Vendor: Microsoft

Exam Code: 70-680

Exam Name: TS: Windows 7, Configuring

Version: Demo

QUESTION 1
Your network consists of an Active Directory domain and a DirectAccess infrastructure.
You install Windows 7 on a new portable computer and join the computer to the domain.
You need to ensure that the computer can establish DirectAccess connections.
What should you do?

A. Install a computer certificate.
B. Create a new network connection.
C. Enable the Network Discovery firewall exception.
D. Add the computer account to the Network Configuration Operators group.

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

QUESTION 2
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 offline.
B. On Server1, configure BitLocker Drive Encryption. On Computer1, make Share1 available offline.
C. On Computer1, make Share1 available offline and enable encryption of offline files.
D. On Computer1, copy the files from Share1 to the Documents library and configure BitLocker Drive
   Encryption.

Correct Answer: C
Explanation:
Offline Files
The 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 Center
You 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.

QUESTION 3
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

Correct Answer: B
Explanation:
ScanState

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

QUESTION 4
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 Go.
B. A HomeGroup should be created.
C. The files should be moved to a Media Library.
D. All BranchCache rules should be enabled in Windows Firewall.
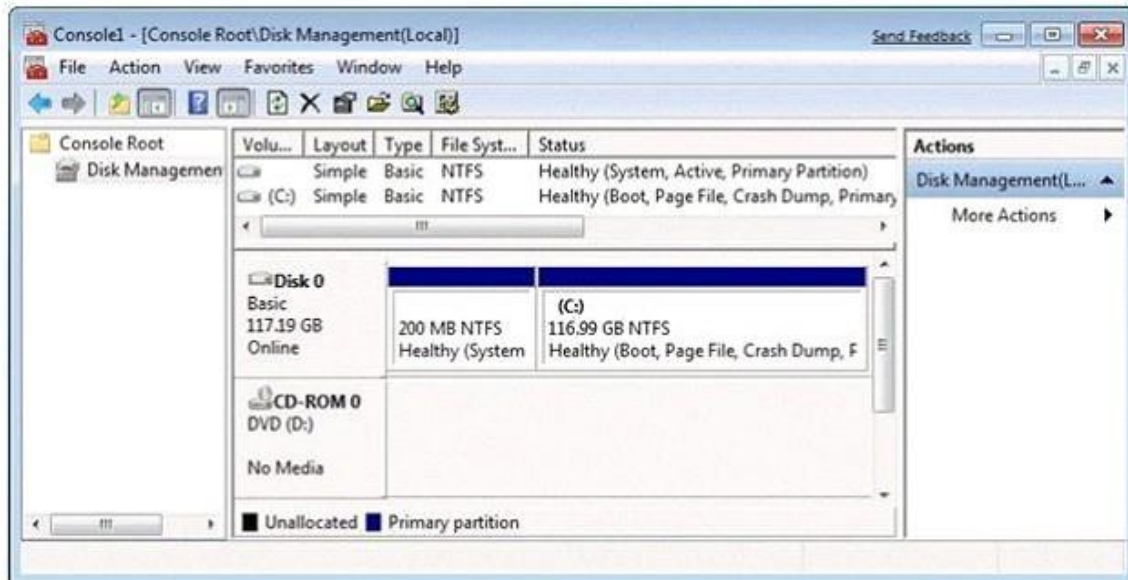
Correct Answer: BC

QUESTION 5
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 Monitor.
B. The informational events should be reviewed from Reliability Monitor.
C. The Software Environment should be reviewed from System Information.
D. The System Diagnostics Report should be reviewed from Performance Monitor.

Correct Answer: B

QUESTION 6

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

Correct 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.

QUESTION 7

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. On Computer2, restore %systemroot%\DigitalLocker.
B. On Computer1, export the data recovery agent certificate. On Computer2, import the data recovery agent certificate.
C. On Computer1, run Secedit.exe and specify the /export parameter. On Computer2, run Secedit.exe and specify the /import parameter.

D. On Computer1, run Cipher.exe and specify the /removeuser parameter. On Computer2, run Cipher.exe and specify the /adduser parameter.

Correct 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.

QUESTION 8
You have a computer that runs Windows 7.

You need to configure the computer to meet the following requirements:

▪ Generate a new security ID (SID) when the computer starts.
▪ Ensure that the Welcome screen appears when the computer starts.

What should you do?

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

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

QUESTION 9
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 Verify.
B. At a command prompt, run Sigverif.exe.
C. From Device Manager, click Scan for hardware changes.
D. From Device Manager, select the Devices by connection view.

Correct 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.

QUESTION 10
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-ons.
B. From Control Panel, open Default Programs and then click Set Associations.
C. From the local Group Policy, expand Computer Configuration and then click Software Settings.
D. From Window Explorer, right-click %programfiles%\Internet Explorer\iexplore.exe and then click Properties.

Correct Answer: B

QUESTION 11
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.)
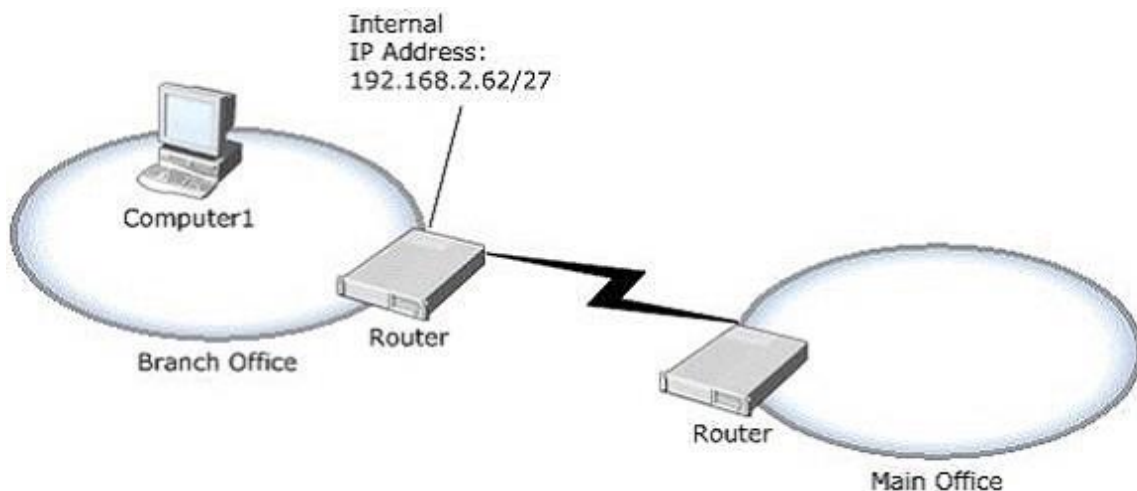
In the branch office, you deploy a new computer named Computer1 that runs Windows 7.
You need to assign an IP address to Computer1. Which IP address should you use?

