[Pass Ensure VCE Dumps PassLeader Share New 580q 70-680 Exam Questions With VCE and PDF Download (16-30)

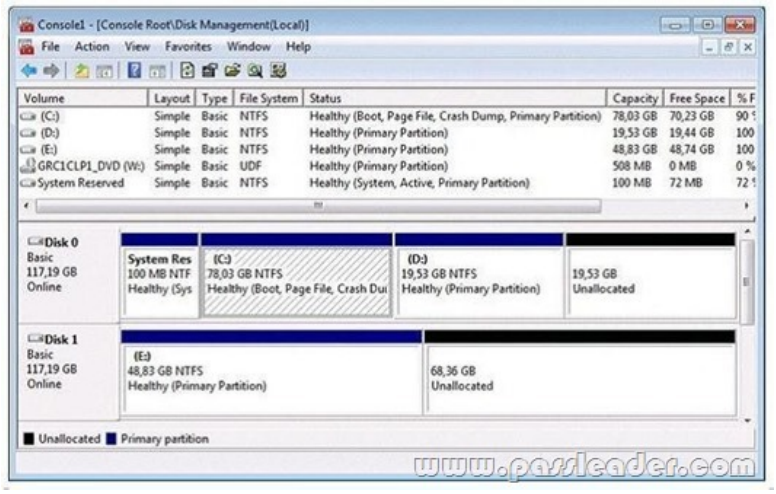
Valid Tips For 100% Pass Exam 70-680: PassLeader now is providing the best 580q 70-680 VCE dumps and PDF dumps for your 70-680 certification exam. We offer the latest 580q 70-680 exam questions to ensure that you can 100 percent pass 70-680 exam, and what's more, we will offer you the new updated 70-680 exam dumps for one year free and free new version VCE Player. Welcome to visit our site -- passleader.com and get the valid 580q 70-680 braindumps to pass exam as soon as possible. **keywords: 70-680 exam,580q 70-680 exam dumps,580q 70-680 exam questions,70-680 pdf dumps,70-680 vce dumps,70-680 practice test,70-680 study guide,TS: Windows 7, Configuring Exam**

QUESTION 16 Your company has an internal Web site that requires HTTPS. The Web site's certificate is self-signed. You have a computer that runs Windows 7 and Windows Internet Explorer 8. You use HTTPS to browse to the Web site and receive the following warning message. There is a problem with this website's security certificate. You need to prevent the warning message from appearing when you access the Web site. What should you do? A.   From Internet Explorer, enable InPrivate Browsing. B.   From Internet Explorer, add the Web site to the Trusted sites zone. C.   From Certificate Manager, import the Web sites certificate into your Personal store. D.   From Certificate Manager, import the Web sites certificate into your Trusted Root Certification Authorities store. Answer: D Explanation: Certificate Manager A certificate manager can approve certificate enrollment and revocation requests, issue certificates, and manage certificates. This role can be configured by assigning a user or group the Issue and Manage Certificatespermission. When you assign this permission to a user or group, you can further refine their ability to manage certificates by group and by certificate template. For example, you might want to implement a restriction that they can only approve requests or revoke smart card logon certificates for users in a certain office or organizational unit that is the basis for a security group.Importing CertificatesYou may restore certificates and the corresponding private keys from a file. *. Right-click the certificate store you want to import, and click Install PFX on the context menu. *. The Certificate Import Wizard launches. Click Next. *. In the File name text box, type the name of the certificate file that you want to import. Alternatively, you can find the file by clicking Browse. *. Click Next. If the file specified is a Personal Information Exchange-KCS #12 (*.pfx), you will be prompted for the password. Enter the password to import the file. Click Next. *. On the next page, select where you'd like to store the certificate. Click Next. *. The next wizard page contains summary information about the file that you are importing. Click Finish to import the file. The certificate(s) are now ready for use by the system. QUESTION 17 Your network has a main office and a branch office. The branch office has five client computers that run Windows 7. All client computers are configured to use BranchCache. At the branch office, a computer named Computer1 is experiencing performance issues. You need to temporarily prevent all computers from retrieving cached content from Computer1. What should you do on Computer1? A.   At the command prompt, run Netsh branchcache flush. B.   At the command prompt, run Netsh branchcache dump. C.   Modify the Configure BranchCache for network files Group Policy setting. D.   Modify the Set percentage of disk space used for client computer cache Group Policy setting. Answer: A Explanation: Flush Deletes the contents of the local BranchCache cache. QUESTION 18 You have a standalone computer that runs Windows 7. Multiple users share the computer. You need to ensure that you can read the content of all encrypted files on the computer. What should you do? A.   Run the Certificates Enrollment wizard and then run Certutil.exe -importpfx. B.   Run the Certificates Enrollment wizard and then run Certutil.exe -installcert. C.   Run Cipher.exe /r and then add a data recovery agent from the local security policy. D.   Run Cipher.exe /rekey and then import a security template from the local security policy. Answer: C Explanation: Cipher Displays or alters the encryption of folders and files on NTFS volumes. Used without parameters, cipher displays the encryption state of the current folder and any files it contains. Administrators can use Cipher.exe to encrypt and decrypt data on drives that use the NTFS file system and to view the encryption status of files and folders from a command prompt. The

