Vendor: Microsoft

Exam Code: AZ-305

Exam Name: Designing Microsoft Azure Infrastructure Solutions

Version: 13.01

Q & As: 209

Topic 1, Litware, Inc

Case Study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview
General Overview
Litware, Inc. is a medium-sized finance company.

Overview
Physical Locations
Litware has a main office in Boston.

Existing Environment
Identity Environment
The network contains an Active Directory forest named Litware.com that is linked to an Azure Active Directory (Azure AD) tenant named Litware.com. All users have Azure Active Directory Premium P2 licenses.

Litware has a second Azure AD tenant named dev.Litware.com that is used as a development environment.

The Litware.com tenant has a conditional acess policy named capolicy1. Capolicy1 requires that when users manage the Azure subscription for a production environment by using the Azure portal, they must connect from a hybrid Azure AD-joined device.

Existing Environment
Azure Environment
Litware has 10 Azure subscriptions that are linked to the Litware.com tenant and five Azure subscriptions that are linked to the dev.Litware.com tenant. All the subscriptions are in an Enterprise Agreement (EA).

The Litware.com tenant contains a custom Azure role-based access control (Azure RBAC) role named Role1 that grants the DataActions read permission to the blobs and files in Azure Storage.

Existing Environment

On-premises Environment
The on-premises network of Litware contains the resources shown in the following table.

Name	Type	Configuration
SERVER1 SERVER2 SERVER3	Ubuntu 18.04 vitual machines hosted on Hyper-V	The vitual machines host a third-party app named App1. App1 uses an external storage solution that provides Apache Hadoop-compatible data storage. The data storage supports POSIX access control list (ACL) file-level permissions.
SERVER10	Server that runs Windows Server 2016	The server contains a Microsoft SQL Server instance that hosts two databases named DB1 and DB2.

Existing Environment
Network Environment
Litware has ExpressRoute connectivity to Azure.

Planned Changes and Requirements
Planned Changes
Litware plans to implement the following changes:

- Migrate DB1 and DB2 to Azure.
- Migrate App1 to Azure virtual machines.
- Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

Planned Changes and Requirements
Authentication and Authorization Requirements
Litware identifies the following authentication and authorization requirements:

- Users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).
- The Network Contributor built-in RBAC role must be used to grant permission to all the virtual networks in all the Azure subscriptions.
- To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.
- Role1 must be used to assign permissions to the storage accounts of all the Azure subscriptions.
- RBAC roles must be applied at the highest level possible.

Planned Changes and Requirements
Resiliency Requirements
Litware identifies the following resiliency requirements:

Once migrated to Azure, DB1 and DB2 must meet the following requirements:

- Maintain availability if two availability zones in the local Azure region fail.
- Fail over automatically.
- Minimize I/O latency.

App1 must meet the following requirements:

- Be hosted in an Azure region that supports availability zones.
- Be hosted on Azure virtual machines that support automatic scaling.

- Maintain availability if two availability zones in the local Azure region fail.

Planned Changes and Requirements
Security and Compliance Requirements
Litware identifies the following security and compliance requirements:

- Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.
- On-premises users and services must be able to access the Azure Storage account that will host the data in App1.
- Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.
- All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.
- App1 must not share physical hardware with other workloads.

Planned Changes and Requirements
Business Requirements
Litware identifies the following business requirements:

- Minimize administrative effort.
- Minimize costs.

QUESTION 1
You plan to migrate App1 to Azure. The solution must meet the authentication and authorization requirements. Which type of endpoint should App1 use to obtain an access token?

A. Azure Instance Metadata Service (IMDS)
B. Azure AD
C. Azure Service Management
D. Microsoft identity platform

Correct Answer: D
Explanation:
Scenario: To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

QUESTION 2
You need to implement the Azure RBAC role assignments for the Network Contributor role. The solution must meet the authentication and authorization requirements. What is the minimum number of assignments that you must use?

A. 1
B. 2
C. 5
D. 10
E. 15