A. 192.168.2.30
B. 192.168.2.40
C. 192.168.2.63
D. 192.168.2.65

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

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

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

Acceptable IP range: 192.168.2.33 - 192.168.2.62

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

```
Accepable IP ranges for those interested (excluding the 2 reserved IP addersses):
Segment 1: 192.168.2.1   - 192.168.2.30
Segment 2: 192.168.2.33  - 192.168.2.62
Segment 3: 192.168.2.65  - 192.168.2.94
Segment 4: 192.168.2.97  - 192.168.2.126
Segment 5: 192.168.2.129 - 192.168.2.158
Segment 6: 192.168.2.161 - 192.168.2.190
Segment 7: 192.168.2.193 - 192.168.2.222
Segment 8: 192.168.2.225 - 192.168.2.254
```

```
Segments for those interested (including the 2 reserved IP addersses):
Segment 1: 192.168.2.0   - 192.168.2.31
Segment 2: 192.168.2.32  - 192.168.2.63
Segment 3: 192.168.2.64  - 192.168.2.95
Segment 4: 192.168.2.96  - 192.168.2.127
Segment 5: 192.168.2.128 - 192.168.2.159
Segment 6: 192.168.2.160 - 192.168.2.191
Segment 7: 192.168.2.192 - 192.168.2.223
Segment 8: 192.168.2.224 - 192.168.2.255
```

QUESTION 12
You work in an international company which is named Wiikigo. Before entering this company, you have two years of experience in the IT field, as well as experience implementing and administering any Windows client operating system in a networked environment. You are professional in installing, upgrading and migrating to Windows 7, deploying Windows 7, and configuring Hardware and Applications and son on. You are in charge of a computer that runs Windows Vista. You have Windows 7 installed on a new partition on the computer. You have to make sure that the computer always starts Windows Vista by default. So what action should you perform to make sure of this?

A. In order to make sure that the computer always starts Windows Vista by default, a boot.ini file should be created in the root of the Windows 7 partition.
B. In order to make sure that the computer always starts Windows Vista by default, a boot.ini file should be created in the root of the Windows Vista partition.
C. In order to make sure that the computer always starts Windows Vista by default, Bcdedit.exe should be run and the /default parameter should be specified.
D. In order to make sure that the computer always starts Windows Vista by default, Bcdedit.exe should be run and the /bootems parameter should be specified.

Correct Answer: C

QUESTION 13
You have a computer that runs Windows 7. You run Ipconfig as shown in the exhibit. (Click the Exhibit button.)
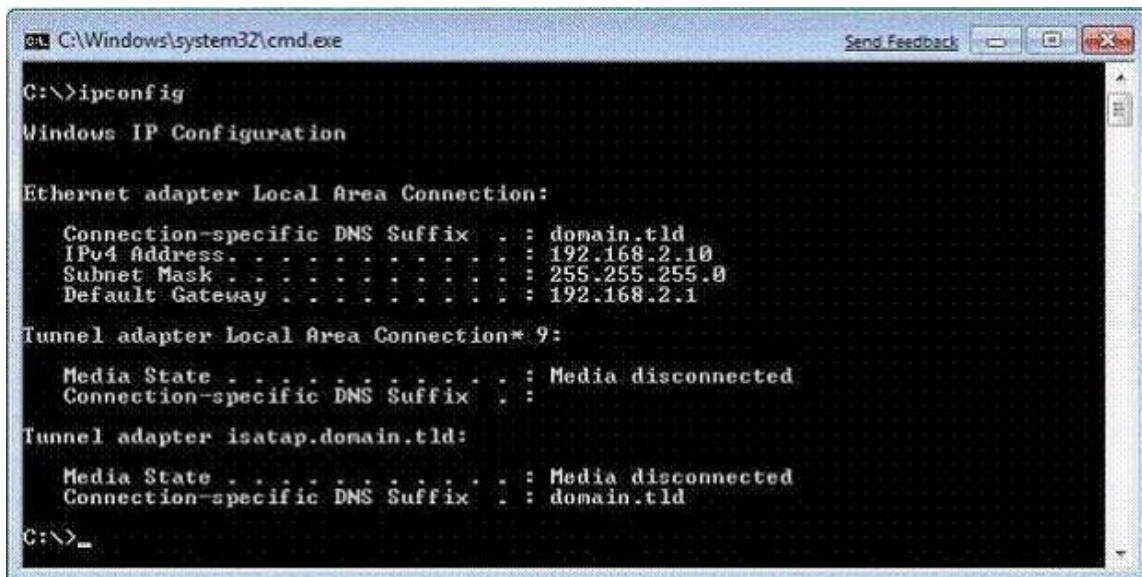
You need to ensure that you can establish a DirectAccess connection to the network. What should you do first?

A. Create a new VPN connection.
B. Configure a static IPv4 address.
C. Enable IPv6 on the network adapter.
D. Add an additional default gateway address.

Correct Answer: C

QUESTION 14
You have a computer that runs Windows Vista. The computer contains a custom application. You need to export the user state and the settings of the custom application. What should you do?

A. Run Loadstate.exe and specify the /config parameter.
B. Run Scanstate.exe and specify the /genconfig parameter.
C. Modify the miguser.xml file. Run Loadstate.exe and specify the /ui parameter.
D. Modify the migapp.xml file. Run Scanstate.exe and specify the /i parameter.

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

QUESTION 15
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.

Correct 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.

QUESTION 16
You have a computer that runs Windows 7. You discover that an application named App1 runs during the startup process. You need to prevent only App1 from running during startup. Users must be allowed to run App1 manually. What should you do?

