



# AZ-305<sup>Q&As</sup>

Designing Microsoft Azure Infrastructure Solutions

**Pass Microsoft AZ-305 Exam with 100% Guarantee**

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

<https://www.pass4itsure.com/az-305.html>

100% Passing Guarantee  
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





**QUESTION 1**

**HOTSPOT**

You plan to deploy an Azure web app named App1 that will use Azure Active Directory (Azure AD) authentication.

App1 will be accessed from the internet by the users at your company. All the users have computers that run Windows 10 and are joined to Azure AD.

You need to recommend a solution to ensure that the users can connect to App1 without being prompted for authentication and can access App1 only from company-owned computers.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

The users can connect to App1 without being prompted for authentication:

	▼
An Azure AD app registration	
An Azure AD managed identity	
Azure AD Application Proxy	

The users can access App1 only from company-owned computers:

	▼
A Conditional Access policy	
An Azure AD administrative unit	
Azure Application Gateway	
Azure Blueprints	
Azure Policy	

Correct Answer:



### Answer Area

The users can connect to App1 without being prompted for authentication:

	▼
An Azure AD app registration	
An Azure AD managed identity	
Azure AD Application Proxy	

The users can access App1 only from company-owned computers:

	▼
A Conditional Access policy	
An Azure AD administrative unit	
Azure Application Gateway	
Azure Blueprints	
Azure Policy	

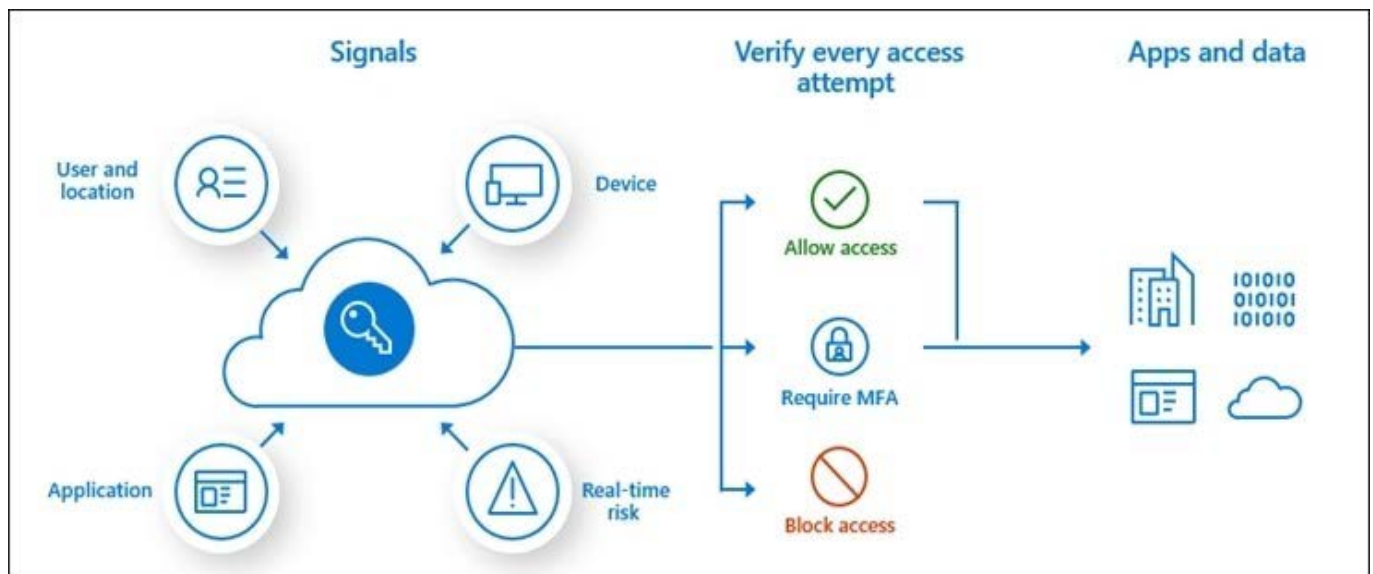
Box 1: An Azure AD app registration

Azure active directory (AD) provides cloud based directory and identity management services. You can use azure AD to manage users of your application and authenticate access to your applications using azure active directory. You register your application with Azure active directory tenant.

Box 2: A conditional access policy

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.



**QUESTION 2**

You have an application that is used by 6,000 users to validate their vacation requests. The application manages its own credential

Users must enter a username and password to access the application. The application does NOT support identity providers.

You plan to upgrade the application to use single sign-on (SSO) authentication by using an Azure Active Directory (Azure AD) application registration.

Which SSO method should you use?

