Question #10 *Topic 2*

HOTSPOT -

Your company has 20 web APIs that were developed in-house.

The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company's Azure Active Directory (Azure

AD) tenant. The web APIs are published by using Azure API Management.

You need to recommend a solution to block unauthorized requests originating from the web apps from reaching the web APIs. The solution must meet the following requirements:

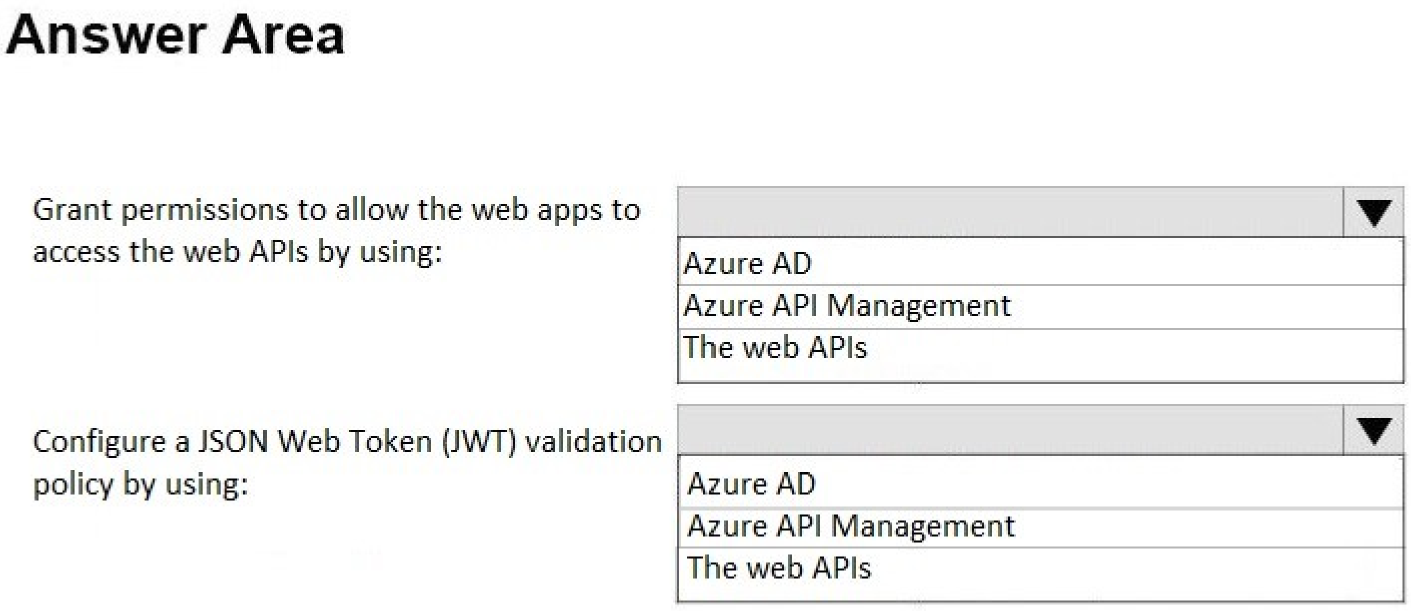
⇨ Use Azure AD-generated claims.

⇨ Minimize configuration and management effort.

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

NOTE: Each correct selection is worth one point.

Hot Area:

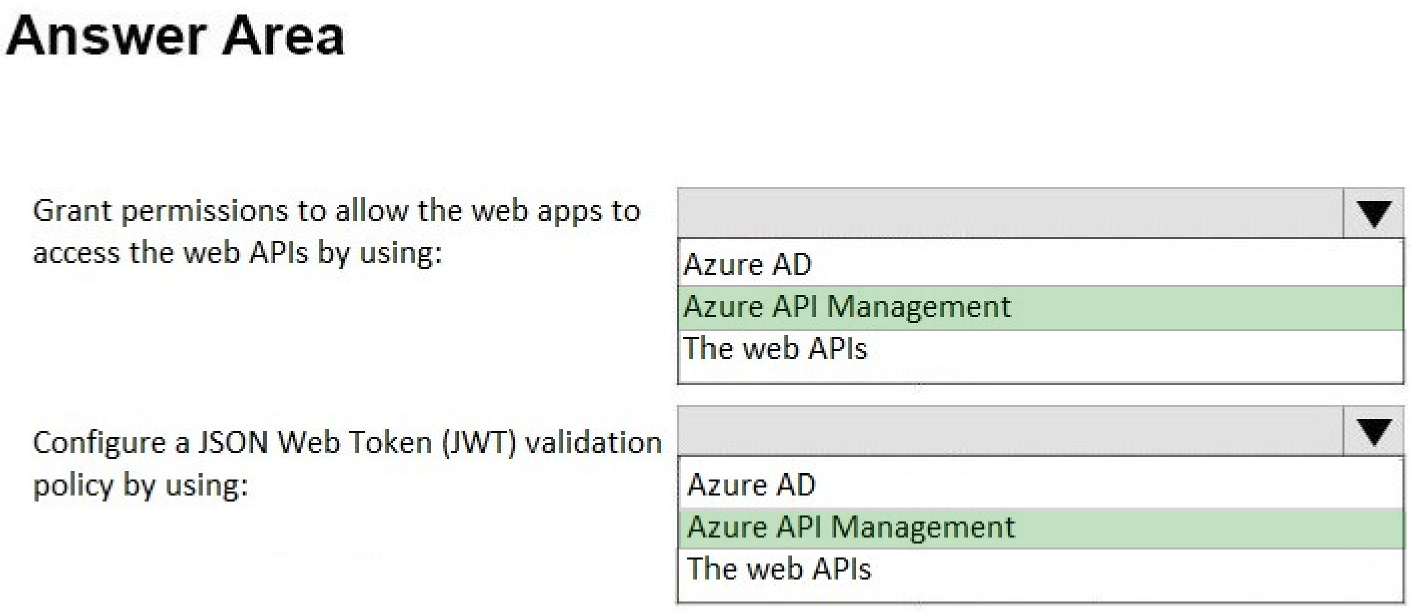


Answer Area

Grant permissions to allow the web apps to access the web APIs by using:
- Azure AD
- Azure API Management
- The web APIs

Configure a JSON Web Token (JWT) validation policy by using:
- Azure AD
- Azure API Management
- The web APIs

Correct Answer:



Answer Area

Grant permissions to allow the web apps to access the web APIs by using:
- Azure AD
- [✓ Azure API Management]
- The web APIs

Configure a JSON Web Token (JWT) validation policy by using:
- Azure AD
- [✓ Azure API Management]
- The web APIs

Question #11 *Topic 2*

HOTSPOT -

You are designing an access policy for the sales department at your company.

Occasionally, the developers at the company must stop, start, and restart Azure virtual machines. The development team changes often.

You need to recommend a solution to provide the developers with the required access to the virtual machines. The solution must meet the following requirements:

➾ Provide permissions only when needed.

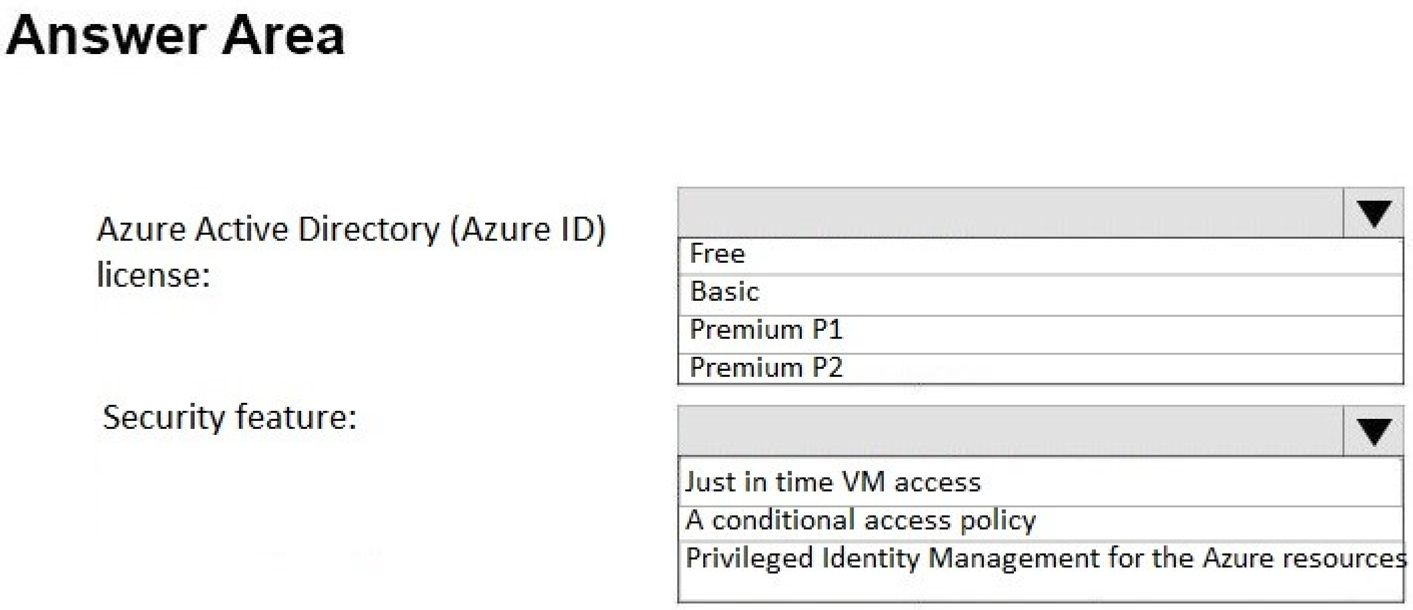
➾ Use the principle of least privilege.

