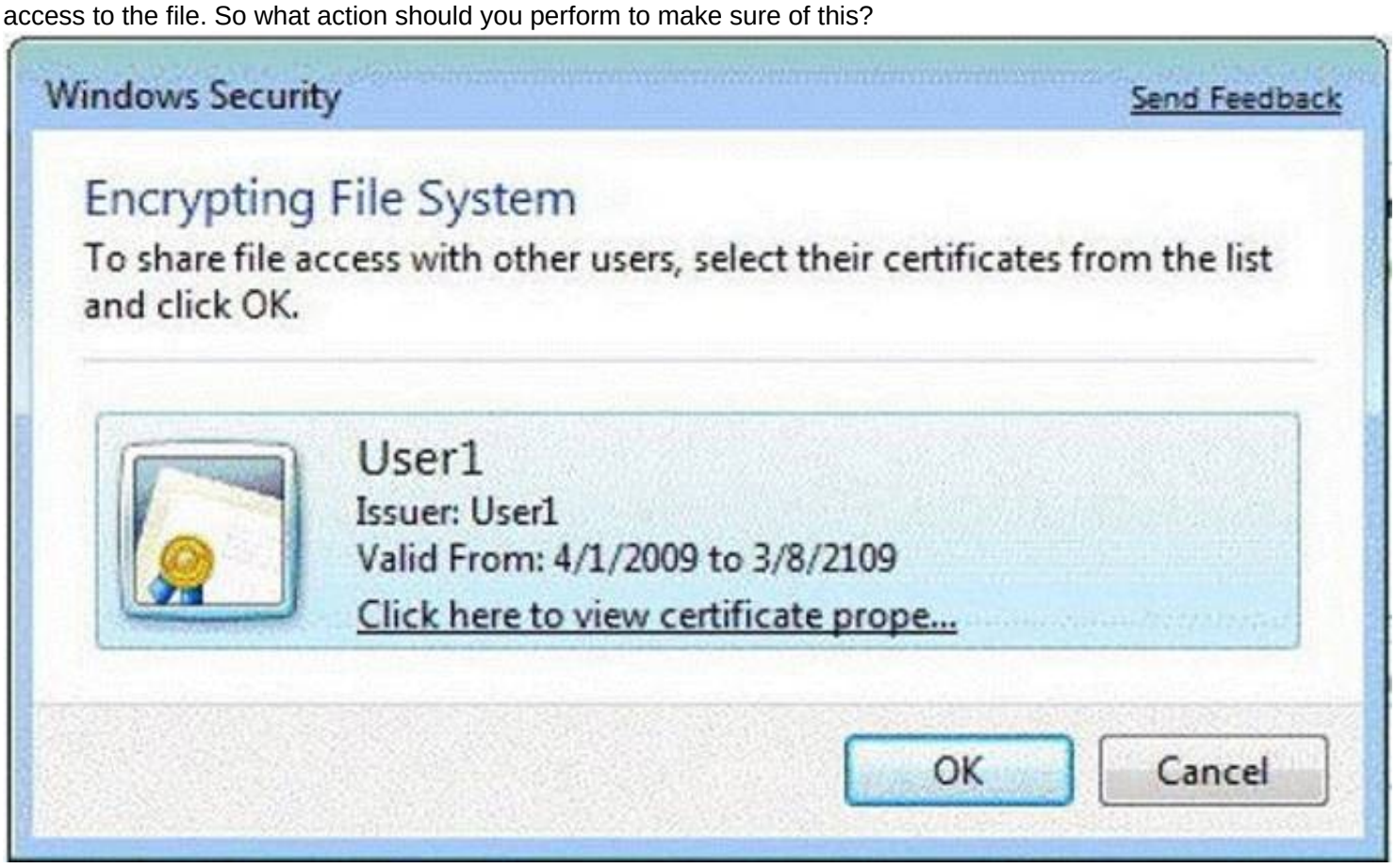
You need to ensure that other computers in the branch office can access the cached content on your computer.
What should you do?

A. Turn on Internet Information Services (IIS).
B. Configure the computer as a hosted cache clien
C. Configure the BranchCache service to start automaticall
D. Modify the Windows Firewall with Advanced Security rule

Answer: D

Explanation:
Distributed Cache Mode Distributed Cache mode uses peer caching to host the branch office cache among clients running Windows 7 on the branch office network. This means that each Distributed Cache mode client hosts part of the cache, but no single client hosts all the cache. When a client running Windows 7 retrieves content over the WAN, it places that content into its own cache. If another BranchCache client running Windows 7 attempts to access the same content, it is able to access that content directly from the first client rather than having to retrieve it over the WAN link. When it accesses the file from its peer, it also copies that file into its own cache. When you configure BranchCache in distributed cache mode, BranchCache client computers use the Hypertext Transfer Protocol (HTTP) for data transfer with other client computers. BranchCache client computers also use the Web Services Dynamic Discovery (WS-Discovery) protocol when they attempt to discover content on client cache servers. You can use this procedure to configure client firewall exceptions to allow incoming HTTP and WS-Discovery traffic on client computers that are configured for distributed cache mode. You must select Allow the connection for the BranchCache client to be able to send traffic on this port.

NEW QUESTION 23
You work in an international company which is named Wiikigo. Before entering this company, you have two years of experience in the IT field, as well as experience implementing and administering any Windows client operating system in a networked environment. You are professional in installing, upgrading and migrating to Windows 7, deploying Windows 7, and configuring Hardware and Applications and son on. You manage a stand-alone computer which has only one partition. Windows 7 is run by this computer. The computer is shared by two users that are respectively named User1 and User2. User01 uses Encrypting File System (EFS) to encrypt a file. User01 tries to grant User2 access to the file as shown in the exhibit. You have to make sure that User1 are able to grant User2 access to the file. So what action should you perform to make sure of this?



A. User02 should be instructed to log on to the computer and take ownership of the fil
B. User02 should be instructed to log on to the computer and encrypt a fil
C. User1 should be instructed to export his certificate to a certificate (.cer) fil
D. User01 should be instructed to move the file to a shared folder on the compute

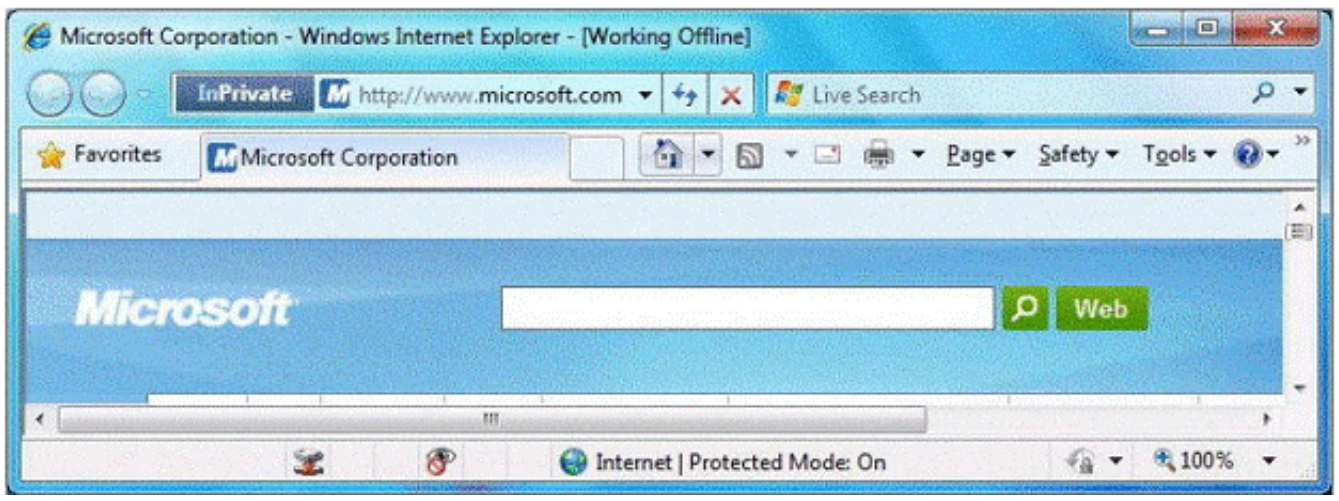
Answer: B

NEW QUESTION 27
You want to prohibit read, write, and execute access to all types of external storage devices.
What computer policy setting do you enable?

A. All Removable Storage: Allow Direct Access In Remote Sessions
B. All Removable Storage Classes: Deny All Access
C. Removable Disks: Deny Read Access
D. Removable Disks: Deny Write Access

Answer: B

NEW QUESTION 30
You have a computer that runs Windows 7. Your company has a corporate intranet Web site. You open Windows Internet Explorer as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that you can access Web pages on both the Internet and the intranet.
What should you do?

A. From the Files menu, click Work Offlin
B. From the Safety menu, click InPrivate Filterin
C. From the Security tab, add the intranet Web site to the Trusted sites zon
D. From the Safety menu, click InPrivate Browsin

Answer: A

Explanation:
Working Offline is activated On Internet Explorer's File menu is a "Work Offline" item that toggles Internet Explorer between online and offline modes of operation. (The question originally stated the Tools menu, maybe in a different version of IE this is the case, but for me and in the TechNet documentation it was under Files, so I'm choosing to believe Tools was a mistake and it should be Files, this has been amended in the question). InPrivate is turned on (does not prevent browsing the internet) InPrivate Browsing helps prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. Toolbars and extensions are disabled by default.

NEW QUESTION 34
You have a computer named Computer1 that runs Windows Vista and a computer named Computer2 that runs Windows 7. You plan to migrate all profiles and user files from Computer1 to Computer2.
You need to identify how much space is required to complete the migration.
What should you do?

A. On Computer1 run Loadstate c:\store /nocompress
B. On Computer1 run Scanstate c:\store /nocompress /p
C. On Computer2 run Loadstate \\computer1\store /nocompress
D. On Computer2 run Scanstate \\computer1\store /nocompress /p

Answer: B

Explanation:
ScanState You run ScanState on the source computer during the migration. You must run ScanState.exe on computers running Windows Vista and Windows 7 from an administrative command prompt. When running ScanState on a source computer that has Windows XP installed, you need to run it as a user that is a member of the local administrators group. The following command creates an encrypted store named Mystore on the file share named Migration on the file server named Fileserver that uses the encryption key Mykey: scanstate \\fileserver\migration\mystore /i:migapp.xml /i:miguser.xml /o /config:config.xml /encrypt /key:"mykey" Space Estimations for the Migration StoreWhen the ScanState command runs, it will create an .xml file in the path specified. This .xml file includes improved space estimations for the migration store. The following example shows how to create this .xml file: Scanstate.exe C:\MigrationLocation [additional parameters] /p:"C:\MigrationStoreSize.xml" To preserve the functionality of existing applications or scripts that require the previous behavior of USMT, you can use the /p option, without specifying "pathtoafile", in USMT 4.0. If you specify only the /p option, the storage space estimations are created in the same manner as with USMT 3.x releases. User State Migration ToolUSMT 4.0 is a command-line utility that allows you to automate the process of user profile migration. The USMT is part of the Windows Automated Installation Kit (WAIK) and is a better tool for performing a large number of profile migrations than Windows Easy Transfer. The USMT can write data to a removable USB storage device or a network share but cannot perform a direct side-by-side migration over the network from the source to the destination computer. The USMT does not support user profile migration using the Windows Easy Transfer cable. USMT migration occurs in two phases, exporting profile data from the source computer using ScanState and importing profile data on the destination computer using LoadState.

NEW QUESTION 38
You have a computer that runs Windows 7.
You need to configure the computer to download updates from a local Windows Server Update Services (WSUS) server. What should you do?

A. From Windows Update, modify the Windows Update setting
B. From the local Group Policy, modify the Windows Update setting
C. From the System settings, modify the System Protection setting
D. From the local Group Policy, modify the Location and Sensors setting

Answer: B

NEW QUESTION 41
To which of the following versions and editions of Windows 7 can you directly upgrade a computer running Windows Vista Enterprise (x86)?

A. Windows 7 Home Professional (x86).
B. Windows 7 Ultimate (x86)
C. Windows 7 Ultimate (x64)
D. Windows 7 Enterprise (x64)

Answer: B

Explanation:
1048 4079
Windows 7 Upgrade paths:
http://technet.microsoft.com/en-us/library/dd772579%28v=ws.10%29.aspx
The only applicable solution is Windows 7 Enterprise (64-bit) as for the following reasons:
All versions are support Hardware wise.
Requirements:
Windows 7 Home Premium, Professional, Ultimate, and Enterprise editions have the following minimum hardware requirements:
1 GHz 32-bit (x86) or 64-bit (x64) processor
1 GB of system memory a 40-GB hard disk drive (traditional or SSD) with at least 15 GB of available space a graphics adapter that supports DirectX 9 graphics, has a Windows Display Driver Model (WDDM) driver, Pixel Shader 2.0 hardware, and 32 bits per pixel and a minimum of 128 MB graphics memory XP Mode
Windows XP Mode is a downloadable compatibility option that is available for the
Professional, Enterprise, and Ultimate editions of Windows 7. Windows XP Mode uses the latest version of Microsoft Virtual PC to allow you to run an installation of Windows XP virtually under Windows 7.
Use all of the installed memory
The x86 version supports a maximum of 4 GB of RAM, whereas the x64 version supports a maximum of 8 GB of RAM.
Windows 7 Professional
Windows 7 Professional is available from retailers and on new computers installed by manufacturers. It supports all the features available in Windows Home Premium, but you can join computers with this operating system installed to a domain. It supports EFS and Remote Desktop Host but does not support enterprise features such as AppLocker, DirectAccess, BitLocker, and BranchCache.
Windows 7 Enterprise and Ultimate Editions
The Windows 7 Enterprise and Ultimate editions are identical except for the fact that Windows 7 Enterprise is available only to Microsoft's volume licensing customers, and Windows 7 Ultimate is available from retailers and on new computers installed by manufacturers. The Enterprise and Ultimate editions support all the features available in other Windows 7 editions but also support all the enterprise features such as EFS, Remote Desktop Host, AppLocker, DirectAccess, BitLocker, BranchCache, and Boot from VHD.

NEW QUESTION 46
You have a reference computer that runs Windows 7.
You plan to deploy an image of the computer.
You create an answer file named answer.xml.
You need to ensure that the installation applies the answer file after you deploy the image.
Which command should you run before you capture the image?

A. Imagex.exe /append answer.xml /check
B. Imagex.exe /mount answer.xml /verify
C. Sysprep.exe /reboot /audit /unattend:answer.xml
D. Sysprep.exe /generalize /oobe /unattend:answer.xml

Answer: D

Explanation:
To prepare the reference computer for the user, you use the Sysprep utility with the /generalize option to remove hardware-specific information from the Windows installation and the /oobe option to configure the computer to boot to Windows Welcome upon the next restart. Open an elevated command prompt on the reference computer and run the following command: c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown Sysprep prepares the image for capture by cleaning up various user-specific and computer-specific settings, as well as log files. The reference installation now is complete and ready to be imaged.

NEW QUESTION 47
You have a standalone computer that runs Windows 7. Multiple users share the computer.
You need to ensure that you can read the content of all encrypted files on the computer.
What should you do?

A. Run the Certificates Enrollment wizard and then run Certutil.exe -importpf
B. Run the Certificates Enrollment wizard and then run Certutil.exe -installcer
C. Run Cipher.exe /r and then add a data recovery agent from the local security polic
D. Run Cipher.exe /rekey and then import a security template from the local security polic

Answer: C

Explanation:
Cipher Displays or alters the encryption of folders and files on NTFS volumes. Used without parameters, cipher displays the encryption state of the current folder and any files it contains. Administrators can use Cipher.exe to encrypt and decrypt data on drives that use the NTFS file system and to view the encryption status of files and folders from a command prompt. The updated version adds another security option. This new option is the ability to overwrite data that you have deleted so that it cannot be recovered and accessed.When you delete files or folders, the data is not initially removed from the hard disk. Instead, the space on the disk that was occupied by the deleted data is "deallocated." After it is deallocated, the space is available for use when new data is written to the disk. Until the space is overwritten, it is possible to recover the deleted data by using a low-level disk editor or data-recovery software.
If you create files in plain text and then encrypt them, Encrypting File System (EFS) makes a backup copy of the file so that, if an error occurs during the encryption process, the data is not lost. After the encryption is complete, the backup copy is deleted. As with other deleted files, the data is not completely removed until it has been overwritten. The new version of the Cipher utility is designed to prevent unauthorized recovery of such data.
/K Creates a new certificate and key for use with EFS. If this option is chosen, all the other options will be ignored. By default, /k creates a certificate and key that conform to current group plicy. If ECC is specified, a self-signed certificate will be created with the supplied key size. /R Generates an EFS recovery key and certificate, then writes them to a .PFX file (containing certificate and private key) and a .CER file (containing only the certificate). An administrator may add the contents of the .CER to the EFS recovery policy to create the recovery for users, and import the .PFX to recover individual files. If SMARTCARD is specified, then writes the recovery key and certificate to a smart card. A .CER file is generated (containing only the certificate). No .PFX file is genereated. By default, /R creates an 2048-bit RSA recovery key and certificate. If EECC is specified, it must be followed by a key size of 356, 384, or 521.

