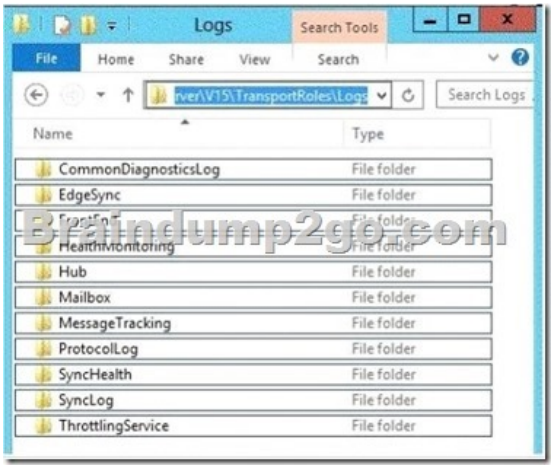
2015 Latest Braindump2go 70-341 New Added Exam Questions Free Share (191-200)

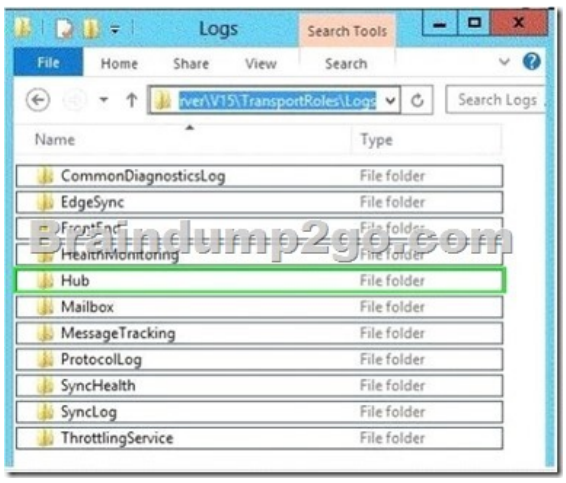
2015 New Updated 70-341 Exam Dumps Questions and Answers are all from Microsoft Official Exam Center! Some new questions added into this new released 70-341 Dumps! Download 70-341 Exam Dumps Full Version Now and Pass one time! Vendor: MicrosoftExam Code: 70-341Exam Name: Microsoft Core Solutions of Microsoft Exchange Server 2013Keywords: 70-341 Exam Dumps,70-341 PDF Download,70-341 VCE Download,70-341 Study Guide,70-341 Study Material,70-341 Braindump,70-341 Exam Questions,70-341 Book

