DP-300 Q&As

Administering Relational Databases on Microsoft Azure

Pass Microsoft DP-300 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/dp-300.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

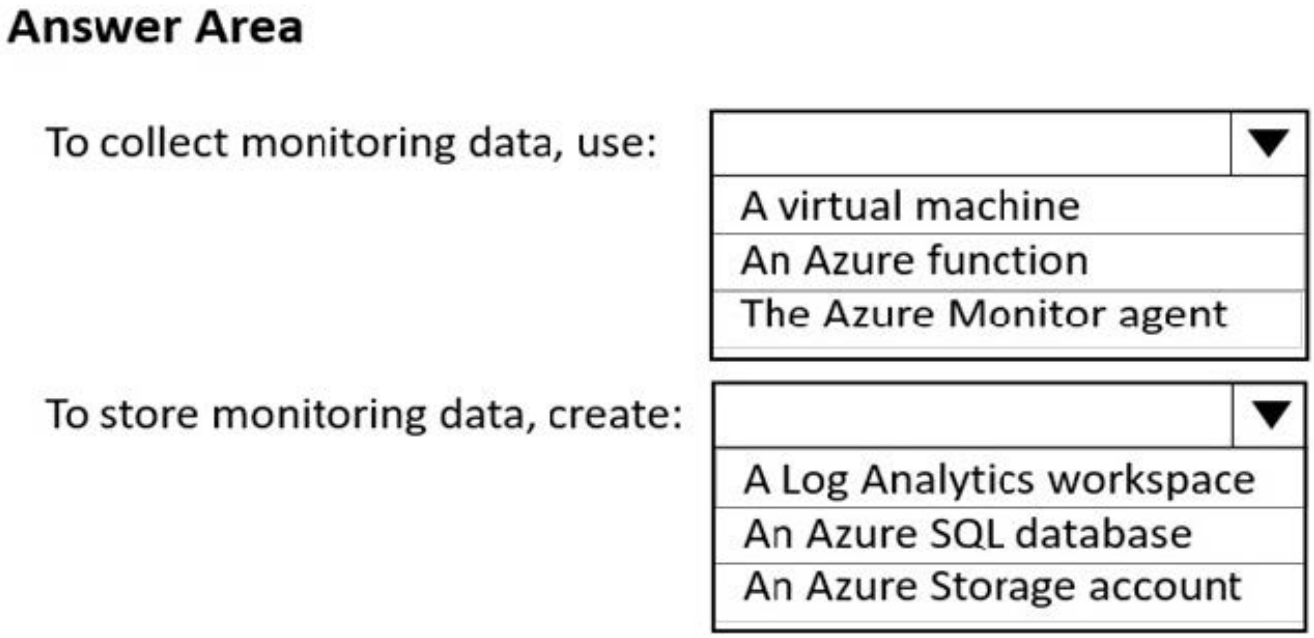
HOTSPOT

You have an Azure SQL database named DB1 in the General Purpose service tier.

You need to monitor DB1 by using SQL Insights.

