[Sep-2019Real Exam Questions-Braindump2go AZ-301 Exam Dumps PDF 200Q Download(New Questions)

Sep/2019 Braindump2go AZ-301 Exam Dumps with PDF and VCE New Updated Today! Following are some new AZ-301 Exam Questions:1.|2019 Latest Braindump2go AZ-301 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/az-301.html2.|2019 Latest Braindump2go AZ-301 Exam Questions & Answers Instant Download:https://drive.google.com/drive/folders/1PXo2CdJp-RE3hybnjjGiHV7uk7r2geY-?usp=sharingNew QuestionsYou are designing an Azure solution.The network traffic for the solution must be securely distributed by providing the following features:- HTTPS protocol- Round robin routing- SSL offloadingYou need to recommend a load balancing option.What should you recommend?A. Azure Load BalancerB. Azure Traffic ManagerC. Azure Internal Load Balancer (ILB)D. Azure Application GatewayAnswer: DExplanation:If you are looking for Transport Layer Security (TLS) protocol termination ("SSL offload") or per-HTTP/HTTPS request, application-layer processing, review Application Gateway.Application Gateway is a layer 7 load balancer, which means it works only with web traffic (HTTP, HTTPS, WebSocket, and HTTP/2). It supports capabilities such as SSL termination, cookie-based session affinity, and round robin for load-balancing traffic. Load Balancer load-balances traffic at layer 4 (TCP or UDP).References:**https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-faq**New QuestionsYou manage a solution in Azure.You must collect usage data including MAC addresses from all devices on the network. You need to recommend a monitoring solution.What should you recommend?A. Activity Log AnalyticsB. Azure Network Security Group AnalyticsC. Network Performance MonitorD. Azure Application Gateway AnalyticsE. Azure Wire DataAnswer: BExplanation:A network security group (NSG) includes rules that allow or deny traffic to a virtual network subnet, network interface, or both. When you enable diagnostic logging for an NSG, you can log the following categories of information: Event: Entries are logged for which NSG rules are applied to VMs, based on MAC address. The status for these rules is collected every 60 seconds.Rule counter: Contains entries for how many times each NSG rule is applied to deny or allow traffic.References: **https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-nsg-manage-log**New QuestionsA partner manages on-premises and Azure environments. The partner deploys an on-premises solution that needs to use Azure services. The partner deploys a virtual appliance.All network traffic that is directed to a specific subnet must flow through the virtual appliance.You need to recommend solutions to manage network traffic.Which two options should you recommend? Each correct answer presents a complete solution.NOTE: Each correct selection is worth one point.A. Configure Azure Traffic ManagerB. Implement an Azure virtual networkC. Configure a routing table with forced tunnelingD. Implement Azure ExpressRouteAnswer: CDExplanation:C: Forced tunneling lets you redirect or "force" all Internet-bound traffic back to your on-premises location via a Site-to-Site VPN tunnel for inspection and auditing.This is a critical security requirement for most enterprise IT policies. Without forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic.Forced tunneling in Azure is configured via virtual network user-defined routes.D: ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365.Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co- location facility. ExpressRoute connections do not go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet.References:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction New QuestionsDrag and Drop QuestionYou plan to move several apps that handle critical line-of-business (LOB) services to Azure.Appropriate personnel must be notified if any critical resources become degraded or unavailable.You need to design a monitoring and notification strategy that can handle up to 100 notifications per hour.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.NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select. Answer: Explanation:Step 1: Create a resource group containing the critical resources.In step 2 the action group should be created within this Resource Group.Step 2: Create an action group for alerts to email addresses.You configure an action to notify a person by email or SMS, they receive a confirmation indicating they have been added to the action group.The rate limit thresholds are:SMS: No more than 1 SMS every 5 minutes.Voice: No more than 1 Voice call every 5 minutes.Email: No more than 100 emails in an hour.Step 3: Monitor service health for incidents and action required notificationsAn action group is a collection of notification preferences defined by the owner

