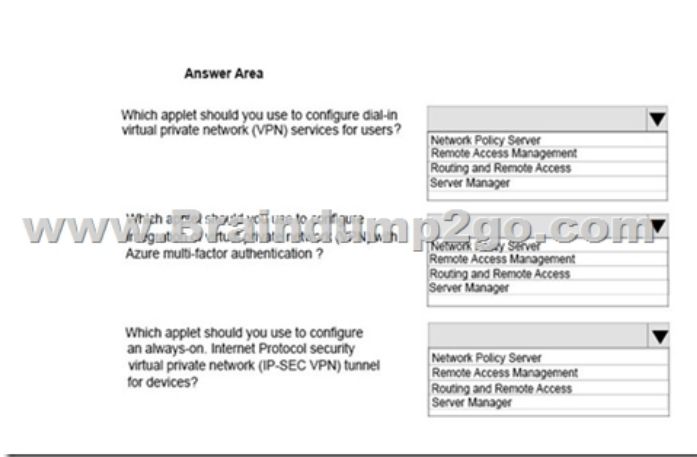
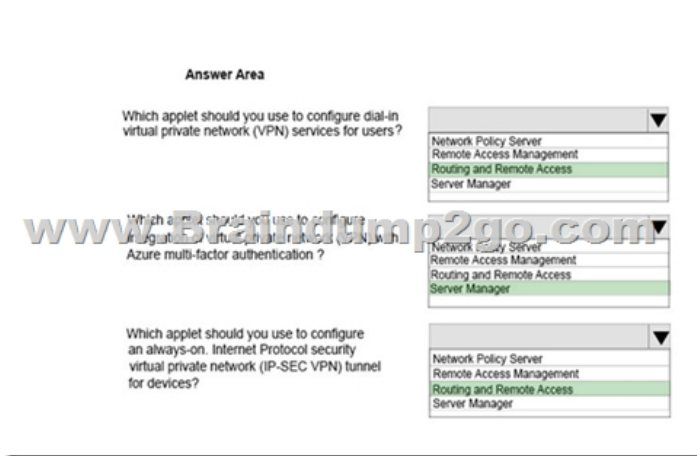


[New 70-398 DumpsFree Microsoft 79Q 70-398 Dumps PDF Braindump2go Offer[53-63

2018/August Braindump2go New Microsoft 70-398 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 70-398 Real Exam Questions: 1.|2018 Latest 70-398 Exam Dumps (PDF & VCE) 79Q&As
Download:<https://www.braindump2go.com/70-398.html>2.|2018 Latest 70-398 Exam Questions & Answers
Download:<https://drive.google.com/drive/folders/0B75b5xYLjSSNSzdxYTQ2Z1FmRU0?usp=sharing>**QUESTION 53**Overview
BackgroundFabrikam, Inc. is a large health services provider that serves the greater Chicago area. The company has three major hospital campus locations and over 30 individual care clinics. Fabrikam has 4,000 employees. Doctors and nurses work in various locations and use shared kiosk workstations. Approximately, 1,000 employees are Information workers that use desktop or laptop computers. All users have their own Active Directory user accounts and Exchange mailboxes. Fabrikam has developed a software-as-a-service application Support app. Support technicians will use the app to resolve issues with medical equipment more quickly.User log in to a Remote Desktop farm that is a member of the global fabrikam.com Active Directory Domain Services (AD DS) domain. All servers in the farm run Windows 2008 R2. Users access a set of line of business apps. They also access personal and departmental files that are located on network file shares by using Microsoft Office 2010 Standard.Users at larger clinics work from company-owned devices that are connected to the global.fabrikam.com AD DS domain over private Wide Area Network links. At smaller clinics, users must connect to the Fabrikam network by using a shared internet connection from either their laptop or a shared workstation.When users travel to smaller clinics or access the Fabrikam network remotely, they must use a Windows virtual private network (VPN) connection. Connections are made to a Windows 2008 R2 Server named RAS01, which hosts the Routing & Remote Access and Network Policy Services roles. These users are members of the Remote Users group, and must carry a two-factor token device and enter a six digit rotating pin when they connect. When they are not connected to the VPN and wish to use existing services, such as Microsoft Outlook on the Web, you must implement additional pre-authentication through Microsoft Threat Management Gateway.All Internet traffic for user and server traffic runs through an access management system. Outbound traffic from the network to the internet must be explicitly granted access. Fabrikam uses System Center Configuration Manager (SCCM) on HTTPS mode to manage computers. All computers have a certificate from the Windows Private Key Infrastructure. Mobile devicesFabrikam has purchased 500 Apple ios devices. The company plans to issue these devices to doctors and nurses so that they can access apps and files from both inside and outside of the network. The company plans to deploy Microsoft Intune to manage laptop computers and mobile devices.Business RequirementsLeadership needsCompany executives have identified the following requirements:- You must minimize the workload for Information Technology teams and reduce operating costs.- Target migration of applications towards a Software as a Service model.- Empower users to work more efficiently no matter what location they are working from.- Allow users to use modern devices.- Secure mobile devices and operating environments.- All communications must remain secure.Information technologyYou must implement features from both Microsoft Office 365 and Enterprise Mobility + Security to improve user productivity and reduce staff workloads.Employees must use existing Active Directory credentials across on-premises and cloud solutions.You must replace the line of business applications with cloud-based applications Reduce infrastructure costs by eliminating as many on-premises physical/virtual services as possible.Secure data moving in and out of the organization.Implement modern remote connectivity methods.Technical requirementsIdentityYou must enforce the following identity requirements:- Deploy federated identity by using Microsoft Azure Active Directory Connect.- Configure Federation Services to support workplace join.- Monitor Federation Services health and report critical alerts to specific users.- Ensure that any reverse proxy solution is capable of providing pre-authentication and two-factor authentication.- You must populate the Azure App Panel with as many cloud-ready applications as possible.- You must implement Azure Active Directory Premium as the preferred self-service password reset solution.- You must use Azure Multi-Factor authentication as the preferred two-factor authentication solution.SecurityYou have the following security requirements:- Implement self-service password management.- Use a minimum of three authentication methods for self-service password reset.- Use AD DS security groups to control access to cloud-based applications.- Integrate Azure Multi-Factor Authentication with existing platforms that support two-factor authentication.- Use Azure Rights Management to secure company files and email that are transmitted outside of the network.OtherYou identify the following additional technical requirements:- All users that operate in shared work spaces must use Windows to Go with BitLocker.- Windows to Go devices must automatically connect to the network by using DirectAccess.- Remote connections to the network must use two-factor authentication.- All laptop computers must be able to act as a mobile hotspot.Hotspot QuestionYou need to configure networking for Fabrikam.In Control Panel, which Administrative Tools applets should you use? To answer, select the appropriate applet from the options in each list.NOTE: Each selection is worth one point.



Answer:



http://examgod.com/bdimages/New-70-398-Dumps53-63_95D5/image_thumb20_thumb.pngExplanation:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-vpn>QUESTION 54A company deploys Enterprise Mobility + Security. The company plans to use Azure Active Directory (AD) Premium to join all new Windows 10 devices.Users must not be allowed to change the PowerSleep option.You need to automatically apply custom power policies to all Windows 10 Azure AD joined devices.What should you do?A. From the Azure AD Premium Configuration page, enable automatic device enrollment.B. Create a custom Poweroption Group Policy in Active Directory Domain Services (AD DS). Set the value of the PowerSleep option to False.C. Configure automatic enrollment into Microsoft Intune. Create and deploy a custom Compliance policy to all Windows 10 devices.D. Configure automatic enrollment into Microsoft Intune for all Azure AD Premium joined devices. Apply a custom set of Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure custom power settings.
Answer: BQUESTION 55Your company runs Windows 10 Enterprise on all devices. You hire a new employee and provide a device for the employee.All drives must be encrypted.You need to determine whether volume C in the device is encrypted. At an elevated command prompt, which command should you run?A. manage-bde -setidentifier C:B. manage-bde -on C:C. manage-bde -unlock C:D. manage-bde -status C:Answer: DExplanation:

[https://technet.microsoft.com/en-us/library/jj647767\(v=ws.11\).aspx#BKMK_managebde](https://technet.microsoft.com/en-us/library/jj647767(v=ws.11).aspx#BKMK_managebde)QUESTION 56A company plans to use Microsoft Azure to manage directory users. In Azure, you create a virtual network and a DNS record.You need to set up the connection between the virtual network and your on-premises network.Which two actions will achieve the goal? Each correct answer presents a complete solution. (Choose two.)NOTE: Each correct selection is worth one point.A. Configure the on-premises routing infrastructure to forward traffic destined for the address space of the Azure Virtual Network to the on-premises virtual private network device.B. Configure the private IP address space of the Azure Virtual Network.C. Manually create DNS records to point to the Azure virtual machines.D. Extract the server license certificate key from the configuration data, and transfer the key to an on- premises hardware security module.
Answer: ABExplanation:

<https://docs.microsoft.com/en-us/office365/enterprise/connect-an-on-premises-network-to-a-microsoft-azure-virtual-network>

QUESTION 57A company plans to deploy 100 new Windows 10 devices. Then pilot users are currently testing Windows 10 is not

corporate network. The pilot users report that the Hibernate option is not available. You need to enable hibernation on the Windows 10 devices. Which command should you run? A. Powercfg -energy B. Powercfg -h off C. Powercfg -h on D. Powercfg -devisenablewake E. Powercfg -setactive Answer: C Explanation:

<https://www.cnet.com/how-to/how-to-enable-or-disable-hibernate-in-windows-10/> QUESTION 58 A company plans to actively manage mobile devices. You need to create a list of all jailbroken devices after they are enrolled. What should you use? A. Azure Active Directory B. System Center 2012 R2 Configuration Manager SP1 C. Intune D. Azure Active Directory Domain Services E. Azure Active Directory Device Registration Service Answer: B QUESTION 59 A company deploys Outlook to all users that have iOS and Android devices. The company uses Microsoft Intune to manage mobile devices. You enforce a conditional access policy that requires users to enroll devices in Intune before they can access Exchange ActiveSync data. Some Android and iOS users access Exchange ActiveSync data by using unmanaged email applications. You need to ensure that users Exchange ActiveSync data only from Outlook. What should you do? A. Create an Exchange access rule. Select Outlook family and Outlook for Android and iOS as the model. B. In Intune, create a new compliance policy that forces email accounts to be managed by Intune. C. Create a security group for all users that are not using Outlook as the email applications. Configure Exchange Online conditional access policy to exempt members of the group. D. Configure a custom Open Mobile Alliance Uniform Resource Identifier setting and deploy the setting to all users. Answer: A QUESTION 60 A company plans to deploy Microsoft Office to mobile device users. You purchase Enterprise Mobility + Security licenses and deploy Microsoft Intune. Company data must only be shared between applications approved by the company and Microsoft Office applications. You need to ensure that users cannot share data with other applications. What should you do? A. Configure a managed application policy that requires a PIN code to access the application on the device. B. Configure a conditional access policy that enforces application encryption on all devices. C. Deploy and configure Azure Rights Management Services. D. Configure a configuration policy that will enable a PIN code and deploy the policy to all Office users. E. Configure a managed application policy that will restrict cut, copy, and paste with other non-managed applications. Answer: E QUESTION 61 Adatum Corporation plans to implement Mobile Device Management (MDM). The company uses the domain name Adatum.com. The company plans to integrate Microsoft Intune with System Center 2012 R2 Configuration Manager. Configuration Manager uses the public IP address 102.157.31.12. Domain Name System (DNS) is not configured to support MDM. You need to create a DNS record for automatically enrolling the device. Which DNS record type should you create? A. a CNAME record named EnterpriseEnrollment.adatum.com that points to manage.microsoft.com. B. a CNAME record named MDMDenrollment.adatum.com that points to manage.microsoft.com. C. a PTR record named 102.157.31.12 that points to EnterpriseEnrollment.Adatum.com. D. an A resource record named autoenroll.adatum.com that points to 102.157.31.12 Answer: A Explanation: <https://docs.microsoft.com/en-us/intune/windows-enroll> QUESTION 62 A company plans to deploy Outlook as a managed app to all users. You deploy Microsoft Intune. You must deploy an internally developed iOS line of business (LOB) app to all users in the sales department. These users must only be able to share data between Outlook and the internally developed LOB app. You need to configure the environment for sales department users. What should you do? A. Configure a security policy that forces encryption. B. Use the Intune App Wrapping Tool to repackage the internally developed LOB application. C. Upload the internally developed LOB app to the Apple App Store. Deploy the app to all users in the sales department. D. Use the Intune App Wrapping Tool to repackage the Outlook application. Set the value for the App ID to match to Application ID of the internally developed LOB application. Answer: B Explanation: <https://docs.microsoft.com/en-us/intune/app-wrapper-prepare-ios> QUESTION 63 A company has an Office 365 E3 subscription. You deploy Enterprise Mobility + Security, Active Directory Federation Services (AD FS), and Microsoft Identity Manager. You need to implement additional security when users remotely connect to corporate resources. What should you implement? A. System Center Configuration Manager B. Microsoft Intune C. Azure Rights Management Service D. Azure Multi-Factor Authentication Answer: B Explanation: <https://docs.microsoft.com/en-us/intune/common-scenarios> !!!RECOMMEND!!! 1. [2018 Latest 70-398 Exam Dumps (PDF & VCE) 79Q&As Download: <https://www.braindump2go.com/70-398.html> 2. [2018 Latest 70-398 Study Guide Video: YouTube Video: [YouTube.com/watch?v=MHSTS37Jabs](https://www.youtube.com/watch?v=MHSTS37Jabs)