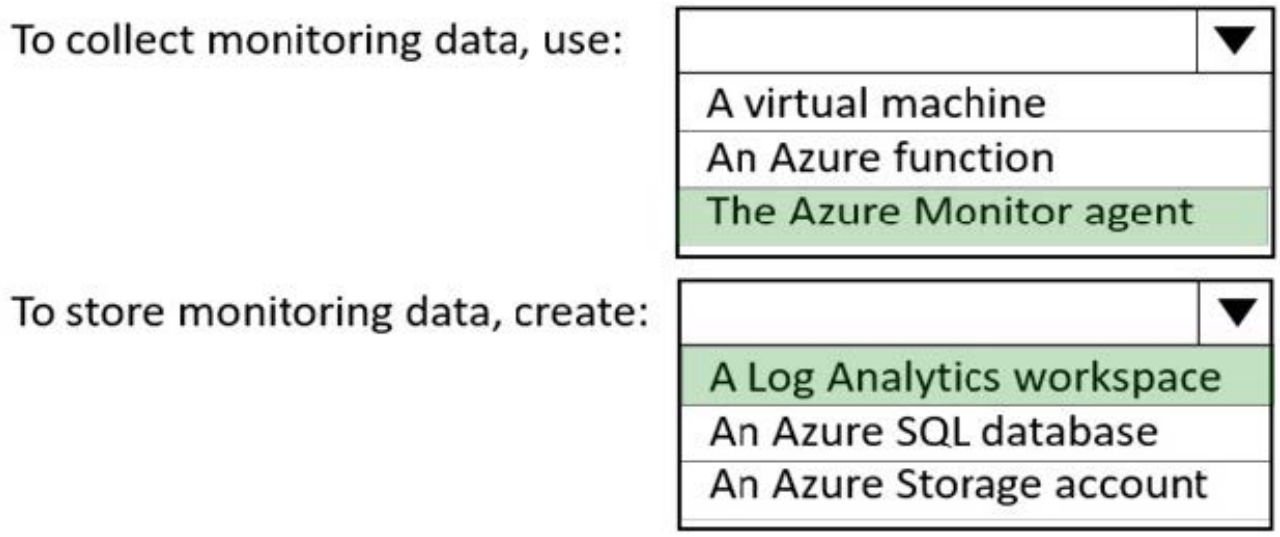
What should you include in the solution? To answer, select the appropriate options in the answer area.

Hot Area:



Correct Answer:

Answer Area



Box 1: The Azure Monitor agent

SQL Insights performs all monitoring remotely. Monitoring agents on dedicated virtual machines connect to your SQL resources and remotely gather data. The gathered data is stored in Azure Monitor Logs to enable easy aggregation,

filtering, and trend analysis. You can view the collected data from the SQL Insights workbook template, or you can delve directly into the data by using log queries.

Box 2: A Log Analytics workspace

Log Analytics workspaces

For the Log Analytics workspaces, you\\'re charged based on the pricing published on the Azure Monitor pricing page. The Log Analytics workspaces that SQL Insights uses will incur costs for data ingestion, data retention, and (optionally) data

export.

Reference:

https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-insights-overview

QUESTION 2

You deploy an instance of SQL Server on Azure Virtual Machines: named SQL1 that hosts multiple databases.

You configure the full recovery model for all the databases.

You perform a full backup of the master database on SQL1.

You need to a perform an additional backup of the master database on SQL1. The solution must minimize how long it takes to perform the backup.

Which type of backup should you perform?

A. log

B. full

C. differential

D. tail-log

Correct Answer: B

Answer is B. running differential/log backup will give you error:

Msg 3024, Level 16, State 0, Line 1

You can only perform a full backup of the master database. Use BACKUP DATABASE to back up the entire master database.

Msg 3013, Level 16, State 1, Line 1

BACKUP DATABASE is terminating abnormally.

QUESTION 3

You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The subscription contains 10 virtual machines that run Windows Server 2019 and host Microsoft SQL Server 2019 instances.

You need to ensure that you can manage the SQL Server instances by using a single user account.

What should you do first?

A. Enable a user-assigned managed identity on each virtual machine.

B. Deploy an Azure Active Directory Domain Services (Azure AD DS) domain and join the virtual machines to the domain.

C. Enable a system-assigned managed identity on each virtual machine.

D. Join the virtual machines to the Azure AD tenant.

Correct Answer: A

Benefits of using user-assigned managed identities (UMI) There are several benefits of using UMI as a server identity.

*

User flexibility to create and maintain their own user-assigned managed identities for a given tenant. UMI can be used as server identities for Azure SQL. UMI is managed by the user, compared to an SMI, which identity is uniquely defined per server, and assigned by the system.

*

Users can choose a specific UMI to be the server or instance identity for all SQL Databases or Managed Instances in the tenant, or have multiple UMIs assigned to different servers or instances. For example, different UMIs can be used in

different servers representing different features. For example, a UMI serving transparent data encryption in one server, and a UMI serving Azure AD authentication in another server.

