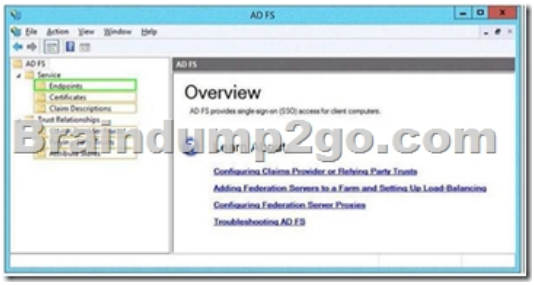
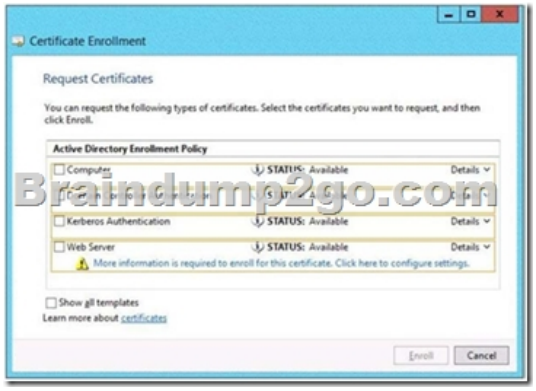
[Oct.-2016-UpdateValid Braindump2go Microsoft 70-417 Exam PDF 252q Offer[NQ11-NQ15

2016/10 New Microsoft 70-417: Upgrading Your Skills to MCSA Windows Server 2012 R2 Exam Questions Updated Today!Free Instant Download 70-417 Exam Dumps (PDF & VCE) 612Q&As from Braindump2go.com Today! 100% Real Exam Questions! 100% Exam Pass Guaranteed! 1.| 2016/10 Latest 70-417 Exam Dumps (PDF & VCE) 612Q&As Download: http://www.braindump2go.com/70-417.html 2.| 2016/10 Latest 70-417 Exam Questions & Answers: https://drive.google.com/folderview?id=0B9YP8B9sF_gNNl9VMTNzaklUbGc&usp=sharing QUESTION 11Hotspot QuestionYour 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 Active Directory Federation Services (AD FS) server role installed.Adatum.com is a partner organization.You are helping the administrator of adatum.com set up a federated trust between adatum.com and contoso.com. The administrator of adatum.com asks you to provide a file containing the federation metadata ofcontoso.com.You need to identify the location of the federation metadata file.Which node in the AD FS console should you select? To answer, select the appropriate node in the answer area.

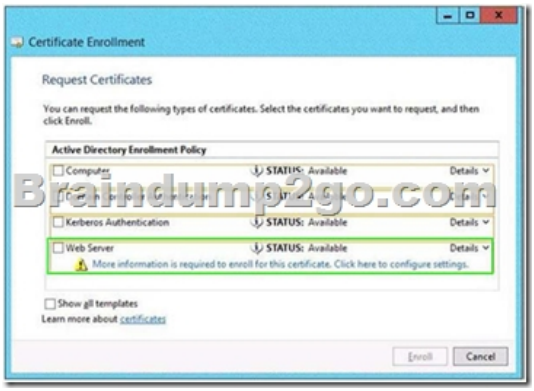
Answer:



QUESTION 12Hotspot QuestionYour network contains an Active Directory domain named contoso.com. The domain contains an enterprise certification authority (CA). The domain contains a server named Server1 that runs Windows Server 2012 R2. You install the Active Directory Federation Services server role on Server1. You plan to configure Server1 as an Active Directory Federation Services (AD FS) server. The Federation Service name will be set to adfsl.contoso.com. You need to identify which type of certificate template you must use to request a certificate for AD FS. Which certificate template should you identify? To answer, select the appropriate template in the answer area.



Answer:

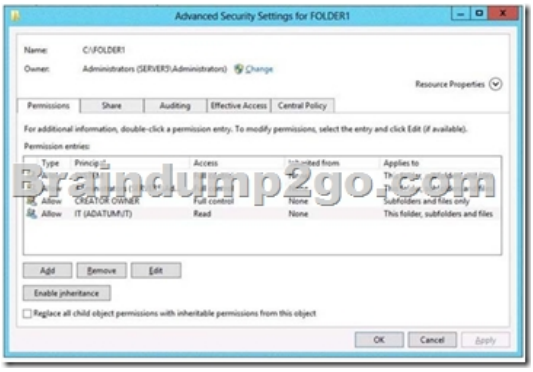


QUESTION 13Your network contains an Active Directory domain named contoso.com. The domain contains four servers. The servers are configured as shown in the following table.

