[Lead2pass Official Easily Pass 70-411 Exam By Training Lead2pass New Microsoft VCE Dumps (281-300)

Lead2pass 2017 September New Microsoft 70-411 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! There are many companies that provide 70-411 braindumps but those are not accurate and latest ones. Preparation with Lead2pass 70-411 new questions is a best way to pass this certification exam in easy way. Following questions and answers are all new published by Microsoft Official Exam Center: https://www.lead2pass.com/70-411.html QUESTION 281Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. All of the DNS servers in both of the domains run Windows Server 2012 R2.The network contains two servers named Server1 and Server2. Server1 hosts an Active Directory-integrated zone for contoso.com. Server2 hosts an Active Directory-integrated zone for fabrikam.com. Server1 and Server2 connect to each other by using a WAN link.Client computers that connect to Server1 for name resolution cannot resolve names in fabrikam.com.You need to configure Server1 to resolve names in fabrikam.com. The solution must NOT require that changes be made to the fabrikam.com zone on Server2.What should you create? A. a secondary zoneB. a stub zoneC. a trust anchorD. a zone delegation Answer: BExplanation:A stub zone is a copy of a zone that contains only those resource records necessary to identify the authoritative Domain Name System (DNS) servers for that zone. A stub zone is used to resolve names between separate DNS namespaces. This type of resolution may be necessary when a corporate merger requires that the DNS servers for two separate DNS namespaces resolve names for clients in both namespaces. QUESTION 282Your network contains an Active Directory domain named contoso.com. Network Access Protection (NAP) is deployed to the domain.You need to create NAP event trace log files on a client computer.What should you run? A. Register-ObjectEventB. Register-EngineEventC. tracertD. logman Answer: DExplanation:Register-ObjectEvent: Monitor events generated from .Net Framework Object.
Register-EngineEvent: Subscribes to events that are generated by the Windows PowerShell engine and by the New-Event cmdlet.
http://technet.microsoft.com/en-us/library/hh849967.aspxtracert: Trace IP routelogman: Manages and schedules performance counter and event trace log collections on a local and remote systems.http://technet.microsoft.com/en-us/library/bb490956.aspx QUESTION 283Your 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. 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 Set-ADServiceAccount cmdlet.B. Run the New-ADServiceAccount cmdlet.C. Modify the properties of the WebApp1 application pool.D. Modify the properties of the Web1 website. Answer: A
Explanation: Independent managed service accounts that were introduced in Windows Server 2008 R2 and Windows 7 are managed domain accounts that provide an automatic password management and simplified management of SPN (Service Principal Names SPNs) - including delegation of management to other administrators. The Group managed service account provides the same functions within the domain, but this also is expanding to multiple servers. When connecting with a service that is hosted in a server farm (for example, a Network Load Balancing), the authentication protocols require with mutual authentication, that all instances of services use the same principal. If group managed service accounts can be used as a service principals, the password for the account from the Windows operating system is managed, rather than leaving the password keeper the Administrator. The Microsoft Key Distribution Service ("kdssvc.dll") provides the mechanism for secure retrieval of current key or a certain key ready for an Active Directory account with a key ID. This service is new in Windows Server 2012 and can not run on older versions of the Windows Server operating system. From the key distribution service secret information to create keys for the account are provided. These keys are changed regularly. In one group managed service account to the Windows Server 2012 domain controller calculates the password for the key specified by the Key Distribution Service - just like any other attributes of the group managed service account. Current and older password values can be 8-member hosts accessed by contacting a Windows Server 2012 domain controller of Windows Server 2012- and Windows. Group Managed Service Accounts provide a single identity solution for services that are running on a server farm or on systems behind a Network Load Balancing. By providing a solution for group managed service accounts (groups-MSA solution) services for the new group MSA principal can be configured, while the password manager of Windows is handled. When using a group managed service account must be managed by services or service administrators no password synchronization between service instances become. The group managed service account supported hosts that are offline

for an extended period, as well as the managing member of hosts for all instances of a service. So you can deploy a server farm that supports a single identity, with respect to the can authenticate existing client computer without knowing with which instance of the service a connection is established. It is most likely that the service account gMSA1 only the name web1.contoso contains .de as registered SPN. To ensure that Kerberos authentication works even when use of the name myweb.certbase.de, must match the service account name myweb.certbase.de be added as additional SPN. This is possible by editing the account Properties or by using the Set-ADServiceAccount. QUESTION 284Your 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. Active Directory Administrative CenterB. Get-ADAccountResultantPasswordReplicationPolicyC. Local Security PolicyD. Get-ADDomainControllerPasswordReplicationPolicy Answer: AExplanation: Up until now, PSOs were created with the ADSI Edit application or PowerShell. Now, we can use the Active Directory Administrative Center.Note:* Password Setting Object (PSO) is another name for Fine Grain Password Policies. These PSOs allowed us to set up a different password policy based on security group membership.* Storing fine-grained password policiesWindows Server 2008 includes two new object classes in the Active Directory Domain Services (AD DS) schema to store fine-grained password policies:/ Password Settings Container/ Password SettingsThe Password Settings Container (PSC) object class is created by default under the System container in the domain. It stores the Password Settings objects (PSOs) for that domain. You cannot rename, move, or delete this container. QUESTION 285Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2012 R2. Server1 has a share named Share1.When users without permission to Share1 attempt to access the share, they receive the Access Denied message as shown in the exhibit. (Click the Exhibit button.) You deploy a new file server named Server2 that runs Windows Server 2012 R2.You need to configure Server2 to display the same custom Access Denied message as Server1.What should you install on Server2? A. The Remote Assistance featureB. The File Server Resource Manager role serviceC. The Enhanced Storage featureD. The Storage Services server role Answer: BExplanation:We need to install the prerequisites for Access-Denied Assistance.Because Access-Denied Assistance relies up on e-mail notifications, we also need to configure each relevant file server with a Simple Mail Transfer Protocol (SMTP) server address. Let's do that quickly with Windows PowerShell:Set-FSRMSetting -SMTPServer mailserver.nuggetlab.com -AdminEmailAddress admingroup@nuggetlab.com -FromEmailAddress admingroup@nuggetlab.comYou can enable Access-Denied Assistance either on a per-server basis or centrally via Group Policy. To my mind, the latter approach is infinitely preferable from an administration standpoint.Create a new GPO and make sure to target the GPO at your file servers' Active Directory computer accounts as well as those of your AD client computers. In the Group Policy Object Editor, we are looking for the following path to configure Access-Denied Assistance:Computer ConfigurationPoliciesAdministrative TemplatesSystemAccess-Denied Assistance The Customize message for Access Denied errors policy, shown in the screenshot below, enables us to create the actual message box shown to users when they access a shared file to which their user account has no access. What's cool about this policy is that we can "personalize" the e-mail notifications to give us administrators (and, optionally, file owners) the details they need to resolve the permissions issue quickly and easily.For instance, we can insert pre-defined macros to swap in the full path to the target file, the administrator e-mail address, and so forth. See this example:Whoops! It looks like you're having trouble accessing [Original File Path]. Please click Request Assistance to send [Admin Email] a help request e-mail message. Thanks!You should find that your users prefer these human-readable, informative error messages to the cryptic, non-descript error dialogs they are accustomed to dealing with.The Enable access-denied assistance on client for all file types policy should be enabled to force client computers to participate in Access-Denied Assistance. Again, you must make sure to target your GPO scope accordingly to "hit" your domain workstations as well as your Windows Server 2012 file servers.Testing the configurationThis should come as no surprise to you, but Access-Denied Assistance works only with Windows Server 2012 and Windows 8 computers. More specifically, you must