*

Etc Reference: https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-azure-ad-user-assigned-managed-identity?view=azuresql

QUESTION 4

You have an Azure subscription that contains an instance of SQL Server on an Azure virtual machine named VM1 and an Azure Active Directory Domain Services (Azure AD DS) domain that contains two users named User1 and User 2.

On the default instance of SQL Server on VM1, you create a credential named Credential1 for User1.

You need to ensure that User2 can create a SQL Server Agent proxy that will use Credential1. The solution must use the principle of least privilege.

Which role should you assign to User2?

A. SQLAgentUserRole

B. SQLAgentReaderRole

C. SQLAgentOperatorRole

D. sysadmin

Correct Answer: D

Only members of the sysadmin fixed server role have permission to create, modify, or delete proxy accounts. Users who are not members of the sysadmin fixed server role must be added to one of the following SQL Server Agent fixed

database roles in the msdb database to use proxies: SQLAgentUserRole, SQLAgentReaderRole, or SQLAgentOperatorRole.

SQL Server Agent Fixed Database Roles

SQL Server has the following msdb database fixed database roles, which give administrators finer control over access to SQL Server Agent. The roles listed from least to most privileged access are:

SQLAgentUserRole

SQLAgentReaderRole

SQLAgentOperatorRole

Incorrect:

*

SQLAgentUserRole SQLAgentUserRole is the least privileged of the SQL Server Agent fixed database roles. It has permissions on only operators, local jobs, and job schedules. Members of SQLAgentUserRole have permissions on only local jobs and job schedules that they own. They cannot use multiserver jobs (master and target server jobs), and they cannot change job ownership to gain access to jobs that they do not already own.

*

SQLAgentReaderRole SQLAgentReaderRole Permissions SQLAgentReaderRole includes all the SQLAgentUserRole permissions as well as permissions to view the list of available multiserver jobs, their properties, and their history. Members of this role can also view the list of all available jobs and job schedules and their properties, not just those jobs and job schedules that they own. SQLAgentReaderRole members cannot change job ownership to gain access to jobs that they do not already own. Only the Jobs node in SQL Server Management Studio Object Explorer is visible to members of the SQLAgentReaderRole.

*

SQLAgentOperatorRole Permissions SQLAgentOperatorRole is the most privileged of the SQL Server Agent fixed database roles. It includes all the permissions of SQLAgentUserRole and SQLAgentReaderRole. Members of this role can also view properties for operators and proxies, and enumerate available proxies and alerts on the server.

Reference: https://learn.microsoft.com/en-us/sql/ssms/agent/create-a-sql-server-agent-proxy
https://learn.microsoft.com/en-us/sql/ssms/agent/sql-server-agent-fixed-database-roles

QUESTION 5

You have an Azure subscription that contains three instances of SQL Server on Azure Virtual Machines.

You plan to implement a disaster recovery solution.

You need to be able to perform disaster recovery drills regularly. The solution must meet the following requirements:

1.

Minimize administrative effort for the recovery drills.

2.

Isolate the recovery environment from the production environment What should you use?

A. native Microsoft SQL Server backup

B. Azure Site Recovery

C. Recovery Services vaults

D. Azure Backup

Correct Answer: B

Set up disaster recovery for SQL Server

You can protect the SQL Server back end of an application. You do so by using a combination of SQL Server business continuity and disaster recovery (BCDR) technologies and Azure Site Recovery.

SQL Server disaster recovery capabilities include:

Failover clustering

Always On availability groups

Database mirroring

Log shipping

Active geo-replication

Auto-failover groups

Note: Azure Recovery Services contributes to your BCDR strategy:

Site Recovery service: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site

to a secondary location. When an outage occurs at your primary site, you fail over to a secondary location, and access apps from there. After the primary location is running again, you can fail back to it.

Backup service: The Azure Backup service keeps your data safe and recoverable.

Site Recovery can manage replication for:

Azure VMs replicating between Azure regions Replication from Azure Public Multi-Access Edge Compute (MEC) to the region Replication between two Azure Public MECs On-premises VMs, Azure Stack VMs, and physical servers

Reference: https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-sql https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview