[Pass Ensure VCE Dumps PassLeader 580q 70-680 VCE Braindumps For Free Download (361-380)

Free Download New 70-680 Exam Dumps: PassLeader now supplying the new version of 70-680 VCE dumps, we ensure our 580q 70-680 exam questions are the most authoritative and valid compared with others', which will ensure your 70-680 exam 100% passing, and now we are offering the free new version VCE Player along with the VCE format 580q 70-680 braindumps, also the PDF format 70-680 practice test is available now, welcome to choose. keywords: 70-680 exam,580q 70-680 exam dumps,580q 70-680 exam questions,70-680 pdf dumps,70-680 practice test,70-680 vce dumps,70-680 study guide,70-680 braindumps,TS: Windows 7, Configuring Exam

QUESTION 361 Your office contains the wireless networks shown the following table:

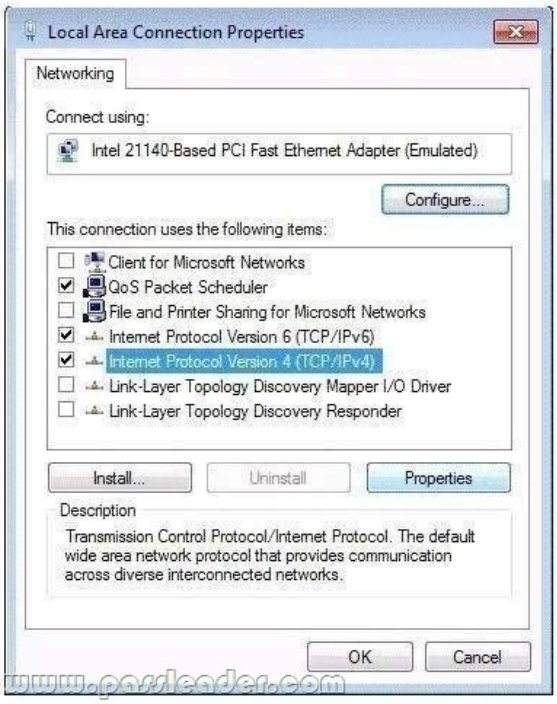
Network name	Network configuration
Network1	802.11b
Network2	802.11g
Network3	802.11n

You have a portable computer that runs Windows 7. The computer successfully connects to all of the wireless networks. You discover that when you start the computer, it connects to Network2. You need to ensure that the computer connects to Network3 by default. What should you do? A.   From Network and Sharing Center, modify the Advanced sharing settings. B.   From Network and Sharing Center, modify the Manage Wireless Networks settings. C.   From Network Connections, modify the properties of the wireless network adapter. D.   From Network Connections, modify the bindings of the wireless network adapter. Answer: B Explanation: Managing Preferred Wireless Networks. If you have a wireless-enabled mobile computer such as a laptop, you can take it to various locations and connect to whatever wireless networks are available at any location. You can see the available networks by opening Network And Sharing Center and clicking Connect To A Network. You can also click the Wireless icon on the Toolbar at the bottom right section of your screen. You can then right-click a network and click Connect. Available networks are listed in the Manage Wireless Networks dialog box. If you have previously connected to various wireless networks, the list of these networks is referred to as your preferred list. The wireless networks on your preferred list are your preferred wireless networks.

You can click Manage Wireless Networks in the Network And Sharing Center and view saved wireless networks. You can change the order in which your computer attempts to connect to preferred networks by dragging the networks up or down in the list.

