[May-2018-New70-744 Dumps VCE(Full Version)160Q Download in Braindump2go[122-132

2018 May New Microsoft 70-743 Exam Dumps with PDF and VCE Just Updated Today! Following are some new 70-743 Real Exam Questions:1.|2018 Latest 70-743 Exam Dumps (PDF & VCE) 160Q Download: **https://www.braindump2go.com/70-744.html**2.|2018 Latest 70-743 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNMDN6VjRLbFVKaWM?usp=sharingQUESTION 122Your network contains an Active Directory forest named corp.contoso.com.You are implementing Privileged Access Management (PAM) by using a bastion forest namedpriv.contoso.com.You need to create shadow groups in priv.contoso.com.Which cmdlet should you use?A. New-RoleGroupB. New-ADGroupC. New-PamRoleD. New-PamGroupAnswer: DExplanation: **https://social.technet.microsoft.com/wiki/contents/articles/33363.mim-2016-privileged-access-managementpam-faq.aspx** **https://docs.microsoft.com/en- us/powershell/identitymanager/mimpam/vlatest/new-pamgroup**QUESTION 123Your network contains an Active Directory domain named contoso.com.The domain contains two servers named Server1 and Server2 that run Windows Server 2016.The Microsoft Advanced Threat Analytics (ATA) Center service is installed on Server1.The domain contains the users shown in the following table. You are installing ATA Gateway on Server2.You need to specify a Gateway Registration account.Which account should you use?A. User1B. User2C. User3D. User4E. User5F. User6G. User7H. User8Answer: FExplanation:**https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-role-groups** The user who installed ATA will be able to access the management portal (ATA Center) as members of the"Microsoft Advanced Threat Analytics Administrators"local group on the ATA Center server.QUESTION 124Your network contains an Active Directory domain named contoso.com.The domain contains a server named Server1 that runs Windows Server 2016.A user named User1 is a member of the local Administrators group.Server1 has the AppLocker rules configured as shown in follow: Rule1 and Rule2 are configured as shown in the following table: You verify that User1 is unable to run App2.exe on Server1.Which changes will allow User1 to run D:\Folder1\Program.exe andD:\Folder2\App2.exe? Choose Two.A. User1 can run D:\Folder1\Program.exe if Program.exe is moved to another folderB. User1 can run D:\Folder1\Program.exe if Program.exe is renamedC. User1 can run D:\Folder1\Program.exe if Program.exe is updatedD. User1 can run D:\Folder2\App2.exe if App2.exe is moved to another folderE. User1 can run D:\Folder2\App2.exe if App2.exe is renamedF. User1 can run D:\Folder2\App2.exe if App2.exe is upgradedAnswer: AFExplanation:**https://technet.microsoft.com/en-us/library/ee449492(v=ws.11).aspx** For "D:\Folder1\Program.exe", it is originally explicitly denied due to Rule1, when moving the "Program,exe" outof "D:\Folder1\", it does not match Rule1.Assume that "Program.exe" is moved to "D:\Folder2", it matches an Explicit Allow rule for group "BUILTIN\Administrators" which User1 is a member of, therefore Ais correct.For "App2",exe, it matches a Explicit Deny rule using its File Hash (created File content), no matter where youmove it to, or how you rename it, it would still matchRule2.Only changing the file content of App2.exe would let it no longer match the explicit deny hash-based rule"Rule2".By upgrading its version and content, it will generate a new hash. so F is correct.QUESTION 125Your network contains an Active Directory domain named contoso.com.You are deploying Microsoft Advanced Threat Analytics (ATA) to the domain.You install the ATA Gateway on a server named Server1.To assist in detecting Pass-the-Hash attacks, you plan to configure ATA Gateway to collect events.You need to configure the query filter for event subscriptions on Server1.How should you configure the query filter? Choose twoA. Event log to configure: ApplicationB. Event log to configure: Directory ServicesC. Event log to configure: SecurityD. Event log to configure: SystemE. Event ID to include: 1000F. Event ID to include: 1009G. Event ID to include: 1025H. Event ID to include: 4776I. Event ID to include: 4997Answer: CHExplanation: **https://docs.microsoft.com/en-us/advanced-threat-analytics/configure-event-collection**To enhance detection capabilities, ATA needs the following Windows events: 4776, 4732, 4733, 4728, 4729,4756, 4757.These can either be read automatically by the ATA Lightweight Gateway or in case the ATA LightweightGateway is not deployed,it can be forwarded to the ATA Gateway in one of two ways, by configuring the ATA Gateway to listen for SIEMevents or by configuring Windows Event Forwarding. Event ID: 4776 NTLM authentication is being used against domain controllerEvent ID: 4732 A User is Added to Security-Enabled DOMAIN LOCAL Group,Event ID: 4733 A User is removed from Security-Enabled DOMAIN LOCAL GroupEvent ID: 4728 A User is Added or Removed from Security-Enabled Global GroupEvent ID: 4729 A User is Removed from Security-Enabled GLOBAL GroupEvent ID: 4756 A User is Added or Removed From Security-Enabled Universal GroupEvent ID: 4757 A User is Removed From Security- Enabled Universal GroupQUESTION 126Your network contains an Active Directory domain named contoso.com. The domain contains 10 computers that are in an organizational unit (OU) named OU1.You deploy the Local Administrator Password Solution (LAPS) client to the computers.You link a Group Policy object (GPO) named GPO1 to OU1, and you configure

the LAPS password policy settings in GPO1.You need to ensure that the administrator passwords on the computers in OU1 are managed by using LAPS.Which two actions should you perform? Each correct answer presents part of the solution.A. Restart the domain controller that hosts the PDC emulator role.B. Update the Active Directory Schema.C. Enable LDAP encryption on the domain controllers.D. Restart the computers.E. Modify the permissions on OU1.**Answer: BE**QUESTION 127Your network contains an Active Directory domain named contoso.com.You plan to deploy an application named App1.exe.You need to verify whether Control Flow Guard is enabled for App1.exe.Which command should you run?A. Dumpbin.exe /dependents /locadconfig App1.exeB. Dumpbin.exe /headers /locadconfig App1.exeC. Dumpbin.exe /relocations /locadconfig App1.exeD. Dumpbin.exe /symbols /locadconfig App1.exeE. Sfc.exe /dependents /locadconfig App1.exeF. Sfc.exe /headers /locadconfig App1.exeG. Sfc.exe /relocations /locadconfig App1.exeH. Sfc.exe /symbols /locadconfig App1.exeI. Sigverif.exe /dependents /locadconfig App1.exeJ. Sigverif.exe /headers /locadconfig App1.exeK. Sigverif.exe /relocations /locadconfig App1.exeL. Sigverif.exe /symbols /locadconfig App1.exeM. Verifier.exe /dependents /locadconfig App1.exeN. Verifier.exe /headers /locadconfig App1.exeO. Verifier.exe /relocations /locadconfig App1.exeP. Verifier.exe /symbols /locadconfig App1.exeAnswer: B Explanation:ttps://msdn.microsoft.com/en-us/library/windows/desktop/mt637065(v=vs.85).aspxControl Flow Guard (CFG) is a highly-optimized platform security feature that was created to combat memorycorruption vulnerabilities.By placing tight restrictions on where an application can execute code from, it makes it much harder for exploitsto execute arbitrary code through vulnerabilitiessuch as buffer overflows.To verify if Control Flow Guard is enable for a certain application executable:-Run the dumpbin.exe tool (included in the Visual Studio 2015 installation) from the Visual Studio commandprompt with the /headers and /loadconfig options:dumpbin.exe /headers /loadconfig test.exe.The output for a binary under CFG should show that the header values include "Guard", and that the loadconfig values include "CF Instrumented" and "FID tablepresent".1 QUESTION 128Your network contains an Active Directory domain named contoso.com.The domain contains 10 servers that run Windows Server 2016 and 800 client computers that run Windows 10.You need to configure the domain to meet the following requirements:- Users must be locked out from their computer if they enter an incorrect password twice.- Users must only be able to unlock a locked account by using a one-time password that is sent to their mobile phone.You deploy all the components of Microsoft Identity Manager (MIM) 2016.Which three actions should you perform before you deploy the MIM add-ins and extensions? Each correct answer presents part of the solution.A. From a Group Policy object (GPO), configure Public Key PoliciesB. Deploy a Multi-Factor Authentication provider and copy the required certificates to the MIM server.C. From the MIM Portal, configure the Password Reset AuthN Workflow.D. Deploy a Multi-Factor Authentication provider and copy the required certificates to the client computers.E. From a Group Policy object (GPO), configure Security Settings.Answer: BCEExplanation:-Users must be locked out from their computer if they enter an incorrect password twice. (E)-Users must only be able to unlock a locked account by using a one-time password that is sent to their mobilephone. (B and C), detailed configuration process inthe following web page.