NEW QUESTION 49
You have a computer that runs Windows 7. The computer contains two volumes, C and D.
You create a new folder called D:\Reports.
You need to ensure that all files stored in the Reports folder are indexed by Windows Search.
What should you do?

A. Enable the archive attribute on the folde
B. Modify the Folder Options from Control Pane
C. Modify the properties of the Windows Search servic
D. Create a new library and add the Reports folder to the librar

Answer: D

Explanation:
Libraries enable you to organize files by using metadata about the file, such as author, date, type, tags, and so on-instantly. You're not limited to just browsing files by folder hierarchy. When you save files in a Library, Windows. 7 indexes the files. You can use Library features like the Arrange By control to instantly browse the files in the Library by metadata or use the Search Builder, which is built into the Search box in Windows Explorer, to instantly search the files in the Library by metadata.

NEW QUESTION 54
All the games including Titan Chess come with which versions of Windows 7? Choose two.

A. Windows Home Edition
B. Windows Professional Edition
C. Windows Ultimate Edition
D. Windows Enterprise Edition

Answer: CD

NEW QUESTION 58
Which of the following Windows 7 Editions allows you to join an Active Directory domain? Choose three.

A. Windows Home Edition
B. Windows Professional Edition
C. Windows Ultimate Edition
D. Windows Enterprise Edition

Answer: BCD

NEW QUESTION 59
A user has a home computer with a cable Internet connection and no other computers on his home network. Which of the following methods can this person use to upgrade from Windows 7 Home Premium to Windows 7 Ultimate?

A. Sysprep
B. Windows PE
C. WDS
D. Windows Anytime Upgrade

Answer: D

Explanation:
Windows Anytime Upgrade With Windows Anytime Upgrade, shown in Figure,you can purchase an upgrade to an application over the Internet and have the features unlocked automatically. This upgrade method is more suitable for home users and users in small businesses where a small number of intra-edition upgrades is required.

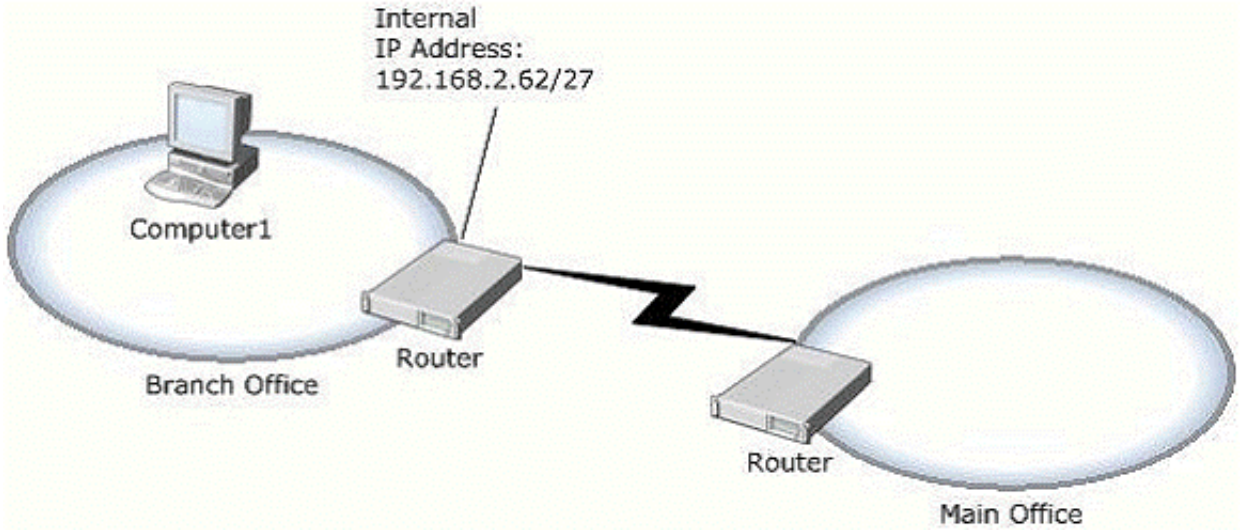
NEW QUESTION 60
You have a computer that runs Windows 7. You create an Encrypting File System (EFS) recovery key and certificate.
You need to ensure that your user account can decrypt all EFS files on the computer.
What should you do?

A. From Credential Manager, add a Windows credentia
B. From Credential Manager, add a certificate-based credentia
C. From the local computer policy, add a data recovery agen
D. From the local computer policy, modify the Restore files and directories settin

Answer: C

Explanation:
EFS Recovery Recovery Agents are certificates that allow the restoration of EFS encrypted files. When a recovery agent has been specified using local policies, all EFS encrypted files can be recovered using the recovery agent private key. You should specify a recovery agent before you allow users to encrypt files on a client running Windows 7. You can recover all files that users encrypt after the creation of a recovery agent using the recovery agent's private key. You are not able to decrypt files that were encrypted before a recovery agent certificate was specified. You create an EFS recovery agent by performing the following steps:
1. Log on to the client running Windows 7 using the first account created, which is the default administrator account.
2. Open a command prompt and issue the command Cipher.exe /r:recoveryagent
3. This creates two files: Recoveryagent.cer and Recoveryagent.pfx. Cipher.exe prompts you to specify a password when creating Recoveryagent.pfx.
4. Open the Local Group Policy Editor and navigate to the \Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System node. Right-click this node and then click Add Data Recovery Agent. Specify the location of Recoveryagent.cer to specify this certificate as the recovery agent.
5. To recover files, use the certificates console to import Recoveryagent.pfx. This is the recovery agent's private key. Keep it safe because it can be used to open any encrypted file on the client running Windows 7.

NEW QUESTION 61
Your company has a main office and a branch office. The relevant portion of the network is configured as shown in the exhibit. (Click the Exhibit button.)



In the branch office, you deploy a new computer named Computer1 that runs Windows 7.
You need to assign an IP address to Computer1.
Which IP address should you use?

A. 192.168.2.30
B. 192.168.2.40

C. 192.168.2.63
D. 192.168.2.65

Answer: B

Explanation:
Internal IP Adress of router is 192.168.2.62/27Leaves 5 bits for range = 32 addresses (including the 2 reserved addresses)Subnet Mask = 255.255.255.224

```
Address: 192.168.2.62          11000000.10101000.00000010.001 11110
Netmask: 255.255.255.224 = 27  11111111.11111111.11111111.111 00000
Wildcard: 0.0.0.31             00000000.00000000.00000000.000 11111
Network: 192.168.2.32/27       11000000.10101000.00000010.001 00000

Network Address       : 192.168.2.32 (reserved)
Address of First Host : 192.168.2.33
Address of Last Host  : 192.168.2.62
Broadcast Address     : 192.168.2.63 (reserved)
```

Acceptable IP range: 192.168.2.33 - 192.168.2.62

Therefore
192.168.2.30: is out of range (in the wrong subnet, not subnet 2).
192.168.2.40: is accepable (in correct subnet, and not reservered).
192.168.2.63: is reserved for Broadcast (in subnet, but reservered).
192.168.2.65: is out of range (in the wrong subnet, not subnet 2).

Accepable IP ranges for those interested (excluding the 2 reserved IP addersses):

```
Segment 1: 192.168.2.1   - 192.168.2.30
Segment 2: 192.168.2.33  - 192.168.2.62
Segment 3: 192.168.2.65  - 192.168.2.94
Segment 4: 192.168.2.97  - 192.168.2.126
Segment 5: 192.168.2.129 - 192.168.2.158
Segment 6: 192.168.2.161 - 192.168.2.190
Segment 7: 192.168.2.193 - 192.168.2.222
Segment 8: 192.168.2.225 - 192.168.2.254
```

Segments for those interested (including the 2 reserved IP addersses):

```
Segment 1: 192.168.2.0   - 192.168.2.31
Segment 2: 192.168.2.32  - 192.168.2.63
Segment 3: 192.168.2.64  - 192.168.2.95
Segment 4: 192.168.2.96  - 192.168.2.127
Segment 5: 192.168.2.128 - 192.168.2.159
Segment 6: 192.168.2.160 - 192.168.2.191
Segment 7: 192.168.2.192 - 192.168.2.223
Segment 8: 192.168.2.224 - 192.168.2.255
```

NEW QUESTION 62
You have a stand-alone computer named Computer1 that runs Windows 7. Several users share Computer1.
You need to prevent all users who are members of a group named Group1 from running Windows Media Player. All other users must be allowed to run Windows Media Player.
You must achieve this goal by using the least amount of administrative effort. What should you do?
A. From Software Restriction Policies, create a path rul
B. From Software Restriction Policies, create a hash rul
C. From Application Control Policies, create the default rule
D. From Application Control Policies, create an executable rul

Answer: D

Explanation:
Executable Rules Executable rules apply to files that have .exe and .com file extensions. AppLocker policies are primarily about executable files, and it is likely that the majority of the AppLocker policies that you work with in your organizational environment will involve executable rules. The default executable rules are path rules that allow everyone to execute all applications in the Program Files folder and the Windows folder. The default rules also allow members of the administrators group to execute applications in any location on the computer. It is necessary to use the default executable rules, or rules that mirror their functionality, because Windows does not function properly unless certain applications, covered by these default rules, are allowed to execute. When you create a rule, the scope of the rule is set to Everyone, even though there is not a local group named Everyone. If you choose to modify the rule, you can select a specific security group or user account. NOT Default rulesDefault rules are a set of rules that can be created automatically and which allow access to default Windows and program files. Default rules are necessary because AppLocker has a built-in fallback block rule that restricts the execution of any application that is not subject to an Allow rule. This means that when you enable AppLocker, you cannot execute any application, script, or installer that does not fall under an Allow rule. There are different default rules for each rule type. The default rules for each rule type are general and can be tailored by administrators specifically for their environments. For example, the default executable rules are path rules. Security-minded administrators might replace the default rules with publisher or hash rules because these are more secure.NOT Path RulesPath rules, allow you to specify a file, folder, or registry key as the target of a Software Restriction Policy. The more specific a path rule is, the higher its precedence. For example, if you have a path rule that sets the file C: \Program files\Application\App.exe to Unrestricted and one that sets the folder C:\Program files\Application to Disallowed, the more specific rule takes precedence and the application can execute. Wildcards can be used in path rules, so it is possible to have a path rule that specifies C:\Program files\Application*.exe. Wildcard rules are less specific than rules that use a file's full path. The drawback of path rules is that they rely on files and folders remaining in place. For example, if you created a path rule to block the application C:\Apps\Filesharing.exe, an attacker could execute the same application by moving it to another directory or renaming it something other than Filesharing.exe. Path rules work only when the file and folder permissions of the underlying operating system do not allow files to be moved and renamed.NOT Hash RulesHash rules, work through the generation of a digital fingerprint that identifies a file based on its binary characteristics. This means that a file that you create a hash rule for will be identifiable

regardless of the name assigned to it or the location from which you access it. Hash rules work on any file and do not require the file to have a digital signature. The drawback of hash rules is that you need to create them on a per-file basis. You cannot create hash rules automatically for Software Restriction Policies; you must generate each rule manually. You must also modify hash rules each time that you apply a software update to an application that is the subject of a hash rule. Software updates modify the binary properties of the file, which means that the modified file does not match the original digital fingerprint.

NEW QUESTION 67
You want to create a 20-GB native VHD called Systemvhd in a folder called Windows 7 on an external U hard disk with the drive designation G:. Which command do you use?

A. create vdisk file=g:\windows7\systemvhd maximum=20000
B. create vdisk file=g:\windows7\systemvhd.vhd maximum=20000
C. create vdisk file=g:\windows7\systemvhd.vhd maximum=20
D. create vdisk file=g:\windows7\systemvhd maximum=20

Answer: B

NEW QUESTION 70
A user wants to install the games included with Windows 7 on his PC. They were not installed by default.
Windows components can be added or removed using which of the following in Windows 7.

A. Click the Start Bar, Control Panel, Add/Remove Programs, and click Windows Component
B. Click the Start Bar, Control Panel, Programs, then click Turn Windows features on or of
C. Click the Start Bar, Settings, Windows Control Cente
D. Right click the "My Computer" icon, Choose Properties, Choose Computer Management, on the left pane choose Add Remove Windows Component

Answer: B

NEW QUESTION 74
You have a computer that runs Windows 7.
You need to configure the computer to meet the following requirements:
. Generate a new security ID (SID) when the computer starts.
. Ensure that the Welcome screen appears when the computer starts.
What should you do?

A. Run Sysprep.exe /oobe /generaliz
B. Run Sysprep.exe /audit /generaliz
C. Run Msconfig.exe and select Selective startu
D. Run Msconfig.exe and select Diagnostic startu

Answer: A

Explanation:
To prepare the reference computer for the user, you use the Sysprep utility with the /generalize option to remove hardware-specific information from the Windows installation and the /oobe option to configure the computer to boot to Windows Welcome upon the next restart. Open an elevated command prompt on the reference computer and run the following command: c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown Sysprep prepares the image for capture by cleaning up various user-specific and computer-specific settings, as well as log files. The reference installation now is complete and ready to be imaged./generalize Prepares the Windows installation to be imaged. If you specify this option, all unique system information is removed from the Windows installation. The SID is reset, system restore points are cleared, and event logs are deleted. The next time the computer starts, the specialize configuration pass runs. A new SID is created, and the clock for Windows activation resets (unless the clock has already been reset three times)./oobeRestarts the computer in Windows Welcome mode. Windows Welcome enables users to customize their Windows 7 operating system, create user accounts, and name the computer. Any settings in the oobeSystem configuration pass in an answer file are processed immediately before Windows Welcome starts.

NEW QUESTION 79
Which of the following must you download from Microsoft's Web site to obtain USMT 4.0?

A. Windows Anytime Upgrade
B. Windows Upgrade Advisor
C. WAIK
D. Microsoft Application Compatibility Toolkit

Answer: C

Explanation:
User State Migration Tool USMT 4.0 is a command-line utility that allows you to automate the process of user profile migration. The USMT is part of the Windows Automated Installation Kit (WAIK) and is a better tool for performing a large number of profile migrations than Windows Easy Transfer. The USMT can write data to a removable USB storage device or a network share but cannot perform a direct side-by-side migration over the network from the source to the destination computer. The USMT does not support user profile migration using the Windows Easy Transfer cable. USMT migration occurs in two phases, exporting profile data from the source computer using ScanState and importing profile data on the destination computer using LoadState.

NEW QUESTION 83
You have a computer that runs Windows 7.
You need to prevent Internet Explorer from saving any data during a browsing session.
What should you do?

A. Disable the BranchCache servic

B. Modify the InPrivate Blocking lis
C. Open an InPrivate Browsing sessio
D. Modify the security settings for the Internet zon

Answer: C

Explanation:
InPrivate Mode consists of two technologies: InPrivate Filtering and InPrivate Browsing.
Both InPrivate Filtering and InPrivate Browsing are privacy technologies that restrict the amount of information available about a user's browsing session. InPrivate Browsing restricts what data is recorded by the browser, and InPrivate Filtering is used to restrict what information about a browsing session can be tracked by external third parties.

NEW QUESTION 86
You have a standalone computer that runs Windows 7. You need to prevent non-administrative users from using Device Manager. Users must be able to access Event Viewer.
What should you do?

A. From Control Panel, modify the default settings for media and device
B. From Control Panel, modify the default settings for device installatio
C. From the local computer policy, modify the application control policie
D. From the local computer policy, modify the Microsoft Management Console (MMC) setting

Answer: D

Explanation:
Controlling MMC usage by using local Group Policy To control MMC usage by using local Group Policy
11. Open MMC 3.0.
12. On the File menu, click Add/Remove Snap-in.
13. In the Available snap-ins list, click the Group Policy editor, and then click Add.
14. In the Select Group Policy Object wizard, use the default setting, Local Computer, in the Group Policy Object field.
15. Click Finish to close the Select Group Policy Object wizard.
16. By default, all available snap-in extensions are enabled. If you want to enable only certain extensions, highlight the snap-in in the Selected snap-ins list, and then click Edit Extensions.
17. By default, snap-ins load as child objects of the Console Root node. Click Advanced to modify this behavior and allow you to choose a different parent snap-in.
18. In the Add or Remove Snap-ins dialog box, click OK.
19. Before closing the new console, perform any of these procedures:
-To restrict access to author mode in MMC
-To restrict access to a permitted list of snap-ins
-To permit or restrict access to a snap-in

NEW QUESTION 90
Which of the following is used to control when the security pop-up notifications are used?

