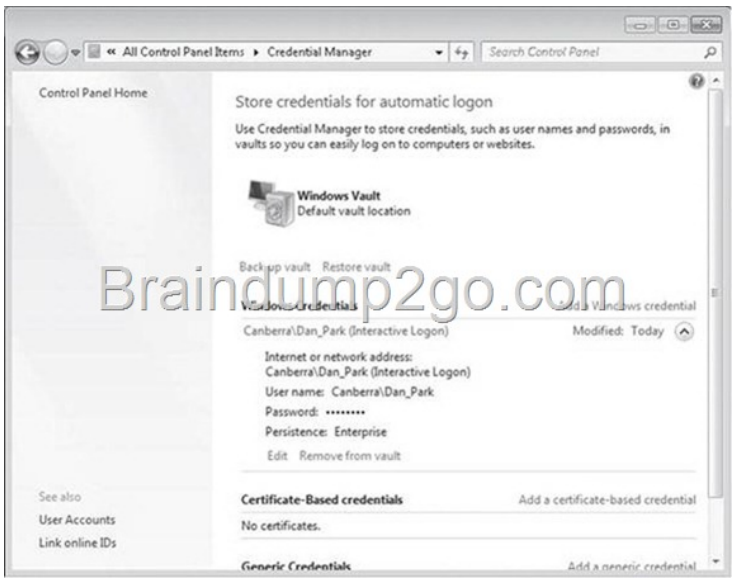
Official 2014 Latest Microsoft 70-680 Exam Dump Free Download(11-20)

QUESTION 11 You have a portable computer that runs Windows 7. You configure the computer to enter sleep mode after 10 minutes of inactivity. You do not use the computer for 15 minutes and discover that the computer has not entered sleep mode. You need to identify what is preventing the computer from entering sleep mode. What should you do? A. At a command prompt, run Powercfg energy. B. At a command prompt, run Systeminfo /s localhost. C. From Performance Monitor, review the System Summary. D. From Performance Information and Tools, review the detailed performance and system information. Answer: A Explanation: Command-line Power Configuration Powercfg.exe is a command-line utility that you can use from an administrative command prompt to manage Windows 7 power settings. It is possible to use Powercfg.exe to configure a number of Windows 7 powerrelated settings that you cannot configure through Group Policy or the Advanced Plan Settings dialog box. You can use Powercfg.exe to configure specific devices so that they are able to wake the computer from the Sleep state. You can also use Powercfg.exe to migrate power policies from one computer running Windows 7 to another by using the import and export functionality. -energy Check the computer for common energy-efficiency and battery life problems. Provides report in Hypertext Markup Language (HTML) format.For more information on Powercfg.exe, consult the following Microsoft TechNet document: http://technet.microsoft.com/en-us/library/cc748940.aspx. QUESTION 12 You have a computer that runs Windows 7. Your network contains a VPN server that runs Windows Server 2008. You need to authenticate to the VPN server by using a smart card. Which authentication setting should you choose? A. CHAP B. EAP C. MS-CHAP v2 D. PAP Answer: B Explanation: VPN Server Software Requirements VPN server software requirements for smart card access are relatively straightforward. The remote access servers must run Windows 2000 Server or later, have Routing and Remote Access enabled, and must support Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). EAP-TLS is a mutual authentication mechanism developed for use in conjunction with security devices, such as smart cards and hardware tokens. EAP-TLS supports Point-to-Point Protocol (PPP) and VPN connections, and enables exchange of shared secret keys for MPPE, in addition to Ipsec. The main benefits of EAP-TLS are its resistance to brute-force attacks and its support for mutual authentication. With mutual authentication, both client and server must prove their identities to each other. If either client or server does not send a certificate to validate its identity, the connection terminates.Microsoft Windows ServerTM 2003 supports EAP-TLS for dial-up and VPN connections, which enables the use of smart cards for remote users. For more information about EAP-TLS, see the Extensible Authentication Protocol (EAP) topic at www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/auth_eap. mspx. For more information about EAP certificate requirements, see the Microsoft Knowledge Base article "Certificate Requirements when you use EAP-TLS or PEAP with EAP-TLS" at http://support.microsoft.com/default.aspx? scid=814394. QUESTION 13 You have a computer named Computer1 that runs Windows 7. The computer is a member of an Active Directory domain. The network contains a file server named Server1 that runs Windows Server 2008. You log on to the computer by using an account named User1. You need to ensure that when you connect to Server1, you authenticate by using an account named Admin1. What should you do on Computer1? A. From User Accounts, select Link online IDs. B. From Windows CardSpace, select Add a card. C. From Credential Manager, select Add a Windows credential. D. From Local Security Policy, modify the Access this computer from the network user right. Answer: C Explanation: Credential Manager Credential Manager stores logon user name and passwords for network resources, including file servers, Web sites, and terminal services servers. Credential Manager stores user name and password data in the Windows Vault. You can back up the Windows Vault and restore it on other computers running Windows 7 as a method of transferring saved credentials from one computer to another. Although Credential Manager can be used to back up some forms of digital certificates, it cannot be used to back up and restore the self- signed Encrypting File System (EFS) certificates that Windows 7 generates automatically when you encrypt a file. For this reason, you must back up EFS certificates using other tools. You will learn about backing up EFS certificates later in this lesson.



QUESTION 14 You have a computer that runs Windows 7. You create a HomeGroup. You need to secure the HomeGroup to meet the following requirements: - Allow access to the HomeGroup when you are connected to private networks. - Block access to the HomeGroup when you are connected to public networks. What should you do? A. From Network and Sharing Center, modify the advanced sharing settings. B. From the HomeGroup settings in Control Panel, modify the advanced sharing settings. C. Configure the HomeGroup exception in Windows Firewall to include Home or work (private) networks and block Public networks. D. Configure the File and Printer Sharing exception in Windows Firewall to include Home or work (private) networks and block Public networks. Answer: C Explanation: Windows Firewall does not allow you to create firewall rules for specific network locations on the basis of port address. Windows Firewall does not allow you to create rules that differentiate between the home and work network locations. You can only create rules that differentiate on the basis of home and work or public network locations. HomeGroup Connections This option decides how authentication works for connections to HomeGroup resources. If all computers in the HomeGroup have the same user name and passwords configured, you can set this option to allow Windows to manage HomeGroup connections. If different user accounts and passwords are present, you should configure the option to use user accounts and passwords to connect to other computers. This option is available only in the Home/Work network profile. QUESTION 15 A user named User1 uses a shared computer that runs Windows 7. User1 is a member of group named Group1. The computer contains a folder named Folder1. You need to configure the permissions on Folder1 to meet the following requirements: - User1 must be allowed to delete all files in Folder1. - Members of Group1 must be able to create files in Folder1. - All other members of Group1 must be prevented from deleting files they did not create in Folder1. - All users must be prevented from modifying the permissions on Folder1. What should you do? A. Assign Group1 the Write permission. Assign User1 the Modify permission. B. Assign Group1 the Modify permission. Assign User1 the Write permission. C. Deny Group1 the Write permission. Assign User1 the Modify permission. D. Deny Group1 the Modify permission. Assign User1 the Write permission. Answer: A Explanation: File and Folder Permissions ReadFolders: Permits viewing and listing of files and subfoldersFiles: Permits viewing or accessing of the file's contentsWriteFolders: Permits adding of files and subfoldersFiles: Permits writing to a fileRead & ExecuteFolders: Permits viewing and listing of files and subfolders as well as executing of files; inherited by files and folders Files: Permits viewing and accessing of the file's contents as well as executing of the fileList Folder ContentsFolders: Permits viewing and listing of files and subfolders as well as executing of files; inherited by folders onlyFiles: N/AModifyFolders: Permits reading and writing of files and subfolders; allows deletion of the folderFiles: Permits reading and writing of the file; allows deletion of the fileFull ControlFolders: Permits reading, writing, changing, and deleting of files and subfoldersFiles: Permits reading, writing, changing and deleting of the file 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. 6. Right-click the certificate store you want to import, and click Install PFX on the context menu. 7. The Certificate Import Wizard launches. Click Next. 8. 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. 9. 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. 10. On the next page, select where you'd like to store the certificate. Click Next. 11. 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. Passing Microsoft 70-680 Exam successfully in a short time! Just using Braindump2go's Latest Microsoft 70-680 Dump: http://www.braindump2go.com/70-680.html