

[March 2018 Lead2pass 70-411 Exam Questions Guarantee 70-411 Certification Exam 100% Success 449q

Lead2pass Free 70-411 Exam Questions Download 100% Pass 70-411 Exam: <https://www.lead2pass.com/70-411.html>

QUESTION 31 Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs. You need to provide an Administrator named Admin1 with the ability to create GPOs in the domain. The solution must not provide Admin1 with the ability to link GPOs. What should you use? A. dcpofix B. Get-GPOReport C. Gpfixup D. Gpresult E. Gptedit.msc F. Import-GPO G. Restore-GPO H.

Set-GPInheritance I. Set-GPLink J. Set-GPPermission K. Gpupdate L. Add-ADGroupMember Answer: L Explanation:

<http://windowsitpro.com/windows/what-group-policy-creator-owners-group> QUESTION 32 Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs. The domain contains a GPO named GPO1. GPO1 contains several Group Policy preferences. You need to view all of the preferences configured in GPO1. What should you use? A. dcpofix B. Get-GPOReport C. Gpfixup D. Gpresult E. Gptedit.msc F. Import-GPO G. Restore-GPO H. Set-GPInheritance I. Set-GPLink J. Set-GPPermission K. Gpupdate L. Add-ADGroupMember Answer: B Explanation: The Get-GPOReport cmdlet generates a report in either XML or HTML format that describes properties and policy settings for a specified GPO or for all GPOs in a domain. The information that is reported for each GPO includes: details, links, security filtering, WMI filtering, delegation, and computer and user configuration

<http://technet.microsoft.com/en-us/library/ee461027.aspx> <http://cmdlet.wordpress.com/2011/08/24/episode-3-get-gporeport>

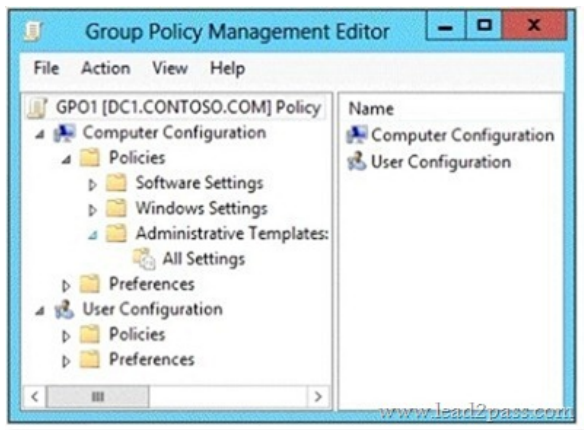
QUESTION 33 Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs. A network Administrator accidentally deletes the Default Domain Policy GPO. You do not have a backup of any of the GPOs. You need to recreate the Default Domain Policy GPO. What should you use? A. dcpofix B. Get-GPOReport C. Gpfixup D. Gptedit.msc E. Import-GPO F. Restore-GPO G. Set-GPInheritance H.

Set-GPLink I. Set-GPPermission J. Gpupdate K. Add-ADGroupMember Answer: A Explanation: Restores the default Group Policy objects to their original state (that is, the default state after initial installation). QUESTION 34 Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs. The domain is renamed to adatum.com. Group Policies no longer function correctly. You need to ensure that the existing GPOs are applied to users and computers. You want to achieve this goal by using the minimum amount of Administrative effort. What should you use? A. dcpofix B. Get-GPOReport C. Gpfixup D. Gpresult E. Gptedit.msc F. Import-GPO G. Restore-GPO H. Set-GPInheritance I. Set-GPLink J. Set-GPPermission K. Gpupdate L.

Add-ADGroupMember Answer: C Explanation: You can use the gpfixup command-line tool to fix the dependencies that Group Policy objects (GPOs) and Group Policy links in Active Directory Domain Services (AD DS) have on Domain Name System (DNS) and NetBIOS names after a domain rename operation. QUESTION 35 Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs. The domain contains a top-level organizational unit (OU) for each department. A group named Group1 contains members from each department. You have a GPO named GPO1 that is linked to the domain. You need to configure GPO1 to apply settings to Group1 only. What should you use? A. dcpofix B. Get-GPOReport C. Gpfixup D. Gpresult E. Gptedit.msc F. Import-GPO G. Restore-GPO H.

Set-GPInheritance I. Set-GPLink J. Set-GPPermission K. Gpupdate L. Add-ADGroupMember Answer: J Explanation: Set-GPPermission grants a level of permissions to a security principal (user, security group, or computer) for one GPO or all the GPOs in a domain. You use the TargetName and targetType parameters to specify a user, security group, or computer for which to set the permission level. -Replace <SwitchParameter> Specifies that the existing permission level for the group or user is removed before the new permission level is set. If a security principal is already granted a permission level that is higher than the specified permission level and you do not use the Replace parameter, no change is made.

<http://technet.microsoft.com/en-us/library/ee461038.aspx> QUESTION 36 Your network contains an Active Directory domain named contoso.com. A user named User1 creates a central store and opens the Group Policy Management Editor as shown in the exhibit.



You need to ensure that the default Administrative Templates appear in GPO1. What should you do? A. Link a WMI filter to GPO1. B. Add User1 to the Group Policy Creator Owners group. C. Configure Security Filtering in GPO1. D. Copy files from %Windir%\PolicyDefinitions to the central store. Answer: D Explanation: In earlier operating systems, all the default Administrative Template files are added to the ADM folder of a Group Policy object (GPO) on a domain controller. The GPOs are stored in the SYSVOL folder. The SYSVOL folder is automatically replicated to other domain controllers in the same domain. A policy file uses approximately 2 megabytes (MB) of hard disk space. Because each domain controller stores a distinct version of a policy, replication traffic is increased. In Group Policy for Windows Server 2008 and Windows Vista, if you change Administrative template policy settings on local computers, Sysvol will not be automatically updated with the new .ADMX or .ADML files. This change in behavior is implemented to reduce network load and disk storage requirements, and to prevent conflicts between .ADMX files and .ADML files when edits to Administrative template policy settings are made across different locales. To make sure that any local updates are reflected in Sysvol, you must manually copy the updated .ADMX or .ADML files from the PolicyDefinitions file on the local computer to the SysvolPolicyDefinitions folder on the appropriate domain controller. To take advantage of the benefits of .admx files, you must create a Central Store in the SYSVOL folder on a domain controller. The Central Store is a file location that is checked by the Group Policy tools. The Group Policy tools use any .admx files that are in the Central Store. The files that are in the Central Store are later replicated to all domain controllers in the domain. To create a Central Store for .admx and .adml files, create a folder that is named PolicyDefinitions in the following location: \FQDN\SYSVOL\FQDN\Policies

<http://support.microsoft.com/kb/929841> QUESTION 37 Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 P.2. Server1 has the Network Policy and Access Services server role installed. Your company's security policy requires that certificate-based authentication must be used by some network services. You need to identify which Network Policy Server (NPS) authentication methods comply with the security policy. Which two authentication methods should you identify? (Each correct answer presents part of the solution. Choose two.) A. MS-CHAP. B. PEAP-MS-CHAP v2. C. Chap. D. EAP-TLSE. MS-CHAP v2 Answer: B Explanation: PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server. When you use EAP with a strong EAP type, such as TLS with smart cards or TLS with certificates, both the client and the server use certificates to verify their identities to each other. QUESTION 38 You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Windows Deployment Services server role installed. Server1 contains two boot images and four install images. You need to ensure that when a computer starts from PXE, the available operating system images appear in a specific order. What should you do? A. Modify the properties of the boot images. B. Create a new image group. C. Modify the properties of the install images. D. Modify the PXE Response Policy. Answer: C QUESTION 39 Your network contains an Active Directory domain named contoso.com. Domain controllers run either Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 R2. You have a Password Settings object (PSOs) named PSO1. You need to view the settings of PSO1. Which tool should you use? A. Get-ADFineGrainedPasswordPolicy. B. Get-ADAccountResultantPasswordReplicationPolicy. C. Get-ADDomainControllerPasswordReplicationPolicy. D. Get-ADDefaultDomainPasswordPolicy Answer: A Explanation: A. Gets one or more Active Directory fine grained password policies. B. Gets the resultant password replication policy for an Active Directory account. C. Gets the members of the allowed list or denied list of a read-only domain controller's password replication policy. D. Gets the default password policy for an Active Directory domain. <http://technet.microsoft.com/en-us/library/ee617231.aspx> <http://technet.microsoft.com/en-us/library/ee617227.aspx>

<http://technet.microsoft.com/en-us/library/ee617207.aspx> <http://technet.microsoft.com/en-us/library/ee617244.aspx> QUESTION

40 You have a failover cluster that contains five nodes. All of the nodes run Windows Server 2012 R2. All of the nodes have BitLocker Drive Encryption (BitLocker) enabled. You enable BitLocker on a Cluster Shared Volume (CSV). You need to ensure that all of the cluster nodes can access the CSV. Which cmdlet should you run next? A. Unblock-TpmB.

Add-BitLockerKeyProtectorC. Remove-BitLockerKeyProtectorD. Enable BitLockerAutoUnlock Answer: B Explanation: Add an Active Directory Security Identifier (SID) to the CSV disk using the Cluster Name Object (CNO) The Active Directory protector is a domain security identifier (SID) based protector for protecting clustered volumes held within the Active Directory infrastructure. It can be bound to a user account, machine account or group. When an unlock request is made for a protected volume, the BitLocker service interrupts the request and uses the BitLocker protect/unprotect APIs to unlock or deny the request. For the cluster service to selfmanage BitLocker enabled disk volumes, an administrator must add the Cluster Name Object (CNO), which is the Active Directory identity associated with the Cluster Network name, as a BitLocker protector to the target disk

volumes. Add-BitLockerKeyProtector <drive letter or CSV mount point> -ADAccountOrGroupProtector - ADAccountOrGroup

\$cno **70-411 dumps full version (PDF&VCE):** <https://www.lead2pass.com/70-411.html> **Large amount of free 70-411 exam**

questions on Google Drive: <https://drive.google.com/open?id=0B3Syig5i8gpDSmRhaVRWcW5Cc1k> You may also need: 70-410

exam dumps: <https://drive.google.com/open?id=0B3Syig5i8gpDcXAzcDVN0WI1bIU> 70-412 exam dumps:

<https://drive.google.com/open?id=0B3Syig5i8gpDcDUzczlzc2N6RkU> 70-413 exam dumps:

<https://drive.google.com/open?id=1b83z5KIZUL3VTF7QfvaVypTlHdaUnZIE> 70-414 exam dumps:

<https://drive.google.com/open?id=0B3Syig5i8gpDdzk4ajRnWG50TzA>