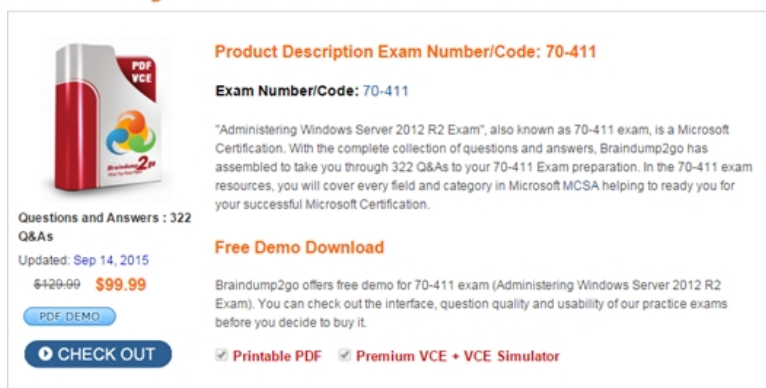# New Released Microsoft 70-411 Dumps PDF Free Download From Braindump2go (271-280)

 MICROSOFT OFFICIAL: New Updated 70-411 Exam Questions from Braindump2go 70-411 PDF Dumps and 70-411 VCE Dumps! Welcome to Download the Newest Braindump2go 70-411 VCE&PDF Dumps: http://www.braindump2go.com/70-411.html (322 Q&As) Braindump2go Guarantees Your Microsoft 70-411 Exam 100% Success with Our Unique Official 70-411 Exam Questions Resources! Braindump2go's 70-411 Braindumps are Developed by Experiences IT Certifications Professionals Working in Today's Prospering Companies and Data Centers! Braindump2go 70-411 Exam Dumps are Checked by Our Experts Team every day to ensure you have the Latest Updated Exam Dumps! Exam Code: 70-411Exam Name Administering Windows Server 2012Certification Provider: MicrosoftCorresponding Certifications: MCSA, MCSA: Windows Server 2012, MCSE, MCSE: Desktop Infrastructure, MCSE: Private Cloud, MCSE: Server InfrastructureKeywords:70-411 Dumps,70-411 Microsoft Exam Questions,70-411 VCE,70-411 PDF,70-411 Practice Exams,70-411 Practice Tests,70-411 Book,70-411 Study Guide

   QUESTION 271Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Remote Desktop Session Host role service installed. The computer account of Server1 resides in an organizational unit (OU) named OU1.You create and link a Group Policy object (GPO) named GPO1 to OU1. GPO1 is configured as shown in the exhibit. (Click the Exhibit button.)
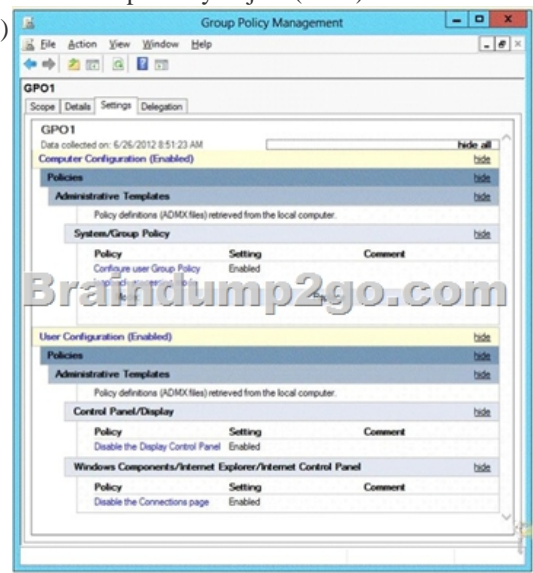
    You need to prevent GPO1 from Applying to your user account when you log on to Server1. GPO1 must Apply to every other user who logs on to Server1.What should you configure? A.   WMI FilteringB.   Item-level TargetingC.   Block InheritanceD.   Security Filtering Answer: D QUESTION 272Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2. DC1 is backed up daily.The domain has the Active Directory Recycle Bin enabled.During routine maintenance, you delete 500 inactive user accounts and 100 inactive groups. One of