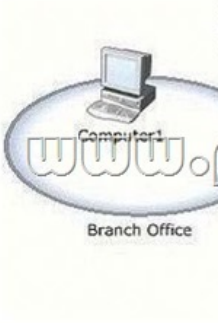
You can also change preferences for the network by right-clicking the network and selecting Properties. QUESTION 362 You need to configure a computer to encrypt all inbound connections by using IPSec. What should you do? A.   From Network and Sharing Center, click Connect to a network. B.   From Network and Sharing Center, click Set up a new connection or network. C.   From Windows Firewall with Advanced Security, click Inbound Rules and then click New Rule. D.   From Windows Firewall with Advanced Security, click Connection Security Rules and then click New Rule. Answer: D Explanation: Connection Security Rules. Connection security rules are a special type of rule that deal with authenticated and encrypted traffic. You can use connection security rules to manage how communication occurs between different hosts on the network. You use the New Connection Security Rule Wizard, to create connection security rules. Connections can be authenticated using the Kerberos V5 protocol requiring a domain computer and user account or a domain computer account. If you select advanced properties, connections can be authenticated using NTLMv2, computer certificates from a particular certificate authority (CA) or using a pre- shared key.Connection Security Rules and IPSec policies The relationship between connection security rules and IPSec policies is similar to the relationship between AppLocker and Software Restriction Policies. Both sets of rules do similar things, but the ones that you use depend on the operating systems used by the client computers in your organization. All editions of Windows 7 and Windows Vista support connection security rules, but Windows XP does not. QUESTION 363 You have a computer named Computer1 that runs Windows 7. You have a server named

Server1 that runs Windows Server 2008. Server1 has a file share named Share1. The network configuration for Computer1 is shown in the exhibit. (Click the Exhibit button.)