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

Correct Answer: D

QUESTION 17
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.)
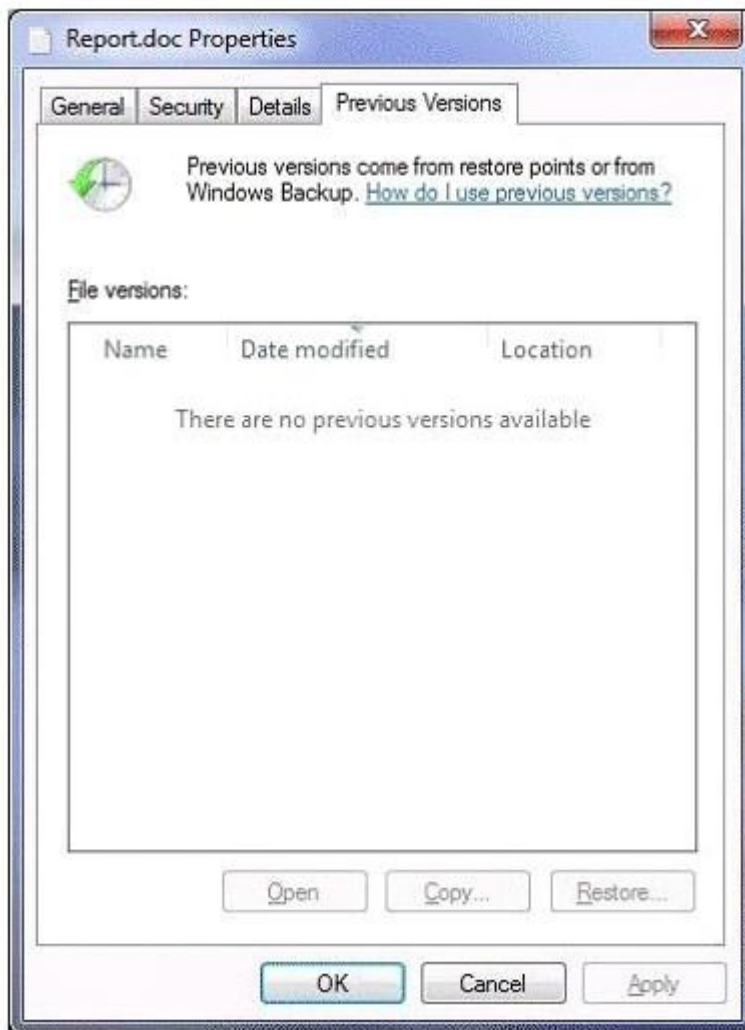
You need to ensure that you can restore the current version of the document if the document is

modified. What should you do first?

A. Run Disk Cleanup on volume D.
B. Enable auditing on the document.
C. Turn on System Protection for volume D.
D. Start the Volume Shadow Copy Service (VSS).

Correct 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.

QUESTION 18
You start a computer by using Windows Preinstallation Environment (Windows PE). You need to dynamically load a network adapter device driver in Windows PE. What should you do?

A. Run Peimg.exe and specify the device driver path.
B. Run Drvload.exe and specify the device driver path.
C. Run Winpeshl.exe and specify a custom Winpeshl.ini file.
D. Run Wpeutil.exe and specify the InitializeNetwork command.

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

QUESTION 19
Your company has an Active Directory domain. All computers are members of the domain. Your network contains an internal Web site that uses Integrated Windows Authentication. From a computer that runs Windows 7, you attempt to connect to the Web site and are prompted for authentication. You verify that your user account has permission to access the Web site. You need to ensure that you are automatically authenticated when you connect to the Web site. What should you do?

A. Create a complex password for your user account.

B. Open Credential Manager and modify your credentials.
C. Add the URL of the Web site to the Trusted sites zone.
D. Add the URL of the Web site to the Local intranet zone.

Correct Answer: D
Explanation:
Local Intranet Sites in the Local Intranet zone are computers on your organizational intranet. Internet Explorer can be configured to detect intranet sites automatically. It is also possible to add Web sites to this zone by clicking the Advanced button on the Local Intranet sites dialog box, as shown in the figure. The default security level of this zone is Medium-Low. Protected Mode is not enabled by default for sites in this zone.
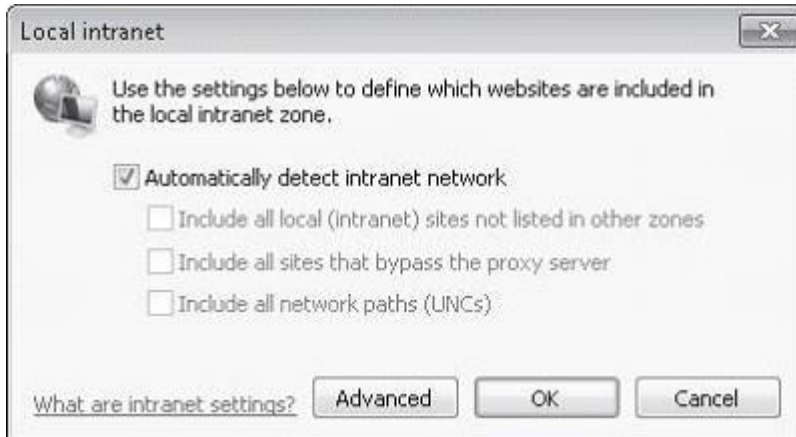
Security settings are configured primarily by assigning sites to zones. Sites that require elevated privileges should be assigned to the Trusted Sites zone. Sites that are on the intranet are automatically assigned to the Local Intranet zone, though this may require manual configuration in some circumstances. All other sites are assigned to the Internet zone. The Restricted Sites zone is used only for Web sites that may present security risks but must be visited.

QUESTION 20
Your network contains a wireless access point. You have a computer that runs Windows 7. The computer connects to the wireless access point. You disable Service Set Identifier (SSID) broadcasts on the wireless access point. You discover that you are now unable to connect to the wireless access point from the Windows 7 computer. You need to ensure that the computer can connect to the wireless access point. What should you do?

A. From Credential Manager, modify the generic credentials.
B. From Credential Manager, modify the Windows credentials.
C. From Network and Sharing Center, turn on Network discovery.
D. From Network and Sharing Center, modify the wireless network connection settings.

