

Exam Questions 70-680

TS:Windows 7,Configuring

<https://www.2passeasy.com/dumps/70-680/>



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.

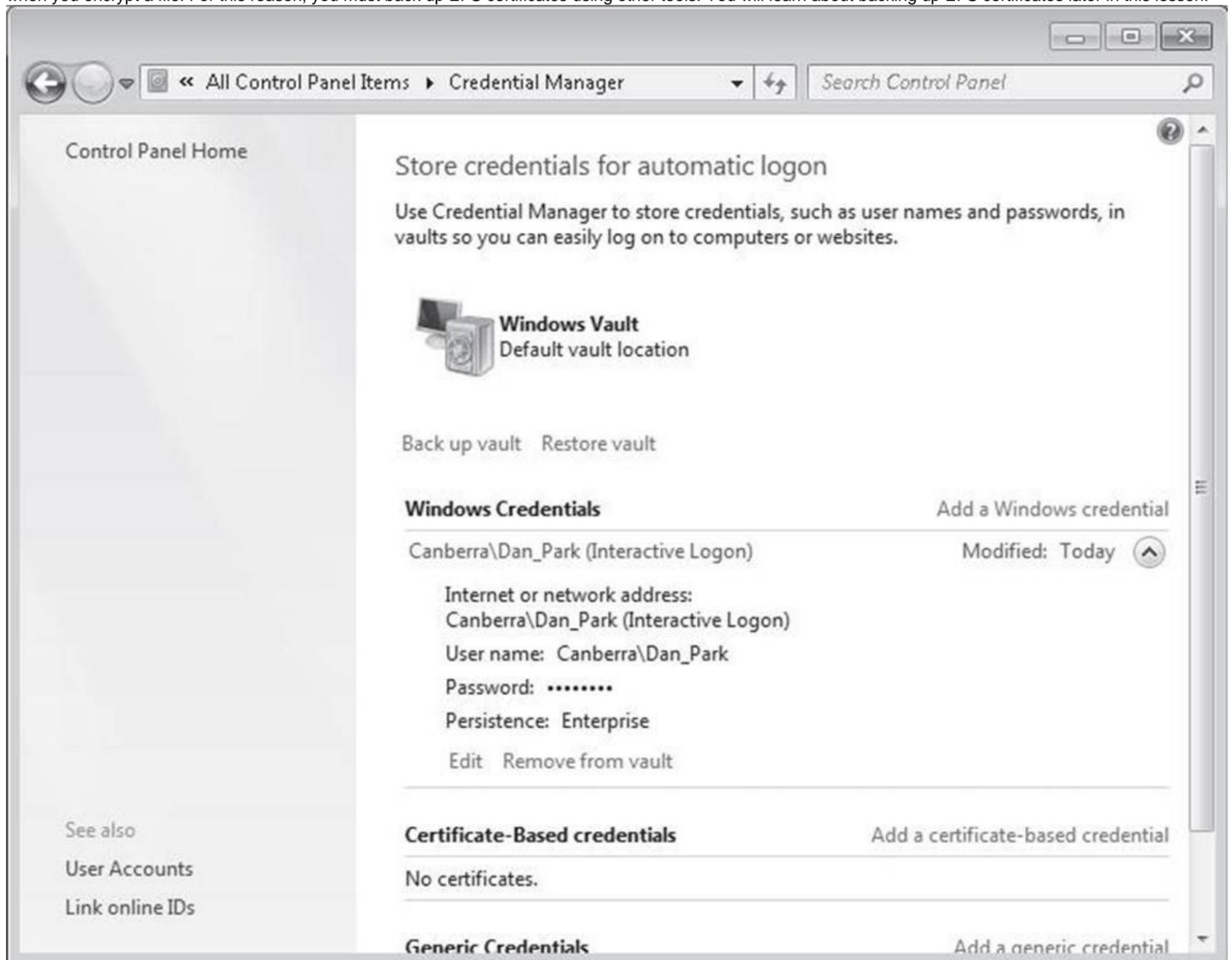
What should you do on Computer1?

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

Answer: C

Explanation:

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

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 domain
- 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 Panel, User Accounts and Family Safety, Setup Parental Controls, and then choose Time Restriction
- D. User Profiles, and then Time Restriction Setting
- E. Go to the Homegroup settings and choose Offline Time Setting

Answer: B

NEW QUESTION 3

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 4

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 Monitor
- D. Check the Windows System Diagnostics Report under the Performance Monitor MMC

Answer: BC

NEW QUESTION 5

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 partition
- C. Run Bootcfg.exe and specify the /default parameter
- 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 6

Which of the following tools can you use to determine if the applications installed on your computer running Windows Vista are known to have problems with Windows 7?

- A. Windows 7 Upgrade Advisor
- B. Sysprep
- C. USMT
- D. Windows PE

Answer: A

Explanation:

Windows 7 Upgrade Advisor Prior to attempting to perform the upgrade from Windows Vista to Windows 7, you should run the Windows 7 Upgrade Advisor. The Windows 7 Upgrade Advisor is an application that you can download from Microsoft's Web site that will inform you if Windows 7 supports a computer running the current hardware and software configuration of Windows Vista.

Prior to running the Windows 7 Upgrade Advisor, you should ensure that all hardware that you want to use with Windows 7, such as printers, scanners, and cameras, are connected to the computer. The Upgrade Advisor generates a report that informs you of which applications and devices are known to have problems with Windows 7.

NEW QUESTION 7

Your network contains 100 computers that run Windows XP.

You need to identify which applications installed on all of the computers can run on Windows 7.

You must achieve this goal by using the minimum amount of administrative effort.

What should you install?

- A. Microsoft Application Compatibility Toolkit (ACT)
- B. Microsoft Assessment and Planning (MAP) Toolkit
- C. Microsoft Deployment Toolkit (MDT)
- D. Windows Automated Installation Kit (AIK)

Answer: A

Explanation:

The Microsoft Application Compatibility Toolkit (ACT) 5.6 enables software developers, independent software vendors (ISVs), and IT professionals who work in a corporate environment to determine, before deployment within the organization, whether their applications are compatible with a new version of the Windows operating system. ACT also enables such individuals to determine how an update to the new version will affect their applications.

You can use the ACT features to:

-Verify your application's, device's, and computer's compatibility with a new version of the Windows operating system, including determining your risk assessment.

- Verify a Windows update's compatibility, including determining your risk assessment.
- Become involved in the ACT Community, including sharing your application assessment with other ACT users.
- Test your applications for issues related to User Account Control (UAC) by using the Standard User Analyzer (SUA) tool.
- Test your Web applications and Web sites for compatibility with new releases and security updates to Internet Explorer., by using the Internet Explorer Compatibility Test Tool.

NEW QUESTION 8

Your network consists of one Active Directory domain. You have two computers named Computer1 and Computer2 that run Windows 7. Both computers are members of the domain.

From Computer1, you can recover all Encrypting File System (EFS) encrypted files for users in the domain.

You need to ensure that you can recover all EFS encrypted files from Computer2.

What should you do?

- A. On Computer1, back up %systemroot%\DigitalLocker
- B. On Computer2, restore %systemroot%\DigitalLocker
- C. On Computer1, export the data recovery agent certificate
- D. On Computer2, import the data recovery agent certificate
- E. On Computer1, run Secedit.exe and specify the /export parameter
- F. On Computer2, run Secedit.exe and specify the /import parameter
- G. On Computer1, run Cipher.exe and specify the /removeuser parameter
- H. On Computer2, run Cipher.exe and specify the /adduser parameter

Answer: B

Explanation:

You can import the recovery agent to another computer running Windows 7 if you want to recover files encrypted on the first computer. You can also recover files on another computer running Windows 7 if you have exported the EFS keys from the original computer and imported them on the new computer. You can use the Certificates console to import and export EFS keys.

NOT Secedit.exe:

You can use both the Local Group Policy Editor and the Local Security Policy console to import and export security-related Group Policy settings. You can use this import and export functionality to apply the same security settings to stand-alone computers that are not part of a domain environment. Exported security files are written in Security Template .inf format. As well as using Local Group Policy Editor and the Local Security Policy console to import policies that are stored in .inf format, you can apply them using the Secedit.exe command-line utility.

NOT Cipher.exe /removeuser /adduser. NOT DigitalLocker.

NEW QUESTION 9

You have a computer that runs Windows 7. The computer has two volumes named volume C and volume D.

You create a document on volume D.

You manually create a restore point and modify the document.

You view the properties of the document as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that you can restore the current version of the document if the document is modified. What should you do first?

- A. Run Disk Cleanup on volume
- B. Enable auditing on the document

- C. Turn on System Protection for volume
- D. Start the Volume Shadow Copy Service (VSS).

Answer: C

Explanation:

System Protection System protection regularly creates and saves information about your computer's system files and settings. It also saves previous versions of files that you have modified. It saves these files in restore points, which are created just before significant system events, such as the installation of a program or device driver. Restore points are also created automatically every seven days if no other restore points were created in the previous seven days. You can create restore points manually at any time. System protection is automatically on for the drive that holds the operating system and can be enabled only for drives that are formatted using the NTFS file system. It enables you to use system restore and to restore files to previous versions. You will configure system protection, create a restore point, and perform a system restore in the practice later in this lesson.

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:

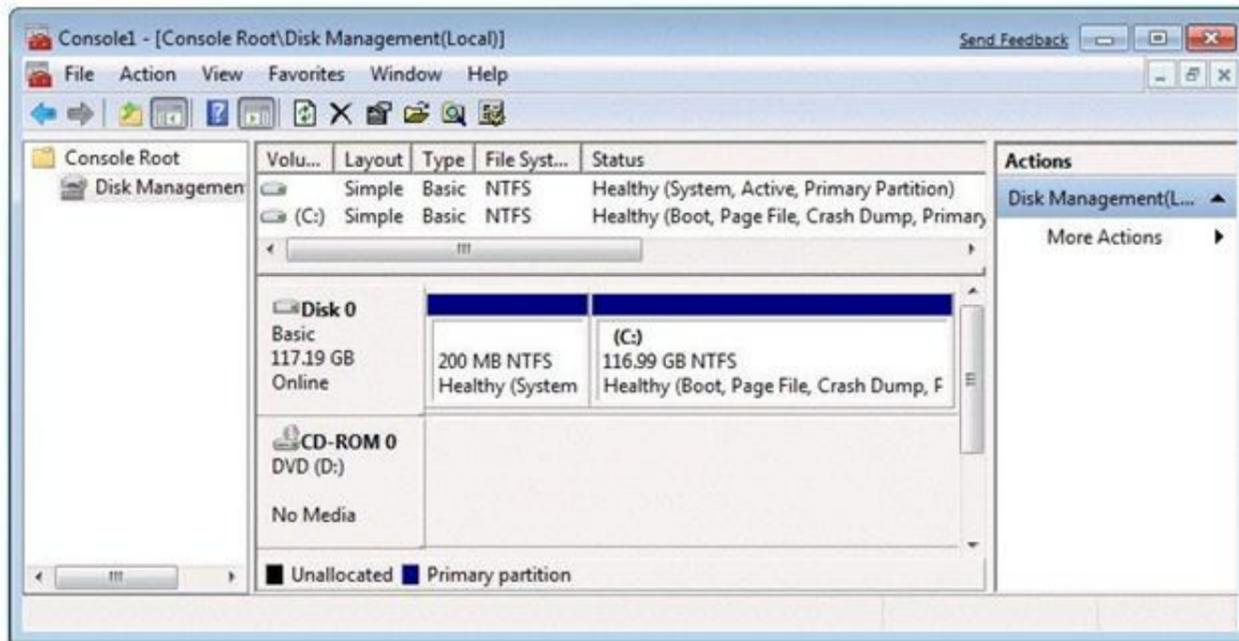
Offline FilesThe Offline Files feature of Windows 7 allows a client to locally cache files hosted in shared folders so that they are accessible when the computer is unable to connect directly to the network resource. The Offline Files feature is available to users of the Professional, Enterprise, and 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 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 11

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 15

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 18

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 20

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 "pathtofile", 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 22

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 26

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 31

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 generated. 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 34

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 37

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 computer that runs Windows 7. You run Runas and specify the /savecred parameter to start an application. The stored password needs to be deleted. What action should you perform?

- A. The Windows credentials should be modified from Credential Manage
- B. The Authorization Manager options should be modified from Authorization Manage
- C. Del should be run and the /p parameter should be specifie
- D. Runas should be run and the /nopprofile parameter should be specifie

Answer: A

NEW QUESTION 40

The Aero Shake feature will work if which of the following conditions are met? Choose Two.

- A. A display adapter compatible with WDDM is installe
- B. Aero features are downloaded from Microsof
- C. The windows experience index is at least 2.
- D. The Windows Experience Index is 3 or greate

Answer: AD

NEW QUESTION 44

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

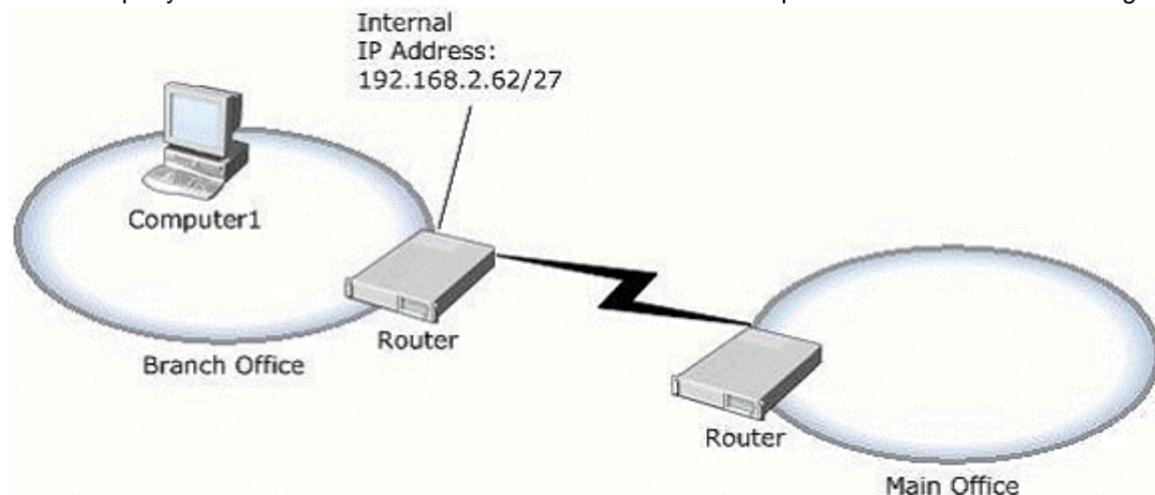
Explanation:

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 49

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 Address 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 acceptable (in correct subnet, and not reserved).
 192.168.2.63: is reserved for Broadcast (in subnet, but reserved).
 192.168.2.65: is out of range (in the wrong subnet, not subnet 2).

Acceptable IP ranges for those interested (excluding the 2 reserved IP addresses):

```
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 addresses):

```
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 53

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 rule
- B. From Software Restriction Policies, create a hash rule
- C. From Application Control Policies, create the default rule
- D. From Application Control Policies, create an executable rule

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 rules Default 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 Rules Path 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 Rules Hash 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 55

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 58

You have a computer that runs Windows 7.

You perform an image backup.

A virus infects the computer and causes the computer to become unresponsive.

You need to restore the computer as quickly as possible.

What should you do?

- A. Start the computer by using the Last Known Good Configuration feature
- B. Start the computer from the Windows 7 DVD and then use the Startup Repair tool
- C. Start the computer from the Windows 7 DVD and then use the System Image Recovery tool
- D. Start the computer from Windows Preinstallation Environment (Windows PE) and then run Imagex.exe

Answer: C

NEW QUESTION 63

You have a computer that runs Windows 7 Professional. A USB disk is attached to the computer.

You need to ensure that you can enable BitLocker to go on the USB disk.

What should you do?

- A. Enable Encrypting File System (EFS).
- B. Upgrade the computer to Windows 7 Enterprise
- C. Initialize the Trusted Platform Module (TPM) hardware
- D. Obtain a client certificate from an enterprise certification authority (CA).

Answer: B

Explanation:

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 64

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.exe
- C. From Device Manager, click Scan for hardware change
- D. From Device Manager, select the Devices by connection view

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 68

You have a computer that runs Windows 7.

Multiple users log on to your computer.

You enable auditing on a folder stored on your computer.

You need to ensure that each access to the folder is logged.

What should you do?

- A. Start the Problem Steps Recorder
- B. From Event Viewer, modify the properties of the Security log
- C. From the local Group Policy, configure the Audit object access setting
- D. From the local Group Policy, configure the Audit directory service Access setting

Answer: C

Explanation:

Audit object access Determines whether to audit the event of a user accessing an object (for example, file, folder, registry key, printer, and so forth) which has its own system access control list (SACL) specified. By default, this value is set to No auditing in the Default Domain Controller Group Policy object (GPO) and in the local policies of workstations and servers. If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object that has a SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified. You can select No auditing by defining the policy setting and unchecking Success and Failure.

NEW QUESTION 73

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:

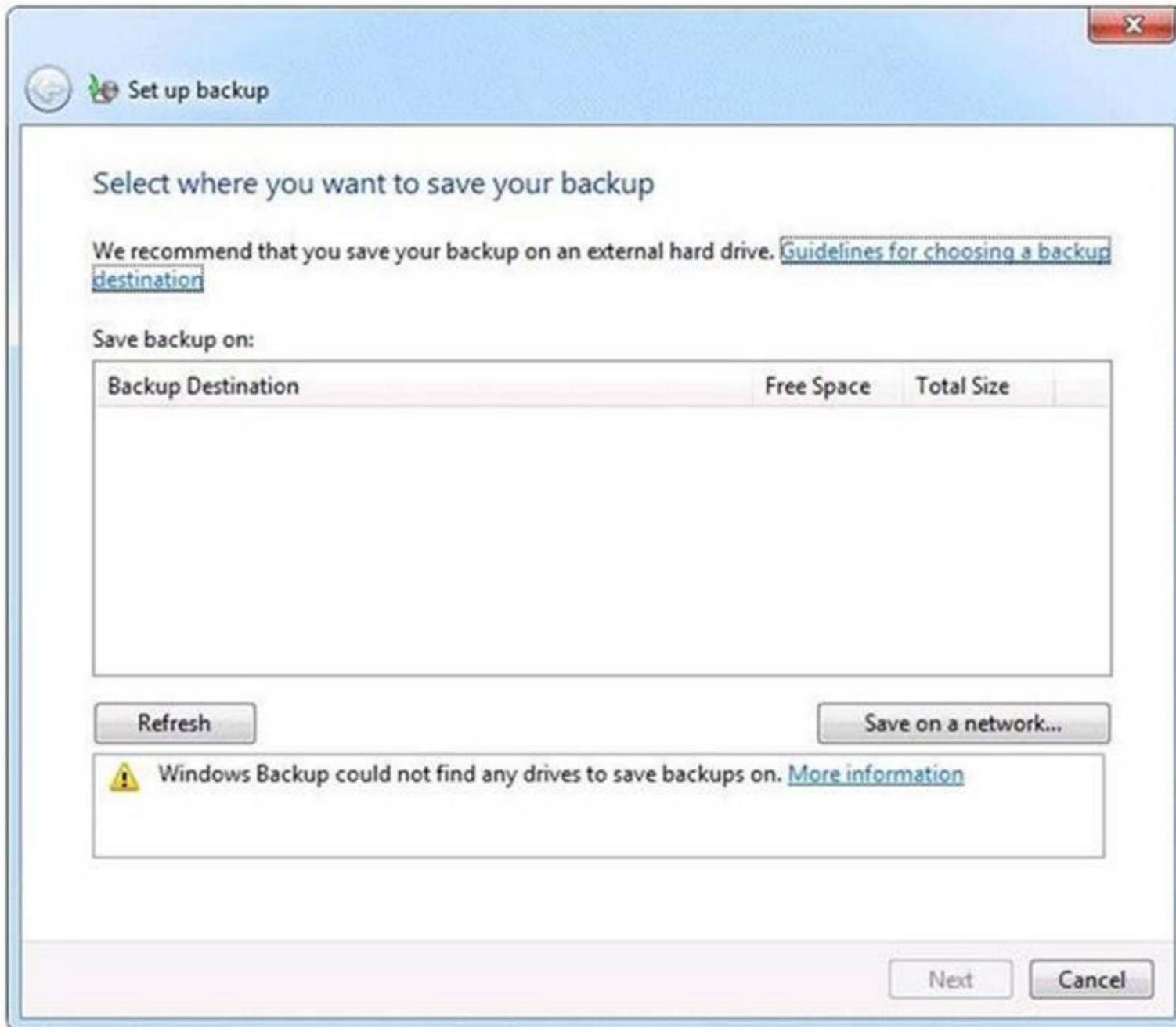
- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

If you want to use AES and to use computer certificates rather than a PSK, you would choose WPA2- Enterprise. WPA2-Personal If you have a small network that is not in a domain and cannot access a CA server, but you install a modern WAP 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 77

You have a computer that runs Windows 7.

You run the Configure Backup wizard as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that you can back up the computer to a local disk drive. What should you do before you run the Configure Backup wizard?

- A. Connect a removable disk
- B. Log on as an administrator
- C. Start the Volume Shadow Copy Service (VSS).
- D. Add your user account to the Backup Operators group

Answer: A

Explanation:

An external hard drive External hard drives can be removed and stored in a secure location. However, they are typically slower than internal hard drives and tend to be less reliable, mainly because they are by default formatted using FAT rather than NTFS. You cannot use an external hard drive for a System Image backup unless you convert its filing system to NTFS. Because it is easily removable, it is more likely that an external hard drive will be missing when a scheduled backup is required. (Local disk drive was specified, not internal) NOT Administrator You need administrator credentials to configure scheduled backups or to manually initiate a backup. However, restoring files does not require administrator privileges unless a user attempts to restore another user's file. (NOTE: The issue was a lack of location to store the Backup, not being about to run the Configure Backup, thus it was assumed that the user in this scenario had administrator credentials) NOT Backup Operators Members of this group are able to override file and folder access restrictions for the purpose of backing up data. You can allow a user to back up files and directories by assigning them to the Backup Operators group rather than by modifying the Back Up Files and Directories policy. NOT VSS VSS is installed on computers running Windows 7. Its startup type is Manual. The service starts as needed. If the service does not start when required, shadow copies are unavailable for backup and Windows Backup does not succeed. Nor can you create restore points and previous versions. In this case, check the service and ensure that it has not been disabled.

NEW QUESTION 81

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 use a computer that runs Windows 7. Now your company assigns a task to you. You are asked to prevent users from copying unencrypted files to removable drives. What action should you perform?

- A. The Trusted Platform Module (TPM) settings should be modified from a local Group Policy
- B. TPM should be initialized from the Trusted Platform Module (TPM) snap-in
- C. The BitLocker Drive Encryption settings should be modified from Control Panel
- D. The BitLocker Drive Encryption settings should be modified from a local Group Policy

Answer: D

NEW QUESTION 83

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

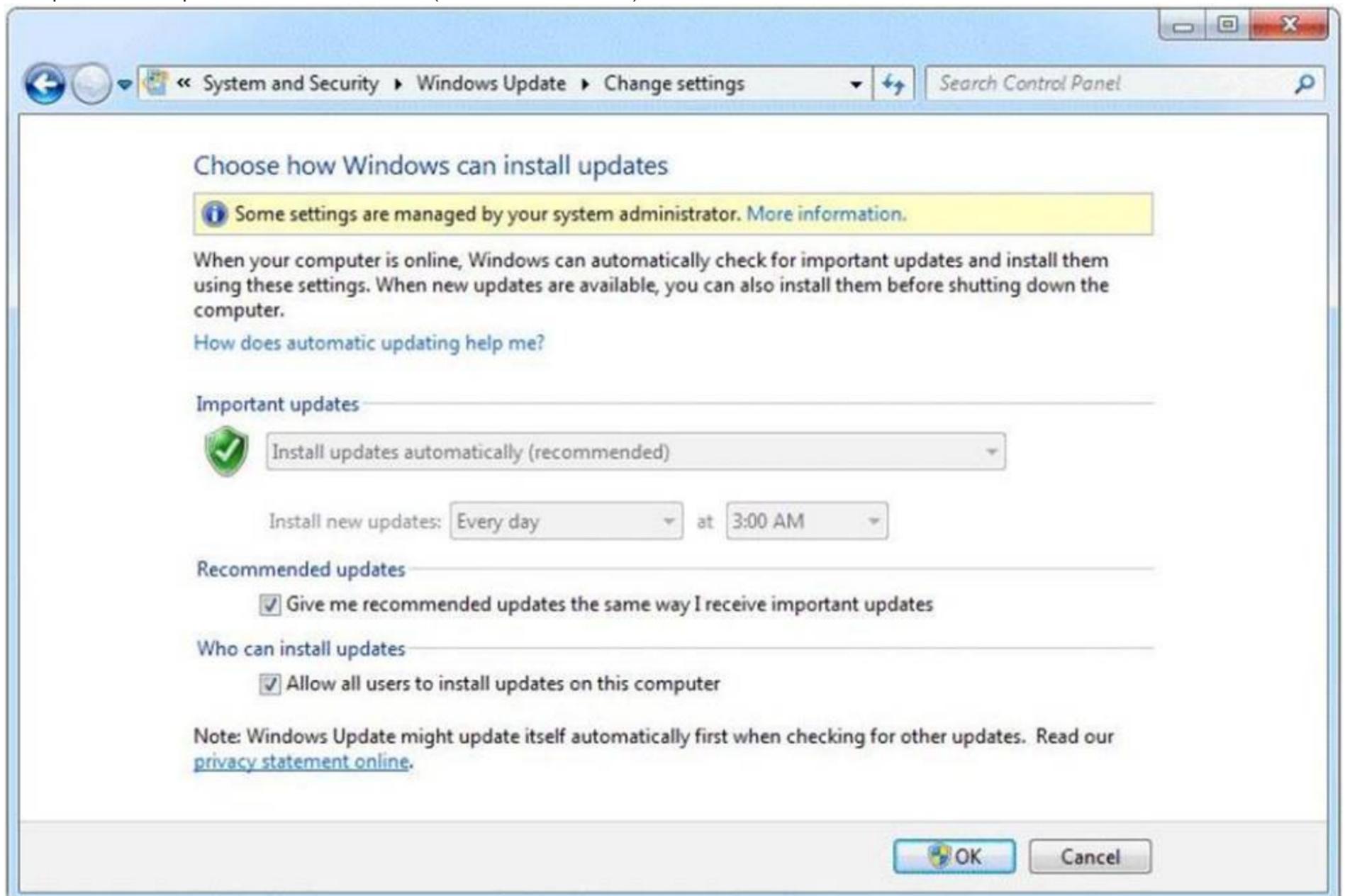
experience implementing and administering any Windows client operating system in a networked environment. You are professional in installing, upgrading and migrating to Windows 7, deploying Windows 7, and configuring Hardware and Applications and son on. You have a workgroup which contains five computers. 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 88

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?

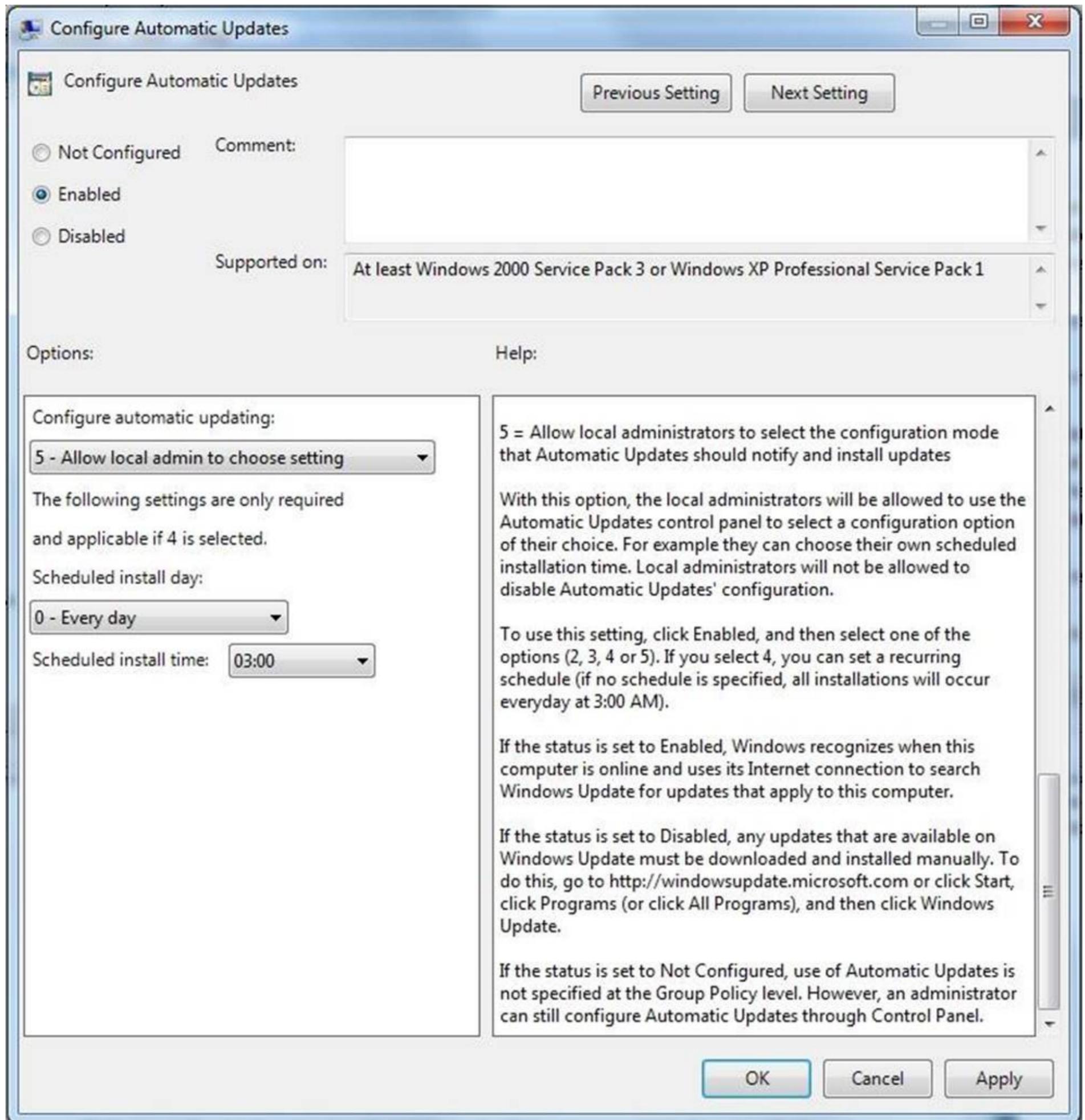
- A. Log on to Windows 7 as member of the Administrators grou
- B. From the local Group Policy, modify the Windows Update setting
- C. Right-click Windows Update and select Run as administrato
- D. Right-click the command prompt, select Run as administrator, and then run Wuapp.ex

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 89

Which of the following will cause the Online Compatibility Check to fail during a Window 7 installation? Choose two.

- A. 512MB of RAM
- B. A display adapter with WDDM Support
- C. A display adapter without WDDM Support but with SVIDEO
- D. An 80 GB Hard Disk

Answer: AC

NEW QUESTION 91

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 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. 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 Mode Hosted 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 Extension The 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 Server The 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 Scheduler The 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 93

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 98

You have a computer that runs Windows 7.
A printer is installed on the computer.
You remove the Everyone group from the access control list (ACL) for the printer, and then you share the printer.
You need to ensure that members of the Sales group can modify all the print jobs that they submit.
You must prevent Sales group members from modifying the print jobs of other users.
What should you do?

- A. From the printer's properties, assign the Print permission to the Sales grou
- B. From the printer's properties, assign the Manage Documents permission to the Sales grou
- C. From the local Group Policy, assign the Increase scheduling priority user right to the Sales grou
- D. From the local Group Policy, assign the Take ownership of files or other objects user right to the Sales grou

Answer: A

Explanation:

The available permissions are:

- Print This permission allows a user to print to the printer and rearrange the documents that they have submitted to the printer.
- Manage This Printer Users assigned the Manage This Printer permission can pause and restart the printer, change spooler settings, adjust printer permissions, change printer properties, and share a printer.
- Manage Documents This permission allows users or groups to pause, resume, restart, cancel, or reorder the documents submitted by users that are in the current print queue.

NEW QUESTION 102

You have a computer named Computer1 that runs Windows 7.
You need to ensure that Computer1 can connect to File Transfer Protocol (FTP) servers only while it is connected to a private network.
What should you do?

- A. From Windows Firewall with Advanced Security, create a new rul
- B. From the local Group Policy, modify the application control policie
- C. From Windows Firewall, modify the Allowed Programs and Features lis
- D. From Network and Sharing Center, modify the Advanced Sharing setting

Answer: A

Explanation:

Creating WFAS Rules The process for configuring inbound rules and outbound rules is essentially the same: In the WFAS console, select the node that represents the type of rule that you want to create and then click New Rule. This opens the New Inbound (or Outbound) Rule Wizard. The first page, shown in Figure 7-7, allows you to specify the type of rule that you are going to create. You can select between a program, port, predefined, or custom rule. The program and predefined rules are similar to what you can create using Windows Firewall. A custom rule allows you to configure a rule based on criteria not covered by any of the other options. You would create a custom rule if you wanted a rule that applied to a particular service rather than a program or port. You can also use a custom rule if you want to create a rule that involves both a specific program and a set of ports. For example, if you wanted to allow communication to a specific program on a certain port but not other ports, you would create a custom rule.

