

Case Study : 1

General Overview :-

ABC, Inc. is a medium-sized finance company.

Physical Locations :-

ABC company has a main office in Boston.

Existing Environment :- Identity Environment :-

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

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

The ABC.com.com tenant has a conditional access policy named policy1. policy1 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 :-

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

The ABC.com.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 ABC.com contains the resources shown in the following table.

Name	Type	Configuration
SERVER1 SERVER2 SERVER3	Ubuntu 18.04 virtual machines hosted on Hyper-V	The virtual 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 :-

ABC.com has ExpressRoute connectivity to Azure.

Planned Changes and Requirements:- Planned Changes :-

- ABC.com 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:-

- 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 :-

ABC.com identifies the following resiliency requirements:

1. 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.
2. 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.

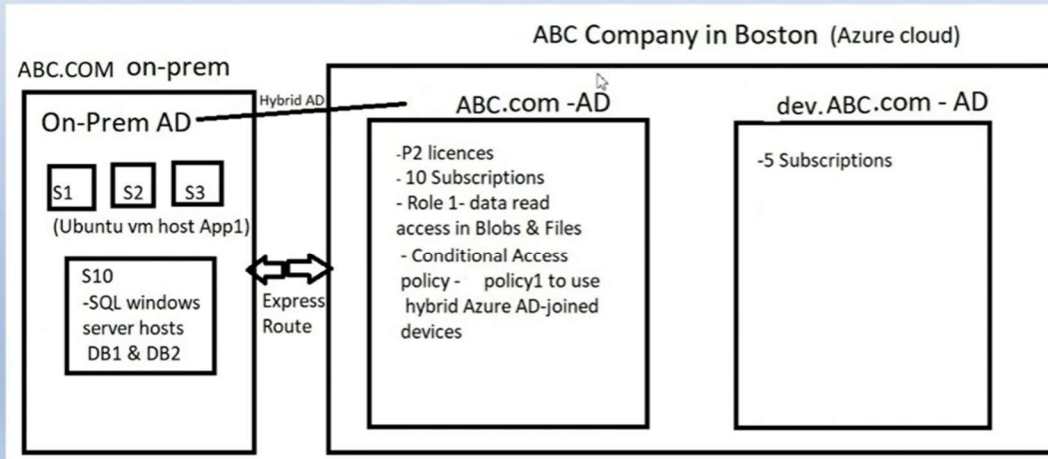
Planned Changes and Requirements:- Security and Compliance Requirements:-

- 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 :-

- Minimize administrative effort.
- Minimize costs.

Visualization of Case Study :-



Q.1. 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 register the users for Azure MFA, use :

1. Azure AD Identity Protection
2. Security defaults in Azure AD
3. Azure AD authentication methods policy

To enforce Azure MFA authentication, configure

1. Grant control in Policy1
2. Session control in Policy1
3. Sign-in risk policy in Azure AD Identity Protection

Q.1. 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 register the users for Azure MFA, use :

1. Azure AD Identity Protection ←
2. Security defaults in Azure AD
3. Azure AD authentication methods policy

To enforce Azure MFA authentication, configure

1. Grant control in Policy1 ←
2. Session control in Policy1
3. Sign-in risk policy in Azure AD Identity Protection

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).

Microsoft Azure

Search resources, services, and docs (G+)

Home > Identity Protection

Identity Protection | Multifactor authentication registration policy

Search

Dashboard (Preview)

