KillTest

품질은 좋고 서비스도 더욱 좋습니다

덤프

http://www.killtest.kr

우리는 고객에게 년 동안 무상업데이트 서비스를 제공합니다

Exam : **AZ-305**

Title : Designing Microsoft Azure Infrastructure Solutions

Version : DEMO

1.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.

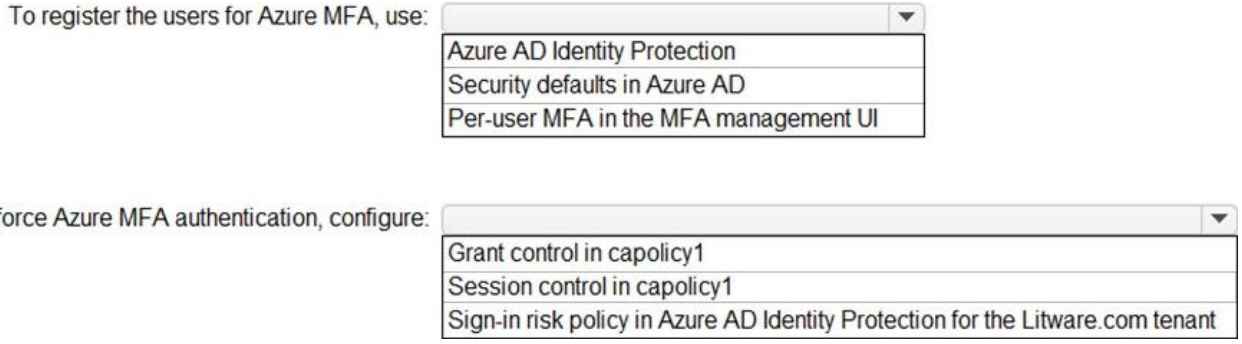
Planned Changes and Requirements. Security and Compliance Requirements
Litware identifies the following security and compliance requirements:
☞ Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period 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.

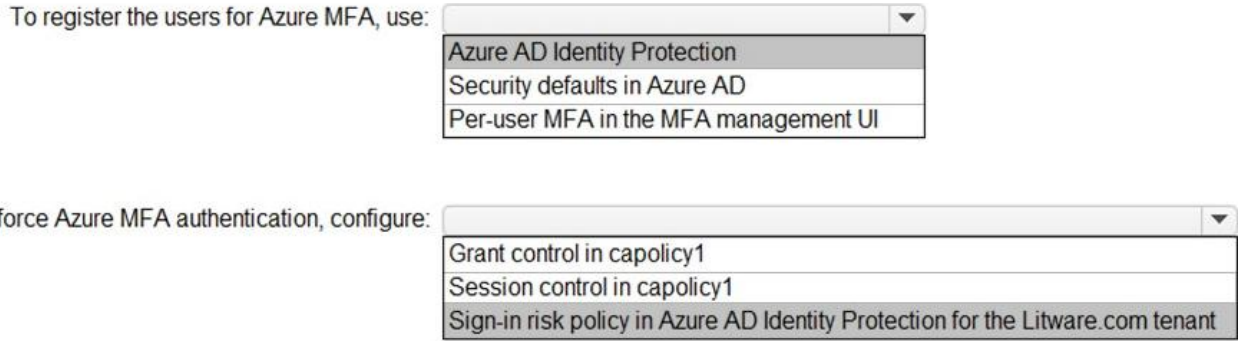
You plan to migrate App1 to Azure. The solution must meet the authentication and authorization requirements.
Which type of endpoint should App1 use to obtain an access token?
A. Azure Instance Metadata Service (IMDS)
B. Azure AD
C. Azure Service Management
D. Microsoft identity platform
Answer: D
Explanation:
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

2.HOTSPOT
You need to ensure that users managing the production environment are registered for Azure MFA and

must authenticate by using Azure MFA when they sign in to the Azure portal. The solution must meet the authentication and authorization requirements.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:

