[70-535 New Dumps70-535 Dumps VCE and PDF(Full Version)354Q Download in Braindump2go[326-336

2018 June New Microsoft 70-535 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 70-535 Real Exam Questions:1.|2018 Latest 70-535 Exam Dumps (PDF & VCE) 354Q&As Download:https://www.braindump2go.com/70-535.html2.|2018 Latest 70-535 Exam Questions & Answers Download:https://drive.google.com/drive/folders/1K808iFXD_tKKveGZeLM1H8d81RAL6LCx?usp=sharingQUESTION 326 Hotspot QuestionYou are designing a solution that uses Azure Storage. The solution will store the following information. You need to recommend storage technologies for the solution.What should you recommend? To answer, select the appropriate options in the answer area.NOTE: Each correct selection is worth one point. Answer: QUESTION 327A company plans to use Azure Cosmos DB as the document store for an application.You need to estimate the request units required for the application.Which variable should you include when calculating the estimate?A. item sizeB. consistency levelC. cache sizeD. number of regionsAnswer: B Explanation:When using data consistency levels of Strong or Bounded Staleness, additional units are consumed to read items. References: **https://docs.microsoft.com/en-us/azure/cosmos-db/request-units**QUESTION 328Hotspot QuestionYou manage a hybrid Azure solution for a company.You need to recommend Advanced Threat Detection solutions to guard against hacker attacks in different scenarios.What should you recommend? To answer, select the appropriate options in the answer area.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1 (Alerting about access to a privileged role): Azure Privileged Identity Management (PIM) Azure Privileged Identity Management (PIM) generates alerts when there is suspicious or unsafe activity in your environment. When an alert is triggered, it shows up on the PIM dashboard.Box 2 (Analyzing attack patterns and trends): Azure Security Center Every second counts when you are under attack. Azure Security Center (ASC) uses advanced analytics and global threat intelligence to detect malicious threats, and the new capabilities empower you to respond quickly.Box 3 (Using conditional access policies to secure identities): Azure AD Identity Protection Security is a top concern for organizations using the cloud. A key aspect of cloud security is identity and access when it comes to managing your cloud resources. In a mobile-first, cloud-first world, users can access your organization's resources using a variety of devices and apps from anywhere. As a result of this, just focusing on who can access a resource is not sufficient anymore. In order to master the balance between security and productivity, IT professionals also need to factor how a resource is being accessed into an access control decision. With Azure AD conditional access, you can address this requirement. Conditional access is a capability of Azure Active Directory that enables you to enforce controls on the access to apps in your environment based on specific conditions from a central location.Box 4 (Visualizing real-time security alerts): Operations Management Suite Security and Audit The OMS Security and Audit solution provides a comprehensive view into your organization's IT security posture with built-in search queries for notable issues that require your attention. The Security and Audit dashboard is the home screen for everything related to security in OMS. It provides high-level insight into the security state of your computers. It also includes the ability to view all events from the past 24 hours, 7 days, or any other custom time frame.References:
https://docs.microsoft.com/en-us/azure/active-directory/active-directory-privileged-identity-management- how-to-configure-security-alerts
https://azure.microsoft.com/en-us/blog/how-azure-security-center-helps-analyze-attacks-using- investigation-and-log-search/
https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alertsQUESTION 329 Hotspot QuestionYou manage an Azure solution that processes highly sensitive data.Existing roles are not suited to the granular access control that is required for this data.You need to recommend solutions to limit access to the data based on selected restrictions.What should you recommend? To answer, drag the appropriate restrictions to the correct solutions. Each restriction 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:Automatic access expiration: Privileged Identity Management (PIM) To protect privileged accounts from malicious cyber-attacks, you can use Azure Active Directory Privileged Identity Management (PIM) to lower the exposure time of privileges and increase your visibility into their use through reports and alerts.You can now use PIM with Azure Role-Based Access Control (RBAC) to manage, control, and monitor access to Azure resources. PIM can manage the membership of built-in and custom roles to help you:Enable on-demand, "just in time" access to Azure resources Expire resource access automatically for assigned users and groups Assign temporary access to Azure resources for quick tasks or on-call schedules Get alerts when new users or groups are assigned resource access, and when they activate eligible assignmentsTime-based access restrictions: Conditional AccessConditional access is a capability of Azure Active Directory that enables you to enforce controls on

the access to apps in your environment based on specific conditions from a central location. Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies.Access to Azure Management endpoints: Conditional AccessReferences:
https://docs.microsoft.com/en-us/azure/role-based-access-control/pim-azure-resource
https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad
https://docs.microsoft.com/en-us/azure/role-based-access-control/conditional-access-azure-managementQUESTION 330 Hotspot QuestionA company requires secure communication between virtual machines (VMs) without exposing credentials. The security officer wants to perform proof-of-concept testing using managed service identities.You need to recommend a solution for performing proof-of-concept testing.What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point. Answer: Explanation:?Here's an example of how System Assigned Identities work with Azure Virtual Machines:
https://docs.microsoft.com/en-us/azure/active-directory/managed-service-identity/overviewQUESTION 331Hotspot Question You manage a network that includes an on-premises Active Directory Domain Services domain and an Azure Active Directory (Azure AD).Employees are required 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:Synchronized identity is the simplest way to synchronize on-premises directory objects (users and groups) with Azure AD.While synchronized identity is the easiest and quickest method, your users still need to maintain a separate password for cloud-based resources. To avoid this, you can also (optionally) synchronize a hash of user passwords to your Azure AD directory. Synchronizing password hashes enables users to log in to cloud-based organizational resources with the same user name and password that they use on-premises. Azure AD Connect periodically checks your on-premises directory for changes and keeps your Azure AD directory synchronized. When a user attribute or password is changed on-premises Active Directory, it is automatically updated in Azure AD. Federated identity:For more control over how users access Office 365 and other cloud services, you can set up directory synchronization with single sign-on (SSO) using Active Directory Federation Services (AD FS). Federating your user's sign-ins with AD FS delegates authentication to an on-premises server that validates user credentials. In this model, on-premises Active Directory credentials are never passed to Azure AD. Reference:
https://docs.microsoft.com/en-us/azure/active-directory/choose-hybrid-identity- solution#synchronized-identityQUESTION 332Note: This question is part of a series of questions that present the same scenario. Each ques-tion on 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 planning to create a virtual network that has a scale set that contains six virtual machines (VMs).A monitoring solution on a different network will need access to the VMs inside the scale set.You need to define public access to the VMs.Solution: Implement an Azure Load Balancer.Does the solution meet the goal?A. YesB. NoAnswer: B Explanation:Public IP addresses are necessary because they provide the load balanced entry point for the virtual machines in the scale set. The public IP address will route traffic to the appropriate virtual machines in the scale set.Reference:
https://mitra.computa.asia/articles/msdn-virtual-machine-scale-sets-it-really-about-protecting-your-applications-performanceQUESTION 333Note: This question is part of a series of questions that present the same scenario. Each ques-tion on 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 planning to create a virtual network that has a scale set that contains six virtual machines (VMs).A monitoring solution on a different network will need access to the VMs inside the scale set.You need to define public access to the VMs.Solution: Design a scale set to automatically assign public IP addresses to all VMs.Does the solution meet the goal?A. YesB. NoAnswer: BExplanation:All VMs do not need public IP addresses.Public IP addresses are necessary because they provide the load balanced entry point for the virtual machines in the scale set. The public IP address will route traffic to the appropriate virtual machines in the scale set.Reference:
https://mitra.computa.asia/articles/msdn-virtual-machine-scale-sets-it-really-about-protecting-your-applications-performanceQUESTION 334Note: This question is part of a series of questions that present the same scenario. Each ques-tion on 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 planning to create a virtual network that has a scale set that contains six virtual machines (VMs).A monitoring solution on a different network will need access to the VMs inside the scale set.You need to define public access to the VMs.Solution: Deploy a standalone VM that has a public IP address to the virtual network.Does the solution meet the goal?A. YesB. NoAnswer: AExplanation:Public IP addresses are necessary because they provide the load balanced entry point for the virtual machines in the scale set. The public IP address will route traffic to the appropriate virtual machines in the scale set.
https://mitra.computa.asia/articles/msdn-virtual-machine-scale-sets-it-really-about-protecting-your-applications-performanceQUESTION 335Note: This question is part of a series of questions that present the same scenario. Each ques-tion on 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 solution in Azure. You configure Event Hubs to collect telemetry data from dozens of industrial machines. Hundreds of events per minute are logged in near real-time. You use this data to create dashboards for analysts.The company is expanding their machinery and wants to know if the current telemetry solution will be sufficient to handle the volume of the increasing workload. The volume will increase 10 times by year end and on a regular basis thereafter. Latency will become more and more important as volume increases.Messages must be retained for a week. Data must be captured automatically without price increase.You need to recommend a solution.Solution: Use single-tenant hosting in the dedicated tier to handle the increased volume.Does the solution meet the goal?A. YesB. NoAnswer: AExplanation:Azure Event Hubs Dedicated is ideal for customers that need a single-tenant deployment to manage the most demanding requirements.Note: The dedicated tier option involves Zero maintenance: The service manages load balancing, OS updates, security patches, and partitioning.The following table compares the available service tiers of Event Hubs. The Event Hubs Dedicated offering is a fixed monthly price, compared to usage pricing for most features of Standard. The Dedicated tier offers all the features of the Standard plan, but with enterprise scale capacity for customers with demanding workloads.
https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-dedicated-overviewQUESTION 336Note: This question is part of a series of questions that present the same scenario. Each ques-tion on 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 solution in Azure. You configure Event Hubs to collect telemetry data from dozens of industrial machines. Hundreds of events per minute are logged in near real-time. You use this da-ta to create dashboards for analysts.The company is expanding their machinery and wants to know if the current telemetry solution will be sufficient to handle the volume of the increasing workload. The volume will increase 10 times by year end and on a regular basis thereafter. Latency will become more and more important as volume increases.Messages must be retained for a week. Data must be captured automatically without price increase.You need to recommend a solution.Solution: Use the more flexible deployment model in the dedicated tier for the increased workload.Does the solution meet the goal?A. YesB. NoAnswer: BExplanation:Azure Event Hubs Dedicated is ideal for customers that need a single-tenant deployment, not the flexible deployment model, to manage the most demanding requirements.
Reference: **https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-dedicated-overview**!!!RECOMMEND!!!1.|2018 Latest 70-535 Exam Dumps (PDF & VCE) 354Q&As Download:https://www.braindump2go.com/70-535.html2.|2018 Latest 70-535 Study Guide Video: YouTube Video: YouTube.com/watch?v=kdc5IgSuIjA