A. Security Control Manager
B. User Account Control
C. User Access Control Panel
D. Notification Control Settings Manager

Answer: B

NEW QUESTION 92
You have a computer that runs Windows 7.
You need to confirm that all device drivers installed on the computer are digitally signed.
What should you do?

A. At a command prompt, run Verif
B. At a command prompt, run Sigverif.ex
C. From Device Manager, click Scan for hardware change
D. From Device Manager, select the Devices by connection vie

Answer: B

Explanation:
Checking Digital Signatures with the File Signature Verification Tool The Dxdiag tool identifies problems with DirectX hardware and tells you whether that hardware has passed the WHQL testing regimen and has been signed digitally. However, it does not test the device drivers that are not associated with DirectX devices. To scan your computer and identify any unsigned drivers, you should use the File Signature Verification (Sigverif) tool.

NEW QUESTION 95
You have a portable computer that runs Windows 7. You configure the computer to enter sleep mode after 10 minutes of inactivity. You do not use the computer for 15 minutes and discover that the computer has not entered sleep mode.
You need to identify what is preventing the computer from entering sleep mode.
What should you do?

A. At a command prompt, run Powercfg energ
B. At a command prompt, run Systeminfo /s localhos
C. From Performance Monitor, review the System Summar

D. From Performance Information and Tools, review the detailed performance and system informatio

Answer: A

Explanation:
Command-line Power Configuration Powercfg.exe is a command-line utility that you can use from an administrative command prompt to manage Windows 7 power settings. It is possible to use Powercfg.exe to configure a number of Windows 7 powerrelated settings that you cannot configure through Group Policy or the Advanced Plan Settings dialog box. You can use Powercfg.exe to configure specific devices so that they are able to wake the computer from the Sleep state. You can also use Powercfg.exe to migrate power policies from one computer running Windows 7 to another by using the import and export functionality. -energy Check the computer for common energy-efficiency and battery life problems. Provides report in Hypertext Markup Language (HTML) format.For more information on Powercfg.exe, consult the following Microsoft TechNet document: http://technet.microsoft.com/en-us/library/cc748940.aspx.

NEW QUESTION 96
You have a wireless access point that is configured to use Advanced Encryption Standard (AES) security. A pre-shared key is not configured on the wireless access point.
You need to connect a computer that runs Windows 7 to the wireless access point.
Which security setting should you select for the wireless connection?

A. 802.1x
B. WPA-Personal
C. WPA2-Enterprise
D. WPA2-Personal

Answer: C

Explanation:
WPA and WPA2 indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. WPA2 enhances WPA, which in turn addresses weaknesses in the previous system, WEP. WPA was intended as an intermediate measure to take the place of WEP while an IEEE 802.11i standard was prepared. 802.1X provides port-based authentication, which involves communications between a supplicant (a client computer), an authenticator (a wired Ethernet switch or WAP), and an authentication server (typically a Remote Authentication Dial In User Service, or RADIUS, server). WPA2-Enterprise WPA-Enterprise and WPA2-Enterprise authenticate through the Extensible Authentication Protocol (EAP) and require computer security certificates rather than PSKs. The following EAP types are included in the certification program:
-EAP-TLS
-EAP-TTLS/MSCHAPv2
-PEAPv0/EAP-MSCHAPv2
-PEAPv1/EAP-GTC
-EAP-SIM
If you want to use AES and to use computer certificates rather than a PSK, you would choose WPA2- Enterprise.WPA2-PersonalIf you have a small network that is not in a domain and cannot access a CA server, but you install a modernWAP that supports AES, you would use WPA2-Personal (with a PSK).WPA-Personal If you have a small network that is not in a domain and cannot access a CA server and your WAP does not support AES, you would use WPA-Personal.802.1x If you have a RADIUS server on your network to act as an authentication server and you want the highest possible level of security, you would choose 802.1X.

NEW QUESTION 97
You have a computer that runs Windows 7. The computer connects to the corporate network by using a VPN connection.
You need to ensure that you can access the Internet when the VPN connection is active. The solution must prevent Internet traffic from being routed through the VPN connection.
What should you do?

A. Configure a static DNS server addres
B. Configure a static IP address and default gatewa
C. Configure the security settings of the VPN connectio
D. Configure the advanced TCP/IP settings of the VPN connectio

Answer: D

Explanation:
To prevent the default route from being created In the properties of the TCP/IP protocol of the dial-up connection object, in the Advanced TCP/IP Settings dialog box, click the General tab, and then clear the Use default gateway on remote network check box.

NEW QUESTION 98
You start a computer by using Windows Preinstallation Environment (Windows PE).
You need to dynamically load a network adapter device driver in Windows PE.
What should you do?

A. Run Peimg.exe and specify the device driver pat
B. Run Drvload.exe and specify the device driver pat
C. Run Winpeshl.exe and specify a custom Winpeshl.ini fil
D. Run Wpeutil.exe and specify the InitializeNetwork comman

Answer: B

Explanation:
Drvload The Drvload tool adds out-of-box drivers to a booted Windows PE image. It takes one or more driver .inf files as inputs. To add a driver to an offline Windows PE image, use the peimg tool.NOT WinpeshlWinpeshl.ini controls whether a customized shell is loaded in Windows PE instead of the default Command Prompt window. To load a customized shell, create a file named Winpeshl.ini and place it in %SYSTEMROOT% \System32 of your customized Windows PE image. The .ini file must have the following section and entry.NOT WpeutilThe Windows PE utility (Wpeutil) is a command-line tool that enables you to run various commands in a Windows PE session. For example, you can shut down or restart Windows PE, enable or disable a firewall, set language settings, and initialize a

network.

NEW QUESTION 102
You work in an international company which is named Wiikigo. Before entering this company, you have two years of experience in the IT field, as well as experience implementing and administering any Windows client operating system in a networked environment.
You are professional in installing, upgrading and migrating to Windows 7, deploying Windows 7, and configuring Hardware and Applications and son on.
You have a workgroup which contains five computers. Windows 7 is run by the computers. A computer named C01 has video and audio files.
You have to share C01s video and audio files on the network.
What should you do? (Choose more than one)

A. Connect a removable drive and enable BitLocker To G
B. A HomeGroup should be create
C. The files should be moved to a Media Librar
D. All BranchCache rules should be enabled in Windows Firewal

Answer: BC

NEW QUESTION 105
Your network contains an Active Directory domain. All servers run Windows Server 2008 R2 and are members of the domain. All servers are located in the main office.
You have a portable computer named Computer1 that runs Windows 7. Computer1 is joined to the domain and is located in a branch office.
A file server named Server1 contains a shared folder named Share1.
You need to configure Computer1 to meet the following requirements:
. Minimize network traffic between the main office and the branch office
. Ensure that Computer1 can only access resources in Share1 while it is connected to the network.
What should you do?

A. On Computer1, enable offline file
B. On Computer1, enable transparent cachin
C. On Server1, configure DirectAcces
D. On Server1, configure Share1 to be available offlin

Answer: B

Explanation:
Transparent Caching When you enable transparent caching, Windows 7 keeps a cached copy of all files that a user opens from shared folders on the local volume. The first time a user opens the file, the file is stored in the local cache. When the user opens the file again, Windows 7 checks the file to ensure that the cached copy is up to date and if it is, opens that instead. If the copy is not up to date, the client opens the copy hosted on the shared folder, also placing it in the local cache. Using a locally cached copy speeds up access to files stored on file servers on remote networks from the client. When a user changes a file, the client writes the changes to the copy of the file stored on the shared folder. When the shared folder is unavailable, the transparently cached copy is also unavailable.
Transparent caching does not attempt to keep the local copy synced with the copy of the file on the remote file server as the Offline Files feature does.
Transparent caching works on all files in a shared folder, not just those that you have configured to be available offline.

NEW QUESTION 109
You have a computer that runs Windows 7. You create a HomeGroup. You need to secure the HomeGroup to meet the following requirements:
. Allow access to the HomeGroup when you are connected to private networks
. Block access to the HomeGroup when you are connected to public networks
What should you do?

A. From Network and Sharing Center, modify the advanced sharing setting
B. From the HomeGroup settings in Control Panel, modify the advanced sharing setting
C. Configure the HomeGroup exception in Windows Firewall to include Home or work (private) networks and block Public network
D. Configure the File and Printer Sharing exception in Windows Firewall to include Home or work (private) networks and block Public network

Answer: C

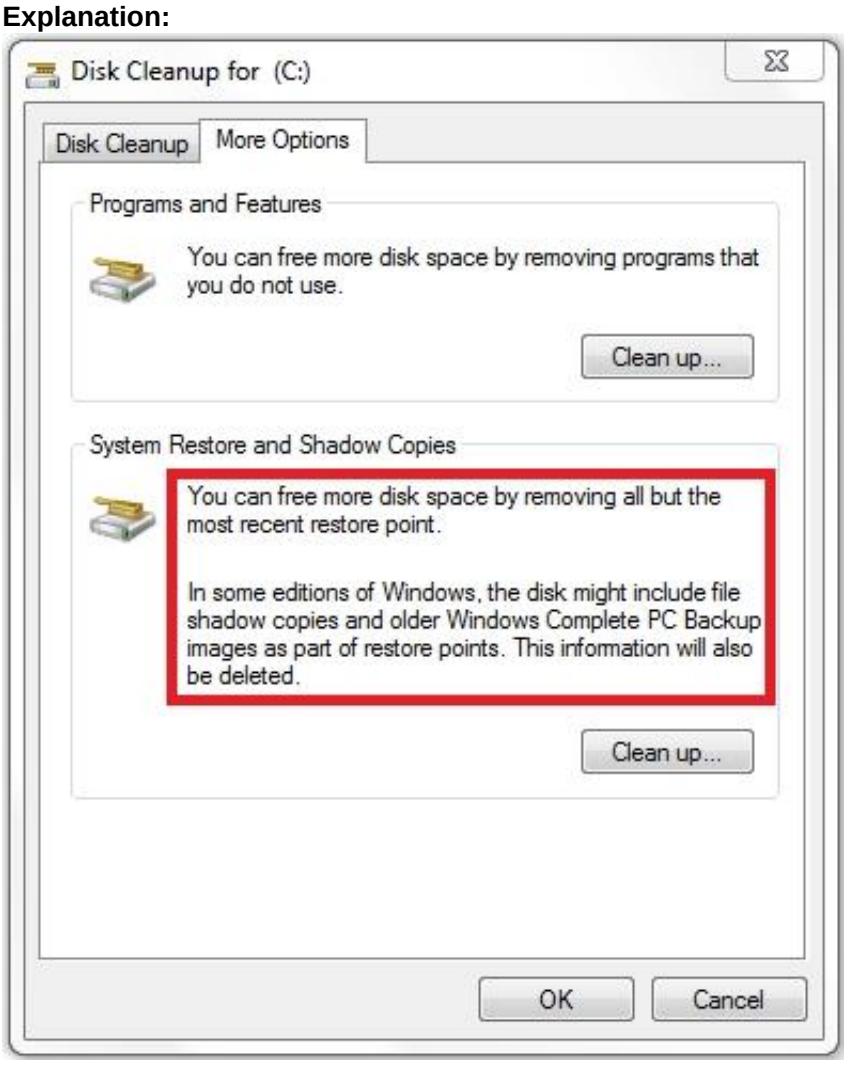
Explanation:
Windows Firewall does not allow you to create firewall rules for specific network locations on the basis of port address. Windows Firewall does not allow you to create rules that differentiate between the home and work network locations. You can only create rules that differentiate on the basis of home and work or public network locations.
HomeGroup Connections This option decides how authentication works for connections to HomeGroup resources. If all computers in the HomeGroup have the same user name and passwords configured, you can set this option to allow Windows to manage HomeGroup connections. If different user accounts and passwords are present, you should configure the option to use user accounts and passwords to connect to other computers. This option is available only in the Home/Work network profile.

NEW QUESTION 112
You have a computer that runs Windows 7. The computer has System Protection enabled.
You need to retain only the last System Protection snapshot of the computer. All other snapshots must be deleted.
What should you do?

A. Run Disk Cleanup for Programs and feature
B. Run Disk Cleanup for System Restore and Shadow Copie
C. From the System Protection Restore settings, select Turn off System Restor
D. From the System Protection Restore settings, select Only restore previous versions of file

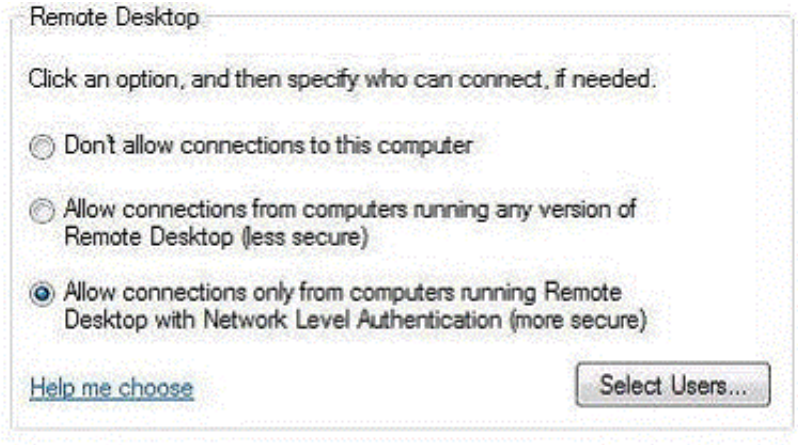
Answer: B

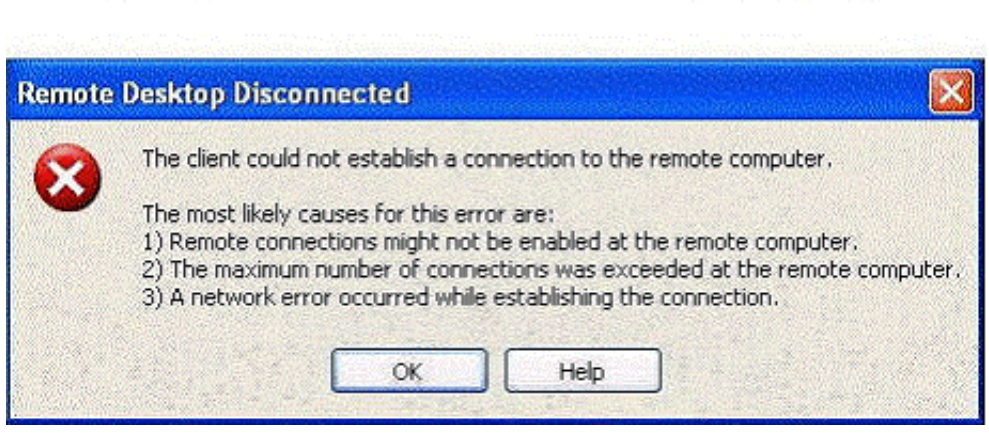
Explanation:



Shadow info: Shadow copies are automatically saved as part of a restore point. If system protection is enabled, Windows 7 automatically creates shadow copies of files that have been modified since the last restore point was created. By default, new restore points are created every seven days or whenever a significant system change (such as a driver or application installation) occurs.

NEW QUESTION 117
You work in an international company which is named Wiikigo. Before entering this company, you have two years of experience in the IT field, as well as experience implementing and administering any Windows client operating system in a networked environment. You are professional in installing, upgrading and migrating to Windows 7, deploying Windows 7, and configuring Hardware and Applications and son on. You are in charge of two computers that are respectively named C01 and C02. C01 runs Windows 7 and C02 runs Windows XP Professional.
On C01, you enable Remote Desktop as shown in the Remote Desktop exhibit. What action should you perform?

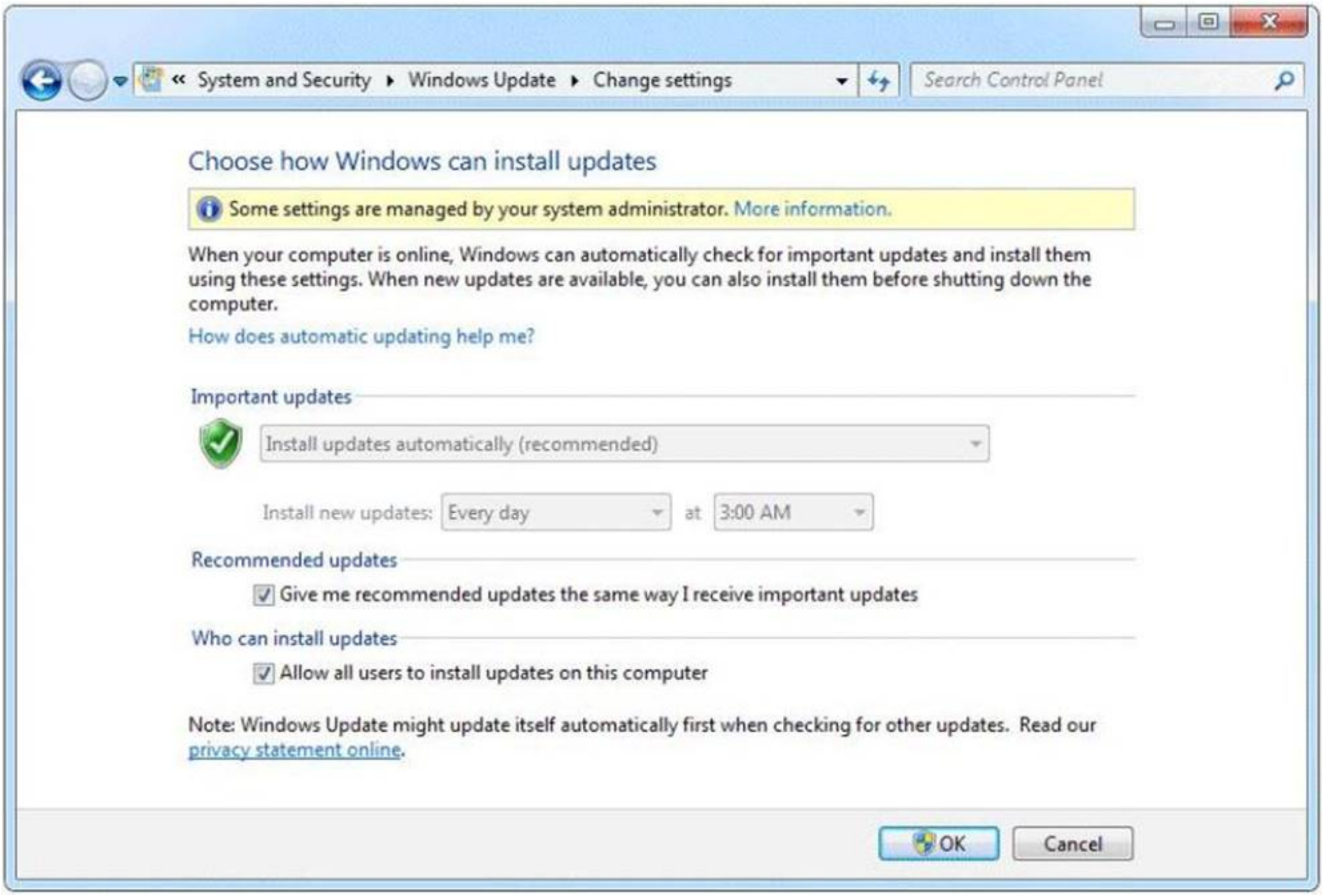




A. You should enable the Allow connections from computers running any version of Remote Desktop setting on C01.
B. The Client (Respond Only) IPSec policy should be assigned on C02.
C. Your user account should be added to the Remote Desktop Users group on C01.
D. A firewall exception should be created for the Remote Desktop Protocol (RDP) should be assigned on C02.

Answer: A

NEW QUESTION 120
You have a stand-alone computer that runs Windows 7.
You open Windows Update as shown in the exhibit. (Click the Exhibit button.)

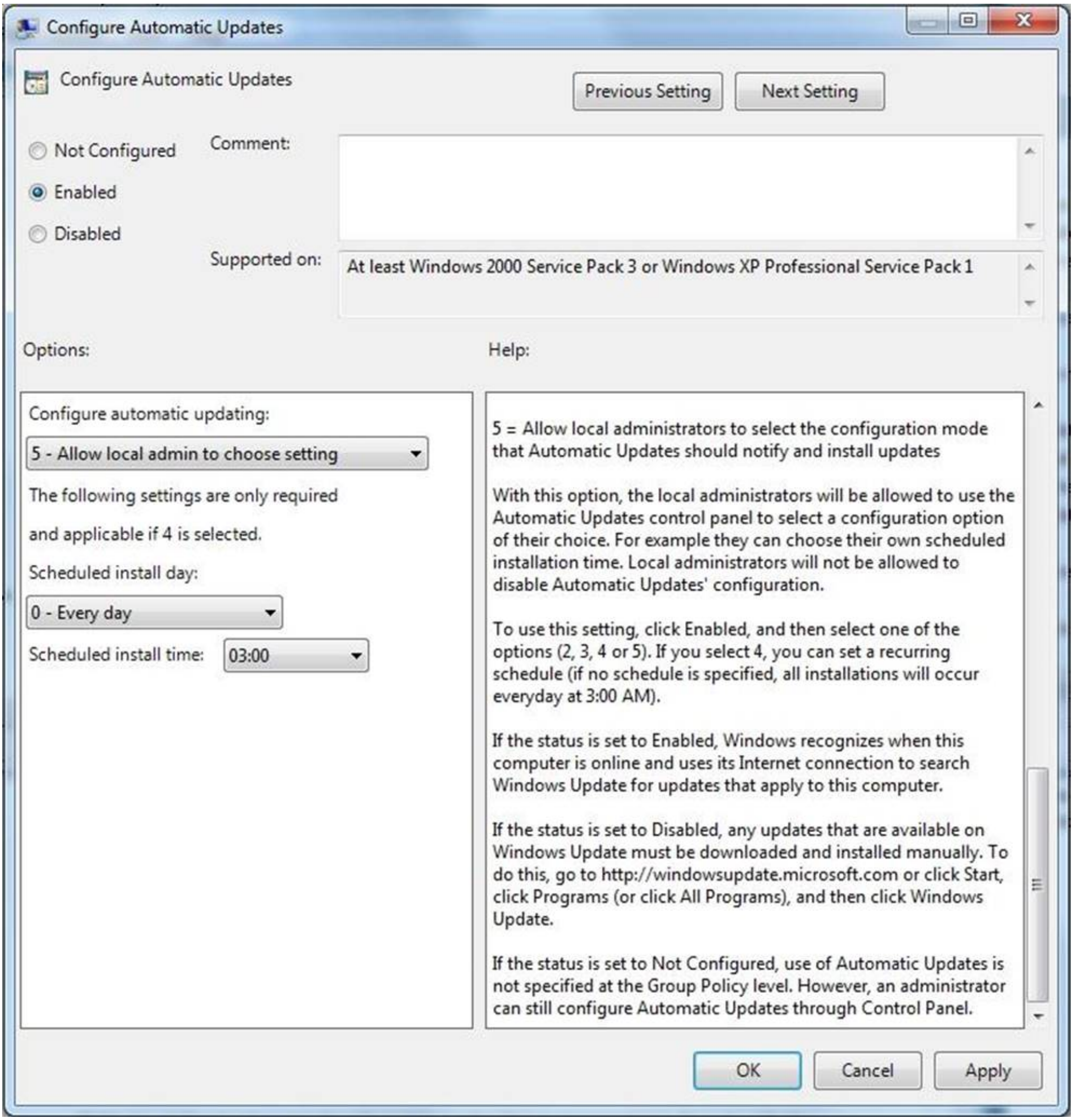


You need to ensure that you can manually change the Windows Update settings on the computer.
What should you do?

A. Log on to Windows 7 as member of the Administrators grou
B. From the local Group Policy, modify the Windows Update setting
C. Right-click Windows Update and select Run as administrato
D. Right-click the command prompt, select Run as administrator, and then run Wuapp.ex

Answer: B

Explanation:
Configuring Automatic Updates by using local Group Policy
1. Click Start, and then click Run.
2. Type gpedit.msc, and then click OK.
3. Expand Computer Configuration.
4. Right-click Administrative Templates, and then click Add/Remove Templates.
5. Click Add, click Wuau.adm in the Windows\Inf folder, and then click Open.
6. Click Close.
7. Under Computer Configuration, expand Administrative Templates, expand Windows Components, and then expand Windows Update.



NEW QUESTION 124
Your network consists of an Active Directory domain and a DirectAccess infrastructure. You install Windows 7 on a new portable computer and join the computer to the domain. You need to ensure that the computer can establish DirectAccess connections.
What should you do?

A. Install a computer certificat
B. Create a new network connectio
C. Enable the Network Discovery firewall exceptio
D. Add the computer account to the Network Configuration Operators grou

Answer: A

Explanation:
Certificates The DirectAccess IPsec session is established when the client running Windows 7 and the DirectAccess server authenticate with each other using computer certificates. DirectAccess supports only certificate-based authentication.DirectAccess Client Configuration Clients receive their DirectAccess configuration through Group Policy. This differs from traditional VPN configuration where connections are configured manually or distributed through the connection manager administration kit. Once you have added the computer's client account to the designated security group, you need to install a computer certificate on the client for the purpose of DirectAccess authentication. An organization needs to deploy Active Directory Certificate Services so that clients can automatically enroll with the appropriate certificates.

NEW QUESTION 129
You have a computer that runs Windows 7.
Your network contains a DHCP server that runs Windows Server 2008 R2.
The server is configured as a Network Access Protection (NAP) enforcement point.
You need to configure the computer as a NAP client.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. From Services, set the Netlogon service Startup Type to Automati
B. From Services, set the Network Access Protection Agent service Startup Type to Automati
C. From the NAP Client Configuration console, configure the user interface setting
D. From the NAP Client Configuration console, enable the DHCP Quarantine Enforcement Clien

Answer: BD

Explanation:
Network Access Protection Network Access Protection (NAP) is a feature in Windows Server 2008 that controls access to network resources based on a client computer's identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.NAP Client ConfigurationNetwork Access Protection (NAP), a new feature in Windows Vista. and Windows Server. 2008, allows you to control the access of client computers to network resources based on computer identity and compliance with corporate governance policy. To implement NAP, you must configure NAP settings on both servers and client computers. There are three tools that you can use to configure NAP client settings: The NAP Client Configuration console provides a graphical user interface with which you can configure NAP client settings on the local computer or in a configuration file that you can save and apply to other computers. The Netsh commands for NAP client provide a command-line tool that you can use to configure client computers or to create a configuration file that you can save and apply to other computers. If you want to manage NAP client settings on domain member client computers, you can use the Group Policy Management Console and the Group Policy Management Editor. When you configure NAP client settings in Group Policy, these settings are applied on NAP-capable domain member client computers when Group Policy is refreshed.To enable and disable the DHCP enforcement client by using the Windows interface
1. To open the NAP Client Configuration console, click Start, click All Programs, click Accessories, click Run, type NAPCLCFG.MSC, and then click OK.
2. Click Enforcement Clients.
3. Right-click DHCP Enforcement Client, and then click Enable or Disable.Network Access Protection Agent
The Network Access Protection (NAP) agent service collects and manages health information for client computers on a network. Information collected by NAP agent is used to make sure that the client computer has the required software and settings. If a client computer is not compliant with health policy, it can be provided with restricted network access until its configuration is updated. Depending on the configuration of health policy, client computers might be automatically updated so that users quickly regain full network access without having to manually update their computer.

NEW QUESTION 134
Your network has a main office and a branch office. The branch office has five client computers that run Windows 7. All servers are located in the main office. All servers have BranchCache enabled.
Users at the branch office report that it takes several minutes to open large files located in the main office.
You need to minimize the amount of time it takes for branch office users to open files located in the main office.
The solution must also reduce the amount of bandwidth used between the two offices.
What should you do?

A. At the main office, configure the Quality of Service (QoS) Packet Scheduler on all server
B. At the main office, configure the servers to use Background Intelligent Transfer Service (BITS).
C. At the branch office, configure the client computers to use BranchCache Hosted Cache mod
D. At the branch office, configure the client computers to use BranchCache Distributed Cache mod

Answer: D

Explanation:
Distributed Cache ModeDistributed Cache mode uses peer caching to host the branch office cache among clients running Windows 7 on the branch office network. This means that each Distributed Cache mode client hosts part of the cache, but no single client hosts all the cache. When a client running Windows 7 retrieves content over the WAN, it places that content into its own cache. If another BranchCache client running Windows 7 attempts to access the same content, it is able to access that content directly from the first client rather than having to retrieve it over the WAN link. When it accesses the file from its peer, it also copies that file into its own cache. The advantage of distributed cache mode is that you can deploy it without having to deploy a server running Windows Server 2008 R2 locally in each branch office. The drawback of Distributed Cache mode is that the contents of the cache available on the branch office LAN depend on which clients are currently online. If a client needs a file that is held in the cache of a computer that is shut down, the client needs to retrieve the file from the host server across the WAN.Hosted Cache ModeHosted Cache mode uses a centralized local cache that hosted on a branch office server running Windows Server 2008 R2. You can enable the hosted cache server functionality on a server running Windows Server 2008 R2 that you use for other functions without a significant impact on performance. This is because if you found that files hosted at another location across the WAN were being accessed so frequently that there was a performance impact, you would use a solution like Distributed File System (DFS) to replicate them to the branch office instead of using BranchCache. The advantage of Hosted Cache mode over Distributed Cache mode is that the cache is centralized and always available. Parts of the distributed cache become unavailable when the clients hosting them shut down.Background Intelligent Transfer Service (BITS)The Background Intelligent Transfer Service (BITS) has two role services: the Compact Server and the IIS Server Extension. The Compact Server is a stand-alone HTTP or HTTPS file server, whereas the IIS Server Extension is an Internet Information Services (IIS) plug-in that requires a server running IIS. IIS Server ExtensionThe BITS IIS Server Extension lets you configure a server that is running IIS to allow BITS clients to perform background, resumable file uploads to IIS virtual directories. On completion of a file upload, the BITS Server can notify a Web application of the newly uploaded file. This allows the application to process the uploaded file. The Web application can then optionally reply to the client responsible for the upload.Compact ServerThe BITS Compact Server is a stand-alone HTTP or HTTPS file server, which allows applications to host files for BITS clients to download, and allows the asynchronous transfer of a limited number of large files between computers.QoS Packet SchedulerThe Quality of Service Packet Scheduler is a Windows platform component that is enabled by default on Windows Vista. and Windows XP computers. It is, however, not enabled by default on Windows 2003 computers. This scheduler is designed to control the IP traffic for various network services, including Real Time Communications traffic. This component must be installed and enabled if the QoS markings described earlier for audio and video traffic are to be implemented by the IP stack.

NEW QUESTION 136
You are configuring static IPv4 addresses for two computers, Perth and Brisbane, on an isolated private wired subnet. You configure Perth with the IPv4 address

172.16.10. 140 and the subnet mask 255.255.255.0. You configure Brisbane with the IPv4 address 172.16.10. 210 and the subnet mask 255.255.255.0. You enter ping 172.16.10.140 on Brisbane, but the command times out. Similarly, entering ping 172.16.10.210 on Perth fails to locate the Brisbane computer's IPv4 address. What is the likely reason for this lack of connectivity?

A. DNS service is not available on the subne
B. The computers should have different subnet mask
C. You have not specified a default gatewa
D. You need to permit ICMPv4 traffic through the firewalls of both computer

Answer: D

NEW QUESTION 140
Federated Search connectors are installed using what method?

A. Purchase the Federated Search Installation Tool Pack online and buying individual search connectors from website
B. Download an .osdx file from a valid sourc
C. Double click on the downloaded file and choose Add to instal
D. Go to Microsoft's websit
E. Only vendors who have signed up with the Microsoft Federated Search Tool Writers Guild can participat
F. Go to Amazon.com and download the Shared Resource Kit for Federated Searche

Answer: B

NEW QUESTION 142
Which of the following utilities can you use to transfer user encryption certificates from a computer running Windows XP Professional to Windows 7 Professional? Choose two.

A. File Settings and Transfer Wizard
B. USMT
C. Windows Easy Transfer
D. Robocopy.exe

Answer: BC

NEW QUESTION 143
Your network contains a wireless access point. You have a computer that runs Windows 7. The computer connects to the wireless access point.
You disable Service Set Identifier (SSID) broadcasts on the wireless access point.
You discover that you are now unable to connect to the wireless access point from the Windows 7 computer.
You need to ensure that the computer can connect to the wireless access point.
What should you do?