QUESTION 191How would you disable the anti malware filtering and ensure that engine updates from microsoft are downloaded and updated. A. Disable-Antimalwareagent.ps1B. Set-malwarefilteringserverC. Disable-Antimalwarescanning.ps1 (probable option)D. Update-MalwareFilteringServer.ps1 (guessed option) Answer: BExplanation:The Line in Bold and Italics is crucial to this question so pay attention!!!Disable or Bypass Anti-Malware ScanningApplies to: Exchange Server 2013In Microsoft Exchange Server 2013, you can disable or bypass malware filtering of all email messages in transit on a server. This must be done on a Mailbox server.You may want to disable Exchange 2013 malware filtering if you are using another product for malware filtering. When malware filtering is disabled, the Exchange malware agent is unhooked and not running, and engine updates are not kept up-to-date.Important: Bypassing malware filtering should only be done when troubleshooting a problem. When malware filtering is bypassed, the Exchange malware agent remains hooked, and engine updates are kept up-to-date. However, malware filtering is skipped while you attempt to resolve whatever problems you are encountering. After you have finished troubleshooting, you should restore malware filtering. What do you need to know before you begin? Estimated time to complete each procedure: 15 minutesYou can only use the Shell to perform this procedure.Disabling or enabling malware filtering restarts the Microsoft Exchange Transport service on the server. This may temporarily disrupt mail flow in your organization.Bypassing or restoring malware filtering doesn't require you to restart any services. However, changes to the setting may take up to 10 minutes to take effect.If you have multiple Exchange servers performing malware filtering, you must perform these steps on each server.You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the ?Anti-malware? entry in the Anti-Spam and Anti-Malware Permissions topic.For information about keyboard shortcuts that may apply to the procedures in this topic, see Keyboard Shortcuts in the Exchange Admin Center.Tip: Having problems? Ask for help in the Exchange forums. Visit the forums at: Exchange Server, Exchange Online, or Exchange Online Protection. What do you want to do? Use the Shell to disable malware filtering on a specific Exchange server To disable malware filtering, run the following command:Copy & $env:ExchangeInstallPath\Scripts\Disable-Antimalwarescanning.ps1Note: To re-enable malware filtering, use Enable-Antimalwarescanning.ps1 instead of Disable-Antimalwarescanning.ps1. How do you know this step worked? To verify that malware filtering is disabled, run the following command and confirm that it returns a value of False:Copy Get-TransportAgent "Malware Agent"Use the Shell to temporarily bypass malware filtering on a specific Exchange server Important: Bypassing malware filtering should only be done when troubleshooting a problem. You should restore malware filtering after you have finished troubleshooting. To temporarily bypass malware filtering, run the following command:Copy Set-MalwareFilteringServer <ServerIdentity> -BypassFiltering $trueTo restore malware filtering, run the following command:Copy Set-MalwareFilteringServer <ServerIdentity> -BypassFiltering $falseHow do you know this step worked? To verify that malware filtering is being bypassed, run the following command and confirm that it returns a value of True: Copy Get-MalwareFilteringServer | Format-List BypassFiltering http://technet.microsoft.com/en-us/library/jj150526(v=exchg.150).aspx http://www.ntweekly.com/?p=2813To disable malware filtering, run the following command:& $env:ExchangeInstallPath\Scripts\Disable-Antimalwarescanning.ps1 QUESTION 192You need to install and configure anti-spam and antimalware filtering.Which servers should you install the anti-spam agents and enable the anti-spam and antimalware filtering? (Choose two) A. You should install the anti-spam agents on the Client Access Servers only.B. You should install the anti-spam agents on the Mailbox servers only.C. You should install the anti-spam agents on the Client Access Servers and the Mailbox Servers.D. You should enable antimalware filtering on the Client Access Servers only.E.

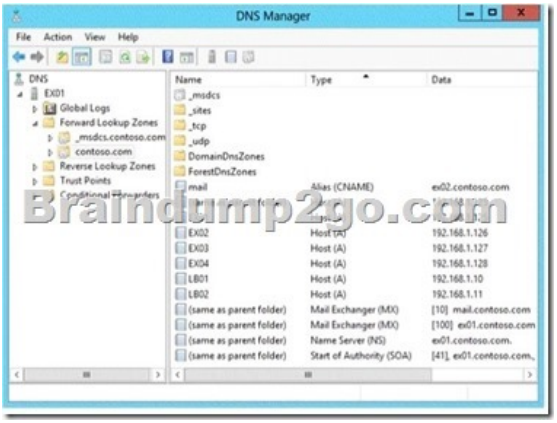
You should enable antimalware filtering on the Mailbox servers only.F. You enable antimalware filtering on the Client Access Servers and the Mailbox Servers. Answer: BEExplanation: http://howexchangeworks.com/2013/06/connection-filtering-in-exchange-2013.htmlIn Exchange 2013, the anti-spam agents can only be installed on the Mailbox role. But, the connection filtering which is very useful in fighting spam emails is not available in 2013. Same goes for the attachment filter. Even though CAS proxies emails back and forth (if setup correctly), it is a stateless proxy and can't have any anti-spam agents on it. http://www.jaapwesselius.com/2013/01/10/installing-exchange-server-2013-part-iii/In Exchange 2013 the anti-spam functionality (through protocol agents) is running on the Mailbox Server and not on the Client Access Server so all mail, including all spam will hit the Mailbox Server when installed in a configuration as outlined in these blog post series. The anti-spam functionality is enabled using a Powershell script (.EnableAntiSpamAgents.ps1) and offers Sender and Recipient filtering, content filtering, Sender Reputation and Sender ID filtering. To activate the ant-spam agents on the Mailbox Server open the Exchange Management Shell and enter the following commands:CD $Exscripts.Install-AntiSpamAgents.ps1 http://www.tlglearning.com/LinkClick.aspx?fileticket=dnonu0glRr8%3D&tabid=238You can't enable the anti-spam agents on an Exchange 2013 Client Access Server http://social.technet.microsoft.com/Forums/exchange/en-US/5c9f1b51-4a93-4de4-964e-1f53afbb8e8b/how-toconfigure-attachment-filter-agent-on-exchange-2013-The Malware Filter runs on every 2013 Mailbox server to protect against malware and viruses. http://blogs.dirteam.com/blogs/davestork/archive/2012/12/06/exchange-and-malware-protection.aspx QUESTION 193Hotspot QuestionYour company has an Exchange Server 2013 organization.You configure domain security with a partner organization.You configure the required connectors.You plan to verify whether the partner organization configured the required settings for domain security.You enable logging for the Send connectors and the Receive connectors.You need to verify that the STARTTLS command is issued by an Exchange server when an email message is sent to the partner organization.Which log folder should you review? (To answer, select the appropriate folder in the answer area.)



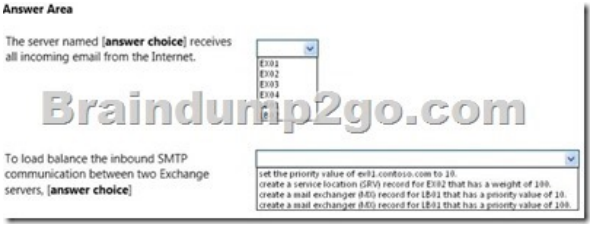
Answer:



QUESTION 194Hotspot QuestionYour company has an Exchange Server 2013 organization. All servers have the Client Access server role and the Mailbox server role installed.The DNS Manager is shown in the exhibit. (Click the Exhibit button.)

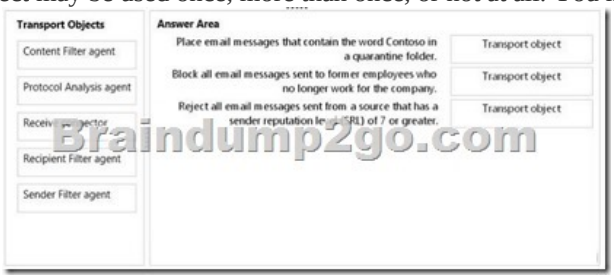


Use the drop-down menus to select the answer choice that completes each statement.



Answer:

QUESTION 195Drag and Drop QuestionYou have an Exchange Server 2013 organization that contains a server named EX1. EX1 has the Mailbox server role and the Client Access server role installed.You plan to enable anti-spam protection on EX1.You need to configure the message hygiene settings for email messages received from the Internet.The solution must meet the following requirements:- Place email messages that contain the word Contoso in a quarantine folder.- Block all email messages sent to former employees who no longer work for the company.- Reject all email messages sent from a source that has a sender reputation level (SRL) of 7 or greater.What should you configure? (To answer, drag the appropriate transport objects to the correct requirements. Each object may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.)

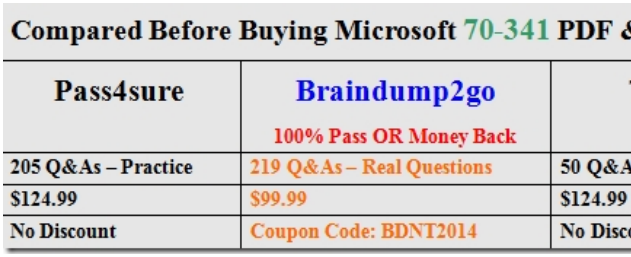


Answer:

QUESTION 196Your company has offices in New York, Paris, and Montreal. An Active Directory site exists for each office.You have an Exchange Server 2013 organization that contains two servers in each site. One server in each site has the Mailbox server role installed and the other server in each site has the Client Access server role installed.You need to ensure that all of the outbound email from each site is routed through the Client Access server in that site.Which should you do? A. Remove the Mailbox servers from the list of source servers on each Send connector.B. Disable the Microsoft Exchange Transport service on each Mailbox server.C. Run the Set-SendConnector cmdlet and specify the -FrontendProxyEnabted.True parameter.D. Run the Set-TransportConfig cmdlet and specify the -InternatSMTPServers:$nult parameter. Answer: CExplanation:
http://exchangeserverpro.com/exchange-2013-front-end-proxy/
http://blogs.technet.com/b/exchange/archive/2013/01/25/exchange-2013-client-access-server-role.aspx
http://www.msexchange.org/articles-tutorials/exchange-server-2013/planning-architecture/exchange-2013-mail-flow-part3.html
QUESTION 197You have an Exchange Server 2010 organization.Users access Outlook Web App by using the name mail.contoso.com.You deploy Exchange Server 2013 to the existing organization.You change the DNS record of mail.contoso.com to point to an Exchange Server 2013 Client Access server.The users report that they can no longer access their mailbox from Outlook Web App.The OWA virtual directory in Exchange Server 2010 is configured as shown in the exhibit. (Click the Exhibit button.)You need to ensure that the users on Exchange Server 2010 can access Outlook Web App.Which setting should you change?