the deleted groups is named Group1. Some of the deleted user accounts are members of some of the deleted groups.For documentation purposes, you must provide a list of the members of Group1 before the group was deleted.You need to identify the names of the users who were members of Group1 prior to its deletion.You want to achieve this goal by using the minimum amount of administrative effort.What should you do first? A.   Mount the most recent Active Directory backup.B.   Perform an authoritative restore of Group1.C.   Use the Recycle Bin to restore Group1.D.   Reactivate the tombstone of Group1. Answer: BExplanation:The Active Directory Recycle Bin does not have the ability to track simple changes to objects. If the object itself is not deleted, no element is moved to the Recycle Bin for possible recovery in the future. In other words, there is no rollback capacity for changes to object properties, or, in other words, to the values of these properties.There is another approach you should be aware of. Tombstone reanimation (which has nothing to do with zombies) provides the only way to recover deleted objects without taking a DC offline, and it's the only way to recover a deleted object's identity information, such as its objectGUID and objectSid attributes. It neatly solves the problem of recreating a deleted user or group and having to fix up all the old access control list (ACL) references, which contain the objectSid of the deleted object.Restores domain controllers to a specific point in time, and marks objects in Active Directory as being authoritative with respect to their replication partners. QUESTION 273Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Both servers run Windows Server 2012 R2.For Server2, you are configuring constrained delegation to a third-party service named Service1 on Server1.When you attempt to add Service1 from Server1 to the delegation setting of Server2, you discover that Service1 is not listed in the Available services list.You need to ensure that you can add Service1 for constrained delegation.What should you do first? A.   From the Services console, modify the properties of Service1B.   From ADSI Edit, create a serviceConnectionPoint (SCP) objectC.   From a command prompt, run the setspn.exe commandD.   From Active Directory Users and Computers, enable the Advanced Features option. Answer: A QUESTION 274You have a file server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed.Files created by users in the human resources department are assigned the Department classification property automatically.You are configuring a file management task named Task1 to remove user files that have not been accessed for 60 days or more.You need to ensure that Task1 only removes files that have a Department classification property of human resources. The solution must minimize administrative effort.What should you configure on Task1? A.   Create a custom action.B.   Configure a file screen.C.   Create a classification rule.D.   Create a condition. Answer: DExplanation:Create a File Expiration TaskThe following procedure guides you through the process of creating a file management task for expiring files. File expiration tasks are used to automatically move all files that match certain criteria to a specified expiration directory, where an administrator can then back those files up and delete them. Property conditions. Click Add to create a new condition based on the file's classification. This will open the Property Condition dialog box, which allows you to select a property, an operator to perform on the property, and the value to compare the property against. After clicking OK, you can then create additional conditions, or edit or remove an existing condition. QUESTION 275Hotspot QuestionYour network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2 and has the Network Policy Server role service installed.An administrator creates a Network Policy Server (NPS) network policy named Policy1.You need to ensure that Policy1 applies to L2TP connections only.Which condition should you modify? To answer, select the appropriate object in the answer area.
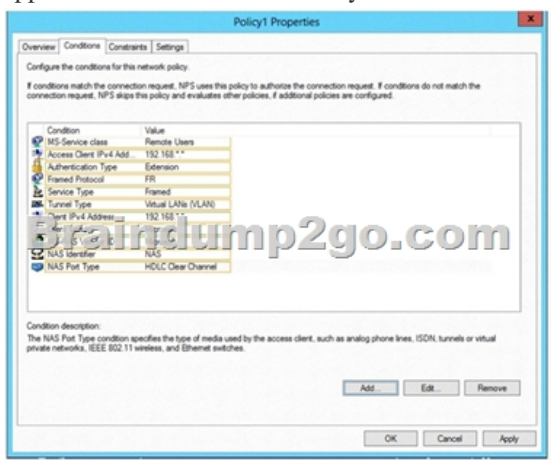
Answer:
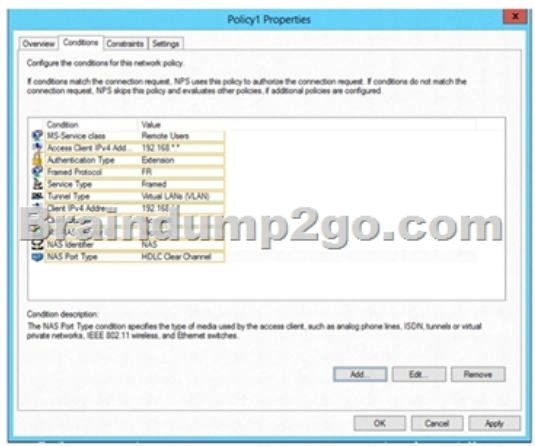
QUESTION 276 Your network contains two DNS servers named Server1 and Server2 that run Windows Server 2012 R2. Server1 hosts a primary zone for contoso.com. Server2 hosts a secondary zone for contoso.com. You need to ensure that Server2 replicates changes to the contoso.com zone every five minutes. Which setting should you modify in the start of authority (SOA) record? A. Retry interval B. Minimum (default) TTL C. Expires after D. Refresh interval Answer: D Explanation: By default, the refresh interval for each zone is set to 15 minutes. The refresh interval is used to determine how often other DNS servers that load and host the zone must attempt to renew the zone.
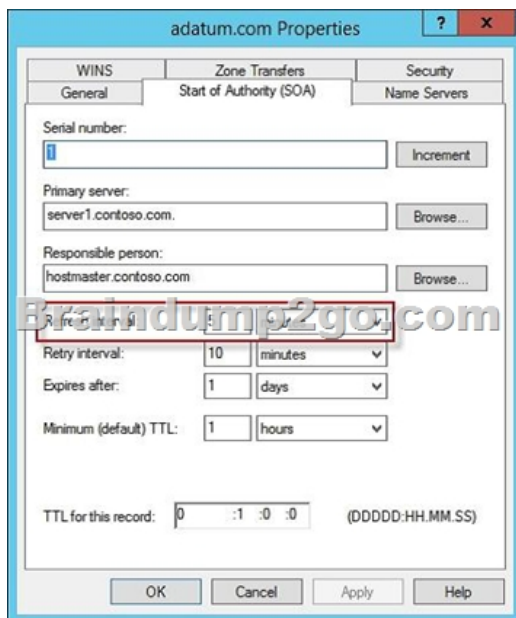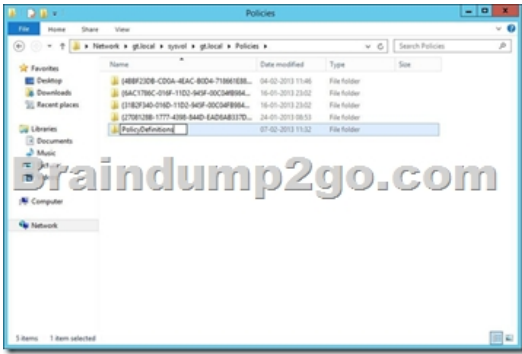

