Braindump2go Microsoft 70-688 Practice Exam Questions Guarantee Your Microsoft 70-688 Real Test Totally Success(111-120)

 QUESTION 111You have client computers that run Windows 7 Enterprise. All users have roaming user profiles. You deploy several client computers that run Windows 8 Enterprise. Users who sign in to both the Windows 8 Enterprise computers and the Windows 7 Enterprise computers report that they no longer see their desktop background and their theme.You suspect that the user profiles are corrupt. You need to resolve the profile corruption issue. What should you do? A.   Move all of the user profiles to a file server that runs Windows Server 2012, and then modify the profile path of each user account.B.   on the Windows 7 computers, configure the Download roaming profiles on primary computers only Group Policy setting.C.   on the Windows 8 computers, configure the Set roaming profile path for all users logging onto this computer Group Policy setting.D.   For each user, set the msDs-PrimaryComputer attribute to use a Windows 8 computer. Answer: CQUESTION 112You install the Microsoft Application Compatibility Toolkit (ACT) on a client computer named Computer1. Computer1 has the ACT Log Processing Service and Microsoft SQL Server 2012 Express installed. You install the ACT on a client computer named Computer2. When Computer2 attempts to connect to a SQL Server database, you receive the following error message: "The SQL Server you entered either does not exist or you do not have the required credentials for access." You need to ensure that Computer2 can connect to the SQL Server database successfully. Which should you do on Computer1? A.   Create firewall exceptions for TCP port 443 and UDP port 389.B.   Add Computer2 to the local Administrators group.C.   Add Computer1 to the local Administrators group.D.   Create firewall exceptions for Sqlservr.exe and Sqlbrowser.exe. Answer: A QUESTION 113Your network contains an Active Directory domain named contoso.com. A user receives the following error message when attempting to sign in to a computer: "The trust relationship between this workstation and the primary domain failed." You need to ensure that the user can sign in to the computer by using a domain user account. Which tool should you use? A.   NetcfgB.   NetshC.   NetdomD.   Netstat Answer: C QUESTION 114Your network contains an Active Directory domain. All client computers run Windows 8 Enterprise. Your company uses virtual smart cards. A user named User1 requires a virtual smart card on a new client computer named Computer1. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.) A.   Enroll User1 for a certificate.B.   Run the Enable-BitLocker cmdlet.C.   Run the tpmvscmgr.exe command.D.   Enroll Computer1 for a certificate. Answer: ACExplanation: A: Smart cards (virtual or otherwise) are based on digital certificates, which means you need a Public Key Infrastructure (PKI). A Windows Server 2012 certification authority (CA) has two default certificate templates that can be used for issuing smart card certificates. The Smartcard Logon template is appropriate when the card's use will be for logging on only. If you want users to be able to use the certificate for encrypting email, use the Smartcard User template.C: To create a Vir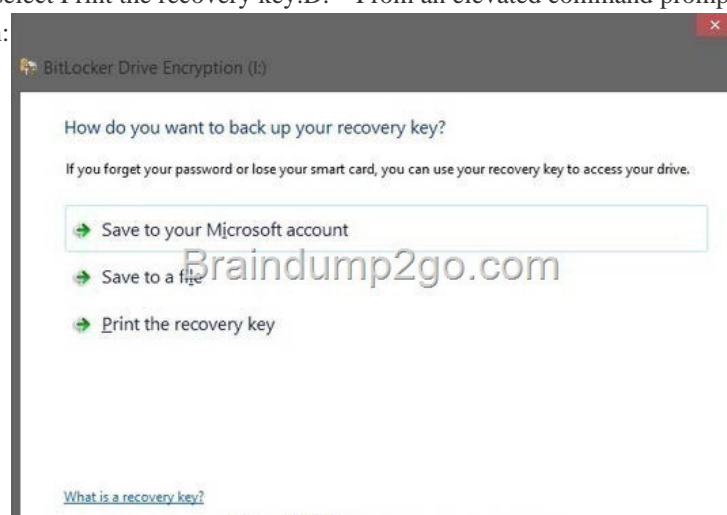tual Smart Card, use the Tpmvscmgr.exe command line utility. QUESTION 115Your network contains a wireless network access point that uses 802.IX certificate-based authentication. You purchase several devices that run Windows RT. You need to ensure that the Windows RT devices can authenticate to the wireless access point. What should you do first? A.   Add a certificate to the Trusted Devices certificate store of the user.B.   Add a certificate to the Trusted Root Certification Authorities certificate store of the computer.C.   Add a certificate to the Trusted Root Certification Authorities certificate store of the user.D.   Add a certificate to the Trusted Devices certificate store of the computer. Answer: B QUESTION 116You support computers that run Windows 8 Enterprise and are members of a workgroup. Users are able to download and install any app from Windows Store. You need to ensure that only approved apps can be installed from Windows Store. What should you do? A.   Configure a Software Restriction Policy Certificate rule.B.   Enable Windows SmartScreen and select the Get administrator approval before running an unrecognized app from the Internet option.C.   Configure an AppLocker Packaged app rule.D.   Configure an AppLocker Publisher rule. Answer: C QUESTION 117You have 100 client computers that run Windows 8 Pro. Each computer has a single local hard disk drive, a DVD drive, and an external USB drive.Each computer has a different set of line-of-business (LOB) desktop applications that are installed locally. All of the applications store their configurations in the HKEY_Local_MachineSoftware registry hive.You need to design a recovery solution to ensure that you can restore the initial state of the locally installed LOB desktop applications if an application is misconfigured. The solution must preserve the existing locally stored user data. What should you do? A.   