A. From Credential Manager, modify the generic credential
B. From Credential Manager, modify the Windows credential
C. From Network and Sharing Center, turn on Network discover
D. From Network and Sharing Center, modify the wireless network connection setting

Answer: D

Explanation:
Wireless Network Connection settingsTo connect to a wireless network that does not broadcast its SSID, you need to know details such as the network name and security type. In Network And Sharing Center, you click Set Up A Connection Or Network, click Manually Connect To A Wireless Network, and click Next. You are prompted for the network name and security type and (if appropriate) encryption type and security key. Alternatively, you can open an elevated command prompt and enter a command with the following syntax: netsh wlan connect name=<profile_name> ssid-<network_ssid> [interface=<interface_name>] (Since the computer has previously been connected, just modify the settings.)NOT Network DiscoveryNetwork Discovery allows the client running Windows 7 to locate other computers and devices on the network. It also makes the client visible to other computers on the network. Disabling Network Discovery does not turn off other forms of sharing.NOT Credential ManagerCredential Manager stores logon user name and passwords for network resources, including file servers, Web sites, and terminal services servers. Credential Manager stores user name and password data in the Windows Vault. You can back up the Windows Vault and restore it on other computers running Windows 7 as a method of transferring saved credentials from one computer to another. Although Credential Manager can be used to back up some forms of digital certificates, it cannot be used to back up and restore the self-signed Encrypting File System (EFS) certificates that Windows 7 generates automatically when you encrypt a file. For this reason, you must back up EFS certificates using other tools. You will learn about backing up EFS certificates later in this lesson.

NEW QUESTION 147
Which of the following operating systems support an offline migration using USMT? Choose three.

A. Windows 2000 Professional
B. Windows XP Professional
C. Windows Vista
D. Windows 7

Answer: BCD

NEW QUESTION 150
You have a computer that runs Windows 7.
You discover that an application named App1 runs during the startup process.
You need to prevent only App1 from running during startup. Users must be allowed to run App1 manually.
What should you do?

A. From the local Group Policy, modify the application control polic
B. From the local Group Policy, modify the software restriction polic
C. From the System Configuration tool, select Diagnostic Startu
D. From the System Configuration tool, modify the Startup application

Answer: D

NEW QUESTION 155
Which of the following is not a rating for games in Windows 7?

A. General Audience (G)
B. Everyone (E)
C. Teen (T)
D. Adults Only (AO)

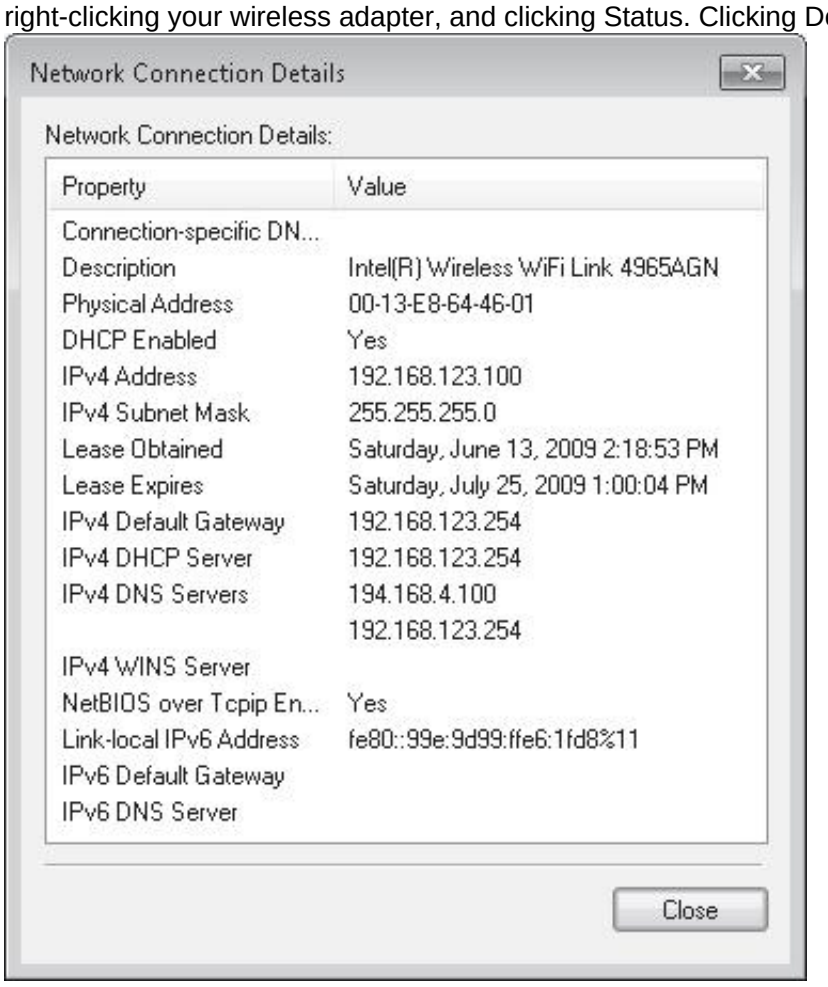
Answer: A

NEW QUESTION 157
You have a computer that runs Windows 7.
The IPv6 address of the computer is configured automatically.
You need to identify the IPV6 address of the computer.
What should you do?

A. At the command prompt, run Netsta
B. At the command prompt run Net confi
C. From the network connection status, click Detail
D. From network connection properties, select Internet Protocol Version 6 (TCP/IPv6) and click Propertie

Answer: C

Explanation: You can view a list of all the connection interfaces (wired and wireless) on a computer by opening Network And Sharing Center and clicking Change Adapter Settings. You can right-click any network connection and select Status. If you click Details on the Local Area Connection Status dialog box, you access the Network Connection Details information box. You can configure wireless connection behavior by clicking Change Adapter Settings in Network And Sharing Center, right-clicking your wireless adapter, and clicking Status. Clicking Details on the Status dialog box displays the adapter configuration.



NEW QUESTION 159
Which of the following can be used to increase the physical memory on your Windows 7 PC and increase the speed?

A. PhysiRAM
B. Aero Glass
C. DirectAccess
D. ReadyBoost

Answer: D

NEW QUESTION 160
You have a computer that runs Windows 7.
Your network contains a VPN server that runs Windows Server 2008.
You need to authenticate to the VPN server by using a smart card.
Which authentication setting should you choose?

A. CHAP
B. EAP
C. MS-CHAP v2
D. PAP

Answer: B

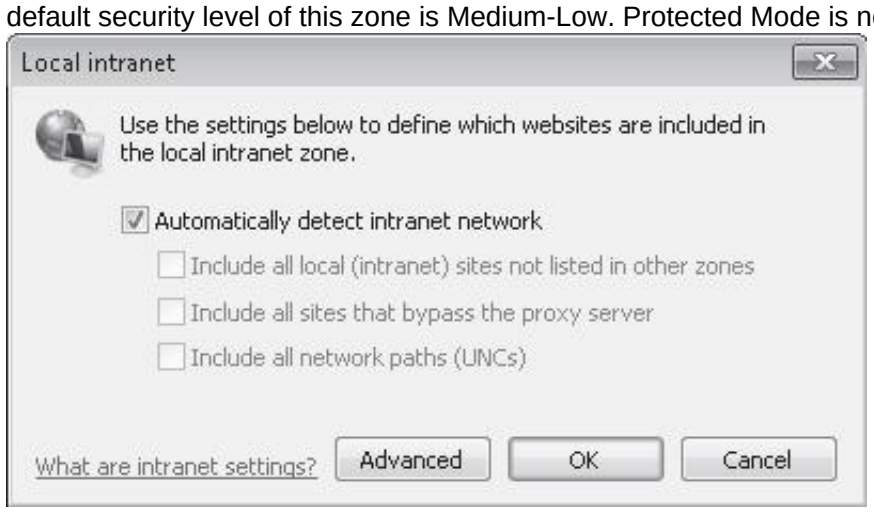
Explanation:
VPN Server Software Requirements VPN server software requirements for smart card access are relatively straightforward. The remote access servers must run Windows 2000 Server or later, have Routing and Remote Access enabled, and must support Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). EAP-TLS is a mutual authentication mechanism developed for use in conjunction with security devices, such as smart cards and hardware tokens. EAP-TLS supports Point-to-Point Protocol (PPP) and VPN connections, and enables exchange of shared secret keys for MPPE, in addition to Ipsec. The main benefits of EAP-TLS are its resistance to brute-force attacks and its support for mutual authentication. With mutual authentication, both client and server must prove their identities to each other. If either client or server does not send a certificate to validate its identity, the connection terminates.Microsoft Windows Server. 2003 supports EAP-TLS for dial-up and VPN connections, which enables the use of smart cards for remote users. For more information about EAP-TLS, see the Extensible Authentication Protocol (EAP) topic at www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/auth_eap. mspx. For more information about EAP certificate requirements, see the Microsoft Knowledge Base article "Certificate Requirements when you use EAP-TLS or PEAP with EAP-TLS" at http://support.microsoft.com/default.aspx? scid=814394.

NEW QUESTION 161
Your company has an Active Directory domain. All computers are members of the domain.
Your network contains an internal Web site that uses Integrated Windows Authentication.
From a computer that runs Windows 7, you attempt to connect to the Web site and are prompted for authentication.
You verify that your user account has permission to access the Web site.
You need to ensure that you are automatically authenticated when you connect to the Web site.
What should you do?

A. Create a complex password for your user accoun
B. Open Credential Manager and modify your credential
C. Add the URL of the Web site to the Trusted sites zon
D. Add the URL of the Web site to the Local intranet zon

Answer: D

Explanation:
Local Intranet Sites in the Local Intranet zone are computers on your organizational intranet. Internet Explorer can be configured to detect intranet sites automatically. It is also possible to add Web sites to this zone by clicking the Advanced button on the Local Intranet sites dialog box, as shown in the figure. The default security level of this zone is Medium-Low. Protected Mode is not enabled by default for sites in this zone.



Security settings are configured primarily by assigning sites to zones. Sites that require elevated privileges should be assigned to the Trusted Sites zone. Sites that are on the intranet are automatically assigned to the Local Intranet zone, though this may require manual configuration in some circumstances. All other sites are assigned to the Internet zone. The Restricted Sites zone is used only for Web sites that may present security risks but must be visited.

NEW QUESTION 164
A user reports that he is unable to start his computer. He provides the following information:
. The boot partition is encrypted by using BitLocker Drive Encryption (BitLocker).
. The user cannot locate his BitLocker recovery key.
You need to start Windows 7 on the computer. The solution must use the minimum amount of administrative effort.
What should you do?

A. From the BIOS, disable the Trusted Platform Module (TPM).
B. Start the computer from the Windows 7 installation media and select Repair your compute
C. Start the computer from the Windows 7 installation media, press SHIFT+F10, and then run CHKDS
D. Start the computer from the Windows 7 installation media and select Install no

Answer: D

Explanation:
No recovery key = no recovery. Time to install.
Any other option defeats the whole point of encrypting it.
Encrypted volumes are locked when the encryption key is not available. When the operating system volume is locked, you can boot only to recovery mode. In recovery mode, you can enter the BitLocker password or you can attach the USB device that has the recovery key stored and restart the computer. Once you enter the recovery password or key, you can boot your computer normally.
The following events trigger recovery mode:
* The boot environment changes. This could include one of the boot files being modified.
* TPM is disabled or cleared.

* An attempt is made to boot without the TPM, PIN, or USB key being provided.
* You attach a BitLocker-encrypted operating system volume to another computer.

NEW QUESTION 167
You have a computer that runs windows 7.
You have an application installation package named app1.msi.
You need to perform a customized installation of app1.msi.
What should you do?

A. Create a transform file named app1.mst and then run Msiexec.exe /i app1.msi /t app1.ms
B. Create a transform file named app1.mst and then run Msinfo.exe /I app1.msi /
C. Create a transform file named app1.msp and then run Msiexec.exe /I app1.msi /app1.
D. Create a transform file named app1.msp and then run Msinfo32.exe /I app1.mst /.

Answer: A

Explanation:
Windows Installer Transform Files A Windows Installer transform (.mst) file provides configuration settings for a customized installation. A transform file contains information about components, features, setup properties, and changes that you can use to customize your installation.
MsiexecProvides the means to install, modify, and perform operations on Windows Installer from the command line. To install or configure a product Syntax msiexec /i {package|ProductCode} /i: Installs or configures a product. /t : Applies transform to advertised package.NOT Msinfo32 Displays a comprehensive view of your hardware, system components, and software environment.

NEW QUESTION 170
You have a computer that runs Windows Vista.
You install Windows 7 on a new partition on the computer.
You need to ensure that the computer always starts Windows Vista by default.
What should you do?

A. Run Bcdedit.exe and specify the /default paramete
B. Run Bcdedit.exe and specify the /bootems paramete
C. Create a boot.ini file in the root of the Windows 7 partitio
D. Create a boot.ini file in the root of the Windows Vista partitio

Answer: A

Explanation:
The Bcdedit.exe utility allows you to manage boot configuration./default - Sets the default entry that the boot manager willl use./bootems - Enable or disables Emergency Management Services for a boot application.NOT boot.ini:Windows (specifically Ntldr) uses

NEW QUESTION 175
You have a computer that runs Windows 7.
You perform regular data backups and system image backups. The computer experiences a hard disk failure. You replace the failed hard disk.
You need to recover the computer to the previous Windows 7 environment.
You start the computer from the Windows 7 installation media.
Which recover option should you select?

A. Command Prompt
B. Startup Repair
C. System Image Recovery
D. System Restore

Answer: C

Explanation:
System Image Recovery Enables you to implement a System Image restore. You would choose this option if your hard disk failed or needed to be wiped. If system changes are causing problems, you would choose the System Restore option.NOT Startup Repair Automatically fixes problems that prevent Windows from starting. If Windows 7 had boot problems during a previous restart, a normal boot (without accessing the Advanced Boot dialog box) gives you the option of selecting Startup Repair.NOT System Restore Gives you another method of starting a system restore to a previous restore point. Because you can access this menu when you boot from a DVD-ROM, this lets you repair your system when recent changes to system settings prevent your computer from booting normally.NOT Command Prompt Gives access to the file system, volumes, and files through a command-line interface.

NEW QUESTION 177
Your company's chief accountant consults you with a question about a financial spreadsheet. She needs to recover the version of this particular spreadsheet that existed six months ago because it is needed for a financial audit. Using Restore Previous Versions, you find that the oldest version stored is dated three months ago. How can you recover the required file?

A. Edit the System Protection properties for the volume that hosts the fil
B. Use the Max Usage slider to increase the maximum proportion of the hard disk capacity used for system protection to 70 percen
C. Perform a system restor
D. Select a system restore point that was created six months ag
E. Edit the System Protection properties for the volume that hosts the fil
F. Select the Only Restore Previous Versions Of Files settin
G. Use the Backup And Restore console to recover the file from a backup set generated six months ag

Answer: D

NEW QUESTION 180
You have a computer that runs Windows Vista (x86).
You need to perform a clean installation of Windows 7 (64-bit).
What should you do?

A. From the Windows 7 installation media, run Rollback.ex
B. From the Windows 7 installation media, run Migsetup.ex
C. Start the computer from the Windows 7 installation medi
D. From the Install Windows dialog box, select the Upgrade optio
E. Start the computer from the Windows 7 installation medi
F. From the Install Windows dialog box, select the Custom (advanced) optio

Answer: D

Explanation:
When you are performing a clean installation, you should select Custom (Advanced). Almost all installations ofm Windows 7 that you will perform will be of the Custom (Advanced) type rather than upgrades. You can initiate upgrade installations only from within Windows Vista or Windows 7.NOT Rollback, Migsetup, or Upgrade:Specified clean installation not migration, update or rollback.

NEW QUESTION 184
An employee who works from home telephones your help desk. A virus attack has deleted his computer's single internal hard disk. He carried out a System Image backup on his computer three months ago and automatically backs up his personal files every night. He uses an external USB hard drive formatted with the NTFS file system to hold his backups.
All his personal files are in his Documents library. What do you advise? (Choose all that apply; the answers form a complete solution.)

A. Carry out a System Image restor
B. Carry out a system restor
C. Use Restore Previous Versions to restore his Documents library from a shadow cop
D. Use Restore My Files in the Backup And Restore console to restore his Documents library folde

Answer: AD

NEW QUESTION 188
You have a computer that runs Windows 7. The computer contains one hard disk. The hard disk is configured as shown in the following table.