Correct Answer: D
Explanation:
Wireless Network Connection settingsTo connect to a wireless network that does not broadcast its SSID, you need to know details such as the network name and security type. In Network And Sharing Center, you click Set Up A Connection Or Network, click Manually Connect To A Wireless Network, and click Next. You are prompted for the network name and security type and (if appropriate) encryption type and security key. Alternatively, you can open an elevated command prompt and enter a command with the following syntax:

netsh wlan connect name=<profile_name> ssid-<network_ssid> [interface=<interface_name>] (Since the computer has previously been connected, just modify the settings.)NOT Network DiscoveryNetwork Discovery allows the client running Windows 7 to locate other computers and devices on the network. It also makes the client visible to other computers on the network. Disabling Network Discovery does not turn off other forms of sharing.NOT Credential ManagerCredential Manager stores logon user name and passwords for network resources, including file servers, Web sites, and terminal services servers. Credential Manager stores user name and password data in the Windows Vault. You can back up the Windows Vault and restore it on other computers running Windows 7 as a method of transferring saved credentials from one computer to another. Although Credential Manager can be used to back up some forms of digital certificates, it cannot be used to back up and restore the self-signed Encrypting File System (EFS) certificates that Windows 7 generates automatically when you encrypt a file. For this reason, you must back up EFS certificates using other tools. You will learn about backing up EFS certificates later in this lesson.

QUESTION 21
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 rule.
B. From the local Group Policy, modify the application control policies.
C. From Windows Firewall, modify the Allowed Programs and Features list.
D. From Network and Sharing Center, modify the Advanced Sharing settings.

Correct 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.

QUESTION 22
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.

Correct Answer: D

QUESTION 23
Your network has a main office and a branch office. The branch office has computers that run
Windows 7. A network administrator enables BranchCache in the main office. You run Netsh on
your computer as shown in the exhibit. (Click the Exhibit button.)

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

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

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

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

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

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

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

QUESTION 24
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 group.
B. From the printer's properties, assign the Manage Documents permission to the Sales group.
C. From the local Group Policy, assign the Increase scheduling priority user right to the Sales group.
D. From the local Group Policy, assign the Take ownership of files or other objects user right to the Sales group.

Correct 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.

QUESTION 25
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 Manager.
B. The Authorization Manager options should be modified from Authorization Manager.
C. Del should be run and the /p parameter should be specified.
D. Runas should be run and the /noprofile parameter should be specified.

Correct Answer: A

QUESTION 26
You have a computer that runs Windows 7. The computer has System Protection enabled. You need to retain only the last System Protection snapshot of the computer. All other snapshots must be deleted. What should you do?

A. Run Disk Cleanup for Programs and features.
B. Run Disk Cleanup for System Restore and Shadow Copies.
C. From the System Protection Restore settings, select Turn off System Restore.
D. From the System Protection Restore settings, select Only restore previous versions of files.

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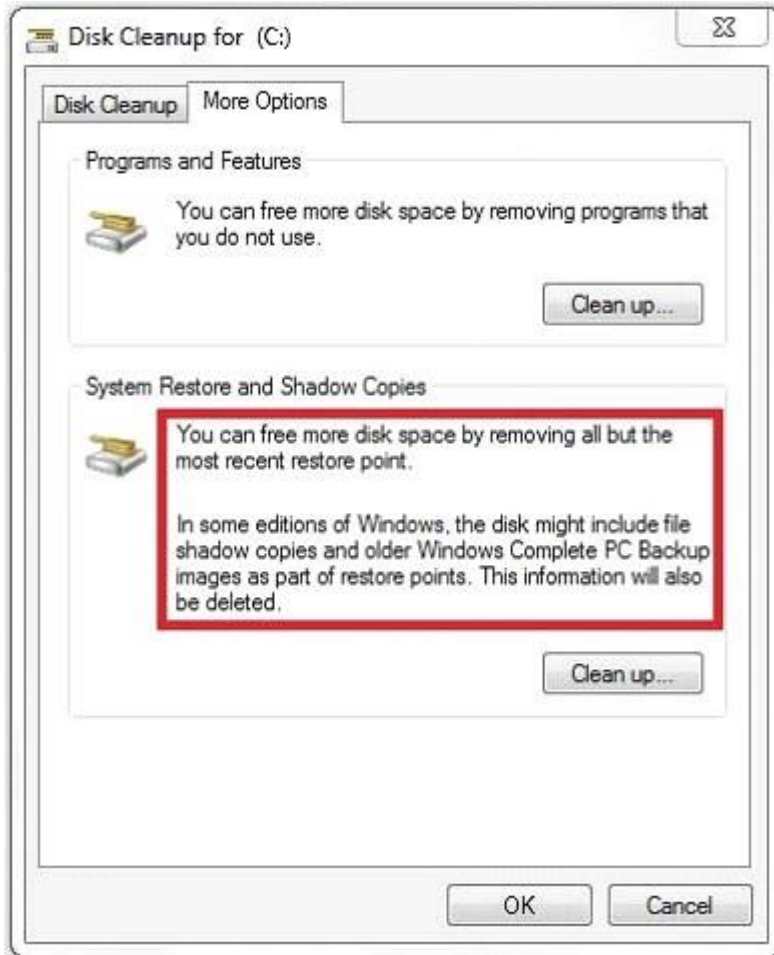
Shadow info:
Shadow copies are automatically saved as part of a restore point. If system protection is enabled,
Windows 7 automatically creates shadow copies of files that have been modified since the last
restore point was created. By default, new restore points are created every seven days or
whenever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

QUESTION 27
You have a reference computer that runs Windows 7. You plan to deploy an image of the
computer. You create an answer file named answer.xml. You need to ensure that the installation
applies the answer file after you deploy the image. Which command should you run before you
capture the image?

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

Correct Answer: D
Explanation:
To prepare the reference computer for the user, you use the Sysprep utility with the /generalize
option to remove hardware-specific information from the Windows installation and the /oobe
option to configure the computer to boot to Windows Welcome upon the next restart. Open an

elevated command prompt on the reference computer and run the following command:
c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown Sysprep prepares the
image for capture by cleaning up various user-specific and computer-specific settings, as well as
log files. The reference installation now is complete and ready to be imaged.

QUESTION 28
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 vdisk.
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 settings.

Correct 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.

QUESTION 29
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 Offline.
B. From the Safety menu, click InPrivate Filtering.
C. From the Security tab, add the intranet Web site to the Trusted sites zone.
D. From the Safety menu, click InPrivate Browsing.

Correct 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.

QUESTION 30
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

Correct Answer: C
Explanation:
WPA and WPA2 indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. WPA2 enhances WPA, which in turn addresses weaknesses in the previous system, WEP. WPA was intended as an intermediate measure to take the place of WEP while an IEEE 802.11i standard was prepared. 802.1X provides port-based authentication, which involves communications between a supplicant (a client computer), an authenticator (a wired Ethernet switch or WAP), and an authentication server (typically a Remote Authentication Dial In User Service, or RADIUS, server).