enable the Desktop Experience feature on your servers to see Access-Denied Assistance messages on server computers.When a Windows 8 client computer attempts to open a file to which the user has no access, the custom Access-Denied Assistance message should appear: If the user clicks Request Assistance in the Network Access dialog box, they see a secondary message: At the end of this process, the administrator(s) will receive an e-mail message that contains the key information they need in order to resolve the access problem:The user's Active Directory identityThe full path to the problematic fileA user-generated explanation of the problemSo that's it, friends! Access-Denied Assistance presents Windows systems administrators with an easy-to-manage method for more efficiently resolving user access problems on shared file system resources. Of course, the key caveat is that your file servers must run Windows Server 2012 and your client devices must run Windows 8, but other than that, this is a great technology that should save admins extra work and end-users extra headaches. http://4sysops.com/archives/access-denied-assistance-in-windows-server-2012/ QUESTION 286Your network contains an Active

Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.Administrators use client computers that run Windows 8 to perform all management tasks.A central store is configured on a domain controller named DC1.You have a custom administrative template file named App1.admx. App1.admx contains application settings for an application named Appl. From a client computer named Computer1, you create a new Group Policy object (GPO) named GPO1.You discover that the application settings for App1 fail to appear in GPO1.You need to ensure that the App1 settings appear in all of the new GPOs that you create.What should you do? A. Copy App1.admx to \Contoso.comSYSVOLContoso.comPoliciesPolicyDefinitionsB. From the Default Domain Controllers Policy, add App1.admx to the Administrative Templates.C. From the Default Domain Policy, add App1.admx to the Administrative TemplatesD. Copy App1.admx to \Contoso.comSYSVOLContoso.comStarterGPOs. Answer: A Explanation: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. QUESTION 287Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. One of the domain controllers is named DC1.The DNS zone for the contoso.com zone is Active Directory-integrated and has the default settings.A server named Server1 is a DNS server that runs a UNIX-based operating system. You plan to use Server1 as a secondary DNS server for the contoso.com zone.You need to ensure that Server1 can host a secondary copy of the contoso.com zone.What should you do? A. From Windows PowerShell, run the Set-DnsServerPrimaryZone cmdlet and specify the contoso.com zone as a target.B. From DNS Manager, modify the Security settings of DC1C. From DNS Manager, modify the Zone Transfers settings of the contoso.com zone.D. From DNS Manager, modify the Advanced settings of DC1. Answer: DExplanation:In DNS Manager open up Properties of DC1, click on the Advanced tab, and select ENABLE BIND SECONDARIES.BIND Secondaries enables the DNS server to communicate with non-Microsoft DNS servers. https://technet.microsoft.com/en-us/library/cc940771.aspx?f=255&MSPPError=-2147217396 QUESTION 288Your 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.You need to enable trace logging for Network Policy Server (NPS) on Server1.Which tool should you use? A. the Network Policy Server consoleB. the Server Manager consoleC. the tracert.exe commandD. the netsh.exe command Answer: DExplanation:You can use log files on servers running Network Policy Server (NPS) and NAP client computers to help troubleshoot NAP problems. Log files can provide the detailed information required for troubleshooting complex problems.You can capture detailed information in log files on servers running NPS by enabling remote access tracing. The Remote Access service does not need to be installed or running to use remote access tracing. When you enable tracing on a server running NPS, several log files are created in %windir%tracing.The following log files contain helpful information about NAP:IASNAP.LOG: Contains detailed information about NAP processes, NPS authentication, and NPS authorization.IASSAM.LOG: Contains detailed information about user authentication and authorization.Membership in the local Administrators group, or equivalent, is the minimum required to enable tracing. Review details about using the appropriate accounts and group memberships at Local and Domain Default Groups(http://go.microsoft.com/fwlink/?LinkId=83477).To create tracing log files on a server running NPSOpen a command line as an administrator.Type netshras set tr * en.Reproduce the scenario that you are troubleshooting.Type netshras set tr * dis.Close the command prompt