updated version adds another security option. This new option is the ability to overwrite data that you have deleted so that it cannot be recovered and accessed.When you delete files or folders, the data is not initially removed from the hard disk. Instead, the space on the disk that was occupied by the deleted data is "deallocated." After it is deallocated, the space is available for use when new data is written to the disk. Until the space is overwritten, it is possible to recover the deleted data by using a low-level disk editor or data-recovery software. If you create files in plain text and then encrypt them, Encrypting File System (EFS) makes a backup copy of the file so that, if an error occurs during the encryption process, the data is not lost. After the encryption is complete, the backup copy is deleted. As with other deleted files, the data is not completely removed until it has been overwritten. The new version of the Cipher utility is designed to prevent unauthorized recovery of such data. /K Creates a new certificate and key for use with EFS. If this option is chosen, all the other options will be ignored. By default, /k creates a certificate and key that conform to current group plicy. If ECC is specified, a self-signed certificate will be created with the supplied key size. /R Generates an EFS recovery key and certificate, then writes them to a .PFX file (containing certificate and private key) and a .CER file (containing only the certificate). An administrator may add the contents of the .CER to the EFS recovery policy to create the recovery for users, and import the .PFX to recover individual files. If SMARTCARD is specified, then writes the recovery key and certificate to a smart card. A .CER file is generated (containing only the certificate). No .PFX file is genereated. By default, /R creates an 2048-bit RSA recovery key and certificate. If EECC is specified, it must be followed by a key size of 356, 384, or 521. QUESTION 19 Your network contains an Active Directory domain. All servers run Windows Server 2008 R2 and are members of the domain. All servers are located in the main office. You have a portable computer named Computer1 that runs Windows 7. Computer1 is joined to the domain and is located in a branch office.A file server named Server1 contains a shared folder named Share1. You need to configure Computer1 to meet the following requirements: - Minimize network traffic between the main office and the branch office. - Ensure that Computer1 can only access resources in Share1 while it is connected to the network. What should you do?
A.   On Computer1, enable offline files. B.   On Computer1, enable transparent caching. C.   On Server1, configure DirectAccess. D.   On Server1, configure Share1 to be available offline. Answer: B Explanation: Transparent Caching When you enable transparent caching, Windows 7 keeps a cached copy of all files that a user opens from shared folders on the local volume. The first time a user opens the file, the file is stored in the local cache. When the user opens the file again, Windows 7 checks the file to ensure that the cached copy is up to date and if it is, opens that instead. If the copy is not up to date, the client opens the copy hosted on the shared folder, also placing it in the local cache. Using a locally cached copy speeds up access to files stored on file servers on remote networks from the client. When a user changes a file, the client writes the changes to the copy of the file stored on the shared folder. When the shared folder is unavailable, the transparently cached copy is also unavailable. Transparent caching does not attempt to keep the local copy synced with the copy of the file on the remote file server as the Offline Files feature does. Transparent caching works on all files in a shared folder, not just those that you have configured to be available offline. QUESTION 20 You have a computer that runs Windows 7. Your network contains a DHCP server that runs Windows Server 2008 R2. The server is configured as a Network Access Protection (NAP) enforcement point. You need to configure the computer as a NAP client. Which two actions should you perform? (Each correct answer presents a part of the solution. Choose two.) A.   From Services, set the Netlogon service Startup Type to Automatic. B.   From Services, set the Network Access Protection Agent service Startup Type to Automatic. C.   From the NAP Client Configuration console, configure the user interface settings. D.   From the NAP Client Configuration console, enable the DHCP Quarantine Enforcement Client. Answer: BD Explanation: Network Access Protection Network Access Protection (NAP) is a feature in Windows Server 2008 that controls access to network resources based on a client computer's identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.NAP Client ConfigurationNetwork Access Protection (NAP), a new feature in Windows Vista?and Windows Server?2008, allows you to control the access of client computers to network resources based on computer identity and compliance with corporate governance policy. To implement NAP, you must configure NAP settings on both servers and client computers. There are three tools that you can use to configure NAP client settings: The NAP Client Configuration console provides a graphical user interface with which you can configure NAP client settings on the local computer or in a configuration file that you can save and apply to other computers. The Netsh commands for NAP client provide a command-line tool that you can use to configure client computers or to create a configuration file that you can save and apply to other computers. If you want to manage NAP client settings on domain member client computers, you can use the Group Policy Management Console and the Group Policy Management Editor. When you

configure NAP client settings in Group Policy, these settings are applied on NAP-capable domain member client computers when Group Policy is refreshed.To enable and disable the DHCP enforcement client by using the Windows interface 1. To open the NAP Client Configuration console, click Start, click All Programs, click Accessories, click Run, type NAPCLCFG.MSC, and then click OK. 2. Click Enforcement Clients. 3. Right-click DHCP Enforcement Client, and then click Enable or Disable.Network Access. Protection Agent The Network Access Protection (NAP) agent service collects and manages health information for client computers on a network. Information collected by NAP agent is used to make sure that the client computer has the required software and settings. If a client computer is not compliant with health policy, it can be provided with restricted network access until its configuration is updated. Depending on the configuration of health policy, client computers might be automatically updated so that users quickly regain full network access without having to manually update their computer. QUESTION 21 You have two computers named Computer1 and Computer2 that run Windows 7. Both computers are members of an Active Directory domain. Windows Remote Management (WinRM) is enabled on both computers. You need to remotely create additional disk volumes on Computer1 from Computer2. What should you do? A.   On Computer2, run Winrs and then run Diskpart. B.   On Computer2, run Winrs and then run Diskmgmt.msc. C.   On Computer1, install the Telnet Client and then run Diskpart from Computer2. D.   On Computer1, install the Telnet Client and then use Disk Management from Computer2. Answer: A Explanation: Winrs You can use WinRS to execute command-line utilities or scripts on a remote computer. To use WinRS, open a command prompt and prefix the command that you want to run on the remote computer with the WinRS -r: RemoteComputerName command. For example, to execute the Ipconfig command on a computer named Aberdeen, issue the command: WinRS -r:Aberdeen ipconfig 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. Diskpart: Microsoft command-line tool Diskpart is used to create and format volumes on the target computer. QUESTION 22 A remote user has a computer that runs Windows 7. The user reports that he receives several error messages while using an application. You do not have remote access to the user's computer. You need to tell the user how to create screenshots of the actions he performs on the computer. The solution must track the mouse actions that the user performs. What should you instruct the user to do? A.   Press ALT + PrintScreen. B.   Run Psr.exe and then click Start Record. C.   From Mouse Properties, select Display pointer trails. D.   Run Snippingtool.exe, click New, and then click Window Snip. Answer: B Explanation: How do I use Problem Steps Recorder?You can use Problem Steps Recorder to automatically capture the steps you take on a computer, including a text description of where you clicked and a picture of the screen during each click (called a screen shot). Once you capture these steps, you can save them to a file that can be used by a support professional or someone else helping you with a computer problem.NotesWhen you record steps on your computer, anything you type will not be recorded. If what you type is an important part of recreating the problem you're trying to solve, use the comment feature described below to highlight where the problem is occurring.

http://www.passleader.com/70-680.html QUESTION 23 You have a computer that runs Windows 7. The computer's disk is configured as shown in the exhibit. (Click the Exhibit button.)



You need to extend volume C. What should you do first? A.   Back up and delete volume D. B.   Convert disk 0 to a dynamic disk. C.   Remove the crash dump from volume C. D.   Move the paging file from volume C to volume E. Answer: A Explanation: Extend a Basic Volume You can add more space to existing primary partitions and logical drives by extending them into adjacent unallocated space on the same disk. To extend a basic volume, it must be raw or formatted with the NTFS file system. You can extend a logical drive within contiguous free space in the extended partition that contains it. If you extend a logical drive beyond the free space available in the extended partition, the extended partition grows to contain the logical drive. For logical drives, boot, or system volumes, you can extend the volume only into contiguous space and only if the disk can be upgraded to a dynamic disk. For other volumes, you can extend the volume into noncontiguous space, but you will be prompted to convert the disk to dynamic. QUESTION 24 You need to increase the size of a paging file. What should you do? A.   From Disk Management, shrink the boot partition. B.   From Disk Management, shrink the system partition. C.   From System, modify the Advanced system settings. D.   From System, modify the System protection settings. Answer: C Explanation: 1. Click Start, right-click My Computer, and then click Properties. 2. In the System Properties dialog box, click the Advanced tab. 3. In the Performance pane, click Settings. 4. In the Performance Options dialog box, click the Advanced tab. 5. In the Virtual memory pane, click Change. 6. Change the Initial size value and the Maximum size value to a higher value, click Set, and then click OK. 7. Click OK to close the Performance Options dialog box, and then click OK to close the System Properties dialog box. QUESTION 25 You have a computer that runs Windows Vista (x86). You need to perform a clean installation of Windows 7 (64-bit). What should you do? A.   From the Windows 7 installation media, run Rollback.exe. B.   From the Windows 7 installation media, run Migsetup.exe. C.   Start the computer from the Windows 7 installation media. From the Install Windows dialog box, select the Upgrade option. D.   Start the computer from the Windows 7 installation media. From the Install Windows dialog box, select the Custom (advanced) option. Answer: D Explanation: When you are performing a clean installation, you should select Custom (Advanced). Almost all installations ofm Windows 7 that you will perform will be of the Custom (Advanced) type rather than upgrades. You can initiate upgrade installations only from within Windows Vista or Windows 7.NOT Rollback, Migsetup, or Upgrade:Specified clean installation not migration, update or rollback. QUESTION 26 Your network consists of a single Active Directory forest. You have 50 portable computers and 50 desktop computers. All computers have 32-bit hardware. You plan to deploy Windows 7 and 10 corporate applications to the computers by using a custom image. You need to prepare for the deployment by using the minimum amount of administrative effort. What should you do first? A.   On one computer, install Windows 7 and the corporate applications. B.   On one portable computer and one desktop computer, install Windows 7 and the corporate applications. C.   On a server, install and run the Microsoft Assessment and Planning (MAP) Toolkit. D.   On a server, install the Windows Automated Installation Kit (AIK) and run Windows System Image Manager (Windows SIM). Answer: A Explanation: To prepare the reference computer for the user, you use the Sysprep utility with the /generalize option to remove hardware-specific information from the Windows installation and the /oobe option to configure the computer to boot to Windows Welcome upon the next restart. Open an elevated command prompt on the reference computer and run the following command: c:windowssystem32sysprepsysprep.exe /oobe /generalize /shutdown. Sysprep prepares the image for capture by cleaning up various user-specific and computerspecific settings, as well as log files. The