QUESTION 277 Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. An organizational unit (OU) named OU1 contains 200 client computers that run Windows 8 Enterprise. A Group Policy object (GPO) named GPO1 is linked to OU1. You make a change to GPO1. You need to force all of the computers in OU1 to refresh their Group Policy settings immediately. The solution must minimize administrative effort. Which tool should you use? A. The Secedit command B. The Set-AdComputer cmdlet C. Active Directory Users and Computers D. The Invoke-GpUpdate cmdlet Answer: D Explanation: Invoke-GPUpdate Schedule a remote Group Policy refresh (gpupdate) on the specified computer. Applies To: Windows Server 2012 R2 The Invoke-GPUpdate cmdlet refreshes Group Policy settings, including security settings that are set on remote computers by scheduling the running of the Gpupdate command on a remote computer. You can combine this cmdlet in a scripted fashion to schedule the Gpupdate command on a group of computers. The refresh can be scheduled to immediately start a refresh of policy settings or wait for a specified period of time, up to a maximum of 31 days. To avoid putting a load on the network, the refresh times will be offset by a random delay. Note: Group Policy is a complicated infrastructure that enables you to apply policy settings to remotely configure a computer and user experience within a domain. When the Resultant Set of Policy settings does not conform to your expectations, a best practice is to first verify that the computer or user has received the latest policy settings. In previous versions of Windows, this was accomplished by having the user run GPUpdate.exe on their