Enable File History. Restore files by using File History.B.   Create a Microsoft Diagnostics and Recovery Toolset (DaRT) recovery image. Start the computer from the DaRT image and perform a file restore.C.   Run recimg.exe. Perform a system refresh.D.   Create a system repair disk by using Windows 7 File Recovery. Start the computer from the Windows 8 Enterprise installation media and perform an automatic repair, Answer: CExplanation:Reinstalling all of your Desktop apps can be time consuming, so Windows 8 offers a command called recimg.exe to make this easier. recimg creates an image which is used by the refresh facility when restoring Windows. Not only will your personal data and Metro style apps be saved, but so will Desktop apps you have installed at the time

you create the image. This can save you a lot of time. QUESTION 118Your network contains an Active Directory domain and a subscription to Microsoft Office 365. Users discover that they must change their Active Directory password more frequently than their Office 365 password. You need to ensure that the password policies for Office 365 and for Active Directory are the same. What should you do? A.   From the Office 365 portal, under Subscriptions, click Manage.B.   From the Windows Azure Active Directory Module for Windows PowerShell, run Set- MsolUserPassword.C.   From the Office 365 portal, under Management, click Users.D.   From the Office 365 portal, under Management, click Domains. Answer: CExplanation:In the Office 365 portal, click Admin > Users (under Management in the navigation pane). On the Users page, select a user, and then click Edit.Note:* Some of the options can be managed by using the Office365 Web interface and some task only by using PowerShell.* Office 365 users Password management verses the "Standard" Domain Active directory is a little bit restricted. For example: configure password policy parameters such as - Enforce password history, Minimum password length, Password must meet complexity requirements cannot be configured by the office 365 administrator. At the current time, the options that related to Office 365 users Password management are: reset the user password and setting the number of maximum number of days or password expiration (the default is 90 days). QUESTION 119You have a client computer named Computer1 that runs Windows 8 Enterprise. Computer1 has a Trusted Platform Module (TPM) chip installed and the operating system volume is encrypted by using BitLocker Drive Encryption (BitLocker). You plan to upgrade the BIOS of Computer1. You need to recommend a solution that meets the following requirements:- Ensures that the drive remains encrypted- Avoids the need to perform a BitLocker recovery- Ensures that Windows can start after the BIOS is upgraded - Minimizes the time required to complete the BIOS upgrade What should you include in the recommendation? A.   From the command prompt, run manage-bde and specify the -protectors parameter and the - disable parameter.B.   From the command prompt, run manage-bde and specify the -protectors parameter and the - delete parameter.C.   From the Trusted Platform Module (TPM) Management console, click Turn TPM Off from the Actions menu.D.   From the command prompt, run tpmvscmgr.exe and specify the destroy parameter. Answer: AExplanation:* For mass BIOS updates, create a script that disables BitLocker, installs the update, reboots the system and then re-enables BitLocker.* manage-bde -autounlock {-enable | -disable | -ClearAllKeys} Volume [-ComputerName Name] -disableDisables automatic unlocking for a data drive.* The Disable-BitLocker cmdlet disables BitLocker Drive Encryption for a BitLocker volume. When you run this cmdlet, it removes all key protectors and begins decrypting the content of the volume. QUESTION 120Your network contains an Active Directory domain. The domain contains client computers that run Windows 8 Enterprise. Users frequently use USB drives to store sensitive files that are used on multiple computers. Your corporate security policy states that all removable storage devices, such as USB data drives, must be encrypted. You need to ensure that if a user forgets the password for a USB disk that is encrypted by using BitLocker To Go, the user can resolve the issue themself. What should you do? A.   Instruct the user to open BitLocker Drive Encryption, select Backup Recovery Key, and then select Save to your Microsoft account.B.   For each computer, create a USB startup key.C.   Instruct the user to open BitLocker Drive Encryption, select Backup Recovery Key, and then select Print the recovery key.D.   From an elevated command prompt, run Manage-BDE -ForceRecovery. Answer: CExplanation: