[Nov-2018Exam AZ-102 Dumps PDF and AZ-102 Dumps VCE Free Download from Braindump2go[Q152-Q176

2018/November Braindump2go AZ-102 Exam Dumps with PDF and VCE New Updated Today! Following are some new AZ-102 Real Exam Questions:1.|2018 Latest AZ-102 Exam Dumps (PDF & VCE) 198Q&As Download:https://www.braindump2go.com/az-102.html2.|2018 Latest AZ-102 Exam Questions & Answers Download:https://drive.google.com/drive/folders/1yGAgUGAZkiDyL4FP1-97kh4N_hjURby9?usp=sharingQUESTION 153You have an Azure DNS zone named adatum.com. You need to delegate a subdomain named research.adatum.com to a different DNS server in Azure. What should you do?A. Create an PTR record named research in the adatum.com zone.B. Create an NS record named research in the adatum.com zone.C. Modify the SOA record of adatum.com.D. Create an A record named ".research in the adatum.com zone.Answer: DExplanation:Configure A records for the domains and sub domains.References: **http://www.stefanjohansson.org/2012/12/how-to-configure-custom-dns-names-for-multiple-subdomain-based-azure-web-sites/**QUESTION 154You have an Azure subscription that contains a storage account named account1. You plan to upload the disk files of a virtual machine to account1 from your on-premises network. The on-premises network uses a public IP address space of 131.107.1.0/24. You plan to use the disk files to provision an Azure virtual machine named VM1. VM1 will be attached to a virtual network named VNet1. VNet1 uses an IP address space of 192.168.0.0/24. You need to configure account1 to meet the following requirements:Ensure that you can upload the disk files to account1.Ensure that you can attach the disks to VM1.Prevent all other access to account1.Which two actions should you perform? Each correct selection presents part of the solution.NOTE: Each correct selection is worth one point.A. From the Firewalls and virtual networks blade of account1, add the 131.107.1.0/24 IP address range.B. From the Firewalls and virtual networks blade of account1, select Selected networks.C. From the Firewalls and virtual networks blade of acount1, add VNet1.D. From the Firewalls and virtual networks blade of account1, select Allow trusted Microsoft services toaccess this storage account.E. From the Service endpoints blade of VNet1, add a service endpoint.Answer: BEExplanation:B: By default, storage accounts accept connections from clients on any network. To limit access to selected networks, you must first change the default action.Azure portalNavigate to the storage account you want to secure.Click on the settings menu called Firewalls and virtual networks. To deny access by default, choose to allow access from 'Selected networks'. To allow traffic from all networks, choose to allow access from 'All networks'.Click Save to apply your changes.E: Grant access from a Virtual NetworkStorage accounts can be configured to allow access only from specific Azure Virtual Networks. By enabling a Service Endpoint for Azure Storage within the Virtual Network, traffic is ensured an optimal route to the Azure Storage service. The identities of the virtual network and the subnet are also transmitted with each request.References: **https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security**QUESTION 155SIMULATIONClick to expand each objective. To connect to the Azure portal, type **https://portal.azure.com** in the browser address bar.When you are finished performing all the tasks, click the `Next' button. Note that you cannot return to the lab once you click the `Next' button. Scoring occur in the background while you complete the rest of the exam.OverviewThe following section of the exam is a lab. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design. Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided. Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.To start the labYou may start the lab by clicking the Next button.Your on-premises network uses an IP address range of 131.107.2.0 to 131.107.2.255. You need to ensure that only devices from the on-premises network can connect to the rg1lod7523691n1 storage account.What should you do from the Azure portal?**A. See solution below explanation**Answer: AExplanation:Step 1: Navigate to the rg1lod7523691n1 storage account. Step 2: Click on the settings menu called Firewalls and virtual networks. Step 3: Ensure that you have elected to allow access from 'Selected networks'. Step 4: To grant access to an internet IP range, enter the address range of 131.107.2.0 to 131.107.2.255 (in CIDR format) under Firewall, Address Ranges. References: **https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security**QUESTION 169Note: This question is part of a series 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 manage a virtual network named Vnet1 that is hosted in the West US Azure region. VNet hosts two virtual machines named VM1 and VM2 run Windows Server. You need to inspect all the network traffic from VM1 to VM2 for a period of three hours. Solution: From Azure Network Watcher, you create a connection monitor.Does this meet the goal?A. YESB. NOAnswer: AExplanation:Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.Capture packets to and from a VMAdvanced filtering options and fine-tuned controls, such as the ability to set time and size limitations, provide versatility. The capture can be stored in Azure Storage, on the VM's disk, or both. You can then analyze the capture file using several standard network capture analysis tools. Network Watcher variable packet capture allows you to create packet capture sessions to track traffic to and from a virtual machine. Packet capture helps to diagnose network anomalies both reactively and proactivity.References:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overviewQUESTION 170You have a virtual network named VNet1 as shown in the exhibit. No devices are connected to VNet1.You plan to peer VNet1 to another virtual network named Vnet2 in the same region. VNet2 has an address space of 10.2.0.0/16.You need to create the peering.What should you do first?A. Modify the address space of VNet1.B. Configure a service endpoint on VNet2C. Add a gateway subnet to VNet1.D. Create a subnet on VNet1 and VNet2.Answer: AExplanation:The virtual networks you peer must have non-overlapping IP address spaces.References:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints
QUESTION 171You have an Azure subscription that contains three virtual networks named VNet1, VNet2, VNet3.VNet2 contains a virtual appliance named VM2 that operates as a router. You are configuring the virtual networks in a hub and spoke topology that uses VNet2 as the hub network.You plan to configure peering between VNet1 and VNet2 and between VNet2 and VNet3. You need to provide connectivity between VNet1 and VNet3 through VNet2. Which two configurations should you perform? Each correct answer presents part of the solution.NOTE: Each correct selection is worth one point.A. On the peering connections, allow forwarded traffic.B. On the peering connections, allow gateway transit.C. Create route tables and assign the table to subnets.D. Create a route filter.E. On the peering connections, use remote gateways.Answer: BEExplanation:Allow gateway transit: Check this box if you have a virtual network gateway attached to this virtual network and want to allow traffic from the peered virtual network to flow through the gateway. The peered virtual network must have the Use remote gateways checkbox checked when setting up the peering from the other virtual network to this virtual network.References:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints
QUESTION 172You are the global administrator for an Azure Active Directory (Azure AD) tenant named adatum.com.You need to enable two-step verification for Azure users.What should you do?A. Configure a playbook in Azure AD conditional access policy.B. Create an Azure AD conditional access policy.C. Create and configure the Identify Hub.D. Install and configure Azure AD Connect.Answer: BExplanation:**https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings**
QUESTION 173From the MFA Server blade, you open the Block/unblock users blade as shown in the exhibit.Block/unblock usersA blocked user will not receive Multi-Factor Authentication requests. Authentication attempts for that user will be automatically denied. A user will remain blocked for 90 days from the time they are blocked. To manually unblock a user, click the "Unblock" action. What caused AlexW to be blocked?A. The user entered an incorrect PIN four times within 10 minutes.B. The user account password expired.C. An administrator manually blocked the user.D. The user reported a fraud alert when prompted for additional authentication.**Answer: D**QUESTION 174You have the Azure virtual networks shown in the following table. To which virtual networks can you establish a peering connection from VNet1?A. VNet2 and VNet3 onlyB. VNet2 onlyC. VNet3 and VNet4 onlyD. VNet2, VNet3, and VNet4Answer: CExplanation:The virtual networks you peer must have non-overlapping IP address spaces. The VNet1 and VNhet2 address spaces overlap. The range of VNet2 is contained inside the range of VNet1.
References:**https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints**QUESTION 175You have two Azure virtual networks named VNet1 and VNet2. VNet1 contains an Azure virtual machine named VM1. VNet2 contains an Azure virtual machine named VM2. VM1 hosts a frontend application that connects to VM2 to retrieve data. Users report that the frontend application is slower than usual. You need to view the average round-trip time (RTT) of the packets from VM1 to VM2.Which Azure Network Watcher feature should you use?A. NSG flow logsB. Connection troubleshootC. IP flow verifyD. Connection monitorAnswer: DExplanation:The Connection Monitor feature in Azure Network Watcher is now generally available in all public regions. Connection Monitor provides you RTT values on a per-minute granularity. You can monitor a direct TCP connection from a virtual machine to a virtual machine, FQDN, URI, or IPv4 address.References:
https://azure.microsoft.com/en-us/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regi

ons/QUESTION 176You are troubleshooting a performance issue for an Azure Application Gateway. You need to compare the total requests to the failed requests during the past six hours.What should you use?A. Metrics in Application GatewayB. Diagnostics logs in Application GatewayC. NSG flow logs in Azure Network WatcherD. Connection monitor in Azure Network WatcherAnswer: AExplanation:Application Gateway currently has seven metrics to view performance counters. Metrics are a feature for certain Azure resources where you can view performance counters in the portal. ForApplication Gateway, the following metrics are available:Total RequestsFailed RequestsCurrent ConnectionsHealthy Host CountResponse StatusThroughputUnhealthy Host countYou can filter on a per backend pool basis to show healthy/unhealthy hosts in a specific backend pool References:
https://docs.microsoft.com/en-us/azure/application-gateway/application-gatewaydiagnostics#Metrics
!!!RECOMMEND!!!1.|2018 Latest AZ-102 Exam Dumps (PDF & VCE) 198Q&As Download:https://www.braindump2go.com/az-102.html2.|2018 Latest AZ-102 Study Guide Video: YouTube Video: YouTube.com/watch?v=zhiZRXWD1Ps