[New Exams!Valid Exam AZ-500 Dumps Provided By Braindump2go for Free Instant Download[Q12-Q22

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 12Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.You have an Azure Subscription named Sub1.You have an Azure Storage account named Sa1 in a resource group named RG1.Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.You discover that unauthorized users accessed both the file service and the blob service.You need to revoke all access to Sa1.Solution: You generate new SASs.Does this meet the goal?A. YesB. NoAnswer: B Explanation:Instead you should create a new stored access policy.To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.References:**https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy** QUESTION 13Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.You have an Azure Subscription named Sub1.You have an Azure Storage account named Sa1 in a resource group named RG1.Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.You discover that unauthorized users accessed both the file service and the blob service.You need to revoke all access to Sa1.Solution: You create a new stored access policy.Does this meet the goal?A. YesB. NoAnswer: AExplanation:To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.References: **https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy**QUESTION 14Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.You have a hybrid configuration of Azure Active Directory (AzureAD).You have an Azure HDInsight cluster on a virtual network.You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.Solution: You deploy the On-premises data gateway to the on-premises network.Does this meet the goal?A. YesB. NoAnswer: BExplanation:Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:Create Azure Virtual Network.Create a custom DNS server in the Azure Virtual Network.Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.Configure forwarding between the custom DNS server and your on-premises DNS server.References: **https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network**QUESTION 15Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.You have a hybrid configuration of Azure Active Directory (AzureAD).You have an Azure HDInsight cluster on a virtual network.You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.You need to configure the environment to support the planned authentication.Solution: You create a site-to-site VPN between the virtual network and the on-premises network.Does this meet the goal?A. YesB. NoAnswer: AExplanation:You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:Create Azure Virtual Network.Create a custom DNS

server in the Azure Virtual Network.Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.Configure forwarding between the custom DNS server and your on-premises DNS server.References: **https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network**QUESTION 16Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.You need to recommend an integration solution that meets the following requirements:- Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant- Minimizes the number of servers required for the solution.Which authentication method should you include in the recommendation?A. federated identity with Active Directory Federation Services (AD FS)B. password hash synchronization with seamless single sign-on (SSO)C. pass-through authentication with seamless single sign-on (SSO)Answer: BExplanation: Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes.Incorrect Answers:A: A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.C: For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.Pass-through Authentication requires unconstrained network access to domain controllers. All network traffic is encrypted and limited to authentication requests. References:**https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta**QUESTION 17Your network contains an on-premises Active Directory domain named corp.contoso.com.You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.You sync all on-premises identities to Azure AD. You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.What should you use?A. Synchronization Rules EditorB. Web Service Configuration Tool C. the Azure AD Connect wizardD. Active Directory Users and ComputersAnswer: AExplanation:Use the Synchronization Rules Editor and write attribute-based filtering rule.References: **https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration**QUESTION 18 Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.You need to configure each subscription to have the same role assignments.What should you use?A. Azure Security CenterB. Azure BlueprintsC. Azure AD Privileged Identity Management (PIM)D. Azure PolicyAnswer: CExplanation:The Azure AD Privileged Identity Management (PIM) service also allows Privileged Role Administrators to make permanent admin role assignments.References: **https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user** QUESTION 19You have an Azure subscription.You create an Azure web app named Contoso1812 that uses an S1 App service plan. You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.You need to ensure that users can access Contoso1812 by using the **https://www.contoso.com** URL.Which two actions should you perform? Each correct answer presents part of the solution.NOTE: Each correct selection is worth one point.A. Turn on the system-assigned managed identity for Contoso1812.B. Add a hostname to Contoso1812.C. Scale out the App Service plan of Contoso1812.D. Add a deployment slot to Contoso1812.E. Scale up the App Service plan of Contoso1812.Answer: BEExplanation:B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN).To do this, you have to create three records:A root "A" record pointing to contoso.comA root "TXT" record for verificationA "CNAME" record for the www name that points to the A recordE: To map a custom DNS name to a web app, the web app's App Service plan must be a paid tier (Shared, Basic, Standard, Premium or Consumption for Azure Functions). IScale up the App Service plan: Select any of the non-free tiers (D1, B1, B2, B3, or any tier in the Production category).References:**https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain** QUESTION 20You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.You create a service endpoint for Subnet1.Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources

and Azure SQL databases by using the service endpoint.A. Create an application security group and a network security group (NSG).B. Edit the docker-compose.yml file.C. Install the container network interface (CNI) plug-in.Answer: CExplanation:The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform.The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods: References: **https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview**QUESTION 21You have Azure Resource Manager templates that you use to deploy Azure virtual machines.You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.What should you use?A. device compliance policies in Microsoft IntuneB. Azure Automation State ConfigurationC. application security groupsD. Azure AdvisorAnswer: B Explanation:You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.References:**https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started** QUESTION 22You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use the auto-generated service principal to authenticate to the Azure Container Registry.What should you create?A. an Azure Active Directory (Azure AD) groupB. an Azure Active Directory (Azure AD) role assignmentC. an Azure Active Directory (Azure AD) userD. a secret in Azure Key VaultAnswer: BExplanation:When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.References: **https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks**!!!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