

## [New Exams!Braindump2go DP-200 PDF Dumps and DP-200 VCE Dumps Free Download

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.html>2.|2019 Latest Braindump2go DP-200 Exam Questions & Answers Instant

Download:[https://drive.google.com/drive/folders/1Lr1phOaAVcbL-\\_R5O-DFweNoShul0W13?usp=sharing](https://drive.google.com/drive/folders/1Lr1phOaAVcbL-_R5O-DFweNoShul0W13?usp=sharing)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.Requirements Tier 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 set

up Azure Data Factory pipelines to meet data movement requirements. Which integration runtime should you use? A. self-hosted integration runtime B. Azure-SSIS Integration Runtime C. .NET Common Language Runtime (CLR) D. Azure integration runtime  
Answer: A  
Explanation: The following table describes the capabilities and network support for each of the integration runtime types: Scenario: The 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. References:

<https://docs.microsoft.com/en-us/azure/data-factory/concepts-integration-runtime>  
New Question  
Case Study 2 - Contoso  
Overview  
Current environment  
Contoso 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. Requirements  
Tier 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 tier  
The 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. Databases  
Contoso 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 tier  
Reporting  
Security and monitoring  
Security  
A 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. Monitoring  
Monitoring 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 Blobs  
Issues  
Team 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 basis  
Note: 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 questions 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 need to configure data encryption for external applications. Solution: 1. Access the Always Encrypted Wizard in SQL Server Management Studio 2. Select the column to be encrypted 3. Set the encryption type to Randomized 4. Configure the master key to use the Windows Certificate Store 5. Validate configuration results and deploy the solution Does the solution meet the goal? A. Yes B. No Answer: B Explanation: Use the Azure Key Vault, not the Windows Certificate Store, to store the master key. Note: The Master Key Configuration page is where you set up your CMK (Column Master Key) and select the key store provider where the CMK will be stored. Currently, you can store a CMK in the Windows certificate store, Azure Key Vault, or a hardware security module (HSM). References:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-always-encrypted-azure-key-vault> New Question Case Study

2 - Contoso Overview Current environment Contoso 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. Requirements Tier 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 tier The 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 every 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. Databases Contoso 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 tier Reporting Security and monitoring Security A 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. Monitoring Monitoring 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 Blobs Issues Team 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 from other applications. This has led to hundreds of databases being provisioned on a per application basis

Note: 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 questions 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 need to configure data encryption for external applications.

Solution: 1. Access the Always Encrypted Wizard in SQL Server Management Studio 2. Select the column to be encrypted 3. Set the encryption type to Deterministic 4. Configure the master key to use the Windows Certificate Store 5. Validate configuration results and deploy the solution

Does the solution meet the goal?

A. Yes B. No

Answer: B

Explanation: Use the Azure Key Vault, not the Windows Certificate Store, to store the master key.

Note: The Master Key Configuration page is where you set up your CMK (Column Master Key) and select the key store provider where the CMK will be stored. Currently, you can store a CMK in the Windows certificate store, Azure Key Vault, or a hardware security module (HSM).

References:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-always-encrypted-azure-key-vault>

New Question

Case Study

2 - Contoso

Overview

Current environment

Contoso 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.

Requirements

Tier 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 tier

The 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.

Databases

Contoso 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 tier

Reporting

Security and monitoring

Security

A 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.

Monitoring

Monitoring 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 Blobs

Issues

Team 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 basisNote: 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 questions 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 need to configure data encryption for external applications.Solution:1. Access the Always Encrypted Wizard in SQL Server Management Studio2. Select the column to be encrypted3. Set the encryption type to Deterministic4. Configure the master key to use the Azure Key Vault5. Validate configuration results and deploy the solutionDoes the solution meet the goal?A. YesB. NoAnswer: AExplanation:We use the Azure Key Vault, not the Windows Certificate Store, to store the master key.Note: The Master Key Configuration page is where you set up your CMK (Column Master Key) and select the key store provider where the CMK will be stored.Currently, you can store a CMK in the Windows certificate store, Azure Key Vault, or a hardware security module (HSM). References:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-always-encrypted-azure-key-vault>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 basisNote: 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 questions 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 need to implement diagnostic logging for Data Warehouse monitoring.Which log should you use?A. RequestStepsB. DmsWorkersC. SqlRequestsD. ExecRequestsAnswer: CExplanation:Scenario:The Azure SQL Data Warehouse cache must be monitored when the database is being used. References:  
<https://docs.microsoft.com/en-us/sql/relational-databases/system-dynamic-management-views/sys-dm-pdw-sql-requests-transact-sq>!!!RECOMMEND!!!1.[2019 Latest Braindump2go DP-200 Exam Dumps (PDF & VCE) Instant Download:<https://www.braindump2go.com/dp-200.html>2.[2019 Latest Braindump2go DP-200 Study Guide Video Instant Download: YouTube Video: [YouTube.com/watch?v=vKbQyUpp3Xs](https://www.youtube.com/watch?v=vKbQyUpp3Xs)