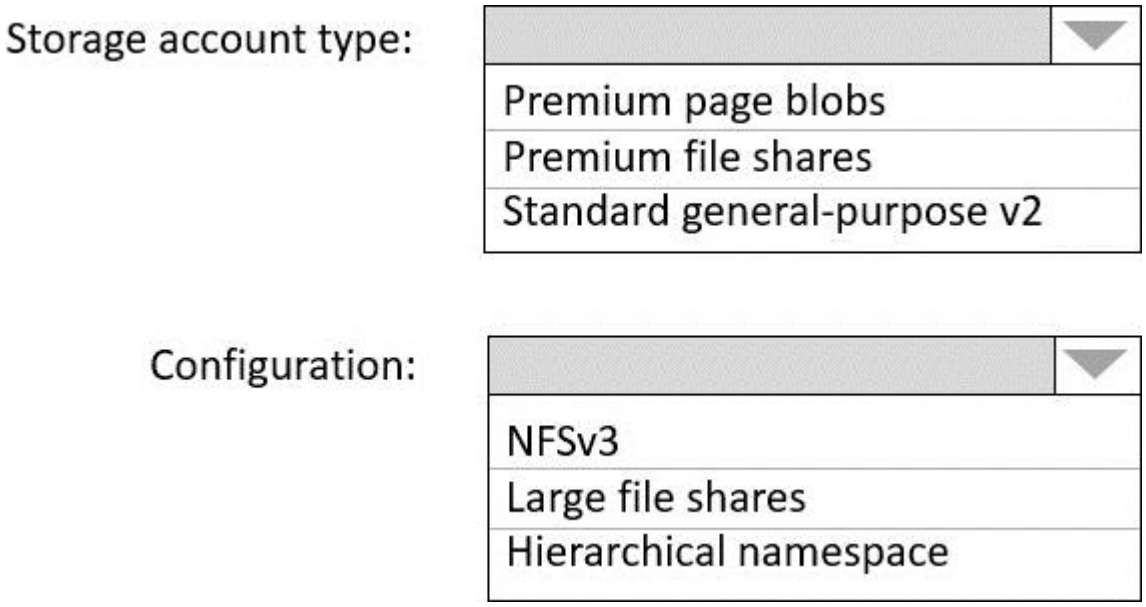


Explanation:
Graphical user interface, text, application
Description automatically generated
Box 1: Azure AD Identity Protection
Azure AD Identity Protection helps you manage the roll-out of Azure AD Multi-Factor Authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you are signing in to.
Scenario: 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).
Box 2: Sign-in risk policy...
Scenario: The Litware.com tenant has a conditional access 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.
Identity Protection policies we have two risk policies that we can enable in our directory.
- Sign-in risk policy
- User risk policy

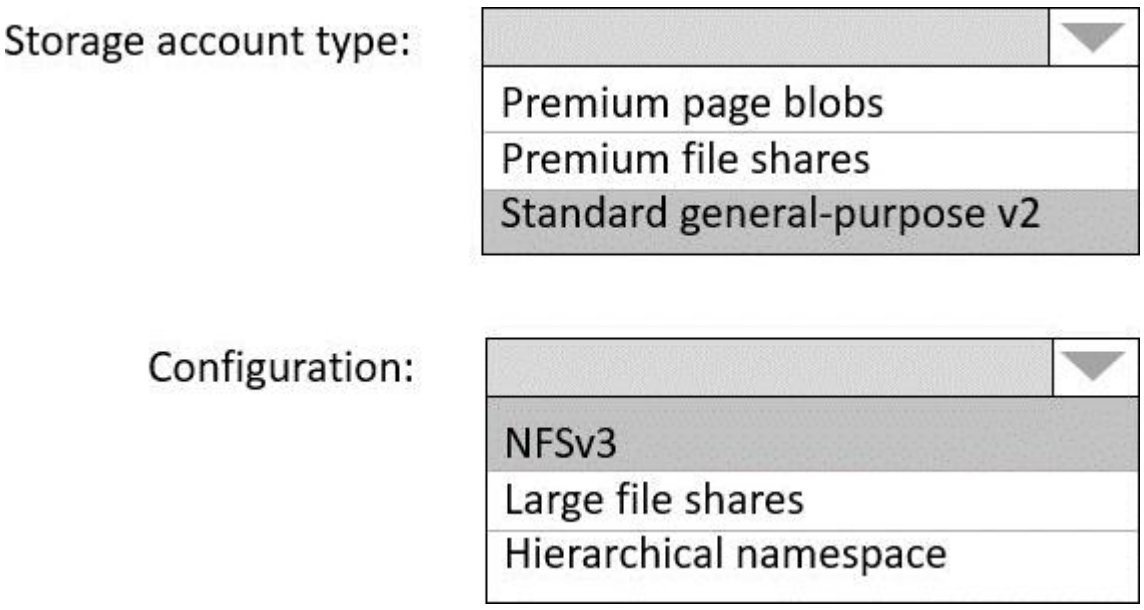
3.You migrate App1 to Azure. You need to ensure that the data storage for App1 meets the security and compliance requirement
What should you do?
A. Create an access policy for the blob

B. Modify the access level of the blob service.
C. Implement Azure resource locks.
D. Create Azure RBAC assignments.
Answer: A
Explanation:
Scenario: 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.
As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

4.HOTSPOT
You plan to migrate App1 to Azure.
You need to recommend a storage solution for App1 that meets the security and compliance requirements.
Which type of storage should you recommend, and how should you recommend configuring the storage? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Text, table

Description automatically generated

Box 1: Standard general-purpose v2

Standard general-purpose v2 supports Blob Storage.

Azure Storage provides data protection for Blob Storage and Azure Data Lake Storage Gen2.

Scenario:

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.

Box 2: NFSv3

Scenario: Plan: Migrate App1 to Azure virtual machines.

Blob storage now supports the Network File System (NFS) 3.0 protocol. This support provides Linux file system compatibility at object storage scale and prices and enables

Linux clients to mount a container in Blob storage from an Azure Virtual Machine (VM) or a computer on-premises.

5.HOTSPOT

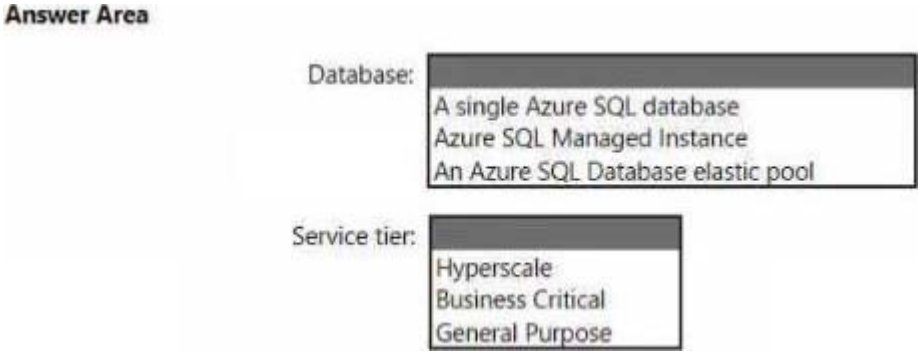
You plan to migrate DB1 and DB2 to Azure.

You need to ensure that the Azure database and the service tier meet the resiliency and business requirements.

What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each

correct selection is worth one point.

Answer Area



Answer:

Answer Area