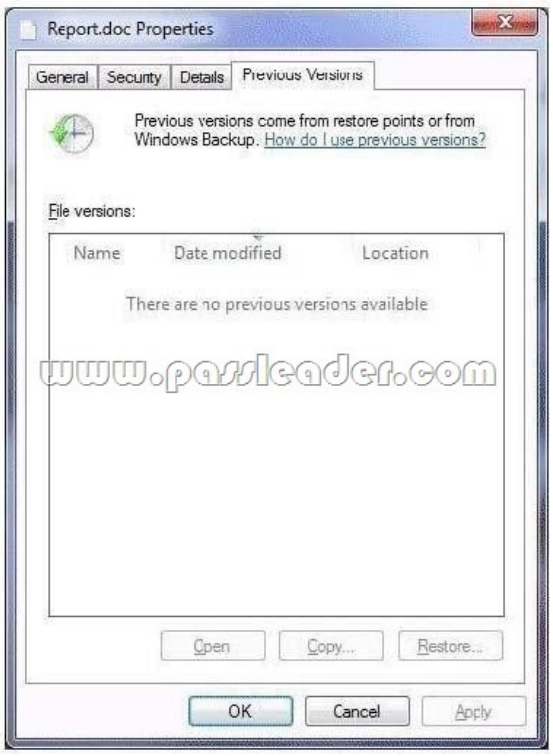


You attempt to connect to \Server1Share1 and receive the following error message: "Windows cannot access \Server1Share1." From Computer1, you successfully ping Server1. You need to connect to \Server1Share1. What should you enable on Computer1? A.   Client for Microsoft Networks B.   File and Printer Sharing for Microsoft Networks C.   Link-Layer Topology Discovery Mapper I/O Driver D.   Link-Layer Topology Discovery Responder Answer: A Explanation: Client for Microsoft Networks Allows the computer to access resources on a Microsoft network.File and Printer Sharing for Microsoft NetworksEnables other computers to access resources on your computer in a Microsoft network (and other networks).Link-layer Topology Discovery Mapper I/O DriverDiscovers and locates other computers, devices, and network infrastructure features on the network, and determines network bandwidth. Link-layer Topology Discovery ResponderAllows a computer to be discovered and located on the network. QUESTION 364 You have three computers that run Windows 7. You use Windows PowerShell to perform remote administration tasks on all three computers. You need to remotely administer all three computers by using PowerShell. Which PowerShell cmdlet should you use? A.   Enable-PSRemoting B.   Enable-PSSessionConfiguration C.   New-PSDrive D.   New-PSSession Answer: D Explanation: New-PSSession. Creates a persistent connection to a local or remote computer. The New- PSSession cmdlet creates a Windows PowerShell session (PSSession) on a local or remote computer. When you create a PSSession, Windows PowerShell establishes a persistent connection to the remote computer. Use a PSSession to run multiple commands that share data, such as a function or the value of a variable. To run commands in a PSSession, use the Invoke-Command cmdlet. To use the PSSession to interact directly with a remote computer, use the Enter-PSSession cmdlet. You can run commands on a remote computer without creating a PSSession by using the ComputerName parameters of Enter-PSSession or Invoke-Command. When you use the ComputerName parameter, Windows PowerShell creates a temporary connection that is used for the interactive session or for a single command and is then closed. QUESTION 365 You have a computer named Computer1 that runs Windows 7. Computer1 has a shared printer. You need to configure Computer1 so that only Administrators are authorized to shut down the computer. What should you do? A.   From User Accounts, modify the user profiles settings. B.   From User Accounts, modify the User Account Control (UAC) settings. C.   From the local comput er policy, modify the Security Options. D.   From the local computer policy, modify the User Rights Assignment. Answer: D Explanation: Shut down the system. Computer ConfigurationWindows SettingsSecurity SettingsLocal PoliciesUser Rights Assignment Description Determines which users logged on locally to the computer can shut down the operating system using the Shut Down command. This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers. QUESTION 366 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?



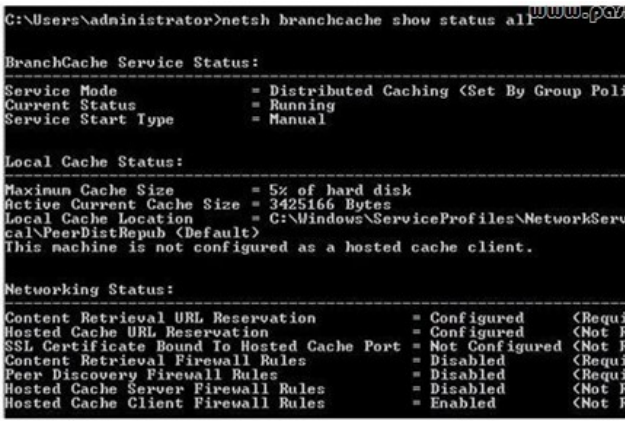
A.   192.168.2.30 B.   192.168.2.40 C.   192.168.2.63 D.   192.168.2.65 Answer: B QUESTION 367 You have a computer that runs Windows Vista. You install Windows 7 on a new partition on the computer. You need to ensure that the computer always starts Windows Vista by default. What should you do? A.   Create a boot.ini file in the root of the Windows 7 partition. B.   Create a boot.ini file in the root of the Windows Vista partition. C.   Run Bcdedit.exe and specify the /default parameter. D.   Run Bcdedit.exe and specify the /bootems parameter. Answer: C QUESTION 368 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. 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 369 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. QUESTION 370 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). 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.

http://www.passleader.com/70-680.html QUESTION 371 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. 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 372 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. 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 373 You have a computer that runs Windows 7. You need to prevent users from copying unencrypted files to removable drives. What should you do? A.   From a local Group Policy, modify the Trusted Platform Module (TPM) settings. B.   From the Trusted Platform Module (TPM) snap-in, initialize TPM. C.   From Control Panel, modify the BitLocker Drive Encryption settings. D.   From a local Group Policy, modify the BitLocker Drive Encryption settings. Answer: D Explanation: How can I prevent users on a network from storing data on an unencrypted drive? In Windows 7, you can enable Group Policy settings to require that data drives be BitLockerprotected before a BitLocker-protected computer can write data to them. The policy settings you use for this are: Computer ConfigurationAdministrative TemplatesWindows ComponentsBitLocker Drive EncryptionFixed Data DrivesDeny write access to fixed drives not protected by BitLocker Computer ConfigurationAdministrative TemplatesWindows ComponentsBitLocker Drive EncryptionRemovable Data DrivesDeny write access to removable drives not protected by BitLocker. When these policy settings are enabled, the BitLocker-protected operating system will mount any data drives that are not protected by BitLocker as read-only. If you are concerned that your users might inadvertently store data in an unencrypted drives while using a computer that does not have BitLocker enabled, use access control lists (ACLs) and Group Policy to configure access control for the drives or hide the drive letter. QUESTION 374 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.)