computer.With Windows Server 2012 R2 and Windows 8, you can remotely refresh Group Policy settings for all computers in an organizational unit (OU) from one central location by using the Group Policy Management Console (GPMC). Or you can use the Invoke-GPUpdate Windows PowerShell cmdlet to refresh Group Policy for a set of computers, including computers that are not within the OU structure--for example, if the computers are located in the default computers container.The remote Group Policy refresh updates all Group Policy settings, including security settings that are set on a group of remote computers, by using the functionality that is added to the context menu for an OU in the Group Policy Management Console (GPMC). When you select an OU to remotely refresh the Group Policy settings on all the computers in that OU, the following operations happen:An Active Directory query returns a list of all computers that belong to that OU. For each computer that belongs to the selected OU, a WMI call retrieves the list of signed in users.A remote scheduled task is created to run GPUpdate.exe /force for each signed in user and once for the computer Group Policy refresh. The task is scheduled to run with a random delay of up to 10 minutes to decrease the load on the network traffic. This random delay cannot be configured when you use the GPMC, but you can configure the random delay for the scheduled task or set the scheduled task to run immediately when you use the Invoke-GPUpdate cmdlet.Reference: Force a Remote Group Policy Refresh (GPUpdate) QUESTION 278Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. The domain contains two servers. The servers are configured as shown in the following table.

Server name	Operating system	Role
Server1	Windows Server 2012 R2	Web Server (IIS) server role Network Load Balancing (NLB) feature
Server2	Windows Server 2012 R2	Web Server (IIS) server role Network Load Balancing (NLB) feature

Server1 and Server2 host a load-balanced website named Web1. Web1 runs by using an application pool named WebApp1. WebApp1 uses a group Managed Service Account named gMSA1 as its identity.Domain users connect to Web1 by using either the name Web1.contoso.com or the alias myweb.contoso.com.You discover the following:- When the users access Web1 by using Web1.contoso.com, they authenticate by using Kerberos.- When the users access Web1 by using myweb.contoso.com, they authenticate by using NTLM.You need to ensure that the users can authenticate by using Kerberos when they connect by using myweb.contoso.com.What should you do? A.   Run the Add-ADComputerServiceAccount cmdlet.B.   Modify the properties of the gMSA1 service account.C.   Modify the properties of the Web1 website.D.   Run the Install-ADServiceAccount cmdlet. Answer: D Explanation: * Install-ADServiceAccountInstalls an Active Directory service account on a computer.* The Install-ADServiceAccount cmdlet installs an existing Active Directory service account on the computer on which the cmdlet is run. This cmdlet verifies that the computer is eligible to host the service account. The cmdlet also makes the required changes locally so that the service account password can be periodically reset by the computer without requiring any user action.* Managed service accounts and virtual accounts are two new types of accounts introduced in Windows Server 2008 R2/2012 and Windows 7/8 to enhance the service isolation and manageability of network applications such as Microsoft SQL Server and Internet Information Services (IIS).* If you configure the application to use a domain account, you can isolate the privileges for the application, but you need to manually manage passwords or create a custom solution for managing these passwords. Many SQL Server and IIS applications use this strategy to enhance security, but this strategy requires additional administration and complexity. In these deployments, service administrators spend a considerable amount of time on maintenance tasks such as managing service passwords and service principal names (SPNs), which are required for Kerberos authentication. In addition, these maintenance tasks can disrupt service.Two new types of accounts available in Windows Server 2008 R2 and Windows 7--the managed service account and the virtual account--are designed to provide crucial applications such as SQL Server or IIS with the isolation of their own accounts, while eliminating the need for an administrator to manually administer the SPN and credentials for these accounts.Reference: Service Accounts Step-by-Step Guide QUESTION 279Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.You create a central store for Group Policy.You receive a custom administrative template named Template1.admx.You need to ensure that the settings in Template1.admx appear in all new Group Policy objects (GPOs).What should you do? A.   Copy Template1.admx to\Contoso.comSYSVOLContoso.comPoliciesPolicyDefinitionsB. From the Default Domain Controllers Policy, add Template1.admx to the Administrative Templates.C.   Copy Template1.admx to \Contoso.comNETLOGOND.   From the Default Domain Policy, add Template1.admx to the Administrative Templates. Answer: A Explanation:Unlike ADM files, ADMX files are not stored in individual GPOs. For domain-based enterprises, administrators can create a central store location of ADMX files that is accessible by anyone with permission to create or edit GPOs.

