[New Exams!DP-200 Exam Dumps PDF 60Q Free Shared by Braindump2go

2019/July Braindump2go DP-200 Exam Dumps with PDF and VCE New Updated Today! Following are some new DP-200 Real Exam Questions: 1.|2019 Latest Braindump2go DP-200 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/dp-200.html2.|2019 Latest Braindump2go DP-200 Exam Questions & Answers Instant Download:https://drive.google.com/drive/folders/1Lr1phOaAVcbL-_R5O-DFweNoShul0W13?usp=sharingNew QuestionCase Study 1 - Proseware, IncBackgroundProseware, Inc, develops and manages a product named Poll Taker. The product is used for delivering public opinion polling and analysis.Polling data comes from a variety of sources, including online surveys, house-to-house interviews, and booths at public events.Polling dataPolling data is stored in one of the two locations:- An on-premises Microsoft SQL Server 2019 database named PollingData- Azure Data Lake Gen 2Data in Data Lake is queried by using PolyBasePoll metadataEach poll has associated metadata with information about the poll including the date and number of respondents. The data is stored as JSON.Phone-based pollingSecurity- Phone-based poll data must only be uploaded by authorized users from authorized devices- Contractors must not have access to any polling data other than their own- Access to polling data must set on a per-active directory user basisData migration and loading- All data migration processes must use Azure Data Factory- All data migrations must run automatically during non-business hours- Data migrations must be reliable and retry when needed PerformanceAfter six months, raw polling data should be moved to a lower-cost storage solution.Deployments- All deployments must be performed by using Azure DevOps. Deployments must use templates used in multiple environments- No credentials or secrets should be used during deploymentsReliabilityAll services and processes must be resilient to a regional Azure outage. MonitoringAll Azure services must be monitored by using Azure Monitor. On-premises SQL Server performance must be monitored.You need to ensure that phone-based poling data can be analyzed in the PollingData database.How should you configure Azure Data Factory?A. Use a tumbling schedule triggerB. Use an event-based triggerC. Use a schedule triggerD. Use manual executionAnswer: CExplanation:When creating a schedule trigger, you specify a schedule (start date, recurrence, end date etc.) for the trigger, and associate with a Data Factory pipeline.Scenario:All data migration processes must use Azure Data FactoryAll data migrations must run automatically during non-business hoursReferences:
https://docs.microsoft.com/en-us/azure/data-factory/how-to-create-schedule-trigger New QuestionCase Study 1 - Proseware, IncBackgroundProseware, Inc, develops and manages a product named Poll Taker. The product is used for delivering public opinion polling and analysis.Polling data comes from a variety of sources, including online surveys, house-to-house interviews, and booths at public events.Polling dataPolling data is stored in one of the two locations:- An on-premises Microsoft SQL Server 2019 database named PollingData- Azure Data Lake Gen 2Data in Data Lake is queried by using PolyBasePoll metadataEach poll has associated metadata with information about the poll including the date and number of respondents. The data is stored as JSON.Phone-based pollingSecurity- Phone-based poll data must only be uploaded by authorized users from authorized devices- Contractors must not have access to any polling data other than their own- Access to polling data must set on a per-active directory user basisData migration and loading- All data migration processes must use Azure Data Factory- All data migrations must run automatically during non-business hours- Data migrations must be reliable and retry when neededPerformanceAfter six months, raw polling data should be moved to a lower-cost storage solution.Deployments- All deployments must be performed by using Azure DevOps. Deployments must use templates used in multiple environments- No credentials or secrets should be used during deployments ReliabilityAll services and processes must be resilient to a regional Azure outage.MonitoringAll Azure services must be monitored by using Azure Monitor. On-premises SQL Server performance must be monitored.Drag and Drop QuestionYou need to ensure that phone-based polling data can be analyzed in the PollingData database.Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer are and arrange them in the correct order. Answer: Explanation:Scenario:All deployments must be performed by using Azure DevOps. Deployments must use templates used in multiple environments No credentials or secrets should be used during deployments?New QuestionCase Study 1 - Proseware, Inc BackgroundProseware, Inc, develops and manages a product named Poll Taker. The product is used for delivering public opinion polling and analysis.Polling data comes from a variety of sources, including online surveys, house-to-house interviews, and booths at public events.Polling dataPolling data is stored in one of the two locations:- An on-premises Microsoft SQL Server 2019 database named PollingData- Azure Data Lake Gen 2Data in Data Lake is queried by using PolyBasePoll metadataEach poll has associated metadata with information about the poll including the date and number of respondents. The data is stored as JSON.Phone-based pollingSecurity- Phone-based poll data must only be uploaded by authorized users from authorized devices- Contractors must not have access to any polling data other than their own- Access to polling data must set on a per-active directory user basisData migration and loading- All data migration processes must use Azure Data Factory- All data migrations must run automatically

