Free Microsoft 70-243 Practice Test Questions Download From Braindump2go! (11-20)

QUESTION 11 Your network contains a System Center 2012 Configuration Manager environment. The Client Status node .n the Configuration Manager console shows a downward trend in client health. You verify the logs on several clients. You discover that the clients are healthy and are communicating normally to management points. You need to identify the reasons why the Configuration Manager console displays a downward trend in client health. Which reasons should you identify? (Choose all that Apply.) A.   In Client Status Settings Properties, the Heartbeat discovery during the following days interval is shorter than the Heartbeat Discovery interval. B.   The age set in the Delete Aged Discovery Data maintenance task is shorter than the Heartbeat Discovery interval. C.   The Delete Obsolete Client Discovery Data maintenance task is disabled. D.   The Active Directory sites that are members of boundary groups are modified. E.   Microsoft SQL Server replication to the management points stopped. Answer: BD Explanation: http://technet.microsoft.com/en-us/library/gg712308.aspx#BKMK_HeartbeatDisc Planning for Discovery in Configuration Manager - About Heartbeat Discovery Heartbeat Discovery differs from other Configuration Manager discovery methods. It is enabled by default and runs on each computer client to create a discovery data record (DDR). Heartbeat Discovery runs either on a schedule configured for all clients in the hierarchy, or if manually invoked, on a specific client by running the Discovery Data Collection Cycle on the Action tab in a client's Configuration Manager program. When Heartbeat Discovery runs, it creates a discovery data record (DDR) that contains the client's current information including network location, NetBIOS name, and operational status details. It is a small file, about 1KB, which is copied to a management point, and then processed by a primary site. The submission of a Heartbeat Discovery DDR can maintain an active client's record in the database, and also force discovery of an active client that might have been removed from the database, or that has been manually installed and not discovered by another discovery method. The default schedule for Heartbeat Discovery is set to every 7 days. If you change the heartbeat discovery interval, ensure that it runs more frequently than the site maintenance task Delete Aged Discovery Data, which deletes inactive client records from the site database. You can configure the Delete Aged Discovery Data task only for primary sites.
http://technet.microsoft.com/en-us/library/gg712679.aspx Planning for Boundaries and Boundary Groups in Configuration Manager In System Center 2012 Configuration Manager, a boundary is a network location on the intranet that can contain one or more devices that you want to manage. Boundaries can be an IP subnet, Active Directory site name, IPv6 Prefix, or an IP address range, and the hierarchy can include any combination of these boundary types. To use a boundary, you must add the boundary to one or more boundary groups. Boundary groups are collections of boundaries. By using boundary groups, clients on the intranet can find an assigned site and locate content when they have to install software, such as applications, software updates, and operating system images. When clients are on the Internet, or they are configured as Internet-only clients, they do not use boundary information. These clients cannot use automatic site assignment and always download content from any distribution point in their assigned site when the distribution point is configured to allow client connections from the Internet. Site Assignment You can configure each boundary group with an assigned site for clients. Clients join the assigned site of a boundary group that contains the client's current network location. When a boundary is added to multiple boundary groups that have different assigned sites, clients will nondeterministically select one of the sites. System Center 2012 Configuration Manager does not support this overlapping boundary configuration for site assignment. If you make a change to the site assignment configuration of a boundary group, only new site assignment actions are affected. Clients that have previously been assigned to a site, do not re-evaluate their site assignment based on changes to the configuration of a boundary group. Further information: http://technet.microsoft.com/en-us/library/bb632879.aspx Delete Obsolete Client Discovery Data Task Overview The Delete Obsolete Client Discovery Data task deletes obsolete client records from the Configuration Manager 2007 site database. A record that is marked obsolete typically was superseded by a newer record for the same client. The newer record becomes the client's current record, and the older record becomes obsolete. When you enable this task, you should configure the schedule to run at an interval greater than the heartbeat discovery schedule. This allows clients to send Discovery Data Records (DDRs) so that the obsolete bit is set correctly.
http://technet.microsoft.com/en-us/library/gg682132.aspx#BKMK_ClientHealth Introduction to Client Deployment in Configuration Manager - Monitoring the Status of Client Computers in Configuration Manager Use the Client Status node in the Monitoring workspace of the Configuration Manager console to monitor the health and activity of client computers in your hierarchy. Configuration Manager uses the following two methods to evaluate the overall status of client computers. Client Activity: You can configure thresholds to determine whether a client is active, for example: Whether the client requested policy during the last seven days. Whether Heartbeat Discovery found the client during the last seven days. Whether the client sent hardware inventory during the last seven days. When all these thresholds are exceeded, the client is determined to be inactive. Client Check: A client evaluation