Partition	Size
C	100 GB
D	100 GB
Unallocated	50 GB

You install a new 250-GB hard disk in the computer.
You need to ensure that all the files on the computer are available if a single disk fails.
What should you do?

A. Create a mount point on C and D and then create a striped volum
B. Create a mount point on C and D and then create two striped volume
C. Convert both disks to dynamic disks and then create a mirrored volum
D. Convert both disks to dynamic disks and then create two mirrored volume

Answer: D

Explanation:
Creating a Mirrored Volume (RAID-1)A mirrored or RAID-1 volume provides availability and fault tolerance but does not improve performance. It uses two disks (or two portions on separate disks) that are the same size. Any changes made to the first disk of a mirror set are also made to its mirror disk. If the first disk fails, the mirror is broken and the second disk is used until the first is repaired or replaced. The mirror is then re-created, and the information on the working disk is mirrored on the repaired disk. The disadvantage of RAID-1 is that you need (for example) two 200-GB disks to hold 200 GB of data. The advantage is that you can mirror a system disk containing your operating system.You create a mirrored volume using a very similar procedure to the one that creates a striped volume, except that you right-click the first disk of your mirror and click New Mirrored Volume to start the appropriate wizard. You then select the second disk. The second disk needs to have a portion of unallocated space that is at least as large as the disk you want to mirror. The drive letter for a mirrored volume is the same as the drive letter of the first disk. You can also use the Diskpart tool to create a mirrored volume. At the DISKPART> prompt you first use the select disk command to select the first disk. You then enter a command with the syntax add disk=<n>to specify the mirror disk.

NEW QUESTION 189
You have a computer that runs Windows 7. You connect to your company's network by using a VPN connection.
You discover that when you establish the VPN connection, you are unable to access Internet Web sites.
When you disconnect the VPN connection, you can access Internet Web sites.
You need to access Internet Web sites while you are connected to the VPN.
What should you do?

A. Configure the VPN connection to use only PPT
B. Configure the VPN connection to use only L2TP/IPSe
C. From the Internet Protocol Version 4 (TCP/IPv4) properties of the local area connection, disable the Automatic metric settin
D. From the Internet Protocol Version 4 (TCP/IPv4) properties of the VPN connection, disable the Use default gateway on remote network settin

Answer: D

Explanation:
To prevent the default route from being created In the properties of the TCP/IP protocol of the dial-up connection object, in the Advanced TCP/IP Settings dialog box, click the General tab, and then clear the Use default gateway on remote network check box.

NEW QUESTION 194
You have a computer that runs Windows 7. The computer is in a workgroup.
You need to ensure that you can decrypt Encrypting File System (EFS) files on the computer if you forget your password.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A. From Credential Manager, select Back up vaul
B. From User Accounts, select Create a password reset dis
C. From User Accounts, select Manage your file encryption certificate
D. From Authorization Manager, modify the Authorization Manager option

Answer: BC

Explanation:
Password reset disks It is not unusual for users to forget their passwords to local user accounts from time to time, especially when they use strong passwords. Before the advent of password reset disks, the only way for administrators to restore a forgotten local user account password was to manually reset the user's password. In the process, the following information was lost: E-mail that was encrypted with the user's public key Internet passwords that were saved on the computer Files that the user had encrypted Password reset disks offer another solution to the problem of a forgotten password for a local user account. If users create password reset disks for their local accounts before they forget their passwords, they can reset the passwords without losing valuable data that was lost previously with administrative password resets. When you create a password reset disk, a public key and private key pair are created. The private key is stored on a disk: the password reset disk. The public key encrypts the local user account password. If users forget their passwords, they can insert the password reset disk, which contains the private key, and decrypt the current password. The Forgotten Password Wizard prompts the user for a new password, which is then encrypted with the public key. Data is not lost because, basically, the user is simply changing a password. It is essential that password reset disks be stored in secured locations.Back up your Encryption Certificate
1. Open User Accounts by clicking the Start button, clicking Control Panel, clicking User Accounts and Family Safety (or clicking User Accounts, if you are connected to a network domain), and then clicking User Accounts.
2. In the left pane, click Manage your file encryption certificates.
3. In the Encrypting File System wizard, click Next.
4. Click Use this certificate, and then click Next. If you need more details to identify the certificate that is listed, click View certificate. If you want to choose a different certificate, click Select certificate, and then click the certificate
you want to back up.
5. Click Back up the certificate and key now.
6. Type or navigate to the location where you want to store the backup. We recommend that you store the backup on removable media such as a disc or USB flash drive.
7. Type and then confirm a password for the backup file, and then click Next. We recommend that you protect the backup file with a strong password.
8. Select the I'll update my encrypted files later check box, and then click Next.

NEW QUESTION 198
You have a customized image of Windows 7 Professional.
You need to create a new unattended file to automate the deployment of the image. You must achieve this goal by using the minimum amount of administrative effort.
What should you do first?

A. Run Imagex.exe and specify the /mount paramete
B. Run Dism.exe and specify the /mount-WIM paramete
C. From Microsoft Deployment Toolkit (MDT), add the custom Windows image (WIM).
D. From Windows System Image Manager (Windows SIM), open the custom Windows image (WIM).

Answer: D

Explanation:
Windows SIMOpens Windows images, creates answer files, and manages distribution shares and configuration sets.NOT DismDeployment Image Servicing and Management (DISM) is a command-line tool used to service Windows. images offline before deployment. You can use it to install, uninstall, configure, and update Windows features, packages, drivers, and international settings. Subsets of the DISM servicing commands are also available for servicing a running operating system.NOT ImagexImageX is a command-line tool that enables original equipment manufacturers (OEMs) and corporations to capture, to modify, and to apply file-based disk images for rapid deployment. ImageX works with Windows image (.wim) files for copying to a network, or it can work with other technologies that use .wim images, such as Windows Setup, Windows Deployment Services (Windows DS), and the System Management Server (SMS) Operating System Feature Deployment Pack./mountMounts a .wim file from Windows XP with Service Pack 2 (SP2), Windows Server 2003 with Service Pack 1 (SP1), or Windows Vista with read-only permission to a specified directory. Once the file is mounted, you may view, but not modify, all the information contained in the directory.NOT MDT MDT 2010 is the Microsoft solution accelerator for operating system and application deployment and offers flexible driver management, optimized transaction processing, and access to distribution shares from any location. You can use the MDT on imaging and deployment servers to implement the automatic deployment of Windows 7 (for example) on client computers. It is possible to run MDT 2010 on a client running Windows 7, but in practice it would typically run from a distribution server running Windows Server 2008. The MDT provides detailed guidance and job aids and offers a common deployment console that contains unified tools and processes that you can use for client and server deployment. The toolkit offers standardized desktop and server images, along with improved security and ongoing configuration management.

NEW QUESTION 199
You work as the desktop support technician. The network consists of a single Active Directory domain named CK.com.
You need to perform a clean installation of Microsoft Windows 7 Professional on the workstations in the Research department.
All workstations in the Research department have identical hardware as listed below:
1.2 GHz Dual-Core processor.
1024 MB of RAM.
20 GB hard drive.
DirectX 10 video display card.

Integrated sound card.
10/100 integrated network adapter.
You need to ensure that the workstations able to support Windows 7 and are able to support Windows XP mode.
What should you do? (Each correct answer presents part of the solution. Choose two.)

A. You should upgrade the processo
B. You should upgrade the RA
C. You should upgrade the video car
D. You should upgrade the hard driv
E. You should upgrade the network adapte

Answer: BD

NEW QUESTION 201
Kim Akers has an administrator account on a computer running Windows 7 Enterprise.
Don Hall has a standard account on the same computer. Both users have Microsoft Office Word and Microsoft Office Excel files saved in their Documents library.
Don stores Microsoft Office PowerPoint presentations in a subfolder of his Documents library named Presentations. He also stores digital photographs in his Pictures library.
Don has created a folder called Secret in his Documents library and has encrypted the folder and its contents. He stores confidential files in that folder.
When Don last logged on, he deleted some personal files but did not empty his Recycle Bin.
Kim is logged on to the computer. She has plugged in a USB flash memory device that holds personal files but has not yet copied any of these files to the computer. She has never formatted the flash memory device.
The computer is configured to let Windows decide what files and folders to back up.
Kim opens the Backup And Restore console but does not change any settings. She clicks Backup Now.
Which files are backed up? (Choose all that apply.)

A. The Word and Excel files in Don's Documents library
B. The Word and Excel files in Kim's Documents library
C. The PowerPoint files in Don's Presentation folder
D. The digital photographs in Don's Pictures library
E. The files in Don's Secret folder
F. The files in Don's Recycle Bin
G. The files on Kim's USB flash memory device

Answer: ABCD

NEW QUESTION 204
A user telephones your help desk. She has just accidentally deleted a file she was working on earlier that day.
You have configured her computer to carry out backups every evening, and you installed a new graphics driver two days ago.
How should you advise the user to retrieve her file?

A. Open the Backup And Restore console and restore the file from backu
B. Use the Restore Previous Versions feature to restore the fil
C. Open her Recycle Bin, right-click the file, and choose Restor
D. Perform a system restor

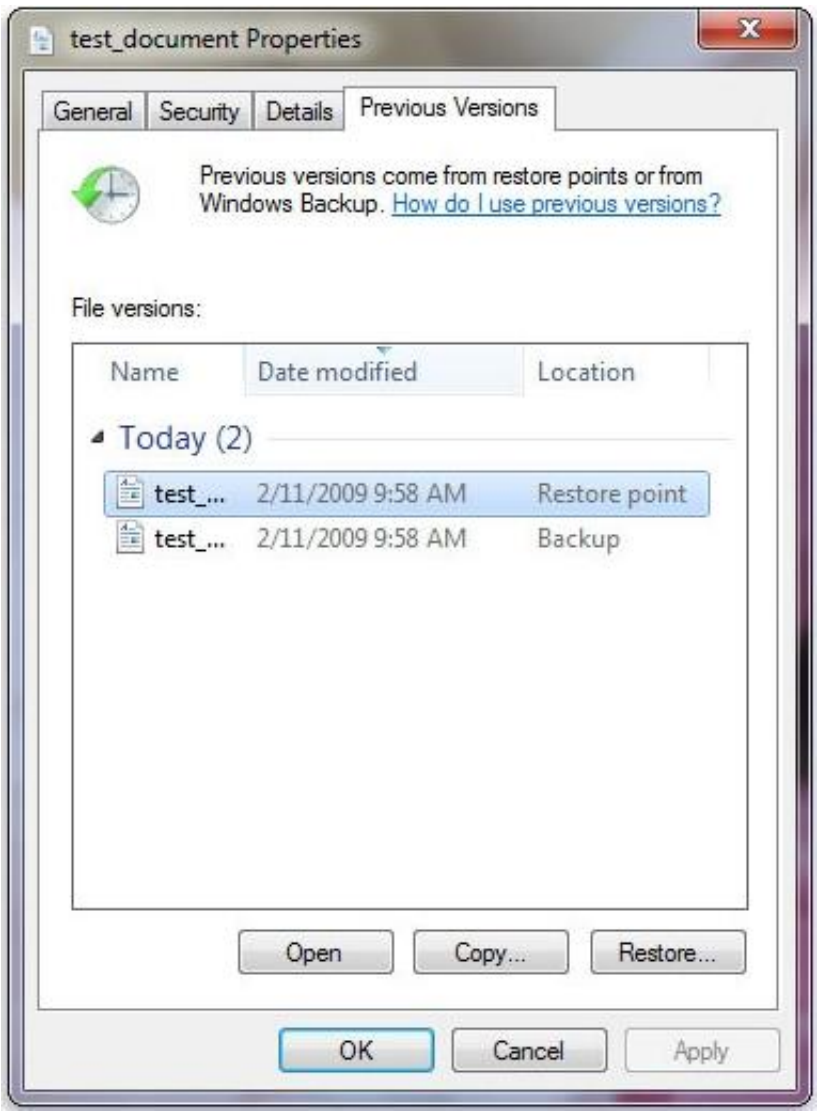
Answer: C

NEW QUESTION 208
You have a computer that runs Windows 7.
You manually create a system restore point.
You need to restore a copy of a file stored on a drive C from two days ago.
You must act with minimum administrative effort.
What should you do?

A. From recovery, select System Restor
B. From Backup and restore, select Rrestore my file
C. From the command prompt, run Wbadmin get item
D. From the properties of the file, select Previous Version

Answer: D

Explanation:
How do I view or restore previous versions of a file and folder? Right-click the file or folder, and then click Restore previous versions. You'll see a list of available previous versions of the file or folder. The list will include files saved on a backup (if you're using Windows Backup to back up your files) as well as restore points. To restore a previous version of a file or folder that's included in a library, right-click the file or folder in the location where it's saved, rather than in the library. For example, to restore a previous version of a picture that's included in the Pictures library but is stored in the My Pictures folder, right-click the My Pictures folder, and then click Restore previous versions. For more information about libraries, see Include folders in a library.



The Previous Versions tab, showing some previous versions of files
NOT System Restore: System Restore restores system files and settings and does not affect any of your documents, pictures, or other personal data.
NOT Backup and Restore: System restore point was created, no backup meantioned.NOT Wbadmin: The Backup And Restore console does not provide a graphical tool for scheduling System Image backups. You need to create a System Image backup manually from the Backup And Restore console whenever you have made significant changes to a computer's configuration. Take care that if you restore a System Image backup and boot from it, or if you make the VHD bootable for failover protection, your computer could be vulnerable unless the System Image includes security updates. Although you cannot use Backup And Restore to schedule System Image backups, you can use the Wbadmin command-line utility to perform this function. For example, to initiate a System Image backup of the C: drive to the H: drive, you run the following command from an elevated command prompt: wbadmin start backup –backuptarget:h: -include:c: -quiet

NEW QUESTION 209
You work as the Desktop support technician at Abc.com. The Abc.com network consists of a single Active Directory domain named Abc.com.
The Abc.com management has instructed you to install Microsoft Windows 7 on all the client computers at Abc.com. You need to create a Windows 7 image that includes the Office 2007
Microsoft Installer Package (MSI) package for the installation.
What should you do?

A. You should consider installing the MSI package by using the update command with the /slipstream switc
B. You should consider installing the MSI package by using the Msiexec command with the /package /uninstall switche
C. You should consider installing the MSI package by using the Msiexec command with the /package switc
D. You should consider installing the MSI package by using the Install command with the /package switc

Answer: C

NEW QUESTION 210
Your network consists of a single Active Directory forest.
You have 50 portable computers and 50 desktop computers. All computers have 32-bit hardware.
You plan to deploy Windows 7 and 10 corporate applications to the computers by using a custom image.
You need to prepare for the deployment by using the minimum amount of administrative effort.
What should you do first?

A. On one computer, install Windows 7 and the corporate application
B. On one portable computer and one desktop computer, install Windows 7 and the corporate application
C. On a server, install and run the Microsoft Assessment and Planning (MAP) Toolki
D. On a server, install the Windows Automated Installation Kit (AIK) and run Windows System Image Manager (Windows SIM).

Answer: A

Explanation:
To prepare the reference computer for the user, you use the Sysprep utility with the /generalize option to remove hardware-specific information from the Windows installation and the /oobe option to configure the computer to boot to Windows Welcome upon the next restart. Open an elevated command prompt on the reference computer and run the following command: c:\windows\system32\sysprep\sysprep.exe /oobe /generalize
/shutdown.
Sysprep prepares the image for capture by cleaning up various user-specific and computerspecific settings, as well as log files. The reference installation now is complete and ready to be imaged.

NEW QUESTION 211

You have a dual boot PC running both Vista and Windows 7 on partitions on the computer. Which file would you edit to force the PC to book Vista by default?