NEW QUESTION 104

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 computer that runs Windows 7. You have to identify which applications were installed during the last week. So what action should you perform?

- A. The System Performance Data Collector Set should be run from Performance Monito
- B. The informational events should be reviewed from Reliability Monito
- C. The Software Environment should be reviewed from System Informatio
- D. The System Diagnostics Report should be reviewed from Performance Monito

Answer: B

NEW QUESTION 107

You have two computers named Computer1 and Computer2 that run Windows 7. You need to ensure that you can remotely execute commands on Computer2 from Computer1. What should you do?

- A. Run Winrm quickconfig on Computer1
- B. Run Winrm quickconfig on Computer2
- C. Enable Windows Remote Management (WinRM) through Windows Firewall on Computer1
- D. Enable Windows Remote Management (WinRM) through Windows Firewall on Computer2

Answer: B

Explanation:

Windows Remote Management Service The Windows Remote Management service allows you to execute commands on a remote computer, either from the command prompt using WinRS or from Windows PowerShell. Before you can use WinRS or Windows PowerShell for remote management tasks, it is necessary to configure the target computer using the WinRM command. To configure the target computer, you must run the command WinRM quickconfig from an elevated command prompt. Executing WinRM quickconfig does the following:

- Starts the WinRM service
- Configures the WinRM service startup type to delayed automatic start
- Configures the LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users
- Configures the WinRM listener on http://* to accept WS-Man requests
- Configures the WinRM firewall exception

NEW QUESTION 112

You have a computer that runs Windows Vista Service Pack 2 (SP2). You need to upgrade the computer to Windows 7. What should you do?

- A. Start the computer from the Windows 7 installation media and select the Upgrade optio
- B. Start the computer from the Windows 7 installation media and select the Custom (advanced) optio
- C. From Windows Vista, run Setup.exe from the Windows 7 installation media and select the Upgrade optio
- D. From Windows Vista, run Setup.exe from the Windows 7 installation media and select the Custom (advanced) optio

Answer: C

Explanation:

Upgrading Windows Vista to Windows 7 instructionsAccess the Windows 7 installation source and double-click Setup.exe. When prompted by User Account Control, click Allow. This loads the Install Windows page. Click Install Now.Other NotesYou can upgrade computers running Windows Vista to Windows 7. When you upgrade from Windows Vista to Windows 7, all documents, settings, applications, and user accounts that existed on the computer running Windows Vista are available when the upgrade is finished. The advantage to an upgrade is that it allows you to keep the current application configuration. When you perform a migration, you need to reinstall the user's applications on the new computer. As mentioned previously, this can be problematic in organizations that are not careful about keeping track of which specific set of applications are installed on each user's computer. Prior to attempting to perform the upgrade from Windows Vista to Windows 7, you should run the Windows 7 Upgrade Advisor. The Windows 7 Upgrade Advisor is an application that you can download from Microsoft's Web site that will inform you if Windows 7 supports a computer running the current hardware and software configuration of Windows Vista. Prior to running the Windows 7 Upgrade Advisor, you should ensure that all hardware that you want to use with Windows 7, such as printers, scanners, and cameras, are connected to the computer. The Upgrade Advisor generates a report that informs you of which applications and devices are known to have problems with Windows 7. A similar compatibility report is generated during the upgrade process, but the version created by the Windows 7 Upgrade Advisor is more likely to be up to date.

NEW QUESTION 117

You plan to deploy Windows 7 to 100 computers on your corporate network. You install Windows 7 on a computer. You and need to prepare the computer to be imaged. What should you do before you create the image of the computer?

- A. At the command prompt, run the Dism command
- B. At the command prompt, run the Sysprep command
- C. Start the computer from the Windows Preinstallation Environment (Windows PE) and then run the ImageX command
- D. Start the computer from the Windows Preinstallation Environment (Windows PE) and then run the Wpeutil command

Answer: B

Explanation:

Sysprep
Sysprep is a tool designed for corporate system administrators, OEMs, and others who need to deploy the Windows XP operating system on multiple computers. After performing the initial setup steps on a single system, you can run Sysprep to prepare the sample computer for cloning. 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. NOT ImageX ImageX 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. NOT Dism Deployment 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 Wpeutil The 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 121

You have a computer that runs Windows 7.
You need to modify the file extensions that are associated to Internet Explorer.
What should you do?

- A. From Internet Explorer, click Tools and then click Manage Add-on
- B. From Control Panel, open Default Programs and then click Set Association
- C. From the local Group Policy, expand Computer Configuration and then click Software Setting
- D. From Windows Explorer, right-click %programfiles%\Internet Explorer\iexplore.exe and then click Properties

Answer: B

NEW QUESTION 126

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 127

You have a computer that runs Windows 7.
The computer has a corporate intranet web site.
Your Windows Internet Explorer is shown in the exhibit.



You need to ensure that you can access web pages on both Internet and Intranet.
What should you do?

- A. From the tools menu, click Work Offlin
- B. From the Safety menu, click InPrivate Blockin
- C. From the Safety menu, click Inprivate Browsin
- D. From the Security tab, add the intranet web site to the Trusted sites zon

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 131

Your computer running Windows 7 Enterprise has two internal hard disks.
System protection is configured by default on the C: drive, which holds the operating system and installed applications.
The D: drive is a 500-GB hard disk formatted with the NTFS filing system, and you use it to store your personal files.
You want to store previous versions going back several months and therefore intend to reserve 200 GB of this disk for system protection.
You are not using either of your internal disks for backup; instead, you store your backups on a 1-TB external USB hard disk.
How do you configure system protection on your D: drive? (Choose all that apply; each answer forms part of the complete solution.)

- A. Select Restore System Settings And Previous Versions Of Files
- B. Select Only Restore Previous Versions Of Files
- C. Set the Max Usage slider control to 40 percent
- D. Set the Max Usage slider control to 4 percent

Answer: BC

NEW QUESTION 133

You want to centralize backups by backing up all client computers in your company's production network to a network share on a file server running Windows Server 2008 R2. All your client computers run Windows 7, but because your company has grown through a series of mergers, some run Windows 7 Professional, some run Windows 7 Enterprise, and some run Windows 7 Ultimate.
Which computers can you back up to a network share?

- A. Only the computers running Windows 7 Ultimate
- B. Only the computers running Windows 7 Enterprise
- C. Only the computers running either Windows 7 Ultimate or Windows 7 Enterprise
- D. All your company's client computers

Answer: D

NEW QUESTION 136

You attach a mobile device that runs Windows Mobile Professional 6.1 to a computer. You encounter that windows is unable to install the necessary device drivers for the mobile device.
You need to ensure that you can synchronize file to the mobile device.
What should you do?

- A. From Windows Mobility Center, click Sync setting
- B. From Sync Center, click set up new sync partnership
- C. From Device Manager, click scan for hardware change
- D. From Devices and Printers, right-click the device and click troubleshoo

Answer: D

Explanation:

You cannot sync without the drivers installed. It says unable to install, assuming that it could find the device if it was able to reach attempting to install point. Therefore Troubleshoot.

NEW QUESTION 137

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 /l app1.msi /
- C. Create a transform file named app1.msp and then run Msiexec.exe /l app1.msi /app1.
- D. Create a transform file named app1.msp and then run Msinfo32.exe /l 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. Msiexec Provides 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 142

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 will use. /bootems - Enable or disables Emergency Management Services for a boot application. NOT boot.ini: Windows (specifically Ntldr) uses

NEW QUESTION 143

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 146

You have two computers named Computer1 and Computer2 that run Windows 7. Computer1 is used to remotely manage Computer2. From Computer1, you need to verify that the Windows Remote Management (WinRM) service started on Computer2.
What should you do?

- A. At the command prompt, run Winrs -r:computer2 quer
- B. At the command prompt, run Winrm id -remote:computer2
- C. From Windows Powershell, run Get -PSSession Computer2
- D. From Windows Powershell, run Get -PSSessionConfiguration Computer2

Answer: A

NEW QUESTION 150

You have a computer that runs Windows XP. The computer has one partition.
You install Windows 7 on the computer.
You need to migrate a user profile from the Windows XP installation to Windows 7 installation.
What should you do first?

- A. From Windows 7, run Scanstate.exe /offlineWinOld:c:\window
- B. From Windows 7, run Scanstate.exe /offlineWinOld:c:\windows.ol
- C. At the command prompt, run Xcopy /s /e c:\windows\users*. * c:\users\.
- D. At the command prompt, run Xcopy /s /e c:\windows.old\documents and settings*. * c:\users\.

Answer: B

Explanation:

/offlinewinold: "Windows.old direactory"

This command-line option enables the offline migration mode and starts the migration from the location specified. It is only intended to be used in Windows.old migration scenarios, where the migration is occurring from a Windows.old directory.

NOT Xcopy

Copies files and directories, including subdirectories.

/s Copies directories and subdirectories, unless they are empty. If you omit /s, xcopy works within a single directory.

NEW QUESTION 152

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 setting
- D. From the Internet Protocol Version 4 (TCP/IPv4) properties of the VPN connection, disable the Use default gateway on remote network setting

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 157

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 vault
- B. From User Accounts, select Create a password reset disk
- 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 161

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 parameter
- B. Run Dism.exe and specify the /mount-WIM parameter
- 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 SIM Opens Windows images, creates answer files, and manages distribution shares and configuration sets. **NOT Dism** Deployment 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 Imagex** ImageX 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. /mount Mounts 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

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 163

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 164

You have a computer that runs windows 7.

The windows experience index displays the subscores in the following.

Component Subscore

Processor 6.9

Memory (RAM) 5.3

Graphics 3.2

Gaming graphics 4.1

Primary hard disk 4.5

You need to increase the Windows Experience Index base score.

What should you do?

- A. Add more RA
- B. Add a second hard dis
- C. Upgrade the video adapte
- D. Upgrade to a faster processso

Answer: C

NEW QUESTION 169

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 172

You have a computer that runs Windows 7.

You need to identify which hardware is required to create a system repair disc.

What hardware should you indentify?

- A. CD/DVD burne
- B. Floppy dis
- C. Tape driv
- D. USB dis

Answer: A

NEW QUESTION 177

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 181

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 boot Vista by default?

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

Answer: C

NEW QUESTION 184

You have a computer that runs Windows 7. You need to provide standard users the ability to update the drivers for display adapters. What should you modify from the Local Group Policy?

- A. driver installation settings for the user
- B. device installation settings for the computer
- C. driver installation settings for the computer
- D. display settings for the user

Answer: C

Explanation:

To Update the Drivers you need permissions to install drivers. Apply this to the computer for all local users, as opposed to only one user.

NEW QUESTION 186

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 189

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 193

You are installing a custom Windows 7 system image to a new computer. Perform the following tasks"

- Start the new computer by using the Windows preinstallation Environment (WPE) •
 - Connect to a shared network location that contains the Windows 7 image file.
 - You need to apply the Windows 7 image to the computer.
- What should you do before you apply the image?