https://docs.microsoft.com/en-us/microsoft-identity-manager/working-with-self-service-passwordreset#prepare-mim-to-work-with-multi-factor-authenticationQUESTION 129The network contains an Active Directory domain named contoso.com.The domain contains the servers configured as shown in the following table. All servers run Windows Server 2016.All client computers run Windows 10 and are domain members.All laptops are protected by using BitLocker Drive Encryption (BitLocker).You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.An OU named OU2 contains the computer accounts of the computers in the marketing department.A Group Policy object (GPO) named GP1 is linked to OU1.A GPO named GP2 is linked to OU2.All computers receive updates from Server1.You create an update rule named Update1.You need to ensure that you can encrypt the operating system drive of VM1 by using BitLocker.Which Group Policy should you configure?A. Configure use of hardware-based encryption for operating system drivesB. Configure TPM platform validation profile for native UEFI firmware configurationsC. Require additional authentication at startupD. Configure TPM platform validation profile for BIOS-based firmware configurationsAnswer: CExplanation:As there is not a choice "Enabling Virtual TPM for the virtual machine VM1", then we have to use a fall-backmethod for enabling BitLocker in VM1.
https://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/ QUESTION 130The Job Title attribute for a domain user named User1 has a value of Sales Manager.User1 runs whoami /claims and receives the following output: Kerberos support for Dynamic Access Control on this device has been disabled.You need to ensure that the security token of User1 has a claim for Job Title.What should you do?A. From Windows PowerShell, run the New-ADClaimTransformPolicy cmdlet and specify the -NameparameterB. From Active Directory Users and Computers, modify the properties of the User1 account.C. From Active Directory Administrative Center, add a claim type.D. From a Group Policy object (GPO), configure KDC support for claims, compound authentication, and Kerberos armoring.Answer: CExplanation:From the output, obviously, a claim type is missing (or disabled) so that the domain controller is not issuingtickets with the "Job Title" claim type.QUESTION 131Your network

contains an Active Directory domain named contoso.com.You deploy a server named Server1 that runs Windows Server 2016. Server1 is in a workgroup.You need to collect the logs from Server1 by using Log Analytics in Microsoft Operations Management Suite (OMS).What should you do first?A. Join Server1 to the domain.B. Create a Data Collector Set.C. Install Microsoft Monitoring Agent on Server1.D. Create an event subscription.Answer: CExplanation:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents You need to install and connect Microsoft Monitoring Agent for all of the computers that you You can install the OMS MMA on stand-alone computers, servers, and virtual machines.QUESTION 132Your network contains an Active Directory domain named contoso.com.The domain contains two DNS servers that run Windows Server 2016.The servers host two zones named contoso.com and admin.contoso.com.You sign both zones. You need to ensure that all client computers in the domain validate the zone records when they query the zone.What should you deploy?A. a Microsoft Security Compliance Manager (SCM) policyB. a zone transfer policyC. a Name Resolution Policy Table (NRPT)D. a connection security ruleAnswer: CExplanation:You should use Group Policy NRPT to for a DNS Client to perform DNSSEC validation of DNS zone records. !!!RECOMMEND!!!1.|2018 Latest 70-743 Exam Dumps (PDF & VCE) 160Q Download:**https://www.braindump2go.com/70-744.html**2.|2018 Latest 70-743 Study Guide Video: YouTube Video: YouTube.com/watch?v=vJ7mP1-I7so