WPA2-Enterprise
WPA-Enterprise and WPA2-Enterprise authenticate through the Extensible Authentication Protocol (EAP) and require computer security certificates rather than PSKs. The following EAP types are included in the certification program:

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

If you want to use AES and to use computer certificates rather than a PSK, you would choose WPA2- Enterprise.WPA2-PersonalIf you have a small network that is not in a domain and cannot access a CA server, but you install a modernWAP that supports AES, you would use WPA2-Personal (with a PSK).WPA-Personal
If you have a small network that is not in a domain and cannot access a CA server and your WAP does not support AES, you would use WPA-Personal.802.1x
If you have a RADIUS server on your network to act as an authentication server and you want the highest possible level of security, you would choose 802.1X.

QUESTION 31
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

Correct 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

QUESTION 32
You work in an international company which is named Wiikigo. Before entering this company, you have two years of experience in the IT field, as well as experience implementing and administering any Windows client operating system in a networked environment. You are professional in installing, upgrading and migrating to Windows 7, deploying Windows 7, and configuring Hardware and Applications and son on. You are in charge of two computers that are respectively named C01 and C02. C01 runs Windows 7 and C02 runs Windows XP Professional.

On C01, you enable Remote Desktop as shown in the Remote Desktop exhibit. What action should you perform?

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

Correct Answer: A

QUESTION 33
You have a computer that runs Windows 7. The computer connects to the corporate network by using a VPN connection. You need to ensure that you can access the Internet when the VPN connection is active. The solution must prevent Internet traffic from being routed through the VPN connection. What should you do?

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

Correct 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.

QUESTION 34
You have a stand-alone computer that runs Windows 7. You open Windows Update as shown in the exhibit. (Click the Exhibit button.)
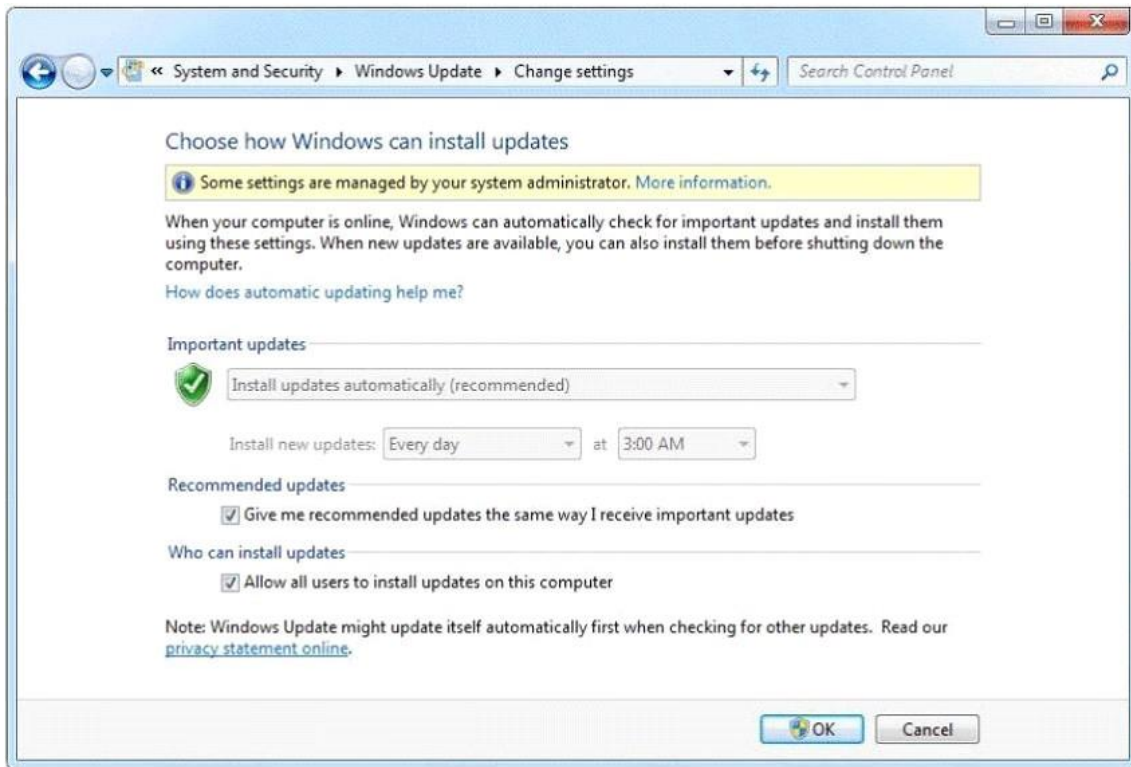
You need to ensure that you can manually change the Windows Update settings on the computer. What should you do?

