[New Exams!Braindump2go AZ-500 Exam Dumps for Free[Q6-Q11

July/2019 Braindump2go AZ-500 Exam Dumps with PDF and VCE New Updated Today! Following are some new AZ-500 Exam Questions:1.|2019 Latest Braindump2go AZ-500 Exam Dumps (PDF & VCE) Instant Download: **https://www.braindump2go.com/az-500.html**2.|2019 Latest Braindump2go AZ-500Exam Questions & Answers Instant Download:https://drive.google.com/drive/folders/1sQAsVdJ79oBKFiswxjUzGT6Gt6a6PYWl?usp=sharingQUESTION 6Case Study 1 - Litware, IncOverviewLitware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.Existing EnvironmentLitware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.The tenant contains the groups shown in the following table. The Azure subscription contains the objects shown in the following table. Azure Security Center is set to the Free tier.Planned changesLitware plans to deploy the Azure resources shown in the following table. Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1. The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment. Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.Platform Protection RequirementsLitware identifies the following platform protection requirements: Microsoft Antimalware must be installed on the virtual machines in Resource Group1. The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role. Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials. Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access. A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.Security Operations RequirementsLitware must be able to customize the operating system security configurations in Azure Security Center.Drag and Drop QuestionYou need to configure SQLDB1 to meet the data and application requirements.Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. Answer: Explanation:Step 1: Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS)Step 2: In SQLDB1, create contained database users.Create a contained user in the database that represents the VM's system-assigned identity.Step 3: In Azure AD,create a system-assigned managed identity.A system-assigned identity for a Windows virtual machine (VM) can be used to access an Azure SQL server. Managed Service Identities are automatically managed by Azure and enable you to authenticate to services that support Azure AD authentication, without needing to insert credentials into your code.References: **https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql** QUESTION 7Case Study 2 - Contoso, LtdOverviewContoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.The company hosts its entire server infrastructure in Azure.Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.Technical requirementsContoso identifies the following technical requirements: Deploy Azure Firewall to VNetWork1 in Sub2. Register an application named App2 in contoso.com. Whenever possible, use the principle of least privilege. Enable Azure AD Privileged Identity Management (PIM) for contoso.comExisting EnvironmentAzure ADContoso.com contains the users shown in the following table. Contoso.com contains the security groups shown in the following table. Sub1Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.User2 creates the virtual networks shown in the following table. Sub1 contains the locks shown in the following table. Sub1 contains the Azure policies shown in the following table. Sub2 Sub2 contains the virtual machines shown in the following table. All virtual machines have the public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.Sub2 contains the network security groups (NSGs) shown in the following table. NSG1 has the inbound security rules shown in the following table. NSG2 has the inbound security rules shown in the following table. NSG3 has the inbound security rules shown in the following table. NSG4 has the inbound security rules shown in the following table. NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table. Contoso identifies the following technical requirements: Deploy Azure Firewall to VNetwork1 in Sub2. Register an application named App2 in contoso.com. Whenever possible, use the principle of least privilege. Enable Azure AD Privileged Identity Management (PIM) for contoso.com.You need to ensure that User2 can implement PIM.What should you do first?A. Assign User2 the Global administrator role.B. Configure authentication methods for contoso.com.C. Configure the identity secure score for contoso.com.D. Enable multi-factor authentication (MFA) for User2.Answer: AExplanation:To start using PIM in

your directory, you must first enable PIM.1. Sign in to the Azure portal as a Global Administrator of your directory.You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-startedQUESTION 8Case Study 2 - Contoso, LtdOverviewContoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.The company hosts its entire server infrastructure in Azure.Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com. Technical requirementsContoso identifies the following technical requirements: Deploy Azure Firewall to VNetWork1 in Sub2. Register an application named App2 in contoso.com. Whenever possible, use the principle of least privilege. Enable Azure AD Privileged Identity Management (PIM) for contoso.comExisting EnvironmentAzure ADContoso.com contains the users shown in the following table. Contoso.com contains the security groups shown in the following table. Sub1Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.User2 creates the virtual networks shown in the following table. Sub1 contains the locks shown in the following table. Sub1 contains the Azure policies shown in the following table. Sub2 Sub2 contains the virtual machines shown in the following table. All virtual machines have the public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.Sub2 contains the network security groups (NSGs) shown in the following table. NSG1 has the inbound security rules shown in the following table. NSG2 has the inbound security rules shown in the following table. NSG3 has the inbound security rules shown in the following table. NSG4 has the inbound security rules shown in the following table. NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table. Contoso identifies the following technical requirements: Deploy Azure Firewall to VNetwork1 in Sub2. Register an application named App2 in contoso.com. Whenever possible, use the principle of least privilege. Enable Azure AD Privileged Identity Management (PIM) for contoso.com.Hotspot QuestionWhat is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: User1, User2, User3, User4Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.Box 2: Only User3Match "*on" is only true for London (User3).Scenario: Contoso.com contains the users shown in the following table. Contoso.com contains the security groups shown in the following table. References:**https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership**
QUESTION 9Case Study 2 - Contoso, LtdOverviewContoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.The company hosts its entire server infrastructure in Azure.Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.Technical requirementsContoso identifies the following technical requirements: Deploy Azure Firewall to VNetWork1 in Sub2. Register an application named App2 in contoso.com. Whenever possible, use the principle of least privilege. Enable Azure AD Privileged Identity Management (PIM) for contoso.comExisting EnvironmentAzure ADContoso.com contains the users shown in the following table. Contoso.com contains the security groups shown in the following table. Sub1Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.User2 creates the virtual networks shown in the following table. Sub1 contains the locks shown in the following table. Sub1 contains the Azure policies shown in the following table. Sub2 Sub2 contains the virtual machines shown in the following table. All virtual machines have the public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.Sub2 contains the network security groups (NSGs) shown in the following table. NSG1 has the inbound security rules shown in the following table. NSG2 has the inbound security rules shown in the following table. NSG3 has the inbound security rules shown in the following table. NSG4 has the inbound security rules shown in the following table. NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table. Contoso identifies the following technical requirements: Deploy Azure Firewall to VNetwork1 in Sub2. Register an application named App2 in contoso.com. Whenever possible, use the principle of least privilege. Enable Azure AD Privileged Identity Management (PIM) for contoso.com.Hotspot QuestionYou are evaluating the security of the network communication between the virtual machines in Sub2.For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: YesNSG1 has the inbound security rules shown in the following table. NSG2 has the inbound security rules shown in the following table. Box 2: YesBox 3: NoNote:Sub2 contains the virtual machines shown in the following table. Sub2 contains the network security groups (NSGs) shown in the following table.
QUESTION 10Case Study 2 - Contoso, LtdOverviewContoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.The company hosts its entire server infrastructure in Azure.Contoso has two Azure

subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.Technical requirementsContoso identifies the following technical requirements: Deploy Azure Firewall to VNetWork1 in Sub2. Register an application named App2 in contoso.com. Whenever possible, use the principle of least privilege. Enable Azure AD Privileged Identity Management (PIM) for contoso.comExisting EnvironmentAzure ADContoso.com contains the users shown in the following table. Contoso.com contains the security groups shown in the following table. Sub1Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.User2 creates the virtual networks shown in the following table. Sub1 contains the locks shown in the following table. Sub1 contains the Azure policies shown in the following table. Sub2 Sub2 contains the virtual machines shown in the following table. All virtual machines have the public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.Sub2 contains the network security groups (NSGs) shown in the following table. NSG1 has the inbound security rules shown in the following table. NSG2 has the inbound security rules shown in the following table. NSG3 has the inbound security rules shown in the following table. NSG4 has the inbound security rules shown in the following table. NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table. Contoso identifies the following technical requirements: Deploy Azure Firewall to VNetwork1 in Sub2. Register an application named App2 in contoso.com. Whenever possible, use the principle of least privilege. Enable Azure AD Privileged Identity Management (PIM) for contoso.com.Hotspot QuestionYou assign User8 the Owner role for RG4, RG5, and RG6.In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: RG4 onlyVirtual Networks are not allowed for Rg5 and Rg6. Box 2: Rg4,Rg5, and Rg6Scenario:Contoso has two Azure subscriptions named Sub1 and Sub2.Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.You assign User8 the Owner role for RG4, RG5, and RG6User8 city Sidney, Role:NoneNote: A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager).References:
https://docs.microsoft.com/en-us/azure/governance/policy/overviewQUESTION 11Case Study 2 - Contoso, LtdOverview Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.The company hosts its entire server infrastructure in Azure.Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.Technical requirementsContoso identifies the following technical requirements: Deploy Azure Firewall to VNetWork1 in Sub2. Register an application named App2 in contoso.com. Whenever possible, use the principle of least privilege. Enable Azure AD Privileged Identity Management (PIM) for contoso.comExisting EnvironmentAzure ADContoso.com contains the users shown in the following table. Contoso.com contains the security groups shown in the following table. Sub1Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.User2 creates the virtual networks shown in the following table. Sub1 contains the locks shown in the following table. Sub1 contains the Azure policies shown in the following table. Sub2 Sub2 contains the virtual machines shown in the following table. All virtual machines have the public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.Sub2 contains the network security groups (NSGs) shown in the following table. NSG1 has the inbound security rules shown in the following table. NSG2 has the inbound security rules shown in the following table. NSG3 has the inbound security rules shown in the following table. NSG4 has the inbound security rules shown in the following table. NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table. Contoso identifies the following technical requirements: Deploy Azure Firewall to VNetwork1 in Sub2. Register an application named App2 in contoso.com. Whenever possible, use the principle of least privilege. Enable Azure AD Privileged Identity Management (PIM) for contoso.com.Hotspot QuestionWhich virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: VNET4 and VNET1 only RG1 has only Delete lock, while there are no locks on RG4.RG2 and RG3 both have Read-only locks.Box 2: VNET4 onlyThere are no locks on RG4, while the other resource groups have either Delete or Read-only locks.Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively. CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.Scenario:User2 is a Security administrator.Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.User2 creates the virtual networks shown in the following table. Sub1 contains the locks shown in the following table. References:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources Question
!!!RECOMMEND!!!1.|2019 Latest Braindump2go AZ-500 Exam Dumps (PDF & VCE) Instant Download: **https://www.braindump2go.com/az-500.html**2.|2019 Latest Braindump2go AZ-500 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=-d1W44dDS2o