A. WindowsAuthenticationB. FormsAuthenticationC. LegacyRedirectTypeD. FailbackUri Answer: AExplanation:Windows Authentication (NTLM) needs to be enabled on the Exchange 2010 Client Access Server to enable the Exchange 2013 Client Acess Server to proxy connections.Exchange Server Deployment AssistantEnable and configure Outlook AnywhereTo allow your Exchange 2013 Client Access server to proxy connections to your Exchange 2007 and Exchange 2010 servers, you must enable and configure Outlook Anywhere on all of the Exchange 2007 and Exchange 2010 servers in your organization. If some Exchange 2007 or Exchange 2010 servers in your organization are already configured to use Outlook Anywhere, their configuration must also be updated to support Exchange 2013. When you use the steps below to configure Outlook Anywhere, the following configuration is set on each Exchange 2007 and Exchange 2010 server:The Outlook Anywhere external URL is set to the external hostname of the Exchange 2013 server.Client authentication, which is used to allow clients like Outlook 2013 to authenticate with Exchange, is set to Basic.Internet Information Services (IIS) authentication, which is used to allow Exchange servers to communicate, set to NTLM and Basic. QUESTION 198You have an Exchange Server 2013 organization that contains two Mailbox servers and two Client Access servers.You have a database availability group (DAG) that contains both Mailbox servers.You need to deploy public folders.What should you do first? A. Run the New-PublicFolderDatabase cmdlet and specify the -Server parameter.B. Run the New-PublicFolder cmdlet and specify the -Path parameter.C. Run the New-Mailbox cmdlet and specify the -Publicfolder parameter.D. Run the New-MailboxDatabase cmdlet and specify the -PublicFotderDatabase parameter. Answer: CExplanation:Set Up Public Folders in a New OrganizationNew-Mailbox -PublicFolder -Name MasterHierarchy
http://www.msexchange.org/articles-tutorials/exchange-server-2013/migration-deployment/migrating-publicfolders-exchange-2013-part1.html
http://www.msexchange.org/articles-tutorials/exchange-server-2013/migration-deployment/migrating-publicfolders-exchange-2013-part2.html QUESTION 199You have an Exchange Server 2013 organization. You need to install the Hub Transport server role on a new server. You install all the prerequisites for the Hub Transport role on the server. What should you do next? A. From Windows PowerShell, run the Add-WindowsFeature cmdlet.B. From Windows PowerShell, run the Install-TransportAgent.ps1 script.C. At the command prompt, run Setup.com /M:Install /R:HT.D. At the command prompt, run ServerManagerCmd.exe -IP Exchange-HUB.xml. Answer: C QUESTION 200You have an Exchange Server 2013 server that has the Mailbox, Hub Transport, and Client Access server roles installed. You need to ensure that users can send and receive e-mail by using Windows Live Mail or Microsoft Outlook Express. What should you do on the server? A. Install and then configure the SMTP server feature.B. Start the Microsoft Exchange POP3 service and then set the startup type to Automatic.C. Modify the properties of the MSExchangePOP3 (TCP-in) Windows Firewall rule.D. Modify the properties of the MSExchangeMailSubmission - RPC (TCP-in) Windows Firewall rule. Answer: BExplanation:By default, pop3 is set to manual. For those who feel the overwhelming

anxiety before their 70-341 exam,Braindump2go Latest updated 70-341 Exam Dumps will help you Pass 100% in a short time preparation! 70-341 Exam Dumps PDF & VCE Full Version Instant Download!



http://www.braindump2go.com/70-341.html