QUESTION 280Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2 and has the Network Policy Server role service installed.An administrator creates a RADIUS client template named Template1.You create a RADIUS client named Client1 by using Template1.You need to modify the shared secret for Client1.What should you do first? A.   Clear Select an existing template for Client1B.   Set the Shared secret setting of Template1 to Manual.C.   Clear Enable this RADIUS client for Client1.D.   Configure the Advanced settings of Template1. Answer: AExplanation:Clear checkmark for Select an existing template in the new client wizard.In New RADIUS Client, in Shared secret, do one of the following:Ensure that Manual is selected, and then in Shared secret, type the strong password that is also entered on the RADIUS client. Retype the shared secret in Confirm shared secret.
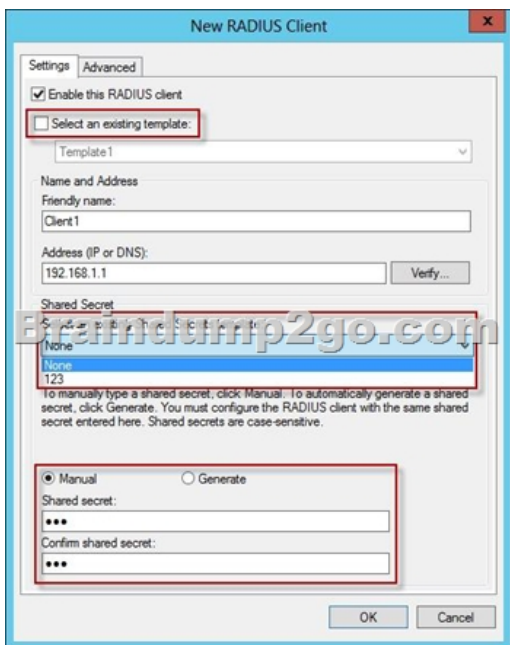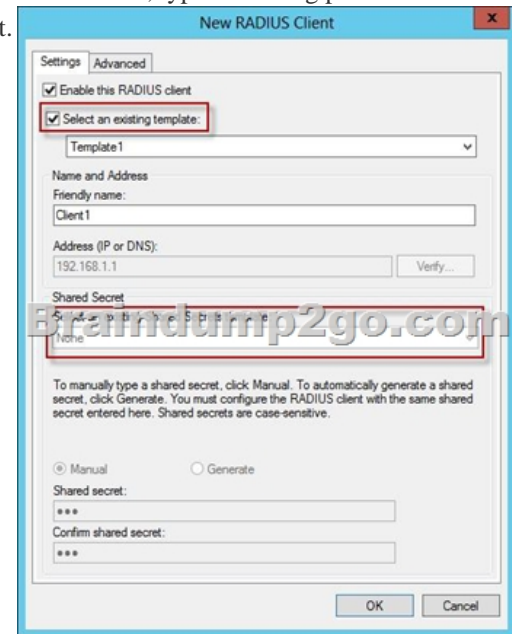
Braindump2go Offers 100% money back guarantee on all products! Our products remain valid for a lifetime! Recently we update our 70-411 Exam Questions since the Microsoft Official Exam Center adds some new questions in 70-411 Exam Dumps. Braindump2go checks all Exam Dumps every day and guarantee all the exam questions are the latest and correct!

FREE DOWNLOAD: NEW UPDATED 70-411 PDF Dumps & VCE Dumps from Braindump2go:

http://www.braindump2go.com/70-411.html (322 Q&As)