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

Correct 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.
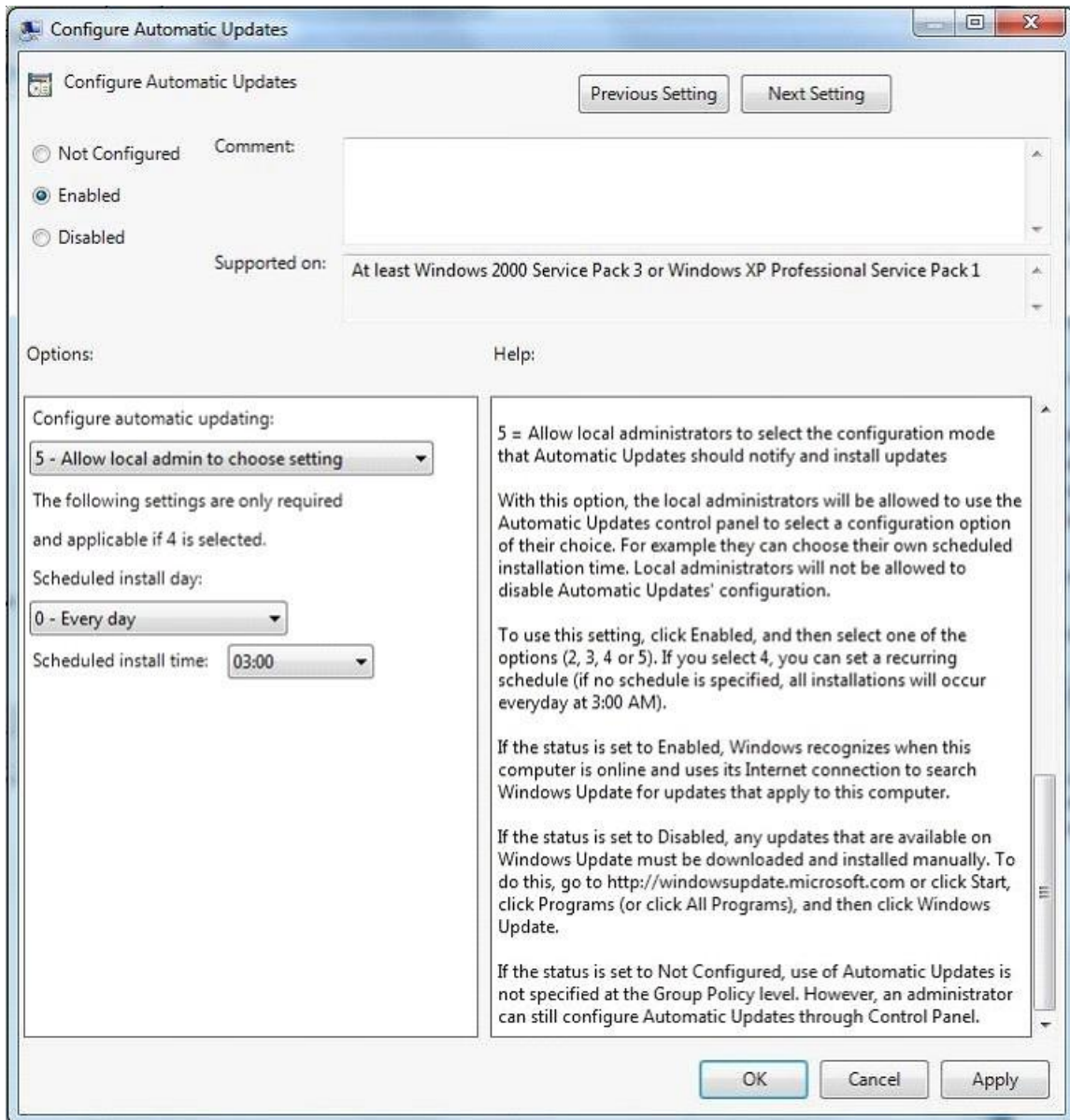
QUESTION 35
You have a computer that runs Windows 7 Professional. A USB disk is attached to the computer.
You need to ensure that you can enable BitLocker to go on the USB disk. What should you do?

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).

Correct Answer: B
Explanation:
Windows 7 ProfessionalWindows 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 EditionsThe 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.

QUESTION 36
You work in an international company which is named Wiikigo. Before entering this company, you have two years of experience in the IT field, as well as experience implementing and administering any Windows client operating system in a networked environment. You are professional in installing, upgrading and migrating to Windows 7, deploying Windows 7, and configuring Hardware and Applications and son on. You manage a stand-alone computer which has only one partition. Windows 7 is run by this computer. The computer is shared by two users that are respectively named User1 and User2. User01 uses Encrypting File System (EFS) to encrypt a file. User01 tries to grant User2 access to the file as shown in the exhibit. You have to make sure that User1 are able to grant User2 access to the file. So what action should you perform to make sure of this?

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

Correct Answer: B

QUESTION 37
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 settings.
B. From the local Group Policy, modify the Windows Update settings.
C. From the System settings, modify the System Protection settings.
D. From the local Group Policy, modify the Location and Sensors settings.

Correct Answer: B

QUESTION 38
You have a reference computer that runs Windows 7. You plan to create an image of the computer and then deploy the image to 100 computers. You need to prepare the reference computer for imaging. What should you do before you create the image?

A. Run Package Manager.
B. Run the System Preparation tool.
C. Install the User State Migration Tool.
D. Install Windows Automated Installation Kit.

Correct 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.

QUESTION 39
You plan to install Windows 7 by using a Windows 7 DVD.You need to perform an automated installation of Windows 7. What should you do?

A. Create an answer file named oobe.xml. Copy the file to a network share.
B. Create an answer file named winnt.sif. Place the file on a removable drive.
C. Create an answer file named sysprep.inf. Copy the file to a network share.
D. Create an answer file named autounattend.xml. Place the file on a removable drive.

Correct Answer: D

QUESTION 40
You have a computer that runs Windows 7. You need to prevent Internet Explorer from saving any data during a browsing session. What should you do?

A. Disable the BranchCache service.
B. Modify the InPrivate Blocking list.
C. Open an InPrivate Browsing session.
D. Modify the security settings for the Internet zone.

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

QUESTION 41
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.

Correct Answer: C

QUESTION 42
You have a computer that runs Windows 7. You run the Configure Backup wizard as shown in the exhibit. (Click the Exhibit button.)
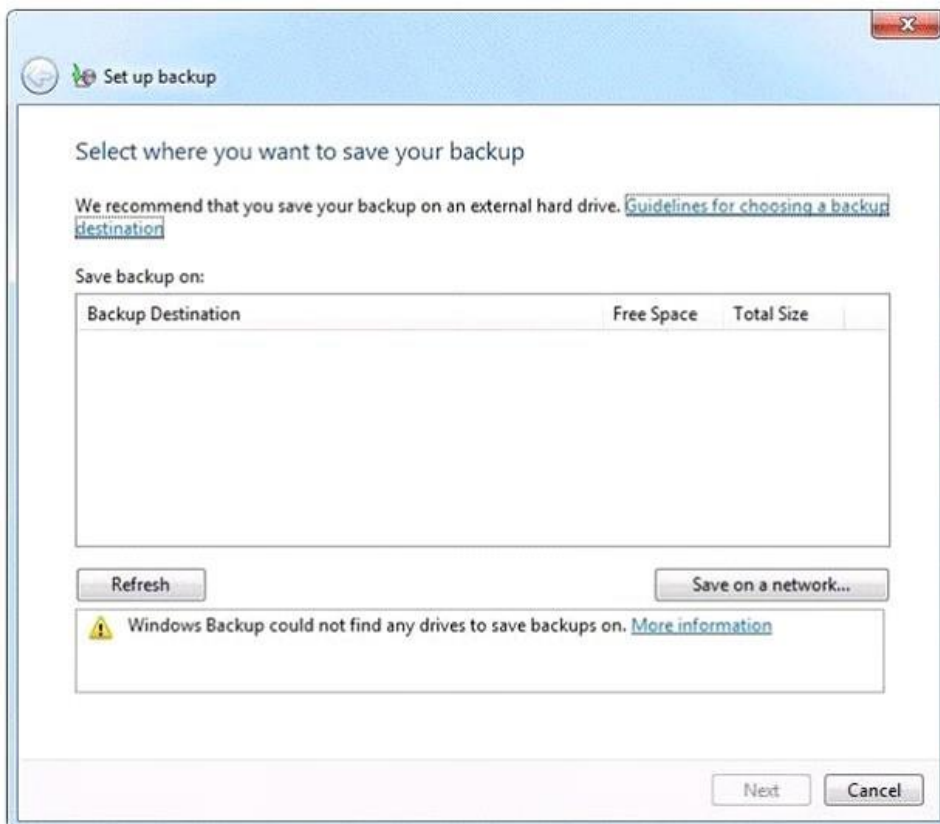
You need to ensure that you can back up the computer to a local disk drive. What should you do before you run the Configure Backup wizard?

