Microsoft 70-663 Free Braindumps - Pass 70-663 Exam With Braindump2go Free Microsoft 70-663 Q&As (91-100)

 MICROSOFT NEWS: 70-663 Exam Questions has been Updated Today! Get Latest 70-663 VCE and 70-663 PDF Instantly! Welcome to Download the Newest Braindump2go 70-663 VCE&70-663 PDF Dumps:

http://www.braindump2go.com/70-663.html (291 Q&As) Microsoft 70-663 Exam Questions has already been updated recently! Braindump2go Provide you the Latest 70-663 Exam Dumps: 70-663 PDF and 70-663 VCE! Braindump2go helps you keep in step with Microsoft Official Exam Center! Exam Code: 70-663 Exam Name: Pro: Designing and Deploying Messaging Solutions with Microsoft Exchange Server 2010 Certification Provider: Microsoft Corresponding Certifications: MCITP, MCITP: Enterprise Messaging Administrator on Exchange 201070-663 Dumps,70-663 Dumps PDF,70-663 Dumps VCE,70-663 PDF,70-663 VCE,70-663 Study Guide,70-663 Braindump,70-663 Book,70-663 Exam Questions,70-663 Practice Test,70-663 Practice Exam,70-663 eBook,70-663 Preparation
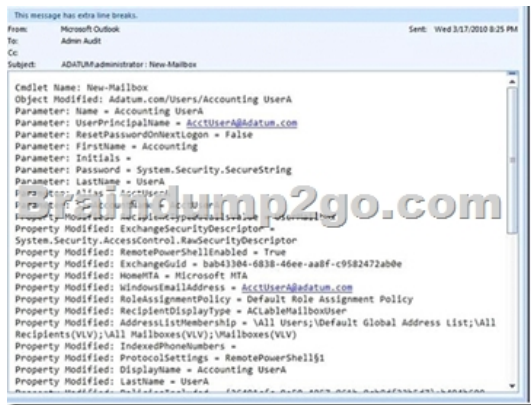

    QUESTION 91You have an Exchange Server 2010 organization.You plan to delegate administration of the organization.You have a group named Technicians that contains all the level-two technicians in the organization.You need to ensure that the Technicians group can manage the properties of all the mailbox databases. The solution must minimize the number of permissions assigned to the Technicians group.Which management role should you assign to the Technicians group? A.   Help DeskB.   Organization ManagementC.   Recipient ManagementD.   Server Management Answer: DExplanation:Server Management applies the Databases Management Role enabling administrators to create, manage, mount, and dismount mailbox and public folder databases on individual serversThe Organization Management Role applies more than the required permission level