engine is installed with the Configuration Manager client, which periodically evaluates the health of the Configuration Manager client and its dependencies. This engine can check or remediate some problems with the Configuration Manager client. Client status uses the monitoring and reporting capabilities of Configuration Manager to provide information in the Configuration Manager console about the health and activity of the client. You can configure alerts to notify you when clients check results or client activity drops below a specified percentage of clients in a collection or when remediation fails on a specified percentage of clients. QUESTION 12 Your network contains a System Center 2012 Configuration Manager environment. The hierarchy contains a Central Administration at Site1 and a primary site named Site. You discover that none of the packages created on Site1 are displayed in Site2. You need to identify whether there is a replication issue between the sites. What should you review? A.   the Inventoryagent.log file B.   the Rcmctrl.log file C.   the Microsoft SQL Server replication diagnostic files D.   the Despool.log file Answer: B Explanation: Rcmctrl.log Records the activities of database replication between sites in the hierarchy. QUESTION 13 Your network contains two Active Directory forests named contoso.com and litwareinc.com. You implement System Center 2012 Configuration Manager in the contoso.com forest. You deploy the Configuration Manager client to alt of the client computers in contoso.com by using a logon script. You need to ensure that the Configuration Manager client is automatically deployed to all of the client computers in the litwareinc.com forest. What should you do? (Choose all that Apply.) A.   Configure a Client Push Installation account. B.   Enable Client Push installation. C.   Enable Active Directory System Discovery. D.   Configure an administrative user. E.   Enable Active Directory Forest Discovery. Answer: ABC Explanation: http://technet.microsoft.com/en-us/library/gg682042.aspx#BKMK_prereqs_computers Prerequisites for Windows Client Deployment in Configuration Manager - Prerequisites for Computer Clients Installation Method Dependencies Client push installation: Client push installation accounts are used to connect to computers to install the client and are specified on the Accounts tab of the Client Push Installation Properties dialog box. The account must be a member of the local administrators group on the destination computer. If you do not specify a client push installation account, the site server computer account will be used. The computer on which you are installing the client must have been discovered by at least one System Center 2012 Configuration Manager discovery method. The computer has an ADMIN$ share. Enable client push installation to assigned resources must be selected in the Client Push Installation Properties dialog box if you want to automatically push the System Center 2012 Configuration Manager client to discovered resources. The client computer must be able to contact a distribution point or a management point to download the supporting files. You must have the following security permissions to install the Configuration Manager client by using client push: To configure the Client Push Installation account: Modify and Read permission for the Site object. To use client push to install the client to collections, devices and queries: Modify Resource and Read permission for the Collection object. The Infrastructure Administrator security role includes the required permissions to manage client push installation. Further information:
http://blogs.technet.com/b/configmgrteam/archive/2011/03/30/active-directory-forest-discovery-and-publishing-in-configuration-manager-2012-beta-2.aspx Active Directory Forest Discovery and Publishing in Configuration Manager 2012 Beta 2 Forest Discovery and Publishing Overview To improve manageability of an ever-changing network environment, Active Directory Forest Discovery is added in Configuration Manager 2012 Beta 2. With it, Configuration Manager can discover Active Directory forests, their domains, AD Sites and IP subnets. Because domain users (or domain computer accounts) have permission to query forest relationships, Active Directory Forest Discovery can return information about other forests and their trust direction. The system can programmatically connect to all the forests and build a complete mapping of the corporate environment. It can also cross forest boundaries using specific credentials for each forest regardless of the trust type. The information obtained through Active Directory Forest Discovery can be directly exported as boundaries or boundary groups. Changes to discovered data are updated dynamically and aged out from the database if no longer present in Active Directory Domain Services. The discovered data is also used when clients request a management point or distribution point to ensure they receive the best possible site system.
http://technet.microsoft.com/en-us/library/gg712308.aspx#BKMK_DiscoveryMethods Planning for Discovery in Configuration Manager Discovery Methods in Configuration Manager

http://technet.microsoft.com/en-us/library/gg682132.aspx#BKMK_DeployClientComputers Introduction to Client Deployment in Configuration Manager - Deploying the Configuration Manager Client to Windows-Based Computers The following table lists the

various methods that you can use to install the Configuration Manager client software on computers: Client push installation - Automatically installs the client to assigned resources and manually installs the client to resources that are not assigned. Software update point installation - Installs the client by using the Configuration Manager software updates feature. Group Policy installation - Installs the client by using Windows Group Policy. Logon script installation - Installs the client by using a logon script. Manual installation - Manually installs the client software. Upgrade installation by using application management - Upgrades clients to a newer version by using Configuration Manager application management. You can also use Configuration Manager 2007 software distribution to upgrade clients to System Center 2012 Configuration Manager. Automatic client upgrade Client imaging - Prestages the client installation in an operating system image. QUESTION 14 Your network contains a System Center 2012 Configuration Manager environment. The environment contains a angle primary site. You need to provide users with the ability to remotely reset their mobile device to the factory settings. What should you install? A.   Application Catalog web service point and Application Catalog website point B.   out of band service point and Application Catalog web service point C.   device management point and System Health Validator point D.   System Health Validator point and Application Catalog website point Answer: A Explanation: The Application Website point and the Application Web Service point are not required for client deployment. However, you might want to install them as part of your client deployment process, so that users can perform the following actions as soon as the Configuration Manager client is installed on Windows computers: Wipe their mobile devices. Search for and install applications from the Application Catalog. http://technet.microsoft.com/en-us/library/gg681976.aspx to get your mobile devices managed in SCCM 2012. The basic steps are: Set up a working Microsoft PKI infrastructure Install and configure certificates to SCCM servers Install Enrollment Point Roles may also want Enrollment Proxy Point for legacy mobile device. These site system roles are not required if you will manage mobile devices by using the Exchange Server connector, or if you install the mobile device legacy client (for example, for Windows CE), or if you request and install the client certificate on Mac computers independently from Configuration Manager. When using Network Access Protection (NAP) in Configuration Manager 2007, the System Health Validator point is needed to validate the statement of health from NAP-capable Configuration Manager clients to produce a client health state of compliant or non-compliant, It must be installed on a NAP health policy server. QUESTION 15 Your network contains a Windows Server Update Services (WSUS) server. All client computers are configured as WSUS clients. All of the client computers have Windows Firewall enabled. Windows Firewall is configured to block File and Printer Sharing. Users are not configured as local Administrators on their client computers. You deploy System Center 2012 Configuration Manager. You need to identify which methods you can use to deploy the Configuration Manager client to an of the client computers. Which client installation methods should you identify? (Choose all that Apply.) A.   a logon script installation B.   a manual client installation C.   a software update-based client installation D.   a Client Push Installation E.   an Active Directory Group Policy-based installation Answer: C Explanation: The Logon script runs with the user's credentials. Manual installation also runs with the user's credentials. Software update point uses the Local System account and All client computers are configured as WSUS clients. So the firewall should not affect functionality. Client Push Installation requires File and Printer Sharing. Group Policy Installation requires File and Printer Sharing. http://technet.microsoft.com/en-us/library/cc787076%28v=ws.10%29.aspx The firewall will block the client push installation and the GPO installation. For A and B you need administrative rights. The WSUS installation is performed with local system account and since they are WSUS clients the firewall will be opened for this type of installation. QUESTION 16 Drag and Drop Question Your network contains a System Center 2012 Configuration Manager environment. You create a collection named All Managed Servers. You need to inventory the environment variables of the All Managed Servers collection. What should you do? To answer, move the four appropriate actions from the list of actions to the answer area and arrange.
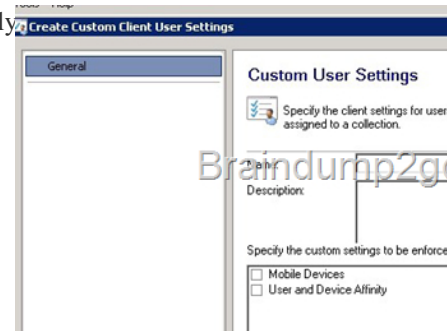