of an Azure subscription. Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered. References:**https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-rate-limiting**New QuestionsDrag and Drop QuestionYou manage a solution in Azure.The solution is performing poorly.You need to recommend tools to determine causes for the performance issues.What should you recommend? To answer, drag the appropriate monitoring solutions to the correct scenarios. Each monitoring solution may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: Azure MonitorMetrics in Azure Monitor are stored in a time-series database which is optimized for analyzing time-stamped data. This makes metrics particularly suited for alerting and fast detection of issues.Box 2: Azure Log AnalyticsLog data collected by Azure Monitor is stored in a Log Analytics workspace, which is based on Azure Data Explorer. Logs in Azure Monitor are especially useful for performing complex analysis across data from a variety of sources.Box 3: Azure Log AnalyticsReferences:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-logs New QuestionsHotspot QuestionYou manage a network that includes an on-premises Active Directory Domain Services domain and an Azure Active Directory (Azure AD).Employees are requires to use different accounts when using on-premises or cloud resources. You must recommend a solution that lets employees sign in to all company resources by using a single account. The solution must implement an identity provider. You need provide guidance on the different identity providers.How should you describe each identity provider? To answer, select the appropriate description from each list in the answer area.NOTE: Each correct selection is worth one point. Answer: Explanation:Box1: User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. Azure AD Domain Services for hybrid organizationsOrganizations with a hybrid IT infrastructure consume a mix of cloud resources and on-premises resources. Such organizations synchronize identity information from their on-premises directory to their Azure AD tenant. As hybrid organizations look to migrate more of their on-premises applications to the cloud, especially legacy directory-aware applications, Azure AD Domain Services can be useful to them.Example: Litware Corporation has deployed Azure AD Connect, to synchronize identity information from their on-premises directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, their credential hashes for authentication (password hash sync) and group memberships. User accounts, group memberships, and credentials from Litware's on-premises directory are synchronized to Azure AD via Azure AD Connect. These user accounts, group memberships, and credentials are automatically available within the managed domain.Box 2: User management occurs on-premises. The on-promises domain controller authenticates employee credentials. You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises. References:
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed New QuestionsDrag and Drop QuestionA company has an existing web application that runs on virtual machines (VMs) in Azure.You need to ensure that the application is protected from SQL injection attempts and uses a layer-7 load balancer. The solution must minimize disruption to the code for the existing web application.What should you recommend? To answer, drag the appropriate values to the correct items. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: Azure Application GatewayAzure Application Gateway provides an application delivery controller (ADC) as a service. It offers various layer 7 load-balancing capabilities for your applications.Box 2: Web Application Firwewall (WAF)Application Gateway web application firewall (WAF) protects web applications from common vulnerabilities and exploits. This is done through rules that are defined based on the OWASP core rule sets 3.0 or 2.2.9.There are rules that detects SQL injection attacks.References:
https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-faq
https://docs.microsoft.com/en-us/azure/application-gateway/waf-overview New QuestionsHotspot QuestionYour company deploys several Linux and Windows virtual machines (VMs) to Azure. The VMs are deployed with the Microsoft Dependency Agent and the Log Analytics Agent installed by using Azure VM extensions. On-premises connectivity has been enabled by using Azure ExpressRoute.You need to design a solution to monitor the VMs.Which Azure monitoring services should you use? To answer, select the appropriate Azure monitoring services in the answer area.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: Azure Traffic AnalyticsTraffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud. With traffic analytics, you can:Identify security threats to, and secure your network, with information such as open-ports, applications attempting internet access, and virtual machines (VM) connecting to

rogue networks.Visualize network activity across your Azure subscriptions and identify hot spots.Understand traffic flow patterns across Azure regions and the internet to optimize your network deployment for performance and capacity.Pinpoint network misconfigurations leading to failed connections in your network.Box 2: Azure Service MapService Map automatically discovers application components on Windows and Linux systems and maps the communication between services. With Service Map, you can view your servers in the way that you think of them: as interconnected systems that deliver critical services. Service Map shows connections between servers, processes, inbound and outbound connection latency, and ports across any TCP-connected architecture, with no configuration required other than the installation of an agent.References:
https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/service-map New QuestionsNote: This question is part of 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.Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.Several VMs are exhibiting network connectivity issues.You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.Solution: Use the Azure traffic analytics solution in Azure Log Analytics to analyze the network traffic.Does the solution meet the goal?A. YesB. NoAnswer: B Explanation:Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.References:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview New QuestionsNote: This question is part of 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.Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.Several VMs are exhibiting network connectivity issues. You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.Does the solution meet the goal?A. YesB. NoAnswer: A Explanation:The Network Watcher Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.Note:IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.IP flow verify looks at the rules for all Network Security Groups (NSGs) applied to the network interface, such as a subnet or virtual machine NIC. Traffic flow is then verified based on the configured settings to or from that network interface. IP flow verify is useful in confirming if a rule in a Network Security Group is blocking ingress or egress traffic to or from a virtual machine.References:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview New QuestionsNote: This question is part of 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.Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.Several VMs are exhibiting network connectivity issues. You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.Solution: Install and configure the Log Analytics and Dependency Agents on all VMs. Use the Wire Data solution in Azure Log Analytics to analyze the network traffic.Does the solution meet the goal?A. YesB. NoAnswer: BExplanation:Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.References:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview New QuestionsYour network contains an on-premises Active Directory forest named contoso.com. The forest is synced to an Azure Active Directory

(Azure AD) tenant named contoso.com and an Azure AD Domain Services (Azure AD DS) domain named contoso-aad.com.You have an Azure Storage account named Storage1 that contains a file share named Share1.You configure NTFS permissions on Share1. You plan to deploy a virtual machine that will be used by several users to access Share1.You need to ensure that the users can access Share1.Which type virtual machine should you deploy?A. a virtual machine that runs Windows Server 2016 and is joined to the contoso.com domainB. a virtual machine that runs Windows 10 and is joined to the contoso-add.com domainC. a virtual machine that runs Windows 10 and is hybrid Azure AD joined to the contoso.com domainD. an Azure virtual machine that runs Windows Server 2016 and is joined to the contoso-add.com domainAnswer: DExplanation:You join the Windows Server virtual machine to the Azure AD DS-managed domain, here named contoso- aad.com.Note: Azure Files supports identity-based authentication over SMB (Server Message Block) (preview) through Azure Active Directory (Azure AD) Domain Services. Your domain-joined Windows virtual machines (VMs) can access Azure file shares using Azure AD credentials.Incorrect Answers:B, C: Azure AD authentication over SMB is not supported for Linux VMs for the preview release. Only Windows Server VMs are supported.References:
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-enable#mount-a-file-share-from-a-domain-joined-vm New QuestionsNote: This question is part of 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.Your company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM).Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant.The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).Solution: Deploy one Azure Key Vault to each region. Create two Azure AD service principals. Configure the virtual machines to use Azure Disk Encryption and specify a different service principal for the virtual machines in each region.Does this meet the goal?A. YesB. NoAnswer: BExplanation:You would also have to import Import the security keys from the HSM into each Azure key vault.References:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites-aad New QuestionsNote: This question is part of 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.Your company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM).Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant.The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).Solution: Export a security key from the on-premises HSM. Create one Azure AD service principal. Configure the virtual machines to use Azure Storage Service Encryption.Does this meet the goal?A. YesB. NoAnswer: B Explanation:We use the Azure Premium Key Vault with Hardware Security Modules (HSM) backed keys.The Key Vault has to be in the same region as the VM that will be encrypted.References:**https://www.ciraltos.com/azure-disk-encryption-v2/**New QuestionsNote: This question is part of 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.Your company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM).Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant.The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).Solution:- Deploy one Azure key vault to each region-