window. http://technet.microsoft.com/en-us/library/dd348461%28v=ws.10%29.aspx QUESTION 289Hotspot QuestionYour network contains an Active Directory forest named contoso.com. The forest contains a single domain. The forest contains two Active Directory sites named Site1 and Site2.You plan to deploy a read-only domain controller (RODC) named DC10 to Site2. You pre-create the DC10 domain controller account by using Active Directory Users and Computers.You need to identify which domain controller will be used for initial replication during the promotion of the RODC.Which tab should you use to identify the domain controller? To answer, select the appropriate tab in the answer area. Answer: QUESTION 290Your 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 DNS Server server role installed.Server1 is configured to delete automatically the DNS records of client computers that are no longer on the network. A technician confirms that the DNS records are deleted automatically from the contoso.com zone.You discover that the contoso.com zone has many DNS records for servers that were on the network in the past, but have not connected to the network for a long time.You need to set the time stamp for all of the DNS records in the contoso.com zone.What should you do? A. From DNS Manager, modify the Advanced settings from the properties of Server1B. From Windows PowerShell, run the Set-DnsServerResourceRecordAging cmdletC. From DNS Manager, modify the Zone Aging/Scavenging PropertiesD. From Windows PowerShell, run the Set-DnsServerZoneAging cmdlet. Answer: BExplanation: https://technet.microsoft.com/en-us/library/jj649936.aspx QUESTION 291Your network contains an Active Directory domain

named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2.You enable and configure Routing and Remote Access (RRAS) on Server1.You create a user account named User1.You need to ensure that User1 can establish VPN connections to Server1.What should you do? A. Modify the members of the Remote Management Users group.B. Add a RADIUS client.C. Modify the Dial-in setting of User1.D. Create a connection request policy. Answer: CExplanation: Access permission is also granted or denied based on the dial-in properties of each user account.
http://technet.microsoft.com/en-us/library/cc772123.aspx QUESTION 292Your network contains an Active Directory domain named contoso.com.All user accounts reside in an organizational unit (OU) named OU1. All of the users in the marketing department are members of a group named Marketing. All of the users in the human resources department are members of a group named HR.You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preferences of GPO1 to add two shortcuts named Link1 and Link2 to the desktop of each user.You need to ensure that Link1 only appears on the desktop of the users in Marketing and that Link2 only appears on the desktop of the users in HR.What should you configure? A. Security FilteringB. WMI FilteringC. Group Policy InheritanceD. Item-level targeting Answer: DExplanation: You can use item-level targeting to change the scope of individual preference items, so they apply only to selected users or computers. Within a single Group Policy object (GPO), you can include multiple preference items, each customized for selected users or computers and each targeted to apply settings only to the relevant users or computers.
http://technet.microsoft.com/en-us/library/cc733022.aspx QUESTION 293Your network contains a single Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.The domain contains 400 desktop computers that run Windows 8 and 10 desktop computers that run Windows XP Service Pack 3 (SP3). All new desktop computers that are added to the domain run Windows 8.All of the desktop computers are located in an organizational unit (OU) named OU1.You create a Group Policy object (GPO) named GPO1. GPO1 contains startup script settings. You link GPO1 to OU1.You need to ensure that GPO1 is applied only to computers that run Windows XP SP3.What should you do? A. Create and link a WML filter to GPO1B. Run the Set-GPInheritance cmdlet and specify the -target parameter.C. Run the Set-GPLink cmdlet and specify the -target parameter.D. Modify the Security settings of OU1. Answer: AExplanation:WMI Filtering is used to get information of the system and apply the GPO on it with the condition is met. Security filtering: apply a GPO to a specific group (members of the group) QUESTION 294 Your network contains an Active Directory domain named contoso.com.Network Policy Server (NPS) is deployed to the domain. You plan to deploy Network Access Protection (NAP).You need to configure the requirements that are validated on the NPS client computers.What should you do? A. From the Network Policy Server console, configure a network policy.B. From the Network Policy Server console, configure a health policy.C. From the Network Policy Server console, configure a Windows Security Health Validator (WSHV) policy.D. From a Group Policy object (GPO), configure the NAP Client Configuration security setting. E. From a Group Policy object (GPO), configure the Network Access Protection Administrative Templates setting. Answer: C Explanation:The settings of the Windows Security Health verification. The client computer requirements are defined, of which a connection to your network is established Windows Security Health Checks can Windows be created 7 and Windows Vista for Windows XP or for Windows 8. Guidelines for Windows XP does not support testing of Antispywarefuntkionen. QUESTION 295 Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 is configured as a Network Policy Server (NPS) server and as a DHCP server.The network contains two subnets named Subnet1 and Subnet2. Server1 has a DHCP scope for each subnet.You need to ensure that noncompliant computers on Subnet1 receive different network policies than noncompliant computers on Subnet2.Which two settings should you configure? (Each correct answer presents part of the solution. Choose two.) A. The NAP-Capable Computers conditionsB. The NAS Port Type constraintsC. The Health Policies conditionsD. The MS-Service Class conditionsE. The Called Station ID constraints Answer: CDExplanation:The network contains two subnets named Subnet1 and Subnet2. Server1 has a DHCPscope for each subnet.The MS-Service Class conditions can be used to identify DHCP scope, i.e subnet,The MS-Service Class = DHCP > Network access protection tab > Use custom profile > Profile NameYou need to create health policy :Noncompliant health policy for NonCompliant computers.At first, you need to create health policy for noncompliant computers :Right-click Health Policies, and then click New.On the Create New Health Policy dialog box, under Policy Name, type Noncompliant.Under Client SHV checks, select Client fails one or more SHV checks.Under SHVs used in this health policy, select the Windows Security Health Validator check box, and then click OK.More info : https://technet.microsoft.com/en-us/library/dd441008.aspxThan you can create two network policies based on those two health policies and MS-Service Class conditionsNetwork policy 1 = MS-Service Class (Profile name) for subnet1 + Health policy for NonCompliant computers.Network policy 2 = MS-Service Class (Profile name) for subnet2 + Health policy for NonCompliant computers.Network policy :Network policy > Conditions tab > Health policy condition + MS-service class condition.In the NPS management console, in the tree, right-click Network Policies, and then click New.In the

Specify Network Policy Name and Connection Type window, in the Policy name box, type Noncompliant, and then click Next.In the Specify Conditions window, click Add.On the Select condition dialog box, double-click Health Polices.On the Health Policies dialog box, under Health policies, select Noncompliant, and then click OK.In the Specify Conditions window, under Conditions, verify that Health Policy is specified with a value of Noncompliant, and then click Next.If you want to configure the MS-Service Class condition, click MS-Service Class, and then click Add. In Specify the profile name that identifies your DHCP scope,type the name of an existing DHCP profile, and then click Add. QUESTION 296Your network contains an Active Directory domain named contoso.com. The functional level of the forest is Windows Server 2008 R2.Computer accounts for the marketing department are in an organizational unit (OU) named DepartmentsMarketingComputers. User accounts for the marketing department are in an OU named DepartmentsMarketingUsers.All of the marketing user accounts are members of a global security group named MarketingUsers. All of the marketing computer accounts are members of a global security group named MarketingComputers.In the domain, you have Group Policy objects (GPOs) as shown in the exhibit. (Click the Exhibit button.) You create two Password Settings objects named PSO1 and PSO2. PSO1 is applied to MarketingUsers. PSO2 is applied to MarketingComputers.The minimum password length is defined for each policy as shown in the following table. You need to identify the minimum password length required for each marketing user.What should you identify? A. 5B. 6C. 7D. 10E. 12 Answer: D QUESTION 297 Your network contains an Active Directory domain named adatum.com.You need to audit changes to the files in the SYSVOL shares on all of the domain controllers. The solution must minimize the amount of SYSVOL replication traffic caused by the audit. Which two settings should you configure? (Each correct answer presents part of the solution. Choose two.) A. Audit PolicyAudit system eventsB. Advanced Audit Policy ConfigurationDS AccessC. Advanced Audit Policy ConfigurationGlobal Object Access Auditing D. Audit PolicyAudit