http://technet.microsoft.com/en-us/library/dd876868(v=exchg.141).aspx

http://technet.microsoft.com/en-us/library/dd876866(v=exchg.141).aspx QUESTION 92You have an Exchange Server 2010 organization.Your companys security policy states that users must not be able to encrypt e-mail messages by using Outlook Web App (OWA).You need to recommend a client access solution that meets the requirements of the security policy.What should you include in the solution? A.   managed folder mailbox policiesB.   multiple OWA virtual directoriesC.   OWA segmentationD. WebReady Document Viewing Answer: CExplanation:Segmentation lets you enable and disable many features in Outlook Web App. You can manage segmentation using the EMC or the Shell.By default, segmentation changes take effect after 60 minutes of inactivity for users who are signed in to Outlook Web App, or when a user signs in to Outlook Web App. To force the changes to take effect immediately, restart Internet Information Services (IIS) by running the command iisreset/noforce on the Client Access server.
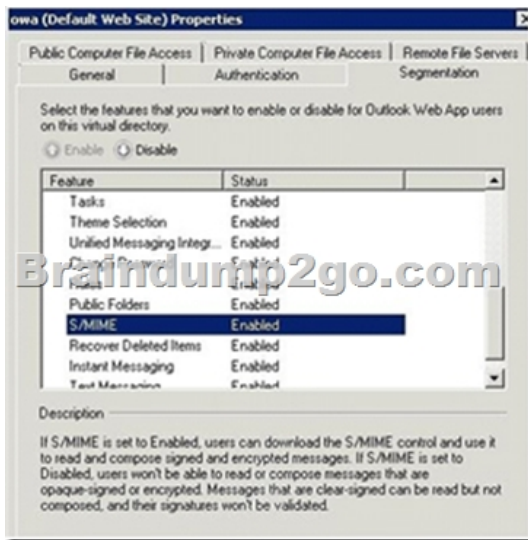
http://technet.microsoft.com/en-us/library/bb123962(v=exchg.80).aspx QUESTION 93You have an Exchange Server 2010 organization that contains five Hub Transport servers, five Mailbox servers and one Edge Transport server.You need to provide a solution to ensure that users can prevent legitimate inbound e-mail messages from being classified as spam.What should you do? A. Enable sender filteringB. Enable Sender ID filteringC. Configure a custom MailTipD. Configure safelist aggregation Answer: DExplanation:Safelist AggregationIn Microsoft Exchange Server 2007, the term safelist aggregation refers to a set of anti- spam functionality that is shared across Microsoft Office Outlook and Microsoft Exchange. This functionality collects data from the antispam Safe Recipients Lists or Safe Senders Lists and contact data that Outlook users configure, and makes this data available to the anti-spam agents on the computer that has the Edge Transport server role installed. Safelist aggregation can help reduce the instances of false-positives in anti-spam filtering that is performed by the Edge Transport server. When you configure safelist aggregation, the Content Filter agent passes safe email messages to the organization's mailbox without additional processing. E-mail messages that Outlook users receive from contacts that those users have added to their Outlook Safe Recipients List or Safe Senders List or have trusted are identified by the Content Filter agent as safe. An Outlook contact is a person, inside or outside the user's organization, about whom the user can save several types of information, such as e-mail and street addresses, telephone and fax numbers, and Web page URLs.Safelist aggregation can help reduce the instances of false-positives in anti-spam filtering that is performed by the Edge Transport server. A false-positive is a positive test or filter result that is in a subject or body of data that does not possess the attribute for which the filter or test is being conducted. In the context of spam filtering, a false-positive occurs when a spam filter incorrectly identifies a message from a legitimate sender as spam.For organizations that filter hundreds of thousands of messages from the Internet every day, even a small percentage of false-positives means that users might not receive many messages that were identified incorrectly as spam and therefore were quarantined or deleted.Safelist aggregation can be the most effective way to reduce false-positives. Outlook 2003 and the next release of Outlook, which is included in Office 2007, let users create Safe Senders Lists. Safe Senders Lists specify a list of domain names and e-mail addresses from which the Outlook user wants to receive messages. By default, e-mail addresses in Outlook Contacts and in the Exchange Server global address list are included in this list. By default, Outlook adds all external contacts to which the user sends mail to the Safe Senders List.Information Stored in the Outlook User's Safelist Collection A safelist collection is the combined data from the user's Safe Senders List, Safe Recipients List, BlockedSenders List, and external contacts. This data is stored in Outlook and in the Exchange mailbox. The following types of information are stored in an Outlook user's safelist collection:Safe senders and safe recipients - The P2 From: field of the e-mail message indicates a sender.The To: fieldof the e-mail message indicates a recipient. Safe senders and safe recipients are represented by full Simple Mail Transfer Protocol (SMTP) addresses, such as masato@contoso.com. Outlook users can add senders and recipients to their safe lists.Safe domain - The domain is the part of an SMTP address that follows the @ symbol. For example, contoso. com is the domain in the masato@contoso.com address. Outlook users can add sending domains to their safe lists.External contacts - Two types of external contacts can be included in the safelist aggregation. The first type of external contact includes

contacts to whom Outlook users have sent mail. This class of contact is added to the Safe Senders List only if an Outlook user selects the corresponding option in the Junk E-mail settings in Outlook 2003 or Exchange Server 2007.The second type of external contact includes the users' Outlook contacts. Users can add or import these contacts into Outlook. This class of contact is added to the Safe Senders List only if an Outlook user selects the corresponding option in the Junk E-mail Filter settings in Outlook 2003 or Outlook 2007.How Exchange Uses the Safelist CollectionThe safelist collection is stored on the user's mailbox server. A user can have up to 1,024 unique entries in a safelist collection.In earlier versions of Exchange Server, the user's mailbox server accessed the safelist collection during spam filtering to allow e-mail from senders on the Safe Senders List to pass through.In Exchange Server 2007, the safelist collection is stored on the user's mailbox, but you can push it to the Active Directory directory service, where the safelist collection is stored on each user object. When the safelist collection is stored on the user object in Active Directory, the safelist collection is aggregated with the antispam functionality of Exchange Server 2007 and is optimized for minimized storage and replication so that the Edge Transport server can process the safelist aggregation. The Content Filter agent on the Edge Transport server can access the safelist collection for each recipient. EdgeSync replicates the safelist collection to the Active Directory Application Mode (ADAM) instance on the Edge Transport server.Note Safelist collection entries are one-way hashed (SHA-256) before they are stored in Active Directory. This minimizes storage and replication size, and it renders the safelist collections unreadable by malicious users.Hashing of Safelist Collection EntriesThe safelist collection entries are hashed (SHA-256) one way before they are stored as array sets across two user object attributes, msExchangeSafeSenderHash and msExchangeSafeRecipientHash, as a binary large object. When data is hashed, an output of fixed length is produced; the output is also likely to be unique. For hashing of safelist collection entries, a 4-byte hash is produced. When a message is received from the Internet, Exchange Server hashes the sender address and compares it to the hashes that are stored on behalf of the Outlook user to whom the message was sent. If an inbound hash matches, the message bypasses content filtering. One-way hashing of safelist collection entries performs the following important functions:It minimizes storage and replication space. Most of the time, hashing reduces the size of the data that is hashed. Therefore, saving and transmitting a hashed version of a safelist collection entry conserves storage space and replication time. For example, a user who has 200 entries in his or her safelist collection would create about 800 bytes of hashed data that is stored and replicated in Active Directory. It renders user safelist collections unusable by malicious users. Because one-way hash values are impossible to reverse-engineer into the original SMTP address or domain, the safelist collections do not yield usable e-mail addresses for malicious users who might compromise an Edge Transport server. Enabling Safelist AggregationYou can enable safelist aggregation by running the Exchange Management Shell Update- SafeList command on a user's mailbox. The Update-SafeList command reads the safelist collection from the user's mailbox, hashes each entry, sorts the entries for easy search, and then converts the hash to a binary attribute. Finally, the Update-SafeList command compares the binary attribute that was created to any value that is stored on the attribute. If the two values are identical, the Update-SafeList command does not update the user attribute value with the safelist aggregation data. If the two attribute values are different, the Update-SafeList command updates the safelist aggregation value. This logic, where the binary values are compared before updates, is intended to significantly minimize resource use on Active Directory replication. Periodic use of Update-Safelist ensures that the most up-to-date safelist aggregation is in Active Directory. To make the safelist aggregation data in Active Directory available to Edge Transport servers in the perimeter network, you must install and configure the EdgeSync tool so that the safelist aggregation data is replicated to the Active Directory Application Mode (ADAM) instance on the Edge server. QUESTION 94You have an Exchange Server 2010 organization that contains Windows Mobile 5.0 devices.Your company plans to replace all mobile devices with Windows Mobile 6.5 devices.You need to identify which users accessed their mailboxes by using Windows Mobile 5.0 devices in the past month.What should you do? A.   Create a Data Collector Set.B.   Install and run the Exchange Server User Monitor (ExMon).C.   Export and review the Internet Information Services (IIS) logs.D.   Enable User Agent logging, and then review the agent logs. Answer: C QUESTION 95You have an Exchange Server 2010 organization. You plan to delegate Exchange administrative rights to some users in the organization. You need to recommend a solution that tracks all changes made to the Exchange organization. What should you include in the solution? A.   administrator audit loggingB.   circular loggingC. diagnostic loggingD.   Windows Security Auditing Answer: AExplanation:You can use administrator audit logging in Microsoft Exchange Server 2010 to log when a user or administrator makes a change in your organization. By keeping a log of the changes, you can trace changes to the person who made the change, augment your change logs with detailed records of the change as it was implemented, comply with regulatory requirements and requests for discovery, and more.

By default, audit logging is enabled in new installations of Microsoft Exchange Server 2010 Service Pack 1 (SP1). QUESTION 96 You have an Exchange Server 2010 organization.You need to recommend a solution that prevents the permanent deletion of e-mail messages from the mailboxes of employee who have been dismissed from the company.What should you recommend? A. Implement managed folders.B. Implement a legal hold for each mailbox.C. Implement a Retention Policy for each mailbox.D. Implement an Outlook Protection Rule for each mailbox. Answer: B QUESTION 97You have an Exchange Server 2010 organization. The organization contains a global security group named Group1. You plan to deploy a monitoring solution for the Exchange servers in your organization. You need to recommend a solution that allows members of Group1 to monitor the performance of Exchange Server 2010 servers. Your solution must prevent members of Group1 from modifying the configurations of the Exchanges Server 2010 organization. What should you include in the solution? A. Delegation of Control WizardB. Federation TrustsC. Reliability MonitorD. Role Based Access Control (RBAC) Answer: DExplanation:You can restrict/prevent/disallow functionality for selected group by using RBAC. RBAC is not only for giving control it can be used to restrict it. Management role entries on a management role determine what cmdlets and parameters are available on a management role. By removing role entries or parameters on a role entry, you can restrict what users assigned the management role can perform. Remove-ManagementRoleEntry "Seattle Server AdministratorsEnable-MailUser" To check what Role Enties are assigned to a Management Role use this command:
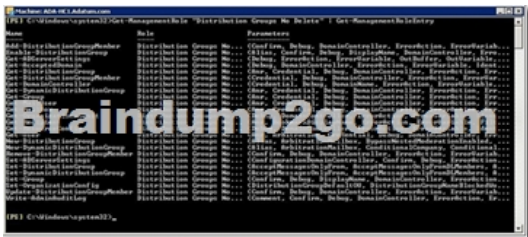
QUESTION 98Your company has a main office and 10 branch offices. You have an Exchange Server 2010 organization. All Exchange servers are installed on virtual machines. You need to create a monitoring plan for the Exchange servers that meets the following requirements:- Identify Exchange server errors- Provide alerts when Exchange services are stopped- Produce statistical analysis and reportingWhich tool should you include in the plan? A. Microsoft System Center Service ManagerB. Microsoft System Center Operations ManagerC. Microsoft System Center Configuration ManagerD. Microsoft System Center Virtual Machine Manager Answer: BExplanation:System Center Operations Manager 2007 R2, Microsoft's end-to-end service-management product, is your best choice for Windows environments. It works seamlessly with Microsoft infrastructure servers, such as Windows Server, and application servers, such as Microsoft Exchange, helping you to increase efficiency while enabling greater control of the IT environment.http://www.microsoft.com/en-us/server-cloud/system-center/operations-manager.aspx QUESTION 99Your network consists of an Active Directory domain that contains the domain controllers shown in the following table.You plan to deploy an Exchange Server 2010 server in each site.You need to recommend changes to the domain controllers to support the installation of Exchange Server 2010.What should you do?

Site	Server	Role	Operating System	Platform
Site1	Server1	Global catalog	Windows Server 2008 Service Pack 2 (SP2)	x64
	Server2		Windows Server 2008	
Site2	Server3	Read-only domain controller	Windows Server 2008	x64

A.   Enable Server2 as a global catalog server.B.   Enable Server3 as a global catalog server.C.   Upgrade Server2 to Windows Server 2008 SP2 (x64).D.   Upgrade Server3 to Windows Server 2008 SP2 (x64). Answer: AExplanation:The global catalog maintains an index of the Active Directory database for objects within its domain.Additionally, it stores partial copies of data for all other domains within a forest. Exchange Server relies on global catalog servers to resolve email addresses for users within the organization.Failure to contact a global catalog server causes emails to bounce, as the recipient's name cannot be resolved.Microsoft Exchange Server 2010 stores all configuration and recipient information in the Active Directory directory service database. When a computer that is running Exchange 2010 requires information about recipients and information about the configuration of the Exchange organization, it must query Active Directory to access the information. Active Directory servers must be available for Exchange 2010 to function correctly. By default, whenever an Exchange 2010 server starts, it binds to a randomly selected domain controller and global catalog server in its own site. You can view the selected directory servers by viewing the properties of the Exchange 2010 server in the Exchange Management Console or by using the Get-ExchangeServer cmdlet in the Exchange Management Shell. You can also use the Set-ExchangeServer cmdlet to configure a static list of domain controllers to which an Exchange 2010 server should bind or a list of domain controllers that should be excluded.You can't deploy an Exchange 2010 server in any site that contains only read-only directory servers. QUESTION 100Your company has a main office and 50 branch offices. Each office is configured as an Active Directory site. Each branch office site contains a domain controller. The main office site contains all the global catalog servers in the forest. Each branch office contains a WAN link that connects to the main office.You need to plan the deployment of new Mailbox servers to meet the following requirements:- Ensure that users in the branch offices can access their mailboxes if their local domain controller fails- Deploy the minimum number of Exchange serversWhat should you include in the plan? A.   One Mailbox server in each office and global catalog servers in each branch officeB.   One Mailbox server in each office and Universal Group Membership Caching in each branch officeC.   One Mailbox server in each branch office onlyD.   Multiple Mailbox servers in the main office only Answer: DExplanation:This is an interesting question however if you break it down it starts to make sense Main Office has the Global Catalog Servers - not the Branch Offices Branch Offices connect to the main office via a Wan Link While each branch office does have a domain controller they are not Global Catalog Servers. Further there are 50 branch offices so it makes no sense to deploy a mailbox server in each branch office or to have 50 Global Catalog ServersThe best answer is D as this would meet the requirement of deploying the least amount of Exchange Servers Guaranteed 100% Microsoft 70-663 Exam Pass OR Full Money Back! Braindump2go Provides you the latest 70-663 Dumps PDF & VCE for Instant Download!

FREE DOWNLOAD: NEW UPDATED 70-663 PDF Dumps &70-663 VCE Dumps from Braindump2go: http://www.braindump2go.com/70-663.html (291 Q&As)