Export two security keys from the on-premises HSM- Import the security keys from the HSM into each Azure key vault- Create two Azure AD service principals- Configure the virtual machines to use Azure Disk Encryption- Specify a different service principal for the virtual machines in each regionDoes this meet the goal?A. YesB. NoAnswer: AExplanation:We use the Azure Premium Key Vault with Hardware Security Modules (HSM) backed keys.The Key Vault has to be in the same region as the VM that will be encrypted.Note: If you want to use a key encryption key (KEK) for an additional layer of security for encryption keys, add a KEK to your key vault. Use the Add-AzKeyVaultKey cmdlet to create a key encryption key in the key vault. You can also import a KEK from your on-premises key management HSM.References:**https://www.ciraltos.com/azure-disk-encryption-v2/ https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites-aad**New QuestionsNote: This question is part of 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.Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.Several VMs are exhibiting network connectivity issues. You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.Solution: Use Azure Advisor to analyze the network traffic.Does the solution meet the goal?A. YesB. NoAnswer: BExplanation:Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.Note: Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.With Advisor, you can:Get proactive, actionable, and personalized best practices recommendations.Improve the performance, security, and high availability of your resources, as you identify opportunities to reduce your overall Azure spend.Get recommendations with proposed actions inline.References:**https://docs.microsoft.com/en-us/azure/advisor/advisor-overview**New QuestionsYour network contains an Active Directory domain named contoso.com that is federated to an Azure Active Directory (Azure AD) tenant. The on-premises domain contains a VPN server named Server1 that runs Windows Server 2016.You have a single on-premises location that uses an address space of 172.16.0.0/16.You need to implement two-factor authentication for users who establish VPN connections to Server1.What should you include in the implementation?A. In Azure AD, create a conditional access policy and a trusted named locationB. Install and configure Azure MFA Server on-premisesC. Configure an Active Directory Federation Services (AD FS) server on-premisesD. In Azure AD, configure the authentication methods. From the multi-factor authentication (MFA) service settings, create a trusted IP rangeAnswer: BExplanation:You need to download, install and configure the MFA Server.References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfaserver-deploy New QuestionsNote: This question is part of 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 are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting.Solution: Create a resources group for each resource type. Assign tags to each resource group.Does this meet the goal?A. YesB. NoAnswer: A Explanation:Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags New QuestionsNote: This question is part of 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 are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting.Solution: Place all resources in the same resource group. Assign tags to each resource.Does this meet the goal?A. YesB. NoAnswer: BExplanation:Instead, create a resources group for each resource type. Assign tags to each resource Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags New QuestionsNote: This question

is part of 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 are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting.Solution: Create a new subscription for each department.Does this meet the goal?A. YesB. NoAnswer: BExplanation:Instead, create a resources group for each resource type. Assign tags to each resource Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags New QuestionsYou plan to store data in Azure Blob storage for many years. The stored data will be accessed rarely.You need to ensure that the data in Blob storage is always available for immediate access. The solution must minimize storage costs.Which storage tier should you use?A. CoolB. ArchiveC. HotAnswer: AExplanation:Azure cool tier is equivalent to the Amazon S3 Infrequent Access (S3-IA) storage in AWS that provides a low cost high performance storage for infrequently access data.Note: Azure's cool storage tier, also known as Azure cool Blob storage, is for infrequently-accessed data that needs to be stored for a minimum of 30 days. Typical use cases include backing up data before tiering to archival systems, legal data, media files, system audit information, datasets used for big data analysis and more.The storage cost for this Azure cold storage tier is lower than that of hot storage tier. Since it is expected that the data stored in this tier will be accessed less frequently, the data access charges are high when compared to hot tier. There are no additional changes required in your applications as these tiers can be accessed using APIs in the same manner that you access Azure storage.Incorrect Answers:B: Even though Azure archive storage offers the lowest cost in terms of data storage, its data retrieval charges are higher than that of hot and cool tiers. In fact, the data in the archive tier remains offline until the tier of the data is changed using a process called hydration. The process of hydrating data in the archive storage tier and moving it to either hot or cool tier could take up to 15 hours and, hence, it is only intended for data that can afford that kind of access delay.C: The storage cost for this Azure cold storage tier is lower than that of hot storage tier.References:
https://cloud.netapp.com/blog/low-cost-storage-options-on-azure!!!RECOMMEND!!!1.|2019 Latest Braindump2go AZ-301 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/az-301.html2.|2019 Latest Braindump2go AZ-301 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=06rWEglp8iQ