Overview

Tutorials

Diagnose and solve problems

Protect

User risk policy

Sign-in risk policy

Multifactor authentication registration policy

Report

Risky users

Risky workload identities

Risky sign-ins

Risk detections

Settings

Users at risk detected alerts

Policy Name

Multifactor authentication registration policy

Assignments

Users

All users

Controls

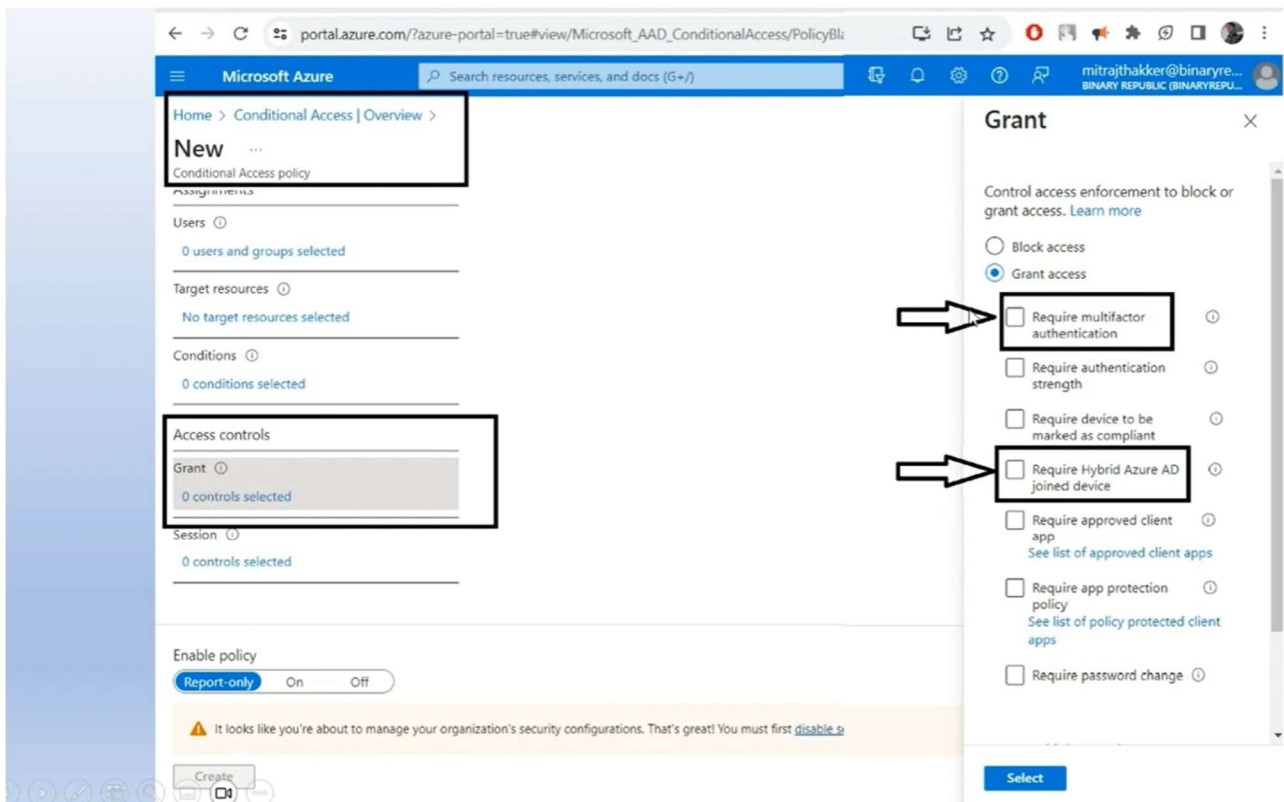
☒ Require Azure AD multifactor authentication registration

Policy enforcement

Enabled Disabled

Save

Multifactor authentication registration policy only affects cloud-based Azure multifactor authentication. If you have multifactor authentication...



Q.2. You need to recommend a network connectivity solution for the Azure Storage account that will host the App1.

- The solution must meet the security and compliance requirements.
What should you include in the recommendation?

Options:

- A. a private endpoint
- B. a service endpoint that has a service endpoint policy
- C. Azure public peering for an ExpressRoute circuit
- D. Microsoft peering for an ExpressRoute circuit

Scenario:


- 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.

Q.2. You need to recommend a network connectivity solution for the Azure Storage account that will host the App1.

- The solution must meet the security and compliance requirements.

What should you include in the recommendation?

Options:

- A. a private endpoint 
- B. a service endpoint that has a service endpoint policy
- C. Azure public peering for an ExpressRoute circuit
- D. Microsoft peering for an ExpressRoute circuit

Scenario:

- 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.

Explanation :- We already have Express-Route connection so from on-premises networks that connect to the VNet using ExpressRoutes with private-peering.

- Private Endpoint also secure your storage account by configuring the storage firewall to block all connections on the public endpoint for the storage service.

Q.3. 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?

Options:

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

Scenario:

- To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.

Q.3. 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?

Options:

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

Scenario:

- To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.

Explanation :-

- A managed identity, assigned by the system, can be enabled on the VM. You can also assign one or more user-assigned managed identities to the VM.
- You can then request tokens for managed identities from IMDS.
- Use these tokens to authenticate with other Azure services, such as Azure Key Vault.

The screenshot shows a web browser window with multiple tabs. The active tab is 'learn.microsoft.com/en-us/azure/virtual-machines/instance-metadata-service?tabs=windows#managed-identity'. The page title is 'Managed identity'. The main content area explains that a managed identity can be enabled on a VM and used to request tokens from IMDS. A sidebar on the left contains a 'Filter by title' search bar and a list of categories: Security, Updates and maintenance, and Monitoring. The Monitoring category is expanded, showing sub-items like 'Monitor virtual machines', 'Monitor virtual machine reference', 'Availability with Resource Graph', 'Tutorials', 'Monitor virtual machines guide', 'VM insights', and 'Azure Monitor Agent'. On the right, the 'Additional resources' section lists 'Documentation', 'az vm extension image', 'az vmss extension', 'az snapshot', and a 'Show 5 more' link.

Channel da x (305) YouTu x (305) az 30 x az-305 cas x SharePoint x Users - Mic x az-305 cas x Which type x Access tok x Azure Insta x +

learn.microsoft.com/en-us/azure/virtual-machines/instance-metadata-service?tabs=windows#managed-identity

Managed identity

A managed identity, assigned by the system, can be enabled on the VM. You can also assign one or more user-assigned managed identities to the VM. You can then request tokens for managed identities from IMDS. Use these tokens to authenticate with other Azure services, such as Azure Key Vault.

For detailed steps to enable this feature, see [Acquire an access token](#).

Load Balancer Metadata

When you place virtual machine or virtual machine set instances behind an Azure Standard Load Balancer, you can use IMDS to retrieve metadata related to the load balancer and the instances. For more information, see [Retrieve load balancer information](#).

Additional resources

- [Documentation](#)
- [az vm extension image](#)
- [az vmss extension](#)
- [az snapshot](#)
- [Show 5 more](#)




Q.4. You need to configure an Azure policy to ensure that the Azure SQL databases have TDE enabled. The solution must meet the security and compliance requirements. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Options:-

1. Create an Azure policy definition that uses the deployIfNotExists effect.
2. Invoke a remediation task.
3. Create an Azure policy definition that uses the modify effect.
4. Create an Azure policy assignment.
5. Create a user assigned managed identity.

Q.4. You need to configure an Azure policy to ensure that the Azure SQL databases have TDE enabled. The solution must meet the security and compliance requirements. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Options:-

1. Create an Azure policy definition that uses the deployIfNotExists effect. 
2. Invoke a remediation task. 
3. Create an Azure policy definition that uses the modify effect.
4. Create an Azure policy assignment. 
5. Create a user assigned managed identity.

Answer in correct order :-

1. Create an Azure policy definition that uses the deployIfNotExists effect.
2. Create an Azure policy assignment.
3. Invoke a remediation task.

Q.5. You plan to migrate App1 to Azure.

You need to recommend a high-availability solution for App1. The solution must meet the resiliency requirements. What should you include in the recommendation?

To answer, select the appropriate options in the answer area.

Answer Area :-

Number of Host Groups :

1
2
3
6

Number of Virtual Machine Scale sets:

0
1
3

Scenario : Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

- App1 must maintain availability if two availability zones in the local Azure region fail.
- Be hosted in an Azure region that supports availability zones.
- Be hosted on Azure virtual machines that support automatic scaling.

Q.5. You plan to migrate App1 to Azure.

You need to recommend a high-availability solution for App1. The solution must meet the resiliency requirements. What should you include in the recommendation?

To answer, select the appropriate options in the answer area.

Answer Area :-

Number of Host Groups :

1
2
3
6



Number of Virtual Machine Scale sets:

0
1
3



Scenario : Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

- App1 must maintain availability if two availability zones in the local Azure region fail.
- Be hosted in an Azure region that supports availability zones.
- Be hosted on Azure virtual machines that support automatic scaling.

Q.6. You plan to migrate App1 to Azure. You need to estimate the compute costs for App1 in Azure. The solution must meet the security and compliance requirements. What should you use to estimate the costs, and what should you implement to minimize the costs? To answer, select the appropriate options in the answer area.

Answer Area :-

To estimate the costs, use :

1. Azure Advisor
2. The Azure cost management Power BI app
3. The Azure total cost of ownership


Implement :-

1. Azure Reservations
2. Azure Hybrid Benefit
3. Azure Spot virtual machine pricing


Q.6. You plan to migrate App1 to Azure. You need to estimate the compute costs for App1 in Azure. The solution must meet the security and compliance requirements. What should you use to estimate the costs, and what should you implement to minimize the costs? To answer, select the appropriate options in the answer area.

Answer Area :-

To estimate the costs, use :

1. Azure Advisor
2. The Azure cost management Power BI app
3. The Azure total cost of ownership 

Implement :-

1. Azure Reservations 
2. Azure Hybrid Benefit
3. Azure Spot virtual machine pricing

Explanation :-

1st Answer :- Azure Total Cost of Ownership calculator. TCO can estimate the cost savings you can realize by migrating your workloads to Azure.

2nd Answer:- Azure Hybrid benefit: save up to 40% on VM

Azure Reserved Instances : save up to 72%

So Azure Reservation is a preferred choice.

Q.7. 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?

Answer Area :-

Storage Account Type :

1. Premium Page Blobs.
2. Premium file shares.
3. Standard general purpose V2.

Configuration :-


1. NFSv3.
2. Large file shares.
3. Hierarchical namespace.

Q.7. 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?

Answer Area :-

Storage Account Type :

1. Premium Page Blobs.
2. Premium file shares.
3. Standard general purpose V2. 

Configuration :-

1. NFSv3.
2. Large file shares.
3. Hierarchical namespace. 

Explanation : -

Standard general-purpose v2 supports Blob Storage. Azure Storage provides data protection for Blob Storage (we need to prevent modification to data for 3 years)

In addition we need Hierarchical Namespace because VMs that need access to the storage account use POSIX ACL file-level permissions storage. (On prem server1, server2, server3 configuration)

Q.8. 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?

Options:

- 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.


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.

Q.8. 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?

Options:

- 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.

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.

Explanation :-

- Immutable storage for Azure Blob Storage enables users to store data in a WORM (Write Once, Read Many) state. While in a WORM state, data cannot be modified or deleted for a user-specified interval.
- By configuring immutability policies for blob data, you can protect your data from overwrites and deletes.

Q.9. How should the migrated databases DB1 and DB2 be implemented in Azure?

Answer Area:

Database :

1. A single Azure SQL database
2. Azure SQL managed instance
3. An Azure SQL database elastic pool

Service Tier :

1. Hyperscale
2. Business Critical
3. General Purpose


Scenario :- 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.


Q.9. How should the migrated databases DB1 and DB2 be implemented in Azure?

Answer Area:

Database :

1. A single Azure SQL database
2. Azure SQL managed instance 
3. An Azure SQL database elastic pool

Service Tier :

1. Hyperscale
2. Business Critical 
3. General Purpose

Scenario :- 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.

Explanation : -

- Azure SQL managed instance provide auto fail over groups to provide availability requirement stated above.
- Business Critical service tier provide low I/O latency.

Q.10. 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?

Options:


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

Scenario :-

- The Network Contributor built-in RBAC role must be used to grant permission to all the virtual networks in all the Azure subscriptions.
- RBAC roles must be applied at the highest level possible.

Q.10. 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?

Options:

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

Scenario :-

- The Network Contributor built-in RBAC role must be used to grant permission to all the virtual networks in all the Azure subscriptions.
- RBAC roles must be applied at the highest level possible.

Explanation :-

- We have two tenants ABC.com and dev.ABC.com so minimum two assignments at management group level is required.