object accessE. Audit PolicyAudit directory service accessF. Advanced Audit Policy ConfigurationObject Access Answer: DFExplanation:Here object access must be monitored on the share \contoso.local ysvol. This is possible on general audit policy and the Advanced Audit Policy Configuration. The nine basic audit policies under Computer Configuration Policies Windows Settings Security Settings Local Policies Audit Policy allow you to configure security monitoring policy settings for various behavior of which generate some much more audit events than others. An administrator must review all generated events, regardless of whether they are of interest or not. Starting with Windows Server 2008 R2 and Windows 7 can monitor the client behavior on the computer or on the network targeted administrators, so that it is easier for them to abnormalities faster identify. For example, there are under Computer Configuration Policies Windows Settings Security Settings Local Policies Audit Policy only one policy setting for logon events: Audit logon events. Under Computer Configuration Policies Windows Settings Security Settings Advanced Audit Policy Configuration System Audit Policies, you can instead select the category logon / logoff eight different policy settings. In this way you can control the aspects of logon and logoff you can track precisely. QUESTION 298Your network contains multiple Active Directory sites.You have a Distributed File System (DFS) namespace that has a folder target in each site.You discover that some client computers connect to DFS targets in other sites.You need to ensure that the client computers only connect to a DFS target in their respective site.What should you modify? A. The properties of the Active Directory sitesB. The properties of the Active Directory site linksC. The delegation settings of the namespaceD. The referral settings of the namespace Answer: DExplanation:When a user accesses a namespace root or DFS folder with targets, the client computer receives an ordered list of servers or locations. This list is called a reference. Upon receipt of the reference to the computer attempts to access the first server in the list. If the server is not available, an attempt is made by the client computer to access the next server. If a server is unavailable, you can configure clients to fail back to the preferred server is running, as soon as it is available again. By default, targets are set within the client's site on the first digits of the sorted list.Then, the following entries for servers in other locations, which can be arranged by different sorting methods If only the folder targets are approved within the client site, the sorting method can exclude targets outside of the client site to be selected. The figure illustrates the configuration options: http://www.windowsnetworking.com/articles_tutorials/Configuring-DFS-Namespaces.html QUESTION 299Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012.You have a Group Policy object (GPO) named GPO1 that contains several custom Administrative templates.You need to filter the GPO to display only settings that will be removed from the registry when the GPO falls out of scope. The solution must only display settings that are either enabled or disabled and that have a comment.How should you configure the filter? To answer, select the appropriate options below. Select three. A. Set Managed to: YesB. Set Managed to: NoC. Set Managed to: AnyD. Set Configured to: YesE. Set Configured to: NoF. Set Configured to: AnyG. Set Commented to: YesH. Set Commented to: NoI. Set Commented to: Any Answer: ADGExplanation:"I change the Set Configured to: any to yes"(Only configured have the choice enabled or disabled) QUESTION 300Your network contains an Active Directory domain named adatum.com. The domain contains five servers. The servers are configured as shown in the following table. All desktop

computers in adatum.com run Windows 8 and are configured to use BitLocker Drive Encryption (BitLocker) on all local disk drives. You need to deploy the Network Unlock feature. The solution must minimize the number of features and server roles installed on the network.To which server should you deploy the feature? A. Server3B. Server1C. DC2D. Server2E. DC1 Answer: B Explanation:The BitLocker-NetworkUnlock feature must be installed on a Windows Deployment Server (which does not have to be configured--the WDSServer service just needs to be running). More free Lead2pass **70-411** exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDSmRhaVRWcW5Cc1k We give you the proper and complete training with free 70-411 Lead2pass updates. Our braindumps will defiantly make you perfect to that level you can easily pass the exam in first attempt. 2017 Microsoft 70-411 (All 449 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/70-411.html [100% Exam Pass Guaranteed]