- A. password-based
- B. OpenID Connect
- C. header-based
- D. SAML

Correct Answer: A

---

**QUESTION 3**

Your company plans to use a separate Azure subscription for each of its business units. You identify the following governance requirements:

1.

Each business unit will analyze costs for different workloads such as production, development, and testing.

2.

The company will analyze costs by business unit and workload. What should you use to meet the governance requirements?

- A. Azure Advisor alerts and Azure Logic Apps
- B. Microsoft Intune and compliance policies
- C. Azure management groups and RBAC
- D. tags and Azure Policy

Correct Answer: D

---

**QUESTION 4**

You are developing an app that will read activity logs for an Azure subscription by using Azure Functions.



You need to recommend an authentication solution for Azure Functions. The solution must minimize administrative effort.

What should you include in the recommendation?

- A. an enterprise application in Azure AD
- B. system-assigned managed identities
- C. shared access signatures (SAS)
- D. application registration in Azure AD

Correct Answer: B

Azure App Service provides built-in authentication and authorization capabilities (sometimes referred to as "Easy Auth"), so you can sign in users and access data by writing minimal or no code in your web app, RESTful API, and mobile back end, and also Azure Functions.

Azure App Service provides built-in authentication and authorization capabilities (sometimes referred to as "Easy Auth"), so you can sign in users and access data by writing minimal or no code in your web app, RESTful API, and mobile back end, and also Azure Functions.

\*

Microsoft Identity Platform

\*

Facebook

\*

Google

\*

Twitter

\*

Any OpenID Connect provider

Note:

A managed identity from Azure Active Directory (Azure AD) allows your app to easily access other Azure AD-protected resources such as Azure Key Vault. The identity is managed by the Azure platform and does not require you to provision

or rotate any secrets. For more about managed identities in Azure AD, see [Managed identities for Azure resources](#).

Your application can be granted two types of identities:

A system-assigned identity is tied to your application and is deleted if your app is deleted. An app can only have one system-assigned identity. A user-assigned identity is a standalone Azure resource that can be assigned to your app. An app



can have multiple user-assigned identities.

Reference: <https://learn.microsoft.com/en-us/azure/app-service/overview-authentication-authorization>

<https://learn.microsoft.com/en-us/azure/app-service/overview-managed-identity>

---

## QUESTION 5

### HOTSPOT

You have the Azure subscriptions shown in the following table.

Name	Location	Azure AD tenant
Sub1	East US	contoso.onmicrosoft.com
Sub2	East US	contoso-recovery.onmicrosoft.com

Contoso.onmicrosoft.com contains a user named User1.

You need to deploy a solution to protect against ransomware attacks. The solution must meet the following requirements:

1.

Ensure that all the resources in Sub1 are backed up by using Azure Backup.

2.

Require that User1 first be assigned a role for Sub2 before the user can make major changes to the backup configuration.

What should you create in each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



### Answer Area

Sub1:

A Recovery Services vault
A Resource Guard
An Azure Site Recovery job
Microsoft Azure Backup Server (MABS)
The Microsoft Azure Recovery Services (MARS) agent

Sub2:

A Recovery Services vault
A Resource Guard
An Azure Site Recovery job
Microsoft Azure Backup Server (MABS)
The Microsoft Azure Recovery Services (MARS) agent

Correct Answer:

### Answer Area

Sub1:

A Recovery Services vault
A Resource Guard
An Azure Site Recovery job
Microsoft Azure Backup Server (MABS)
The Microsoft Azure Recovery Services (MARS) agent

Sub2:

A Recovery Services vault
A Resource Guard
An Azure Site Recovery job
Microsoft Azure Backup Server (MABS)
The Microsoft Azure Recovery Services (MARS) agent

Box 1: A Recovery Services vault

Ensure that all the resources in Sub1 are backed up by using Azure Backup.



A Recovery Services vault is an entity that stores the backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

Azure Backup automatically handles storage for the vault.

Box 2: A Resource Guard

Require that User1 first be assigned a role for Sub2 before the user can make major changes to the backup configuration.

A Resource Guard is an Azure resource that can be created in the same subscription, a different subscription in the same Azure AD tenant, or even a subscription in a different Azure AD tenant! When associated to an RSV (Recovery Service

Vault), a user looking to make risky modifications to it (such as removing soft delete) must have permissions on BOTH the Resource Guard and the RSV. This means it can support separate authorization boundaries at the subscription level or

even completely separate identity and authentication boundaries at the tenant.

Reference:

<https://learn.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview>

<https://journeyofthegEEK.com/2022/10/18/protecting-azure-backups-with-resource-guard-part-1/>

[AZ-305 PDF Dumps](#)

[AZ-305 VCE Dumps](#)

[AZ-305 Exam Questions](#)