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.

Correct 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 AdministratorYou 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 OperatorsMembers 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 VSSVSS 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.

QUESTION 43
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 rules.
D. From Application Control Policies, create an executable rule.

Correct Answer: D
Explanation:
Executable Rules
Executable rules apply to files that have .exe and .com file extensions. AppLocker policies are primarily about executable files, and it is likely that the majority of the AppLocker policies that you work with in your organizational environment will involve executable rules. The default executable rules are path rules that allow everyone to execute all applications in the Program Files folder and the Windows folder. The default rules also allow members of the administrators group to execute applications in any location on the computer. It is necessary to use the default executable rules, or rules that mirror their functionality, because Windows does not function properly unless certain applications, covered by these default rules, are allowed to execute. When you create a rule, the scope of the rule is set to Everyone, even though there is not a local group named Everyone. If

you choose to modify the rule, you can select a specific security group or user account. NOT Default rulesDefault rules are a set of rules that can be created automatically and which allow access to default Windows and program files. Default rules are necessary because AppLocker has a built-in fallback block rule that restricts the execution of any application that is not subject to an Allow rule. This means that when you enable AppLocker, you cannot execute any application, script, or installer that does not fall under an Allow rule. There are different default rules for each rule type. The default rules for each rule type are general and can be tailored by administrators specifically for their environments. For example, the default executable rules are path rules. Security-minded administrators might replace the default rules with publisher or hash rules because these are more secure.NOT Path RulesPath rules, allow you to specify a file, folder, or registry key as the target of a Software Restriction Policy. The more specific a path rule is, the higher its precedence. For example, if you have a path rule that sets the file C: \Program files\Application\App.exe to Unrestricted and one that sets the folder C:\Program files\Application to Disallowed, the more specific rule takes precedence and the application can execute. Wildcards can be used in path rules, so it is possible to have a path rule that specifies C:\Program files\Application*.exe. Wildcard rules are less specific than rules that use a file's full path. The drawback of path rules is that they rely on files and folders remaining in place. For example, if you created a path rule to block the application C:\Apps\Filesharing.exe, an attacker could execute the same application by moving it to another directory or renaming it something other than Filesharing.exe. Path rules work only when the file and folder permissions of the underlying operating system do not allow files to be moved and renamed.NOT Hash RulesHash rules, work through the generation of a digital fingerprint that identifies a file based on its binary characteristics. This means that a file that you create a hash rule for will be identifiable regardless of the name assigned to it or the location from which you access it. Hash rules work on any file and do not require the file to have a digital signature. The drawback of hash rules is that you need to create them on a per-file basis. You cannot create hash rules automatically for Software Restriction Policies; you must generate each rule manually. You must also modify hash rules each time that you apply a software update to an application that is the subject of a hash rule. Software updates modify the binary properties of the file, which means that the modified file does not match the original digital fingerprint.

QUESTION 44
You have a computer that runs Windows 7. Multiple users log on to the computer. You need to deny one user access to removable devices on the computer. All other users must have access to the removable drives. What should you do?

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

Correct Answer: D

QUESTION 45
You have a computer that runs Windows 7. The IPv6 address of the computer is configured automatically. You need to identify the IPV6 address of the computer. What should you do?

A. At the command prompt, run Netstat.
B. At the command prompt run Net config.
C. From the network connection status, click Details.
D. From network connection properties, select Internet Protocol Version 6 (TCP/IPv6) and click Properties.

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

QUESTION 46
You have a computer that runs Windows 7. You need to view the processes that currently generate network activity. What should you do?

A. Open Resource Monitor and click the Network tab.
B. Open Windows Task Manager and click the Networking tab.
C. Open Event Viewer and examine the NetworkProfile Operational log.
D. Open Performance Monitor and add all the counters for network interface.

**Correct Answer:** A
Explanation:
Resource Monitor
Windows 7 offers an enhanced version of the Resource Monitor tool. Windows 7 Resource Monitor allows you to view information about hardware and software resource use in real time.