during non-business hours- Data migrations must be reliable and retry when neededPerformanceAfter six months, raw polling data should be moved to a lower-cost storage solution.Deployments- All deployments must be performed by using Azure DevOps. Deployments must use templates used in multiple environments- No credentials or secrets should be used during deployments ReliabilityAll services and processes must be resilient to a regional Azure outage.MonitoringAll Azure services must be monitored by using Azure Monitor. On-premises SQL Server performance must be monitored.Hotspot QuestionYou need to ensure that Azure Data Factory pipelines can be deployed. How should you configure authentication and authorization for deployments? To answer, select the appropriate options in the answer choices.NOTE: Each correct selection is worth one point. Answer: Explanation:The way you control access to resources using RBAC is to create role assignments. This is a key concept to understand ?it's how permissions are enforced. A role assignment consists of three elements: security principal, role definition, and scope.Scenario:No credentials or secrets should be used during deploymentsPhone-based poll data must only be uploaded by authorized users from authorized devices Contractors must not have access to any polling data other than their ownAccess to polling data must set on a per-active directory user basisReferences:**https://docs.microsoft.com/en-us/azure/role-based-access-control/overview**New QuestionCase Study 1 - Proseware, IncBackgroundProseware, Inc, develops and manages a product named Poll Taker. The product is used for delivering public opinion polling and analysis.Polling data comes from a variety of sources, including online surveys, house-to-house interviews, and booths at public events.Polling dataPolling data is stored in one of the two locations:- An on-premises Microsoft SQL Server 2019 database named PollingData- Azure Data Lake Gen 2Data in Data Lake is queried by using PolyBasePoll metadataEach poll has associated metadata with information about the poll including the date and number of respondents. The data is stored as JSON.Phone-based pollingSecurity- Phone-based poll data must only be uploaded by authorized users from authorized devices- Contractors must not have access to any polling data other than their own- Access to polling data must set on a per-active directory user basisData migration and loading- All data migration processes must use Azure Data Factory- All data migrations must run automatically during non-business hours- Data migrations must be reliable and retry when needed PerformanceAfter six months, raw polling data should be moved to a lower-cost storage solution.Deployments- All deployments must be performed by using Azure DevOps. Deployments must use templates used in multiple environments- No credentials or secrets should be used during deploymentsReliabilityAll services and processes must be resilient to a regional Azure outage. MonitoringAll Azure services must be monitored by using Azure Monitor. On-premises SQL Server performance must be monitored.Hotspot QuestionYou need to ensure phone-based polling data upload reliability requirements are met. How should you configure monitoring? To answer, select the appropriate options in the answer area.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: FileCapacityFileCapacity is the amount of storage used by the storage account's File service in bytes. Box 2: AvgThe aggregation type of the FileCapacity metric is Avg.Scenario:All services and processes must be resilient to a regional Azure outage.All Azure services must be monitored by using Azure Monitor. On-premises SQL Server performance must be monitored.References:**https://docs.microsoft.com/en-us/azure/azure-monitor/platform/metrics-supported**New QuestionCase Study 1 - Proseware, IncBackgroundProseware, Inc, develops and manages a product named Poll Taker. The product is used for delivering public opinion polling and analysis.Polling data comes from a variety of sources, including online surveys, house-to-house interviews, and booths at public events.Polling dataPolling data is stored in one of the two locations:- An on-premises Microsoft SQL Server 2019 database named PollingData- Azure Data Lake Gen 2Data in Data Lake is queried by using PolyBasePoll metadataEach poll has associated metadata with information about the poll including the date and number of respondents. The data is stored as JSON.Phone-based pollingSecurity- Phone-based poll data must only be uploaded by authorized users from authorized devices- Contractors must not have access to any polling data other than their own- Access to polling data must set on a per-active directory user basisData migration and loading- All data migration processes must use Azure Data Factory- All data migrations must run automatically during non-business hours- Data migrations must be reliable and retry when needed PerformanceAfter six months, raw polling data should be moved to a lower-cost storage solution.Deployments- All deployments must be performed by using Azure DevOps. Deployments must use templates used in multiple environments- No credentials or secrets should be used during deploymentsReliabilityAll services and processes must be resilient to a regional Azure outage. MonitoringAll Azure services must be monitored by using Azure Monitor. On-premises SQL Server performance must be monitored.Hotspot QuestionYou need to ensure polling data security requirements are met.Which security technologies should you use? To answer, select the appropriate options in the answer area.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: Azure Active Directory userScenario:Access to polling data must set on a per-active directory user basisBox 2: DataBase Scoped CredentialSQL Server uses a database scoped credential to access non-public Azure blob storage or Kerberos-secured Hadoop clusters with PolyBase.PolyBase cannot authenticate by using Azure AD authentication.References: **https://docs.microsoft.com/en-us/sql/t-sql/statements/create-database-scoped-credential-transact-sql**New QuestionCase Study