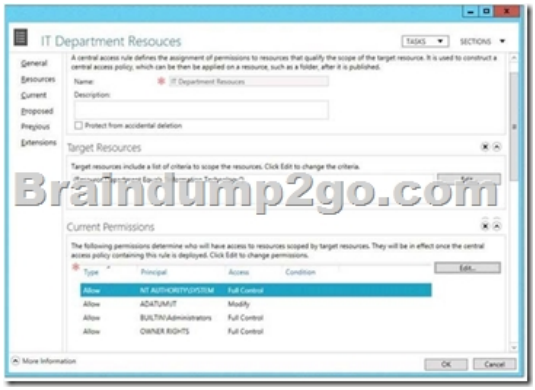
Server name	Configuration	IP address
Server1	Active Directory Domain Services (AD DS)	192.168.1.100
Server2	DHCP server File server	192.168.1.101
Server3	Web server	131.107.100.100
Server4	DNS server Network Policy Server (NPS) server	131.107.100.101

You plan to deploy an enterprise certification authority (CA) on a server named Servers. Server5 will be used to issue certificates to domain-joined computers and workgroup computers. You need to identify which server you must use as the certificate revocation list (CRL) distribution point for Server5. Which server should you identify? A. Server1B. Server3C. Server4D. Server2 Answer: BExplanation:CDP (and AD CS) always uses a Web ServerNB: this CDP must be accessible from outside the AD, but here we don't have to wonder about that as there's only one web server.
http://technet.microsoft.com/fr-fr/library/cc782183%28v=ws.10%29.aspx Selecting a CRL Distribution PointBecause CRLs are valid only for a limited time, PKI clients need to retrieve a new CRL periodically. Windows Server 2003 PKI Applications look in the CRL distribution point extension for a URL that points to a network location from which the CRL object can be retrieved. Because CRLs for enterprise CAs are stored in Active Directory, they can be accessed by means of LDAP. In comparison, because CRLs for stand-alone CAs are stored in a directory on the server, they can be accessed by means of HTTP, FTP, and so on as long as the CA is online. Therefore, you should set the CRL distribution point after the CA has been installed.The system account writes the CRL to its distribution point, whether the CRL is published manually or is published according to an established schedule. Therefore you must ensure that the system accounts for CAs have permission to write to the CRL distribution point. Because the CRL path is also included in every certificate, you must define the CRL location and its access path before deploying certificates. If an Application performs revocation checking and a valid CRL is not available on the local computer, it rejects the certificate. You can modify the CRL distribution point by using the Certification Authority MMC snap-in. In this way, you can change the location where the CRL is published to meet the needs of users in yourorganization. You must move the CRL distribution point from the CA configuration folder to a Web server to change the location of the CRL, and you must move each new CRL to the new distribution point, or else the chain will break when the previous CRL expires.NoteOn root CAs, you must also modify the CRL distribution point in the CAPolicy.inf file so that the root CA certificate references the correct CDP and AIA paths, if specified. If you are using certificates on the Internet, you must have at least one HTTPs-accessible location for all certificates that are not limited to internal use.http://technet.microsoft.com/en-us/library/cc771079.aspx Configuring Certificate RevocationIt is not always possible to contact a CA or other trusted server for information about the validity of a certificate. To effectively support certificate status checking, a client must be able to access revocation data to determine whether the certificate is valid or has been revoked. To support a variety of scenarios, Active Directory Certificate Services (AD CS) supports industry-standard methods of certificate revocation. These include publication of certificate revocation lists (CRLs) and delta CRLs, which can be made available to clients from a variety of locations, including Active Directory Domain Services (AD DS), Web servers, and network file shares. QUESTION 14Your network contains three Active Directory forests. Each forest contains an Active Directory Rights Management Services (AD RMS) root cluster. All of the users in all of the forests must be able to access protected content from any of the forests. You need to identify the minimum number of AD RMS trusts required. How many trusts should you identify? A. 2B. 3C. 4D. 6 Answer: DExplanation:http://technet.microsoft.com/en-us/library/dd772648%28v=ws.10%29.aspx AD RMS Multi-forest Considerations

QUESTION 15Your network contains an Active Directory domain named contoso.com. The network contains a file server named Server1 that runs Windows Server 2012 R2. You create a folder named Folder1. You share Folder1 as Share1. The NTFS permissions on Folder1 are shown in the Folder1 exhibit. (Click the Exhibit button.)

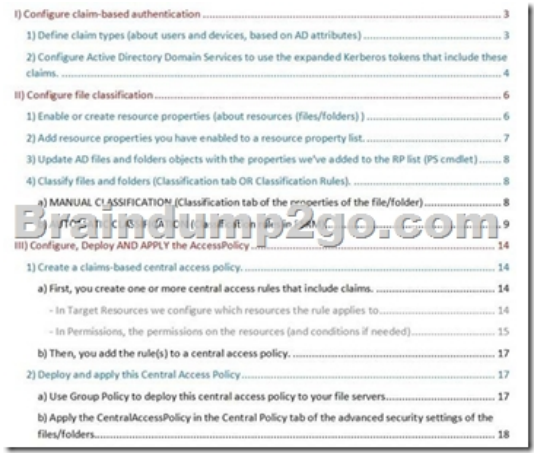


The Everyone group has the Full control Share permission to Folder1. You configure a central access policy as shown in the Central Access Policy exhibit. (Click the Exhibit button.)



Members of the IT group report that they cannot modify the files in Folder1. You need to ensure that the IT group members can modify the files in Folder1. The solution must use central accesspolicies to control the permissions. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.) A. On the Security tab of Folder1, remove the permission entry for the IT group.B. On the Classification tab of Folder1, set the classification to "Information Technology".C. On the Security tab of Folder1, assign the Modify permission to the Authenticated Users group.D. On Share1, assign the Change Share permission to the IT group.E. On the Security tab of Folder1, add a conditional expression to the existing permission entry for the IT group. Answer: BCExplanation:NB added the missing exhibits by searching for a piece of the question on google => i did get an answer (a pdf file with a few questions and exhibits, but how to be sure they're ok...) initial Answer:On the Classification tab of Folder1, set the classification to Information Technology. =>true On the Security tab of Folder1, add a conditional expression to the existing permission entry for the IT group. =>false it took me a whole day and a hole night to find that, but now i'm sure of the answer. Let me explain my point of view You first set the Folder1 classification to "Information Technology" so it meets the target resource requirement and the Central Access Policy can be Applied to it, no problem about that.But my problem is about the second answer, to me none of them is good :A: On the Security tab of Folder1, remove the permission entry for the IT group. => tested => it failed of course, users don't even have read permissions anymoreD: On Share1, assign the Change share permission to the IT group =>Everyone already has the full control share permission => won't solve the problem which is about the NTFS Read permissionE:

On the Security tab of Folder1, add a conditional expression to the existing permission entry for the IT group => how could a condition, added to a read permission, possibly transform a read to a modify permission? if they had said "modify the permission and add a conditional expression" => ok (even if that's stupid, it works) a condition is Applied to the existing permissions to filter existing access to only matching users or groups so if we Apply a condition to a read permission, the result will only be that less users (only them matching the conditions) will get those read permissions, which actually don't solve the problem neither so only one left :C: On the Security tab of Folder1, assign the Modify permission to the Authenticated Users group => for sure it works and it's actually the only one which works, but what about security? well i first did not consider this method => "modify" permission for every single authenticated users? But now it looks very clear :THE MORE RESTRICTIVE PERMISSION IS ALWAYS THE ONE APPLIED!! So "Modify" for Authenticated Users group and this will be filtered by the DAC who only allows IT group. and it matches the current settings that no other user (except admin, creator owner, etc...) can even read the folder. and this link confirms my theory :http://autodiscover.wordpress.com/2012/09/12/configuring-dynamic-access-controls-andfile-classificationpart4-winservr-2012-dac-microsoft-mvpbuzz/ Configuring Dynamic Access Controls and File ClassificationNote:In order to allow DAC permissions to go into play, allow everyone NTFS full control permissions and then DAC will overwrite it, if the user doesn't have NTFS permissions he will be denied access even if DAC grants him access.Andif this can help, a little summary of configuring DAC:



!!!RECOMMEND!!! 1.| 2016/10 Latest 70-417 Exam Dumps (PDF & VCE) 612Q&As Download: http://www.braindump2go.com/70-417.html 2.| 2016/10 Latest 70-417 Exam Questions & Answers: https://drive.google.com/folderview?id=0B9YP8B9sF_gNNl9VMTNzaklUbGc&usp=sharing