Answer:

| Create a custom client user setting named Env.		Create a custom client device setting named Env.
		In the Envcustom setting, select **Hardware Inventory**.
		In the Envcustom setting, select **Environment** (Win32_Environment).
In the Env custom setting, select ~~User Device Affinity~~	→	~~Deploy the Env custom setting to the All Managed Servers collection.~~
In the Envcustom setting, select **Desktop** (Win32_Desktop).		
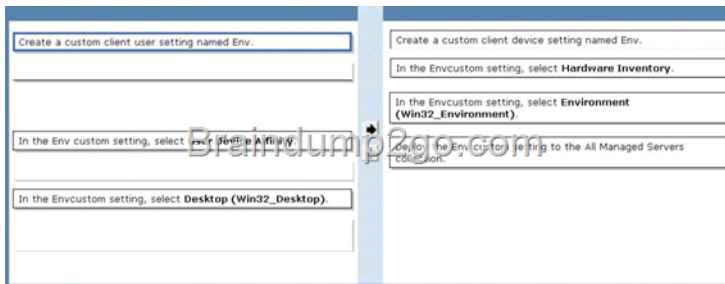
Explanation: Cannot do : custom client user setting because it is for mobile and device affinity only.

Custom User Settings

Specify the client settings for user assigned to a collection.

Description:

Specify the custom settings to be enforce

☐ Mobile Devices
☐ User and Device Affinity

QUESTION 17 Your network contains a single Active Directory domain. The functional level of the domain is windows 2003. The domain contains the following server: - Ten servers that run Windows Server 2003 - Twenty servers that run Windows Server 2008 - One server that has Microsoft Exchange Server 2007 installed - One server that has System Center 2012 Configuration Manager installed Users have mobile devices that run Windows Mobile 6.5 and Windows Phone. You need to ensure that you can manage the settings of the mobile devices and perform remote device wipes by using Configuration Manager. What should you do? A. Upgrade the Exchange server to Exchange Server 2010. Configure an Exchange connector. B.   Change the functional level of the domain to windows 2008. Upgrade the Exchange server to Exchange Server 2010. C.   Upgrade all Windows 2003 domain controllers to Windows 2008. D.   Upgrade all of the domain controllers to Windows 2008 R2. Configure an Exchange connector. Answer: A Explanation: Exchange Server Connector New in Configuration Manager 2012 is the Exchange Server Connector. This enables SCCM to connect to multiple Exchange servers, centralizing management of any device that is able to be managed via Exchange ActiveSync from within ConfigMgr. This feature is just another way to access and control Exchange's mobile device management features, and as such functionality is necessarily limited. The main benefit of the Exchange Server Connector is being able to access functionality such as remote device wipe and settings control for multiple Exchange servers from within SCCM - there's no new management capability for an organization that already manages mobile devices with Exchange ActiveSync. * It's also worth noting that the Exchange Server Connector is only available for use with Exchange 2010 and later, and some versions of Exchange also require Configuration Manager 2012 SP1.
http://myitforum.com/myitforumwp/2013/05/14/three-options-for-managing-mobiledevices-
using-sccm-2012-without-windows-intune/ QUESTION 18 Your network contains a System Center 2012 Configuration Manager environment. You need to change the organization name displayed by Configuration Manager. Which settings should you modify from the Configuration Manager console? A.   Client Policy B.   Computer Agent C.   User and Device Affinity D.   Compliance Settings Answer: B Explanation: Administration -> Client Settings -> Default Client Settings -> Computer Agent
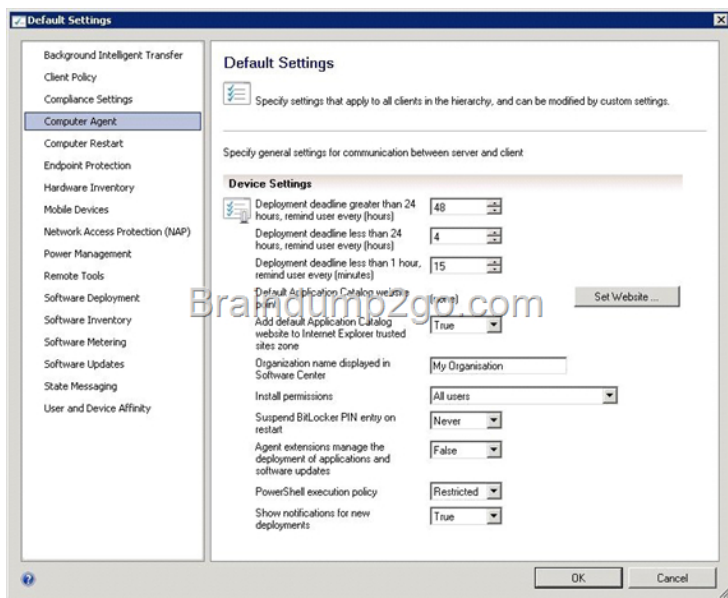
QUESTION 19 Your network contains a System Center 2012 Configuration Manager environment. Software Inventory and Hardware Inventory are enabled for all of the client computers. All of the client computers have an Application named App1 installed. App1 saves files to the C:ABC folder. All of the files saved by App1 have a file name extension of .abc. You configure Software Inventory to inventory all of the files that have the .abc extension and the .exe extension. After six months, you discover that some of the client computers fad to inventory .abc fees. Al of the client computers inventory .exe files. You need to ensure that the .abc files are inventoried. What should you do? A.   Modify C:Program FilesApp1NO_SMS_On_Drive.sms. B.   Delete C:Program FilesApp1NO-SMS_On_Drive.sms. C.   Modify C:ABCSkpswi.dat. D.   Delete C:ABCSkpswi.dat. Answer: D Explanation: http://technet.microsoft.com/en-us/library/hh691018.aspx How to Exclude Folders from Software Inventory in Configuration Manager You can create a hidden file named Skpswi.dat and place it in the root of a client hard drive to exclude it from System Center 2012 Configuration Manager software inventory. You can also place this file in the root of any folder structure you want to exclude from software inventory. This procedure can be used to disable software inventory on a single workstation or server client, such as a large file server. Note: Software inventory will not inventory the client drive again unless this file is deleted from the drive on the client computer. QUESTION 20 Your network contains a System Center 2012 Configuration Manager environment. In Default Client Agent Settings, you enable Hardware Inventory and Software Inventory. You discover that a group of client computers fails to report software inventory data. The client computers report hardware inventory data. You confirm that Configuration Manager can deploy Applications to the group of client computers. You need to identify what is causing the reporting issue. Which log files should you review? (Choose all that Apply.) A.   Filesystemfile.log B.   Dataldr.log C.   Mp_sinv.log D. Inventoryagent.log E.   Hman.log Answer: BD Explanation: http://technet.microsoft.com/en-us/library/hh427342.aspx FileSystemFile.log log for software inventory and file collection InventoryAgent.log logs DDRs (Discovery Data Records) for hardware and software More information: dataldr.log Records information about the processing of Management Information Format (MIF) files and hardware inventory in the Configuration Manager database. The question states ?You discover that a group of client computers fails to report software inventory data?. As per the above definition, dataldr.log is used for the processing of MIF files and Hardware Inventory. Braindump2go New Released Microsoft 70-243 Dump PDF Free Download, 82 Questions in all, Passing Your Exam 100% Easily! http://www.braindump2go.com/70-243.html