- A. Mount the imag
- B. Configure Windows Firewall
- C. Configure and format the haard disk driv
- D. Initializa the Boot Configuration data (BCD) stor

Answer: C

NEW QUESTION 196

You have a computer that runs Windows 7. You need to identify which unsigned drivers have been installed. Which command should you run?

- A. Cipher.exe /s
- B. Driverquery.exe /si
- C. Msinfo32.exe /q
- D. Pnputil.exe -i

Answer: B

Explanation:

Driverquery: Displays a list of all installed device drivers and their properties. /si: Displays digital signature information for both signed and unsigned device drivers.

NEW QUESTION 201

You have a computer that runs windows 7. You have a system image of the computer. You need to restore a single file from the system image. You must achieve the goal using minimum administrative effort. What should you do?

- A. From Disk Management, select Attach VH
- B. From the Backup and Restore, select restore my file
- C. Restart the computer and run system restor
- D. Restart the computer and run system image recover

Answer: A

Explanation:

Attach VHD: Attaching a VHD activates the VHD so that it appears on the host computer as a local hard disk drive. This is sometimes called "surfacing a VHD" because the VHD is now visible to users. If the VHD already has a disk partition and file system volume when you attach it, the volume inside the VHD is assigned a drive letter. The assigned drive letter is then available for use, similar to when you insert a USB flash drive into a USB connector. All users (not just the current user) can use the attached VHD in the same way they use other volumes on local physical hard disk drives (depending on security permissions). Furthermore, because you can attach a VHD that is located on a remote server message block (SMB), you can manage your images remotely. Once attached the single file can be restored. The other answers are overkill or replace all files not just the one required.

<http://technet.microsoft.com/en-us/library/dd440865%28WS.10%29.aspx>

What is system protection? System protection is a feature that regularly creates and saves information about your computer's system files and settings. System protection also saves previous versions of files that you've modified. It saves these files in restore points, which are created just before significant system events, such as the installation of a program or device driver. They're also created automatically once every seven days if no other restore points were created in the previous seven days, but you can create restore points manually at any time.

System protection is automatically on for the drive that Windows is installed on. System protection can only be turned on for drives that are formatted using the NTFS file system.

There are two ways that you can take advantage of system protection:

* If your computer is running slowly or isn't working properly, you can use System Restore to return your computer's system files and settings to an earlier point in time using a restore point.

* If you accidentally modify or delete a file or folder, you can restore it to a previous version that's saved as part of a restore point.

NEW QUESTION 203

You have a workgroup that contains five computers. The computers run Windows 7.

A computer named Computer1 has video and audio files.

You need to share Computer1's video and audio files on the network.

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

- A. Create a HomeGrou
- B. Move the files to a Media Librar
- C. Enable all BranchCache rules in Windows Firewal
- D. Connect a removable drive and enable BitLocker To G

Answer: AB

Explanation:

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. Media Library Sharing Before you turn on Media Library Sharing for a shared folder, you should know that Media Library Sharing bypasses any type of user-account access that you set for the shared folder. For example, let's say that you turn on Media Library Sharing for the Photos shared folder, and you set the Photos shared folder to No Access for a user account named Bobby. Bobby can still stream any digital media from the Photos shared folder to any supported digital media player or DMR. If you have digital media that you do not want to stream in this manner, store the files in a folder that does not have Media Library Sharing turned on. If you turn on Media Library Sharing for a shared folder, any supported digital media player or DMR that can access your home network can also access your digital media in that shared folder. For example, if you have a wireless network and you have not secured it, anybody within range of your wireless network can potentially access your digital media in that folder. Before you turn on Media Library Sharing, make sure that you secure your wireless network. For more information, see the documentation for your wireless access point.

NEW QUESTION 205

Which of the following steps will keep a Microsoft Word shortcut icon on the Taskbar after the next reboot?

- A. Copy and paste a Microsoft Word icon to the Taskba
- B. Right click on the Microsoft Word icon and choose, "Staple to Superbar".
- C. Right click on the Microsoft Word icon and choose, "Pin this programm to taskbar".
- D. Open Microsoft Wor
- E. While the Icon is on the Taskbar, right click the icon and choose, "Pin this program to taskbar".

Answer: D

NEW QUESTION 209

You have a portable computer named Computer1 and a desktop computer named Computer2. Both computers run windows 7.

On computer2, you create a share named Share1 by using Advanced Sharing feature.

You need to ensure that when you connect to Share1 from Computer1, the files that you open are automatically cached.

What should you do?

- A. On Computer1, modify the Offline Files setting
- B. On Computer1, modify the User Profile setting
- C. On Computer2, modify the properties of Share1.
- D. On Computer2, modify the file sharing connection settings for the HomeGroup

Answer: C

Explanation:

The caching feature of Shared Folders ensures that users have access to shared files even when they are working offline without access to the network. You can

also use Shared Folders or Share and Storage Management to enable BranchCache on shared resources. The BranchCache feature in Windows 7 or Windows Server 2008 R2 enables computers in a branch office to cache files downloaded from this shared folder, and then securely serve the files to other computers in the branch. To set caching options for a shared folder by using the Windows interface 1. Open Computer Management. 2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Yes. 3. In the console tree, click System Tools, click Shared Folders, and then click Shares. 4. In the results pane, right-click the shared folder, and then click Properties. 5. On the General tab, click Offline Settings, configure the offline availability options as appropriate and then click OK. Offline availability options Select the following offline availability option for each shared folder: All files and programs that users open from the share are automatically available offline Whenever a user accesses the shared folder or volume and opens a file or program in it, that file or program will be automatically made available offline to that user. Files and programs that are automatically made available offline will remain in the Offline Files cache and synchronize with the version on the server until the cache is full or the user deletes the files. Files and programs that are not opened are not available offline.



NEW QUESTION 214

You have a computer that runs windows 7.
 You log on to the computer by using a user account that is a member of Administrator Group.
 From Windows Explorer you open C:\windows\system32\drivers\etc\hosts in notepad.
 You attempt to save the file and receive the save as dialog box.
 You need to ensure that you can save changes to c:\windows\system32\drivers\
 What should you do?

- A. Stop the windows search service
- B. Remove the inherited permissions from the fil
- C. Start Windows Notepad by using elevated privilege
- D. Change the user account control (UAS) settings to Notify Me Only when programs try to make changes to my compute

Answer: C

Explanation:

Windows 7 does not allow applications to write data to these secure locations.
 User Account Control (UAC) UAC is a security feature of Windows 7 that informs you when the action that you want to undertake requires an elevation of privileges. If you logged on with a user account that was a member of the local administrators group in previous versions of Microsoft Windows, such as Windows XP, you automatically had administrator-level access at all times. This, by itself, was not a problem because recommended good practice was that people logged on with accounts that were members of the local administrator group only when they needed to do something related to administration. The problem with this is that people tended to use their administrator account as their normal user account. It was convenient for them because they did not have to log off and log on again each time they wanted to do something related to systems administration. Unfortunately, this behavior presented a security problem because any program run by a user logged on with an administrative account runs with the rights and privileges of that user. UAC resolves this problem by allowing a user that is a member of the local Administrators group to run as a standard user most of the time and to briefly elevate their privileges so that they are running as administrators when they attempt to carry out specific administration-related tasks. Privilege elevation All users of clients running Windows 7 run with the rights of a standard user. When a user attempts an act that requires administrative privileges, such as creating a new user account, her rights need to be raised from those of a standard user to those of an administrative user. This increase in rights is termed privilege elevation. UAC is a gateway to privilege elevation. It allows users who are members of the local Administrators group to access administrative rights, but ensures that the person accessing the Administrative rights is aware that they are doing so. This privilege elevation occurs only for a specific task. Another task executed at the same time that also requires privilege elevation generates its own UAC

NEW QUESTION 218

You have a computer that runs Windows XP Service Pack 2 (SP2).
 You need to upgrade the operating system to Windows 7.
 You must achieve this goal in the minimum amount of time.
 What should you do?

- A. Upgrade to Windows Vista SP2. From the Windows 7 installation media, run Setup.exe and select the Upgrade optio
- B. Upgrade to Windows Vista SP2. From the Windows 7 installation media, run Setup.exe and select the Custom (advanced) optio
- C. Install Windows XP Service Pack 3 (SP3). Run Setup.exe from the Windows 7 installation media and select the Upgrade optio
- D. Install Windows XP Service Pack 3 (SP3). Run Setup.exe from the Windows 7 installation media and select the Custom (advanced) optio

Answer: A

NEW QUESTION 221

You have a computer that runs Windows 7. Multiple users share the computer. The computer is joined to a domain. You need to prevent the users from using more than 2 GB of disk space on drive C. What should you do?

- A. From a Group Policy object (GPO), enable the Limit profile size setting
- B. Enable System Protection for Local Disk (C) and set the disk space usage
- C. Enable disk quota management on Computer1 and configure a default quota limit
- D. From a Group Policy object (GPO), enable the Limit the size of the entire roaming user profile cache setting

Answer: C

Explanation:

Disk quotas provide administrators with a way to limit each user's utilization of disk space on a volume. In order to set quotas, you must have Administrator rights, and the volume must be formatted with the NTFS file system. Disk quotas are based on file ownership and are independent of the folder location of the user's files within the volume. For example, if users move their files from one folder to another on the same volume, their volume space usage does not change. However, if users copy their files to a different folder on the same volume, their volume space usage doubles. If one user creates a 200 kilobyte (KB) file, and another user takes ownership of that file, the first user's disk use decreases by 200 KB and the second user's disk use increases by 200 KB.

NEW QUESTION 222

You have a computer that runs Windows 7. You create an application shim for a third-party application by using the Microsoft Application Compatibility Toolkit (ACT). You need to ensure that the application shim is applied the next time you run the application. What should you do first?

- A. Run Sdbinst.exe
- B. Run Msiexec.exe
- C. Right-click the application executable file and modify the compatibility setting
- D. Right-click the application executable file and modify the advanced security setting

Answer: A

Explanation:

Deploying a custom shim database to users requires the following two actions: Placing the custom shim database (*.sdb file) in a location to which the user's computer has access (either- locally or on the network)- Calling the sdbinst.exe command-line utility to install the custom shim database locally
 Demystifying Shims - or - Using the Application Compatibility Toolkit to make your old stuff work with your new stuff
 What is a Shim? A shim is one of the very few four-letter words in use by Microsoft that isn't an acronym of some sort. It's a metaphor based on the English language word shim, which is an engineering term used to describe a piece of wood or metal that is inserted between two objects to make them fit together better. In computer programming, a shim is a small library which transparently intercepts an API, changes the parameters passed, handles the operation itself, or redirects the operation elsewhere. Shims can also be used for running programs on different software platforms than they were developed for.
 How Shims work The Shim Infrastructure implements a form of Application Programming Interface (API) hooking. The Windows API is implemented using a collection of DLLs. Each application built for Windows imports these DLLs, and maintains a table of the address of each of these functions in memory. Because the address of the Windows functionality is sitting in a table, it is straightforward for the shim engine to replace this address with the address of the shim DLL instead. The application is generally unaware that the request is going to a shim DLL instead of to Windows itself, and Windows is unaware that the request is coming from a source other than the application (because the shim DLL is just another DLL inside the application's process). In this particular case, the two objects are the application program and Windows, and the shim is additional code that causes the two to behave better together, as shown below:

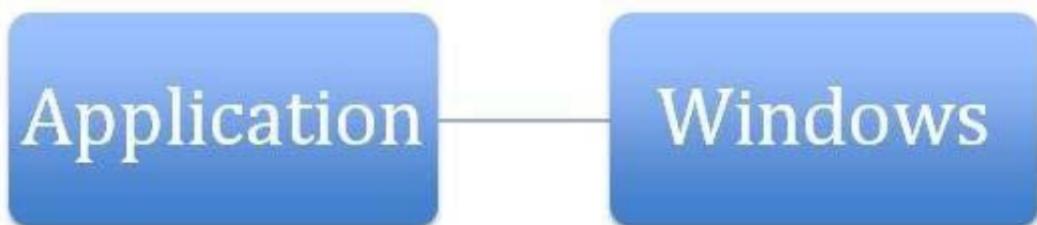


Figure 1 Before the shim is applied, the application interacts directly with Windows.



Figure 2 After the shim is applied, the application interacts with Windows indirectly; the shim code is injected and can modify the request to Windows, the response from Windows, or both.

Specifically, it leverages the nature of linking to redirect API calls from Windows to alternative code—the Shim. Calls to external binary files take place through the Import Address Table (IAT). Consequently, a call into Windows looks like:



Figure 1 Application calling into Windows through the IAT Specifically, you can modify the address of the Windows function resolved in the import table, and then replace it with a pointer to a function in the alternate shim code, as shown in Figure 2



This redirection happens for statically linked .dll files when the application is loaded. You can also shim dynamically linked .dll files by hooking the GetProcAddress API. Why Should we be using Shims This is the cost-saving route—help the application by modifying calls to the operating system before they get there. You can fix applications without access to the source code, or without changing them at all. You incur a minimal amount of additional management overhead (for the shim database), and you can fix a reasonable number of applications this way. The downside is support as most vendors don't support shimmed applications. You can't fix every application using shims. Most people typically consider shims for applications where the vendor is out of business, the software isn't strategic enough to necessitate support, or they just want to buy some time. For example, a very commonly used shim is a version-lie shim. To implement this shim, we intercept several APIs that are used to determine which version of Windows the application is running on. Normally, this information is passed on to Windows itself, and it answers truthfully. With the shim applied, however, these APIs are intercepted. Instead of passing on the request to Windows, a different version of Windows is returned (for example, Windows XP instead of Windows 7). If the application is programmed to run only on Windows XP, this is a way to trick the application into believing it's running on the correct OS. (Frequently this is all that is necessary to resolve an application compatibility problem!) There are a huge number of tricks you can play with shims. For example: The ForceAdminAccess shim tries to trick the application into believing that the current user is a member of the local Administrator group, even if he is not. (Many applications outright fail if you are not a local administrator, though you may be able to use other tricks, such as UAC File and Registry Virtualization, to resolve the issues that caused the check in the first place.) How it implements this check can be fairly straightforward. For example, this shim intercepts the API IsUserAnAdmin from shell32.dll. The complete source code of the shimmed function (which has wonderful performance characteristics compared to the actual API) is simply return TRUE. The WrpMitigation shim tricks application installers into believing they can write to files that are protected by Windows Resource Protection (WRP). If you try to write to a file that's protected, the shim first creates a new temporary file, marks it to be deleted once the handle is closed, and then returns the handle to the temporary file as if it were the actual protected file. The application installs the crusty old version of kernel32.dll or shell32.dll (or whichever other file it picked up while it was being packaged) into a temp file, but then that temp file goes away and the matching, patched, up-to-date version of the protected file remains on the file system. So, WRP can still ensure that you don't end up with an ancient copy of shell32.dll from Windows 95 on your computer, but the installer won't fail with ACCESS_DENIED when you use this shim. The CorrectFilePaths shim can redirect files from one location to another. So, if you have an application that is trying to write to c:\myprogramdir (which isn't automatically fixed using UAC File and Registry Virtualization), you can redirect the files that are modified at runtime to a per-user location. This allows you to run as a standard user without having to loosen access control lists (ACLs), because you know your security folks hate it when you loosen ACLs. NOTE: As shims run as user-mode code inside a user-mode application process, you cannot use a shim to fix kernel-mode code. For example, you cannot use shims to resolve compatibility issues with device drivers or with other kernel-mode code. (For example, some antivirus, firewall, and antispymware code runs in kernel mode.)

When can we use a Shim: You acquired the application from a vendor that is no longer in business. Several applications are from vendors that have since gone out of business; so clearly, support is no longer a concern. However, because the source code is not available, shimming is the only option for compatibility mitigation. You developed the application internally. While most customers would prefer to fix all their applications to be natively compatible, there are some scenarios in which the timing does not allow for this. The team may not be able to fix all of them prior to the planned deployment of new version of Windows, so they may choose to shim the applications that can be shimmed and modify the code on the ones where shims are insufficient to resolve the compatibility issue. You acquired the application from a vendor that will eventually be releasing a compatible version, but support is not critical. When an off-the-shelf application is neither business critical nor important, some customers use shims as a stopgap solution. Users could theoretically wait until a compatible version is available, and its absence would not block the deployment, but being able to provide users with a shimmed and functional version can bridge that gap until a compatible version is available.

Creating an Application Compatibility Shim If you are trying to run an application that was created for 2000 or XP and had problems running in Windows 7, you could always turn on compatibility mode for the executable on your machine. However if you are trying to create a shim that could be used on other machines as well, you could use the following instructions to create the shim and send it. It is a very small size and once executed, will always be associated with that executable on that machine.

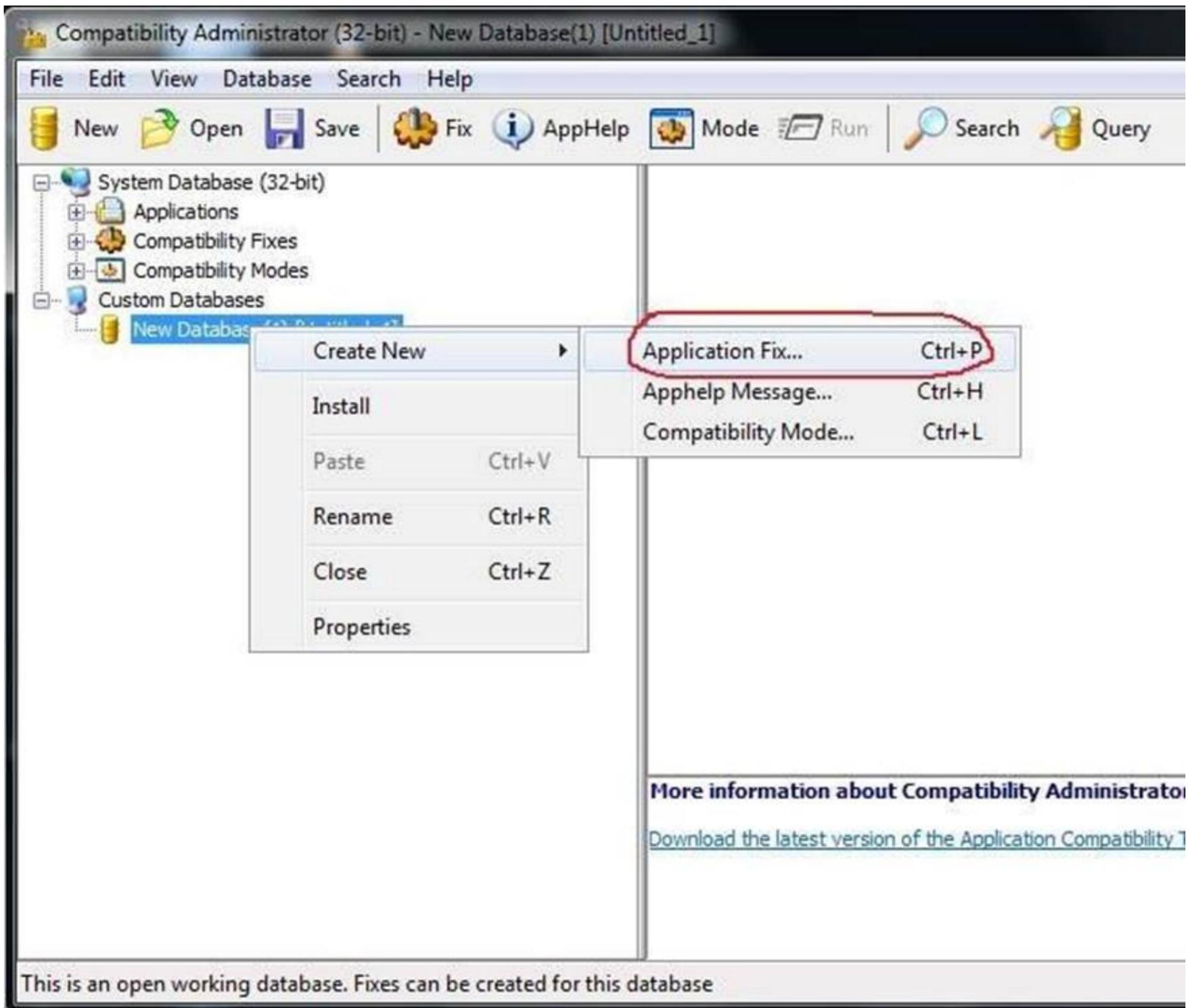
ACT is the Application Compatibility Toolkit. Download it from here:

<http://www.microsoft.com/downloads/details.aspx?familyid=24da89e9-b581-47b0-b45e-492dd6da2971&displaylang=en>

Once we launch the Compatibility Administrator Tool, from Start Menu – Microsoft Application Compatibility Toolkit:

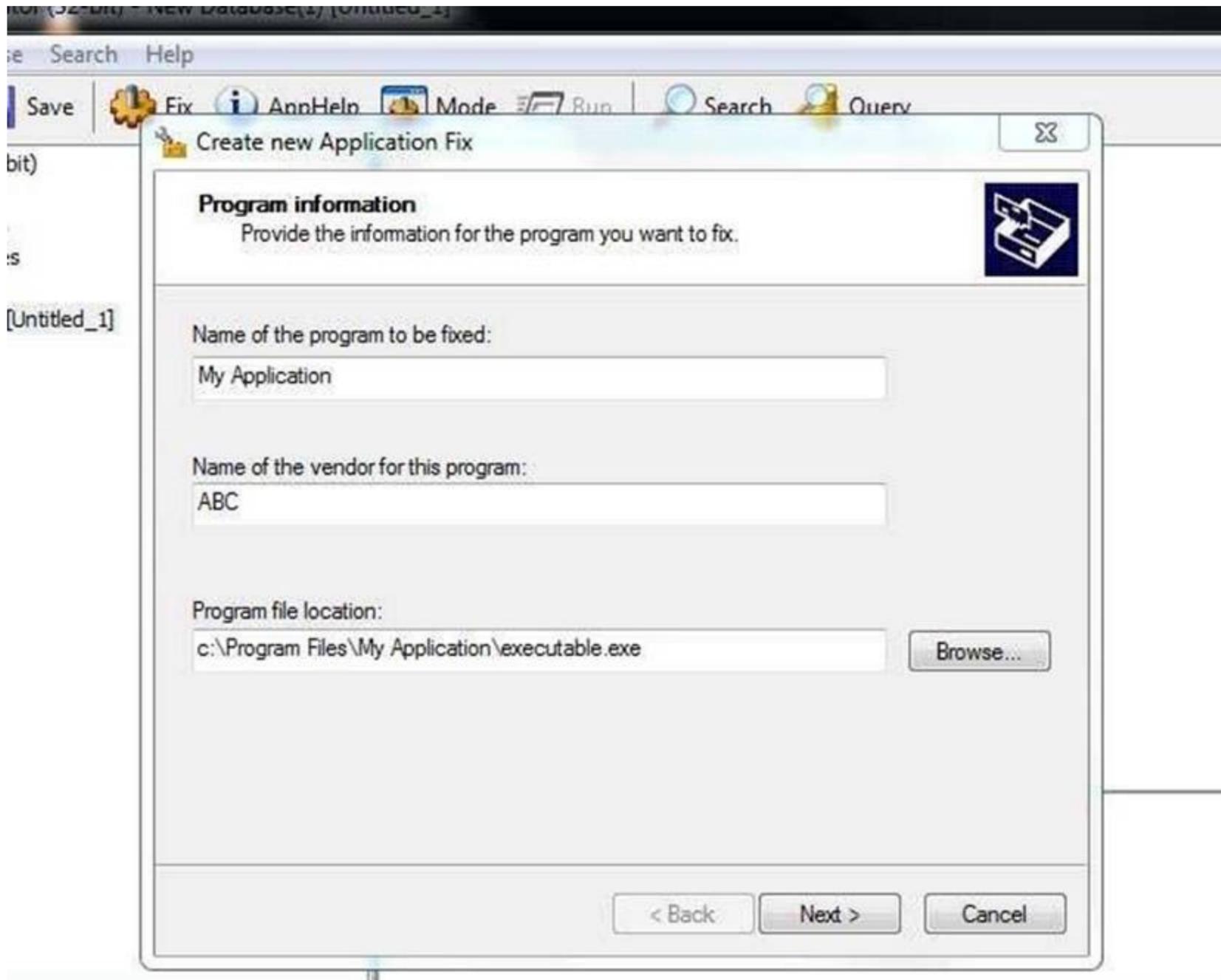


Right-click on New Database:



Choose Application Fix here. In this below dialog, give the application details and the executable you would want to fix:

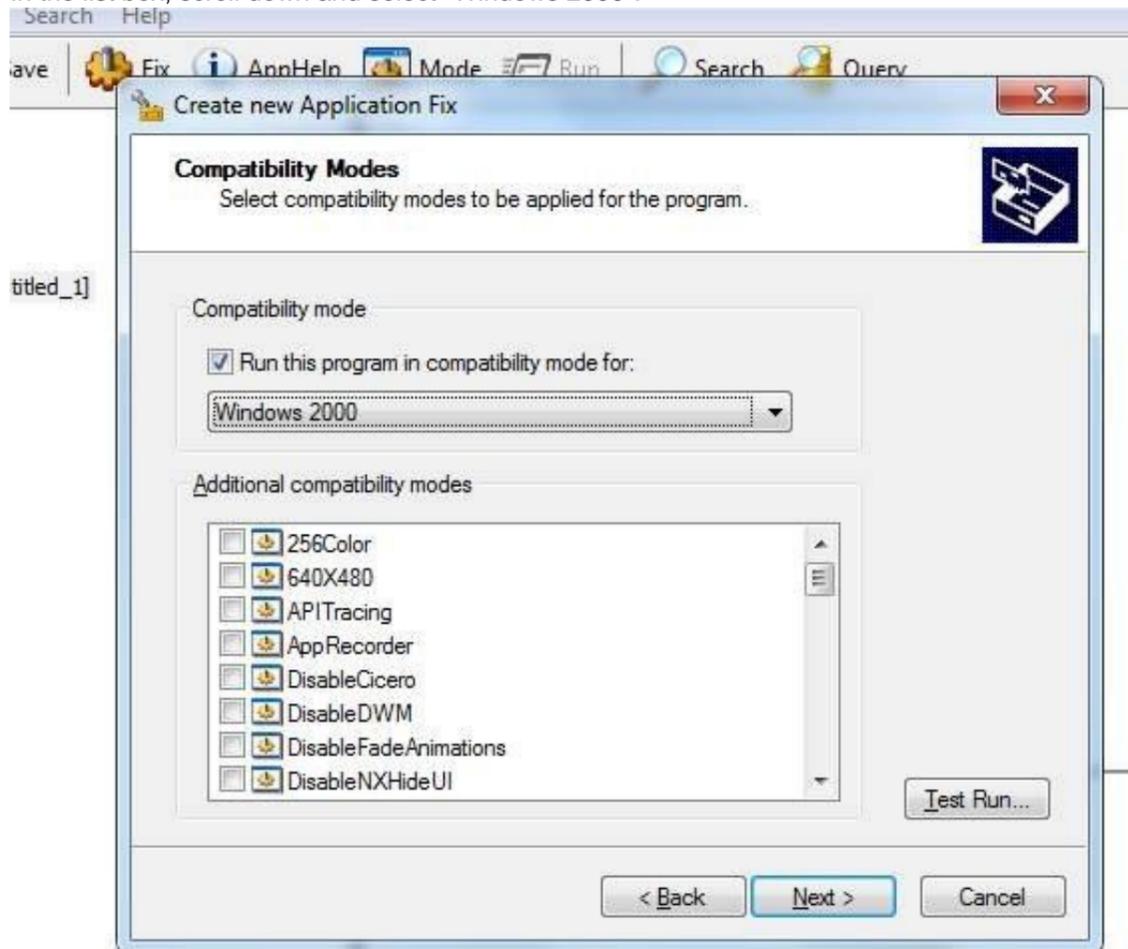
1. Type the name of the program to fix
2. Type the vendor name
3. Browse to location of executable



base. Fixes can be created for this database

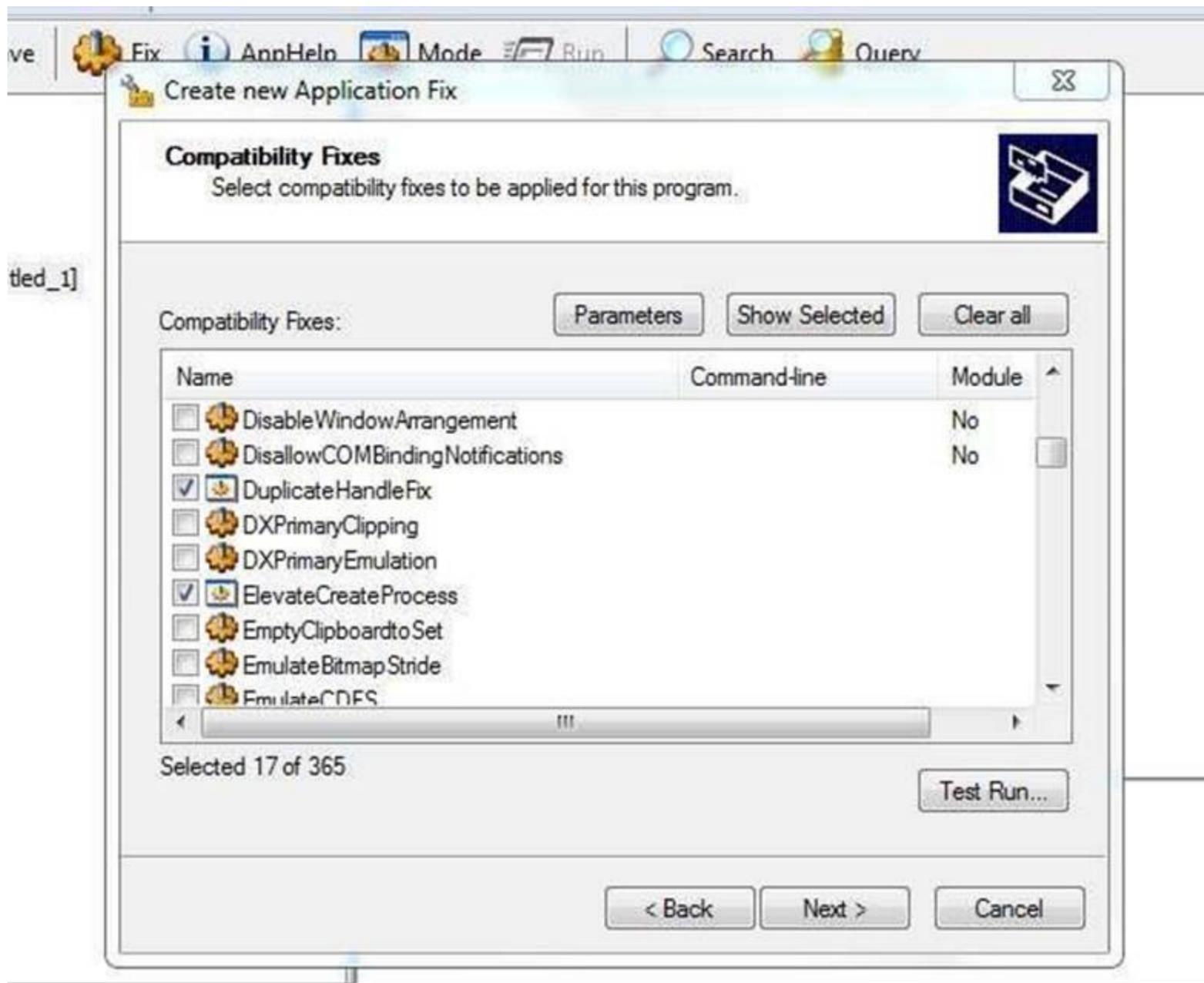
When you press the next button, you will get to see the list of the compatibility modes listed by default. If you have an issue with just version incompatibility then choose the version in which the application was working earlier. At this point I have already determined that Windows 2000 compatibility mode will work for this program.

In the list box, scroll down and select "Windows 2000".



se. Fixes can be created for this database

In the next window (when you have combination of shims to be chosen). As shown below, you have lots of shims to choose from. Select all the shims which would fix your application.

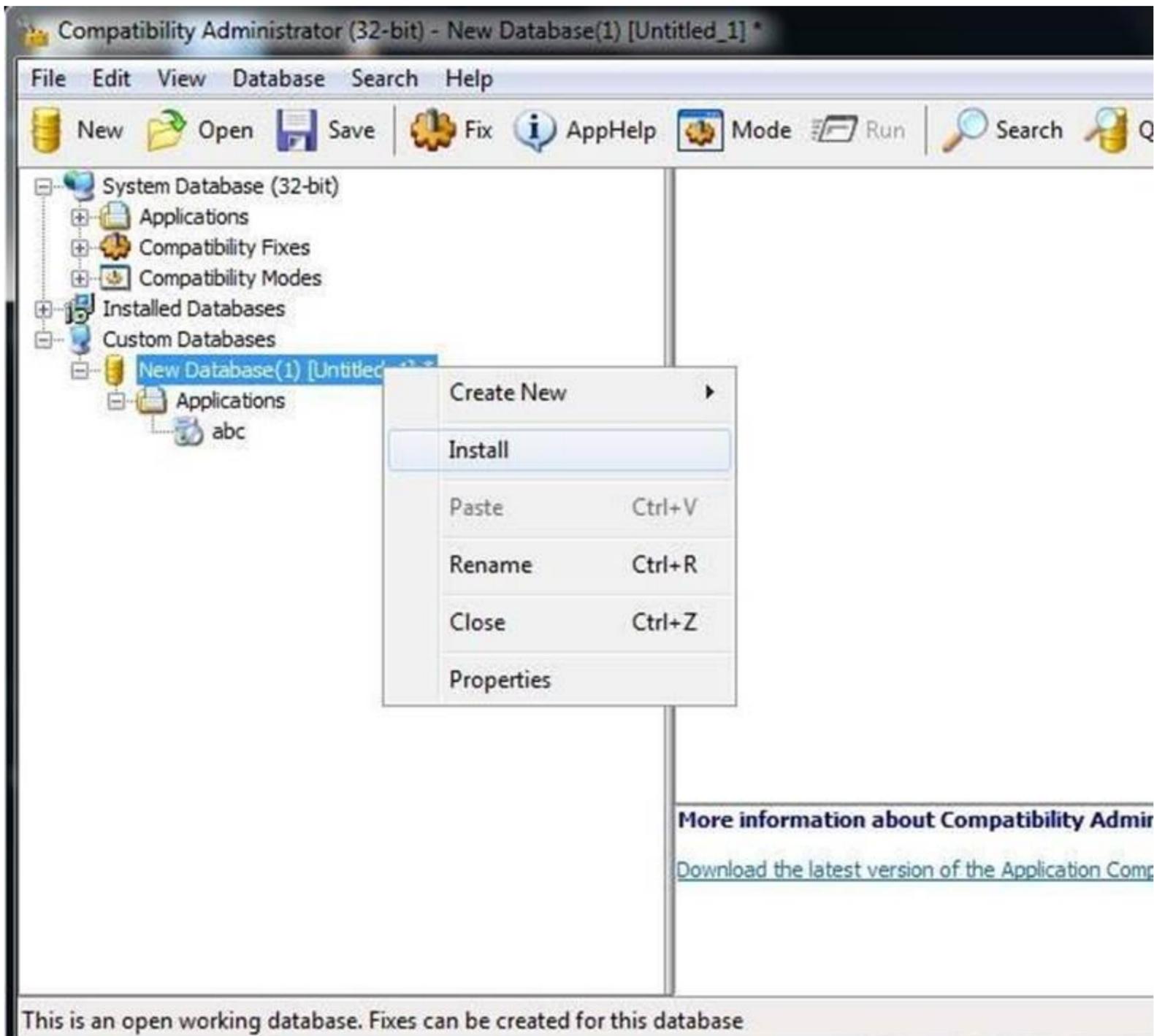


e. Fixes can be created for this database

Click on Finish. This will give you the complete summary of the application and the fixes applied.

Now you need to save this shim database file (A small database including the shim information is created), and install it. You can either install it by right-clicking on the shim and pressing the install button, or by using a command-line option, `sdbinst.exe <database.sdb>`.

NOTE: "sdbinst.exe" is already located by default in `c:\windows\system32`



Once the Application Compatibility Database is installed, we can run the program from the location specified earlier (in the first window). Now the program should be running in the Compatibility mode that you specified during the process.

NEW QUESTION 225

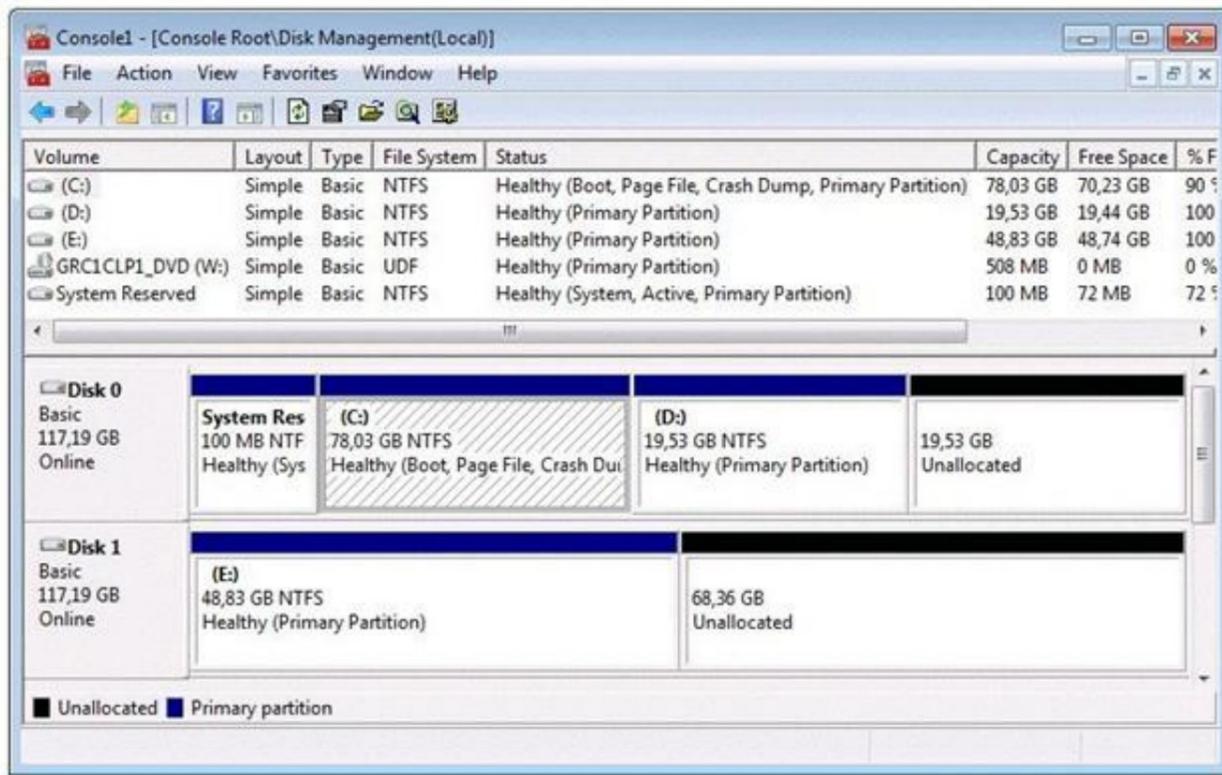
You are investigating instability and boot problems on a computer running Windows 7 Enterprise. You boot using the Last Known Good Configuration (Advanced) option and perform a system restore. This does not solve your problems, and you want to undo the system restore. Can you do this, and what is the reason for your answer?

- A. N
- B. You can undo a system restore only if you initiate it from the System Recovery tool
- C. N
- D. You can undo a system restore only if you carry it out after booting normal
- E. Ye
- F. You can always undo a system restore, no matter how you booted the computer or how you initiated the restor
- G. Ye
- H. You can undo a system restore that you perform after either booting normally or booting using Last Known Good Configuration (Advanced).

Answer: D

NEW QUESTION 230

You have a computer that runs Windows 7. The computer's disk is configured as shown in the exhibit. (Click the Exhibit button.)



You need to extend volume C.
 What should you do first?

- A. Back up and delete volume
- B. Convert disk 0 to a dynamic disk
- C. Remove the crash dump from volume
- D. Move the paging file from volume C to volume

Answer: A

Explanation:

Extend a Basic Volume You can add more space to existing primary partitions and logical drives by extending them into adjacent unallocated space on the same disk. To extend a basic volume, it must be raw or formatted with the NTFS file system. You can extend a logical drive within contiguous free space in the extended partition that contains it. If you extend a logical drive beyond the free space available in the extended partition, the extended partition grows to contain the logical drive. For logical drives, boot, or system volumes, you can extend the volume only into contiguous space and only if the disk can be upgraded to a dynamic disk. For other volumes, you can extend the volume into noncontiguous space, but you will be prompted to convert the disk to dynamic.

NEW QUESTION 235

You have a computer that runs windows vista. The computer has one partition and 1 GB of RAM.
 You need to upgrade the computer to windows 7.
 What should you do?

- A. Add 1 GB of RA
- B. Create a second partitio
- C. Disable User Account Control (UAC).
- D. Install windows Vista Service pack 2 (SP2)

Answer: D

Explanation:

You should keep the following in mind prior to and during the upgrade from Windows Vista to Windows 7:
 -Perform a full backup of the computer running Windows Vista prior to performing the installation. - That way, if things go wrong, you can do a full restore back to Windows Vista. You must ensure that Windows Vista has Service Pack 1 or later installed before you can upgrade it to Windows 7. - Ensure that you have the Windows 7 product key prior to the upgrade. - You cannot upgrade between processor architectures. An x86 version of Windows Vista cannot be upgraded to an x64 version of Windows 7, and vice versa. - You can upgrade only to an equivalent or higher edition of Windows 7. - You can upgrade Windows Vista Home Premium to Windows 7 Home Premium, Professional, Enterprise, or Ultimate, but not to Windows 7 Starter. Windows 7 Professional is equivalent to Windows Vista Business. - Ensure that there is at least 10 GB of free disk space on the Windows Vista volume prior to attempting the upgrade. 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

NEW QUESTION 237

You have a computer that runs Windows Vista. The hard disk is configured as shown in the exhibit. (Click the Exhibit button.)



You need to install Windows 7 in a dual-boot configuration. What should you do?

- A. From Windows Vista, extend Disk 0 Partition 1. Install Windows 7 in Disk 0 Partition 1.
- B. From Windows Vista, create a new partition.
- C. Install Windows 7 in Disk 0 Partition 1.
- D. Start the computer from the Windows 7 installation media.
- E. Install Windows 7 in Disk 0 Partition 1.
- F. Start the computer from the Windows 7 installation media.
- G. Install Windows 7 in the unallocated space on Disk 0.

Answer: D

Explanation:

The key to configuring dual-booting is ensuring that each operating system has its own partition or hard disk drive.

To dual-boot with Windows 7, you need to be able to create a new volume of at least 15 GB. Even if you have more free space available on the volume you want to shrink, you may not be able to create a volume of the appropriate size because Windows Vista may not be able to move some special types of data to a different place on the hard disk drive.

When configuring a new computer to boot between multiple operating systems, it is also necessary to install operating systems in the order that they were released. For example, if you want to boot between Windows XP and Windows 7 on a new computer, you need to install Windows XP before you install Windows 7. If you install Windows XP after Windows 7, the Windows XP installation routine cannot recognize the Windows 7 operating system installation, and the computer only boots into Windows XP. It is possible to repair the computer from this point using Windows 7 startup repair so that it dual-boots, but the simplest course of action is just to install the operating systems in the order in which they were released by Microsoft.

NEW QUESTION 242

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 70-680 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 70-680 Product From:

<https://www.2passeasy.com/dumps/70-680/>

Money Back Guarantee

70-680 Practice Exam Features:

- * 70-680 Questions and Answers Updated Frequently
- * 70-680 Practice Questions Verified by Expert Senior Certified Staff
- * 70-680 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 70-680 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year