You can filter the results according to the processes or services that you want to monitor. You can also use Resource Monitor to start, stop, suspend, and resume processes and services, and to troubleshoot unresponsive applications. You can start Resource Monitor from the Processes tab of Task Manager or by entering resmon in the Search box on the Start menu. To identify the network address that a process is connected to, click the Network tab and then click the title bar of TCP Connections to expand the table. Locate the process whose network connection you want to identify. You can then determine the Remote Address and Remote Port columns to see which network address and port the process is connected to.
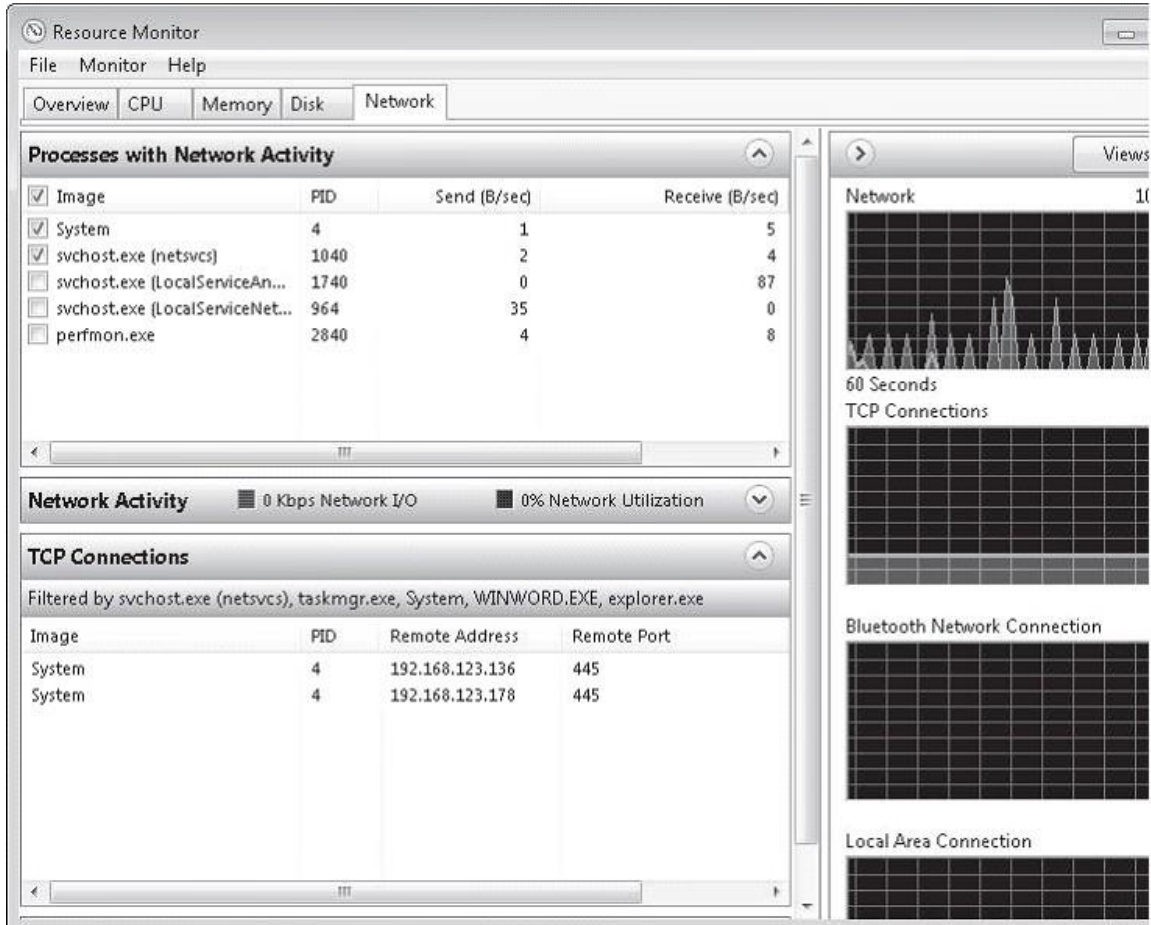
QUESTION 47
You have a computer that runs Windows 7. The computer contains two volumes, C and D.
You create a new folder called D:\Reports. You need to ensure that all files stored in the Reports folder are indexed by Windows Search. What should you do?

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

Correct 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.

QUESTION 48
You have a computer that runs Windows 7. You update the driver for the computer's video card and the computer becomes unresponsive. You need recover the computer in the minimum amount of time. What should you do?

A. Restart in safe mode and then roll back the video card driver.
B. Restart in safe mode and then revert the computer to a previous restore point.
C. Start the computer from the Windows 7 installation media. Select Repair your computer and then select System Restore.
D. Start the computer from the Windows 7 installation media. Select Repair your computer and then select System Image Recovery.

Correct Answer: A
Explanation:
If you install a driver that causes your computer to become unstable, you should first attempt to roll back the driver. If this does not solve the problem, you can restore system files and settings by performing a system restore to restore the computer to its last system restore point. A system restore returns a computer system to a selected restore point. System restores do not alter user files. Note that a system restore is not the same as a System Image restore.

QUESTION 49
You plan to install Windows 7 on a computer that contains a single hard disk drive. The hard disk drive is connected to a RAID controller. During the installation, you discover that the Windows 7 installation media does not include the files required to install the RAID controller. You need ensure that you can install Windows 7 on the hard disk drive. What should you do?

A. Insert the Windows installation media and press F8 during the computer's power-on self test (POST).
B. Insert the Windows installation media and press F6 during the computer's power-on self test (POST).
C. Start the computer from the Windows installation media. From the Install Windows dialog box, click Load Driver.
D. Start the computer from the Windows installation media. From the Install Windows dialog box, click Drive options (advanced).

Correct Answer: C
Explanation:
If your computer has special disk drive hardware, such as a redundant array of independent disks (RAID) array, it may be necessary to use the Load Driver option. It is necessary to use this option only if the disk that you want to install Windows on is not shown as a possible install location. If your disk is shown as an available option, Windows 7 has already loaded the appropriate drivers. Once you select the location where you want to install Windows 7, the Windows 7 installation process begins.

QUESTION 50
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 option.
B. Start the computer from the Windows 7 installation media and select the Custom (advanced) option.
C. From Windows Vista, run Setup.exe from the Windows 7 installation media and select the Upgrade option.
D. From Windows Vista, run Setup.exe from the Windows 7 installation media and select the Custom (advanced) option.

Correct 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.

EnsurePass.com Members Features:

1.   Verified Answers researched by industry experts.
2.   Q&As are downloadable in PDF and VCE format.
3.   98% success Guarantee and **Money Back** Guarantee.
4.   Free updates for **180** Days.
5.   **Instant Access to download the Items**

View list of All Exam provided:
http://www.ensurepass.com/certfications?index=A

To purchase Lifetime Full Access Membership click here:
http://www.ensurepass.com/user/register

Valid Discount Code for 2015: JREH-G1A8-XHC6

To purchase the HOT Microsoft Exams:

Microsoft			
70-243	**70-347**	**70-466**	**70-515**
70-246	**70-410**	**70-467**	**70-516**
70-247	**70-411**	**70-480**	**70-519**
70-321	**70-412**	**70-483**	**70-583**
70-331	**70-413**	**70-484**	**70-640**
70-332	**70-414**	**70-485**	**70-649**
70-336	**70-417**	**70-486**	**70-668**
70-337	**70-461**	**70-487**	**70-680**
70-341	**70-462**	**70-488**	**70-687**
70-342	**70-463**	**70-489**	**70-688**
70-346	**70-464**	**70-513**	**70-689**