[New Exams!Full Version AZ-500 PDF and VCE 60Q for Free Download[Q1-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 1Case 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.You need to meet the identity and access requirements for Group1.What should you do?A.   Add a membership rule to Group1.B.   Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.C.   Modify the membership rule of Group1.D.   Change the membership type of Group1 to Assigned.Create two groups that have dynamic memberships. Add the new groups to Group1.Answer: BExplanation:Incorrect Answers:A, C: You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.D: For assigned group you can only add individual members.Scenario:Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.The tenant currently contain this group: References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal
QUESTION 2Case 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.You need to ensure that users can access VM0. The

solution must meet the platform protection requirements.What should you do?A. Move VM0 to Subnet1.B. On Firewall, configure a network traffic filtering rule.C. Assign RT1 to AzureFirewallSubnet.D. On Firewall, configure a DNAT rule.Answer: AExplanation:Azure Firewall has the following known issue:Conflict with Azure Security Center (ASC) Just-in-Time (JIT) feature.If a virtual machine is accessed using JIT, and is in a subnet with a user-defined route that points to Azure Firewall as a default gateway, ASC JIT doesn't work.This is a result of asymmetric routing ?a packet comes in via the virtual machine public IP (JIT opened the access), but the return path is via the firewall, which drops the packet because there is no established session on the firewall.Solution: To work around this issue, place the JIT virtual machines on a separate subnet that doesn't have a user-defined route to the firewall.Scenario: Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access. References:**https://docs.microsoft.com/en-us/azure/firewall/overview**QUESTION 3Case 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.You need to ensure that you can meet the security operations requirements.What should you do first?A. Turn on Auto Provisioning in Security Center.B. Integrate Security Center and Microsoft Cloud App Security.C. Upgrade the pricing tier of Security Center to Standard.D. Modify the Security Center workspace configuration.Answer: CExplanation:The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.Scenario: Security Operations RequirementsLitware must be able to customize the operating system security configurations in Azure Security Center.References:**https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing**QUESTION 4Case 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.You need to configure WebApp1 to meet the data and application requirements. Which two actions should you perform? Each correct answer presents part of the solution.NOTE: Each correct selection is worth one point.A. Upload a public certificate.B. Turn on the HTTPS Only protocol setting.C. Set the Minimum TLS Version protocol setting to 1.2.D. Change the pricing tier of the App Service plan.E. Turn on the Incoming client certificates protocol setting.Answer: ACExplanation:A: To configure Certificates for use in Azure Websites Applications you need to upload a public Certificate.C: Over time, multiple versions of TLS have been released to mitigate different vulnerabilities. TLS 1.2 is the most current version available for apps running on Azure App Service.Incorrect Answers:B: We need support the http url as well.Note: References:**https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth https://azure.microsoft.com/en-us/updates/app-service-and-functions-hosted-apps-can-now-update-tls-versions/**QUESTION 5 Case 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.Hotspot QuestionYou need to create Role1 to meet the platform protection requirements.How should you complete the role definition of Role1? To answer, select the appropriate options in the answer area.NOTE: Each correct selection is worth one point. Answer: Explanation:Scenario: 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.Azure RBAC template managed disks "Microsoft.Storage/"References: **https://blogs.msdn.microsoft.com/azureedu/2017/02/11/new-managed-disk-storage-option-for-your-azure-vms/** !!!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