2 - ContosoOverviewCurrent environmentContoso relies on an extensive partner network for marketing, sales, and distribution. Contoso uses external companies that manufacture everything from the actual pharmaceutical to the packaging.The majority of the company's data reside in Microsoft SQL Server database. Application databases fall into one of the following tiers: The company has a reporting infrastructure that ingests data from local databases and partner services. Partners services consists of distributors, wholesales, and retailers across the world. The company performs daily, weekly, and monthly reporting.RequirementsTier 3 and Tier 6 through Tier 8 application must use database density on the same server and Elastic pools in a cost-effective manner. Applications must still have access to data from both internal and external applications keeping the data encrypted and secure at rest and in transit.A disaster recovery strategy must be implemented for Tier 3 and Tier 6 through 8 allowing for failover in the case of server going offline.Selected internal applications must have the data hosted in single Microsoft Azure SQL Databases.- Tier 1 internal applications on the premium P2 tier- Tier 2 internal applications on the standard S4 tierThe solution must support migrating databases that support external and internal application to Azure SQL Database. The migrated databases will be supported by Azure Data Factory pipelines for the continued movement, migration and updating of data both in the cloud and from local core business systems and repositories.Tier 7 and Tier 8 partner access must be restricted to the database only.In addition to default Azure backup behavior, Tier 4 and 5 databases must be on a backup strategy that performs a transaction log backup eve hour, a differential backup of databases every day and a full back up every week.Back up strategies must be put in place for all other standalone Azure SQL Databases using Azure SQL-provided backup storage and capabilities.DatabasesContoso requires their data estate to be designed and implemented in the Azure Cloud. Moving to the cloud must not inhibit access to or availability of data.Databases:Tier 1 Database must implement data masking using the following masking logic: Tier 2 databases must sync between branches and cloud databases and in the event of conflicts must be set up for conflicts to be won by on-premises databases.Tier 3 and Tier 6 through Tier 8 applications must use database density on the same server and Elastic pools in a cost-effective manner.Applications must still have access to data from both internal and external applications keeping the data encrypted and secure at rest and in transit.A disaster recovery strategy must be implemented for Tier 3 and Tier 6 through 8 allowing for failover in the case of a server going offline.Selected internal applications must have the data hosted in single Microsoft Azure SQL Databases.- Tier 1 internal applications on the premium P2 tier- Tier 2 internal applications on the standard S4 tierReportingSecurity and monitoringSecurityA method of managing multiple databases in the cloud at the same time is must be implemented to streamlining data management and limiting management access to only those requiring access.MonitoringMonitoring must be set up on every database. Contoso and partners must receive performance reports as part of contractual agreements.Tiers 6 through 8 must have unexpected resource storage usage immediately reported to data engineers.The Azure SQL Data Warehouse cache must be monitored when the database is being used. A dashboard monitoring key performance indicators (KPIs) indicated by traffic lights must be created and displayed based on the following metrics: Existing Data Protection and Security compliances require that all certificates and keys are internally managed in an on-premises storage.You identify the following reporting requirements:- Azure Data Warehouse must be used to gather and query data from multiple internal and external databases- Azure Data Warehouse must be optimized to use data from a cache- Reporting data aggregated for external partners must be stored in Azure Storage and be made available during regular business hours in the connecting regions- Reporting strategies must be improved to real time or near real time reporting cadence to improve competitiveness and the general supply chain- Tier 9 reporting must be moved to Event Hubs, queried, and persisted in the same Azure region as the company's main office- Tier 10 reporting data must be stored in Azure BlobsIssuesTeam members identify the following issues:- Both internal and external client application run complex joins, equality searches and group-by clauses. Because some systems are managed externally, the queries will not be changed or optimized by Contoso- External partner organization data formats, types and schemas are controlled by the partner companies- Internal and external database development staff resources are primarily SQL developers familiar with the Transact-SQL language.- Size and amount of data has led to applications and reporting solutions not performing are required speeds- Tier 7 and 8 data access is constrained to single endpoints managed by partners for access- The company maintains several legacy client applications. Data for these applications remains isolated form other applications. This has led to hundreds of databases being provisioned on a per application basisYou need to process and query ingested Tier 9 data.Which two options should you use? Each correct answer presents part of the solution.NOTE: Each correct selection is worth one point.A. Azure Notification HubB. Transact-SQL statementsC. Azure Cache for RedisD. Apache Kafka statementsE. Azure Event GridF. Azure Stream AnalyticsAnswer: EFExplanation:Event Hubs provides a Kafka endpoint that can be used by your existing Kafka based applications as an alternative to running your own Kafka cluster.You can stream data into Kafka-enabled Event Hubs and process it with Azure Stream Analytics, in the following steps:Create a Kafka enabled Event Hubs namespace.Create a Kafka client that sends messages to the event hub.Create a Stream Analytics job that copies data from the event hub into an Azure blob storage.Scenario: Tier 9 reporting must be moved to Event Hubs, queried, and persisted

in the same Azure region as the company's main office References:
https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-kafka-stream-analytics!!!RECOMMEND!!!1.|2019 Latest Braindump2go DP-200 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/dp-200.html2.|2019 Latest Braindump2go DP-200 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=vKbQyUpp3Xs