reference installation now is complete and ready to be imaged. QUESTION 27 You have a computer that runs Windows 7. You need to copy files to a virtual hard disk (VHD) file. What should you do first? A.   Run Dism.exe and specify the /image and /online parameters. B.   Open Windows Explorer, right-click the VHD file and select Open. C.   Run Diskpart.exe and then run the select and attach commands. D.   Run Imagex.exe and specify the /mountrw and /append parameters. Answer: C Explanation: Diskpart Microsoft command-line tool Diskpart is used to create and format volumes on the target computer.SelectShift the focus to an object.AttachAttaches a virtual disk file. QUESTION 28 You have a computer that runs Windows 7. You create an application shim for a third-party application by using the Microsoft Application Compatibility Toolkit (ACT). You need to ensure that the application shim is applied the next time you run the application. What should you do first? A.   Run Sdbinst.exe. B.   Run Msiexec.exe. C.   Right-click the application executable file and modify the compatibility settings. D.   Right-click the application executable file and modify the advanced security settings. Answer: A QUESTION 29 You have a computer that runs Windows 7. Multiple users log on to the computer. The computer has five removable devices. You need to ensure that users can only access removable devices that have been previously installed on the computer. What should you modify in the Local Group Policy? A.   Enable the Prevent redirection of USB devices setting. B.   Enable the Prevent installation of removable devices setting. C.   Disable the WPD Devices: Deny read access setting. D.   Disable the Allow administrators to override Device Installation Restriction policies setting. Answer: B Explanation: Prevent installation of removable devices This policy setting allows you to prevent Windows from installing removable devices. A device is considered removable when the driver for the device to which it is connected indicates that the device is removable. For example, a Universal Serial Bus (USB) device is reported to be removable by the drivers for the USB hub to which the device is connected. This policy setting takes precedence over any other policy setting that allows Windows to install a device. If you enable this policy setting, Windows is prevented from installing removable devices and existing removable devices cannot have their drivers updated. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of removable devices from a remote desktop client to the remote desktop server. If you disable or do not configure this policy setting, Windows can install and update device drivers for removable devices as allowed or prevented by other policy settings. NOT Prevent redirection of USB devicesThis policy setting prevents redirection of USB devices. If you enable this setting, an alternate driver for USB devices cannot be loaded. If you disable or do not configure this setting, an alternate driver for USB devices can be loaded. QUESTION 30 Your network consists of a single Active Directory domain named contoso.com. You have a server named Server1 that runs a custom network application. Server1 has the following IP addresses: - 192.168.15.10 - 192.168.15.11 You need to ensure that a client computer resolves server1.contoso.com to only the 192.168.15.11 IP address. What should you do from the computer? A.   Edit the hosts file. B.   Edit the lmhosts file. C.   Run Ipconfig.exe /flushdns. D.   Run Netsh interface ipv4 reset. Answer: A Explanation: Differences Between the HOSTS and LMHOSTS Files in Windows NT In Windows NT, the HOSTS file is for TCP/IP utilities, and the LMHOSTS file is for LAN Manager NET utilities. If you cannot PING another computer (using a friendly name), check the HOSTS file. If you cannot NET VIEW a server using only the TCP/IP protocol, check the LMHOSTS file. Hosts fileThe Hosts file is a common way to resolve a host name to an IP address through a locally stored text file that contains IP-address-to-host-name mappings. On most UNIX- based computers, this file is /etc/hosts. On Windows-based computers, this file is the Hosts file in the systemrootSystem32DriversEtc folder. The following describes the attributes of the Hosts file for Windows: A single entry consists of an IP (IPv4 or IPv6) address and one or more host names. The Hosts file is dynamically loaded into the DNS client resolver cache, which Windows Sockets applications use to resolve a host name to an IP address on both local and remote subnets. When you create entries in the Hosts file and save it, its contents are automatically loaded into the DNS client resolver cache. The Hosts file contains a default entry for the host name localhost. The Hosts file can be edited with any text editor. Each host name is limited to 255 characters. Entries in the Hosts file for Windows-based computers are not case sensitive. The advantage of using a Hosts file is that users can customize it for themselves. Each user can create whatever entries they want, including easy-to-remember nicknames for frequently accessed resources. However, the individual maintenance required for the Hosts file does not scale well to storing large numbers of FQDN mappings or reflecting changes to IP addresses for servers and network resources. The solution for the large-scale storage and maintenance of FQDN mappings is DNS. The solution for the maintenance of FQDN mappings for changing IP addresses is DNS dynamic update.NOT LMHOSTS FileThe LMHOSTS file is a local text file that maps IP addresses to NetBIOS names of remote servers with which you want to communicate over the TCP/IP protocol. Windows recognizes names instead of IP addresses for network requests and a name discovery process is used to correctly route network requests with TCP/IP. Because the name discovery process is

generally not routed by an IP router, the LMHOSTS file allows Windows machines to communicate using TCP/IP across a subnet. - LMHOSTS contains IP address to "NetBIOS over TCP/IP" name translations. - LMHOSTS is only used by the NBT (NetBIOS over TCP/IP) interface. - LMHOSTS file contains some valuable additions to the LAN Manager and Windows for Workgroups. - LMHOSTS file, such as the ability to support routed domain logon validation. - LMHOSTS contains static information about TCP/IP addresses, but using logon scripts and/or the replicator service, the "master" file can be distributed transparently across all stations. - By default, the LMHOSTS file should be located in the directory %SYSTEMROOT%SYSTEM32DRIVERS ETC (usually C:WINNTSYSTEM32DRIVERSETC). Other info http://support.microsoft.com/kb/105997

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