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. 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 375 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. 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 376 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. 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 377 You have a computer that runs Windows 7. You run Runas and specify the /savecred parameter to start an application. You need to delete the stored password. What should you do? A.   From Credential Manager, modify the Windows credentials. B.   From Authorization Manager, modify the Authorization Manager options. C.   Run Del and specify the /p parameter. D.   Run Runas and specify the /noprofile parameter. Answer: A QUESTION 378 You have a computer that runs Windows 7. The computer is joined to a domain. You need to ensure that only approved USB drives can be used on the computer. Which two policy settings should you configure? (Each correct answer presents a part of the solution. Choose two.) A.   Enable Prevent installation of removable devices. B.   Enable Prevent installation of devices not described by other policy settings. C.   Enable Prevent installation of devices that match any of these device IDs and enter the device ID for the approved USB drives. D.   Enable Allow installation of devices that match any of these device IDs and enter the device ID for the approved USB drives. Answer: BD QUESTION 379 You have two portable computers named Computer1 and Computer2 that run Windows 7. You configure Computer1 to connect to a wireless network named Network1. You need to configure Computer2 to connect to Network1 by using the same settings as

Computer1. What should you do on Computer1? A.   At the command prompt, run Wecutil.exe -es -gr. B.   At the command prompt, run Winrs.exe -environment. C.   From Windows Firewall with Advanced Security, export the policy. D.   From the wireless network properties of Network1, copy the network profile to a USB flash drive. Answer: D Explanation: The Copy this network profile to a USB flash drive link launches the Copy Network Settings wizard, which writes the wireless network profile settings to a USB flash drive. You can then use this flash drive to automate the wireless network profile configuration of other computers. To save your wireless network settings to a USB flash drive, insert a USB flash drive into the computer, and then follow these steps: 1. Click to open Network and Sharing Center. 2. In the left pane, click Manage wireless networks. 3. Right-click the network, click Properties, and then click Copy this network profile to a USB flash drive. 4. Select the USB device, and then click Next. 5. Follow the instructions in the wizard, and then click Close. QUESTION 380 You are preparing a custom Windows 7 image for deployment. You need to install a third-party network interface card (NIC) driver in the image. What should you do? A.   Run Pkgmgr.exe and specify the /ip parameter. B.   Run Dism.exe and specify the /add-driver parameter. C.   Create a new answer file by using Windows System Image Manager (Windows SIM). Run Pkgmgr.exe and specify the /n parameter. D.   Create a new answer file by using Windows System Image Manager (Windows SIM). Run Dism.exe and specify the /apply-unattend parameter. Answer: B Explanation: 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. Windows 7 introduces the DISM command-line tool. You can use DISM to service a Windows image or to prepare a Windows PE image. DISM replaces Package Manager (Pkgmgr.exe), PEimg, and Intlcfg in Windows Vista, and includes new features to improve the experience for offline servicing. You can use DISM to perform the following actions: - Prepare a Windows PE image. - Enable or disable Windows features within an image. - Upgrade a Windows image to a different edition. - Add, remove, and enumerate packages. - Add, remove, and enumerate drivers. - Apply changes based on the offline servicing section of an unattended answer file. - Configure international settings. - Implement powerful logging features. - Service operating systems such as Windows Vista with SP1 and Windows Server 2008. - Service a 32-bit image from a 64-bit host and service a 64-bit image from a 32-bit host. - Service all platforms (32-bit, 64-bit, and Itanium). - Use existing Package Manager scripts.

http://www.passleader.com/70-680.html