A. boot.ini
B. ntfsboot.cfg
C. bcdedit.exe
D. system.cfg

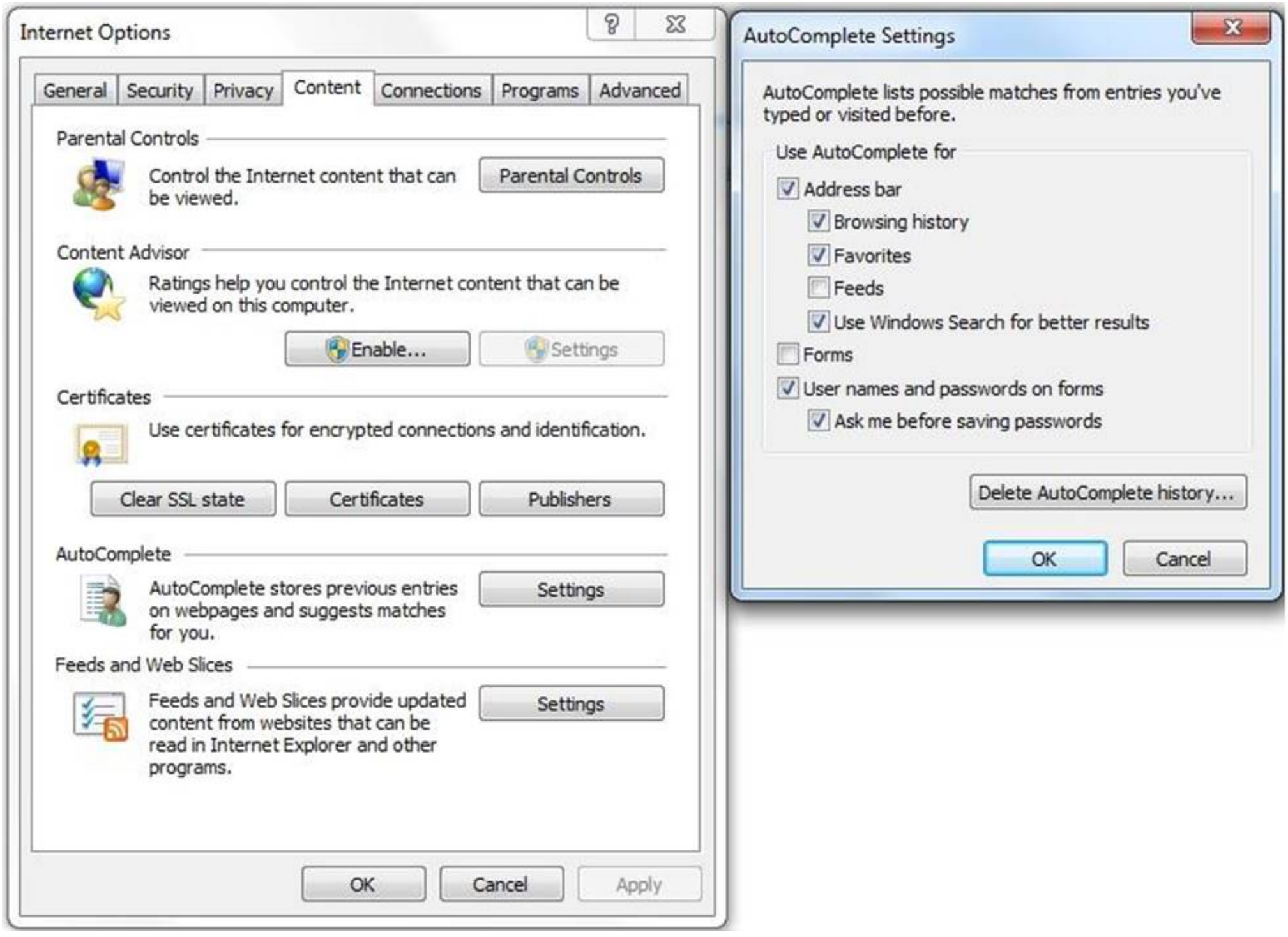
Answer: C

NEW QUESTION 213
Your network contains a public computer that runs Windows 7. Multiple users log on to the computer by using a local user account named User1.
Users report that they can log on to some secure Web sites by using credentials that were saved by other users.
You need to prevent forms-based credentials from being saved on the computer.
What should you do?

A. Remove all generic credentials from Windows Vaul
B. Remove all Windows credentials from Windows Vaul
C. Modify the Windows Internet Explorer certificates setting
D. Modify the Windows Internet Explorer AutoComplete setting

Answer: D

Explanation:
AutoComplete settings AutoComplete is a feature in Internet Explorer that remembers the information you have typed into the Address bar, web forms, or password fields, and which automatically fills in that information if you start to type the same thing again later. This saves you from having to type the same information over and over.



NEW QUESTION 216
You install a local printer on a computer. You share the printer.
You need to ensure that only members of a local group named Group1 can print documents on the printer.
Which settings should you modify on the printer?

A. Printing preferences
B. Priority
C. Security
D. Share

Answer: C

Explanation:
Restricting printer access to selected users by using security groups If you need to restrict the access of certain shared printers to a certain group of network users, do the following:
-Create a security group and then add members to the security group. - Assign printer access permissions.
To create a security group and add member to the group
1. Open the Windows SBS Console.2. On the navigation bar, click the Users and Groups tab, and then click Groups.3. In the task pane, click Add a new group. The Add a New Group Wizard appears. In the Add a New Group Wizard, do the following:1. On the Add a new group page, for Group type, select Security group.2. On the Select groups members for <groupname> page, from the Users and groups list, add the network users who you want to include for the restricted printer access.3. Follow the instructions to complete the wizard. To assign printer access permissions1. Open the Windows SBS Console.2. On the navigation bar, click the Network tab, and then click Devices.3. From the list of printers displayed in the Printers section, click the printer that you want to view the properties for. Then in the task pane, click Printer Properties.4. In the Printer Properties dialog box, click the Security tab, and then remove all entries in the Groups or user names list box except Administrators and Creator Owner.5. To grant access to the printer, click Add, and then enter the names of the group or users that you want to grant access to this printer.

NEW QUESTION 220
You have a Windows 7 Windows image (WIM) that is mounted.
You need to view the list of third-party drivers installed in the image.
What should you do?

A. Run Dism.exe and specify /get-drivers paramete
B. Run Driverquery.exe and specify the /si paramete
C. From Device Manager, view all hidden device
D. From Windows Explorer, open the \Windows\System32\Drivers folder from the mount folde

Answer: A

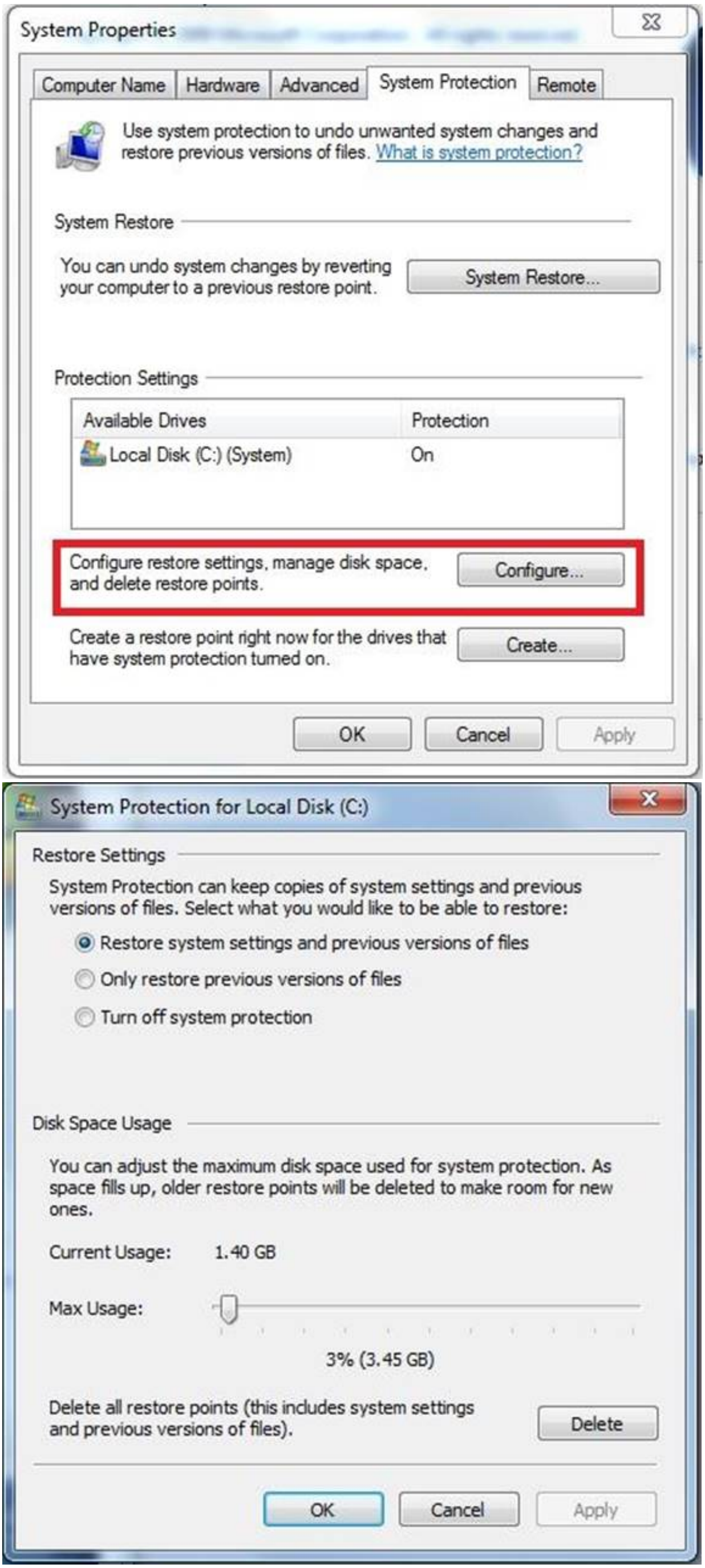
Explanation:
DismDeployment Image Servicing and Management (DISM) is a command-line tool used to service Windows. images offline before deployment. You can use it to install, uninstall, configure, and update Windows features, packages, drivers, and international settings. Subsets of the DISM servicing commands are also available for servicing a running operating system. Windows 7 introduces the DISM command-line tool. You can use DISM to service a Windows image or to prepare a Windows PE image. DISM replaces Package Manager (Pkgmgr.exe), PEimg, and Intlcfg in Windows Vista, and includes new features to improve the experience for offline servicing. You can use DISM to perform the following actions: -Prepare a Windows PE image.
-Enable or disable Windows features within an image.
-Upgrade a Windows image to a different edition.
-Add, remove, and enumerate packages.
-Add, remove, and enumerate drivers.
-Apply changes based on the offline servicing section of an unattended answer file.
-Configure international settings.
-Implement powerful logging features.
-Service operating systems such as Windows Vista with SP1 and Windows Server 2008.
-Service a 32-bit image from a 64-bit host and service a 64-bit image from a 32-bit host.
-Service all platforms (32-bit, 64-bit, and Itanium).
-Use existing Package Manager scripts.
NOT DriverqueryEnables an administrator to display a list of installed device drivers and their properties. If used without parameters, driverquery runs on the local computer. (Could not see documention of images, only computers, therefore assumed this command does not support images) /si : Displays digital signature information for both signed and unsigned device drivers.

NEW QUESTION 222
You have a computer that runs Windows 7.
You need to identify how much disk space is occupied by previous versions.
What should you do?

A. At a command prompt, run Diskpar
B. At a command prompt, run Vaultcm
C. From System, view the System Protection setting
D. From the properties of drive C, view the previous versions setting

Answer: C

Explanation:



NOT Diskpart:
Microsoft command-line tool Diskpart is used to create and format volumes on the target computer.NOT Vaultcmd:Creates, displays and deletes stored credentials.NOT Properties of drive C:Allows you to view contents, but does not show size.

NEW QUESTION 223
You have 20 client computers. The computers run Windows XP. They are joined in a domain.
You plan to perform a clean installation of Windows 7 on the computers.
You need to transfer all users documents and settings. You must exclude music and video files.
You must achieve this goal by using the minimum amount of administrative effort.
What should you do first?

A. Create a config.xml fil
B. Configure a logon script for the Windows XP computers to launch Loadstate.exe
C. Modify the migapp.xml fil
D. Configure a logon script for the Windows XP computers to launch Scanstate.exe
E. Modify the miguser.xml fil
F. Configure a logon script for the Windows XP computers to launch Migwiz.exe
G. Modify the migdocs.xml fil
H. Configure a logon script for the Windows XP computers to launch Scanstate.exe

Answer: D

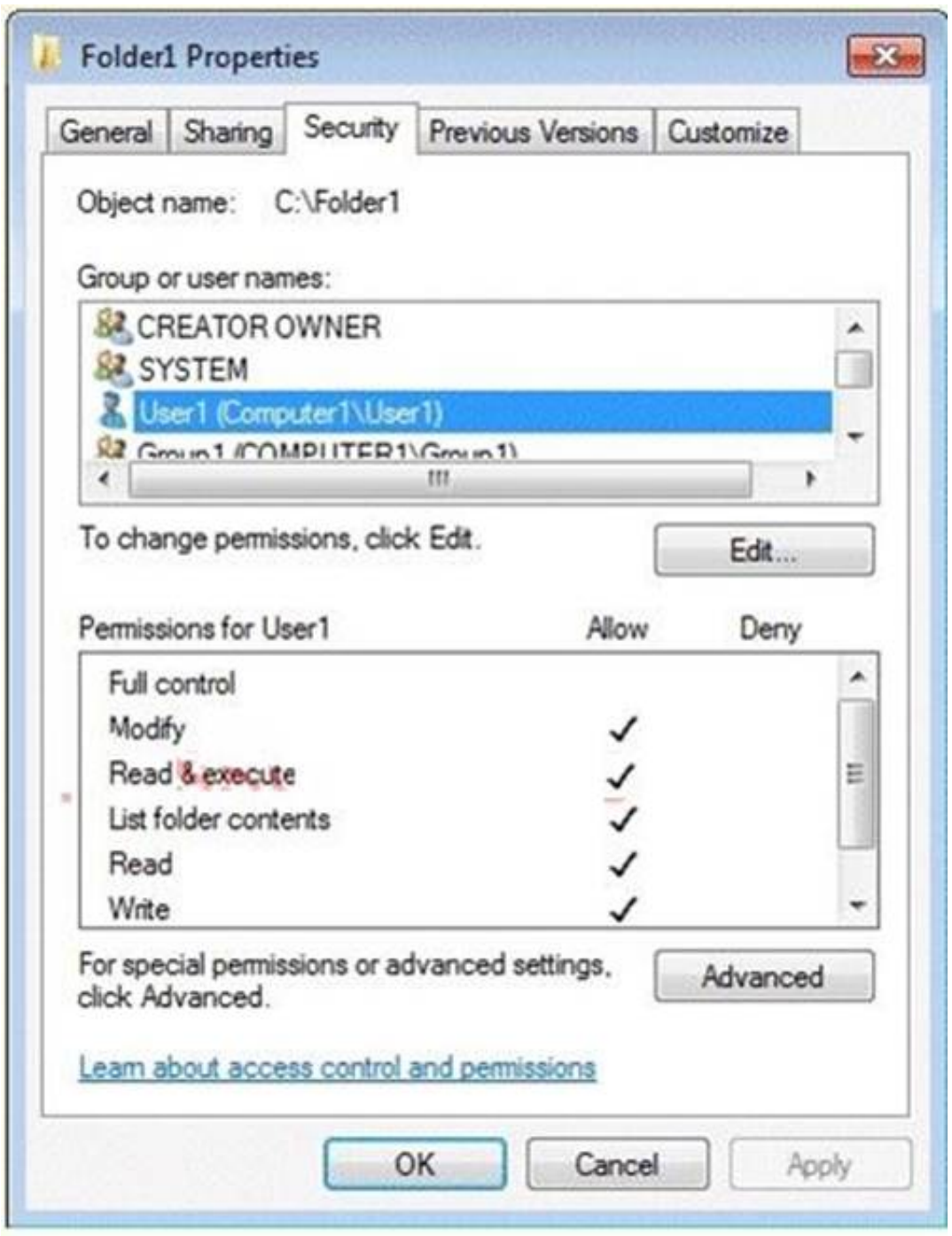
Explanation:
MigDocs.xmlThis file contains information on the location of user documents. NOT Config.xmlThis file is different from the other migration files as it is used to exclude features from the migration. You can create and modify the Config.xml file using ScanState.exe with the /genconfig option.NOT MigUser.xmlMigUser.xml This file contains rules about user profiles and user data. The default settings for this file migrate all data in My Documents, My Video, My Music, My Pictures, desktop files, Start Menu, Quick Launch settings, favorites, Shared Documents, Shared Video, Shared Music, Shared desktop files, Shared Pictures, Shared Start menu, and Shared Favorites. This file also contains rules that ensure that all the following file types are migrated from fixed volumes: .qdf, .qsd, .qel, .qph, .doc, .dot, .rtf, .mcw, .wps, .scd, .wri, .wpd, .xl*, .csv, .iqy, . dqy, .oqy, .rqy, .wk*, .wq1, .slk, .dif, .ppt*, .pps*, .pot*, .sh3, .ch3, .pre, .ppa, .txt, .pst, .one*, .mpp, .vsd, .vl*, .or6, accdb, .mdb, .pub, .xla, .xlb and .xls. The asterisk (*) represents zero or more characters.NOT MigApp.xml This file contains rules about migrating application settings. These include Accessibility settings, dial-up connections, favorites, folder options, fonts, group membership, Open Database Connectivity (ODBC) settings, Microsoft Office Outlook Express mailbox files, mouse and keyboard settings, phone and modem options, Remote Access Service (RAS) connection phone book files, regional options, remote access, screen-saver settings, taskbar settings, and wallpaper settings.

NEW QUESTION 227
You have 20 client computers. The computers run Windows XP. The computers are joined to a domain.
You plan to perform installation of Windows 7 on the computers.
You need to transfer all users' documents and settings. You must exclude music and video files.
You need to use the minimum amount of administration effort.
What should you do first?

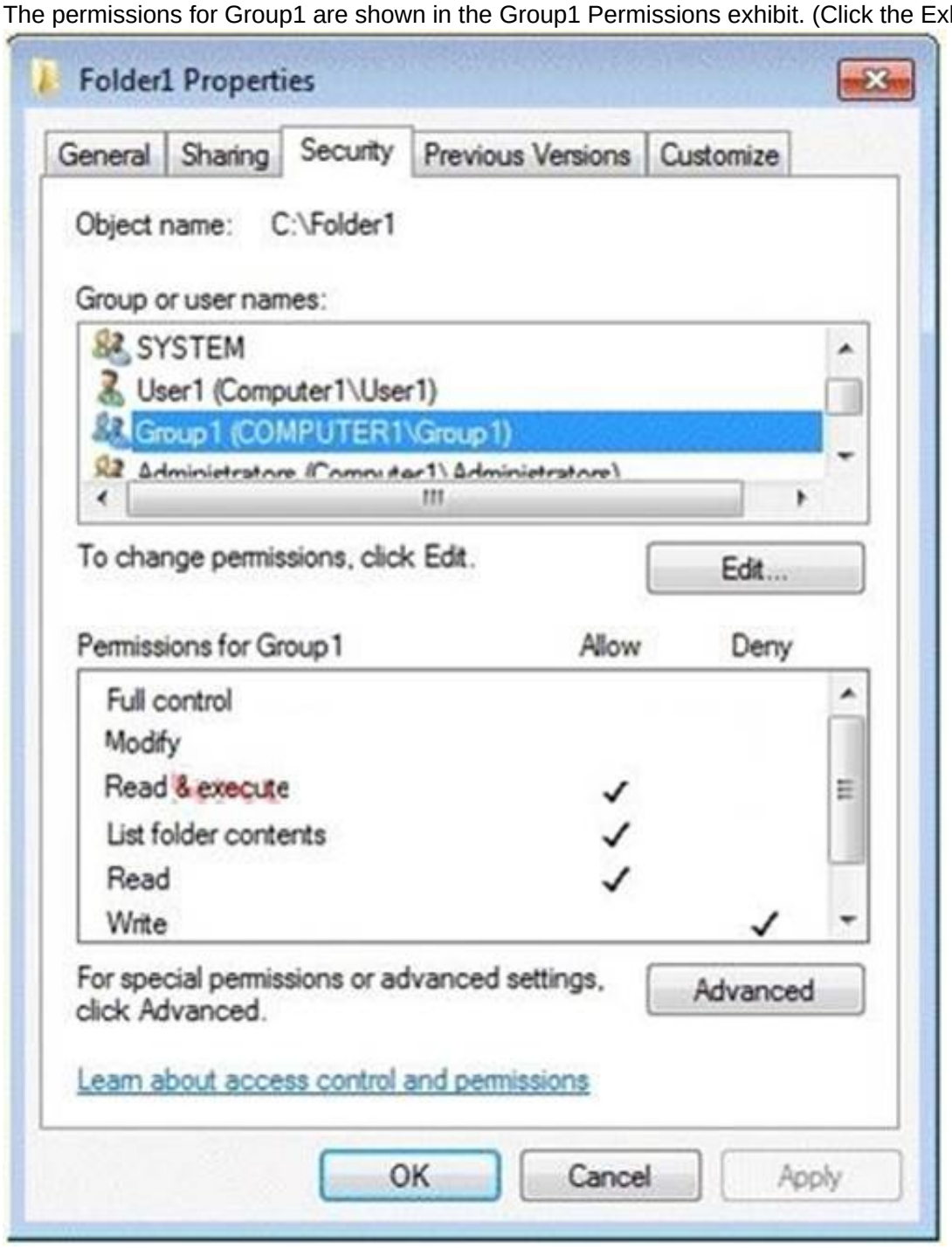
A. Create a config.xml fil
B. Configure a logon script for windows XP computers to launch Windows 7 installation
C. Modify the migapp.xml fil
D. Configure a logon script for the Windows XP computer to launch Windows 7 installatio
E. Modify the miguser.xml fil
F. Configure a logon script for the Windows XP computer to launch Windows 7 installatio
G. Modify the migdocs.xml fil
H. Configure a logon script for the Windows XP computer to launch Windows 7 installatio

Answer: D

NEW QUESTION 228
A user named User1 uses a shared computer that runs Windows 7. User1 is a member of group named
Group1. The computer contains a folder named Folder1. The permissions for User1 are shown in the User1 Permissions exhibit. (Click the Exhibit button.)



The permissions for Group1 are shown in the Group1 Permissions exhibit. (Click the Exhibit button.)



You need to ensure that User1 can create files in Folder1. All other members of Group1 must be prevented from creating files in Folder1. What should you do?

A. On Folder1, assign the Full control permission to User1.
B. On Folder1, remove the Deny - Write permission for Group1.
C. Share Folder1. Assign User1 the Read and Change share permissio
D. Share Folder1. Assign Group1 the Read and Change share permissio

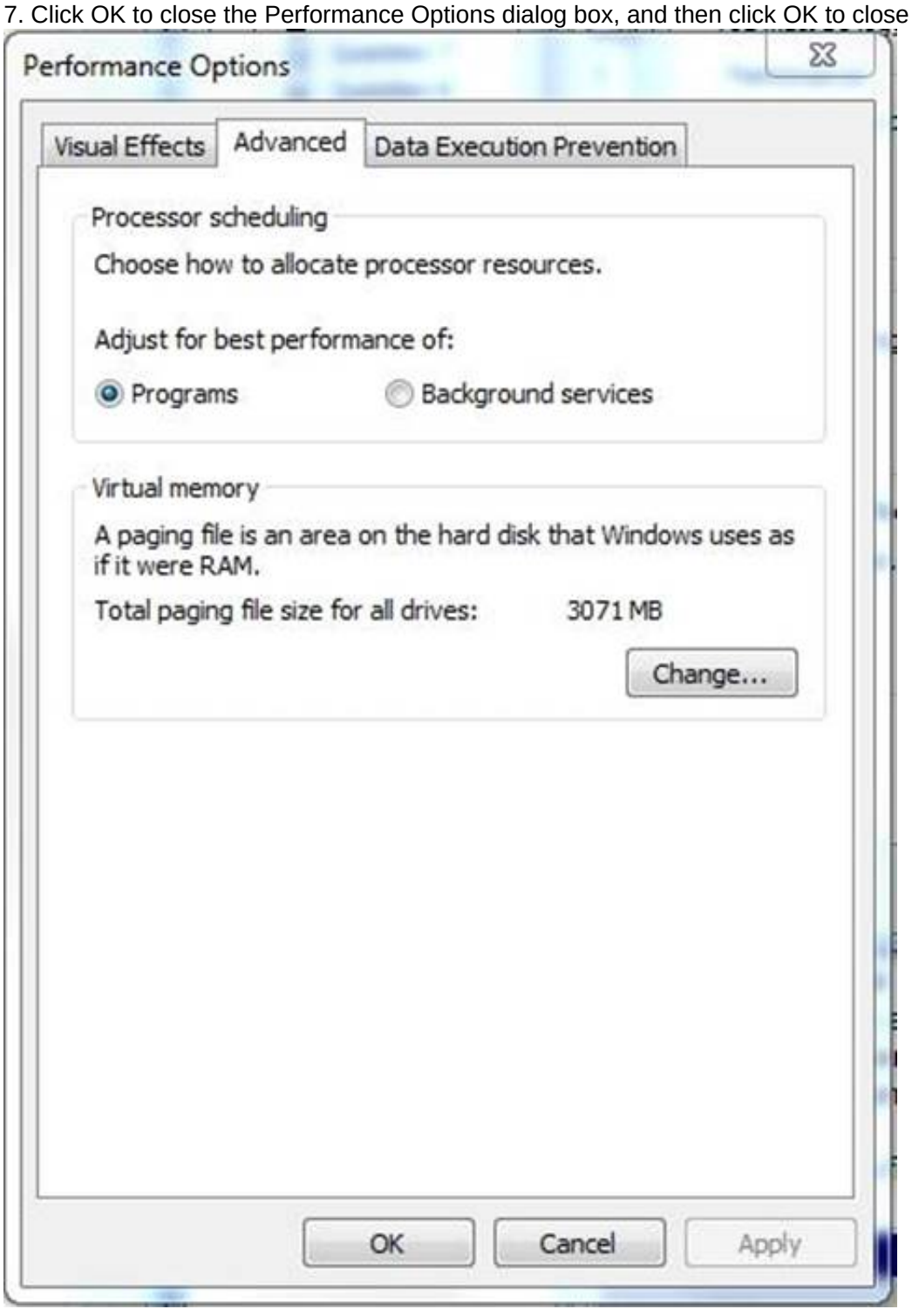
Answer: B

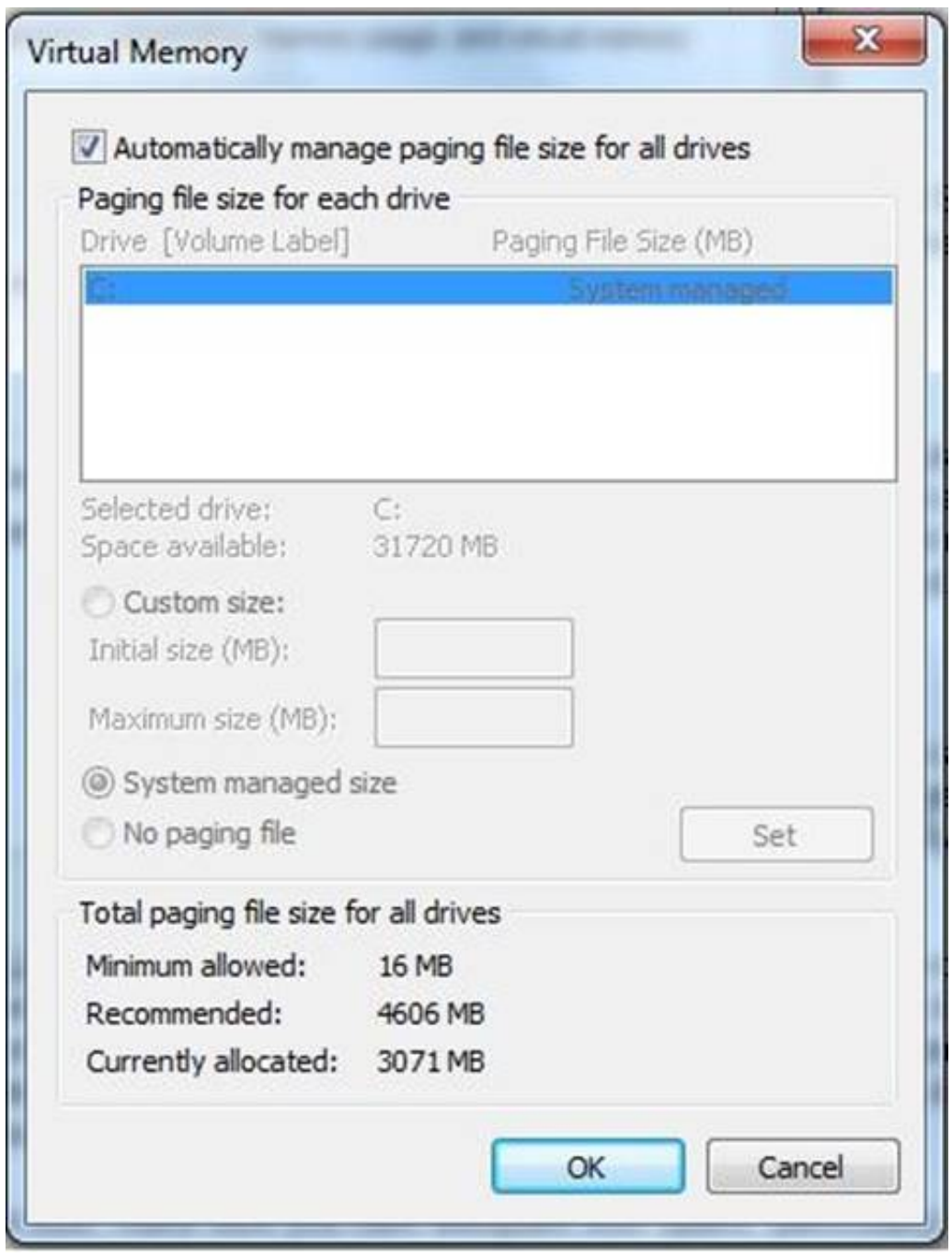
NEW QUESTION 230
You need to increase the size of a paging file.
What should you do?

A. From Disk Management, shrink the boot partitio
B. From Disk Management, shrink the system partitio
C. From System, modify the Advanced system setting
D. From System, modify the System protection setting

Answer: C

Explanation:
1. Click Start, right-click My Computer, and then click Properties.
2. In the System Properties dialog box, click the Advanced tab.
3. In the Performance pane, click Settings.
4. In the Performance Options dialog box, click the Advanced tab.
5. In the Virtual memory pane, click Change.
6. Change the Initial size value and the Maximum size value to a higher value, click Set, and then click OK.
7. Click OK to close the Performance Options dialog box, and then click OK to close the System Properties dialog box.





Adjusting Paging File SizeFor virtual-memory support, Windows 2000 creates one paging file called Pagefile.sys on the disk or volume on which the operating system is installed. The default size is equal to 1.5 times the amount of physical memory. A small paging file limits what can be stored and might exhaust your virtual memory for applications. If you are short on RAM, more paging occurs, which generates extra activity for your disks and slows response times for the system.Expand the Default SizeExpanding the default size of the paging file can increase performance if applications are consuming virtual memory and the full capacity of the existing file is being used. To determine how large your paging file should be based on your system workload, monitor the Process (_Total)\Page File Bytes counter. This indicates, in bytes, how much of the paging file is being used. A large paging file uses disk storage space, so do not create a large paging file on a disk that is very active (for example, one that services heavy application or network activity) or one that has limited space. Change the file size gradually and test performance until you find the optimal balance between paging file and disk space usage. The operating system requires a minimum of 5 MB of free space on a disk. For more information, see "Examining and Tuning Disk Performance" in this book. Before increasing the file size, make sure you have adequate disk space, particularly on your servers.

NEW QUESTION 232
You install an application named app1.exe on a computer
After the installation the computer becomes unresponsive.
You restart the computer and attempt to uninstall App1.exe. The uninstallation of App1.exe fails.
You need to restore the computer to its previous functional state. You must achieve the goal by using the minimum amount of administration.
What should you do?

A. From Recovery, restore a system restore poin
B. From the Previous Versions tab of App1.exe, click Restore butto
C. Start the computer, press F8 and then use the Last Known Good Configuratio
D. Create a system repair disc and then start the computer from the system repair dis

Answer: A

Explanation:
If you install an application that causes your computer to become unstable, you should first attempt to uninstall the application. If this does not solve the problem, you can restore system files and settings by performing a system restore to restore the computer to its last system restore point. A system restore returns a computer system to a selected restore point. System restores do not alter user files. Note that a system restore is not the same as a System Image restore.
Windows 7 creates system restore points on a regular schedule and prior to events such as the installation of applications and drivers. A restore point contains information about registry settings and other system information. Windows 7 generates restore points automatically before implementing significant system changes. You can manually create restore points and restore a computer system to a selected restore point. If you install an application or driver that causes your computer to become unstable, you should first attempt to uninstall the application or roll back the driver. If this does not solve the problem, you can restore system files and settings by performing a system restore to restore the computer to its last system restore point. A system restore returns a computer system to a selected restore point. System restores do not alter user files. Note that a system restore is not the same as a System Image restore.

NEW QUESTION 236
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 70-680 Exam with Our Prep Materials Via below:

https://www.certleader.com/70-680-dumps.html