➾ Minimize costs.

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

NOTE: Each correct selection is worth one point.

Hot Area:

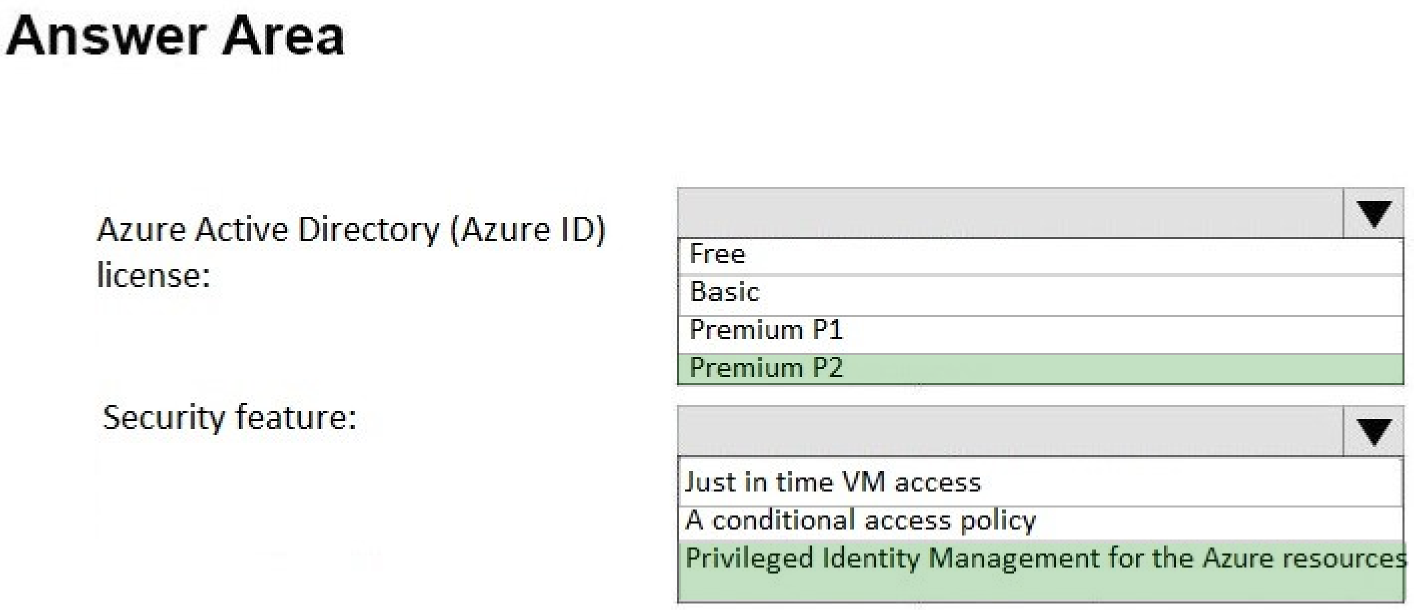


Answer Area

Azure Active Directory (Azure ID) license:
- Free
- Basic
- Premium P1
- Premium P2

Security feature:
- Just in time VM access
- A conditional access policy
- Privileged Identity Management for the Azure resources

Correct Answer:



Answer Area

Azure Active Directory (Azure ID) license:
- Free
- Basic
- Premium P1
- [✓ Premium P2]

Security feature:
- Just in time VM access
- A conditional access policy
- [✓ Privileged Identity Management for the Azure resources]

Question #12 *Topic 2*

Your network contains an on-premises Active Directory forest.

You discover that when users change jobs within your company, the membership of the user groups are not being updated. As a result, the users can access resources that are no longer relevant to their job.

You plan to integrate Active Directory and Azure Active Directory (Azure AD) by using Azure AD Connect.

You need to recommend a solution to ensure that group owners are emailed monthly about the group memberships they manage.

What should you include in the recommendation?

A. Azure AD access reviews

B. Tenant Restrictions

C. Azure AD Identity Protection

D. conditional access policies

Correct Answer: *A*

References:

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

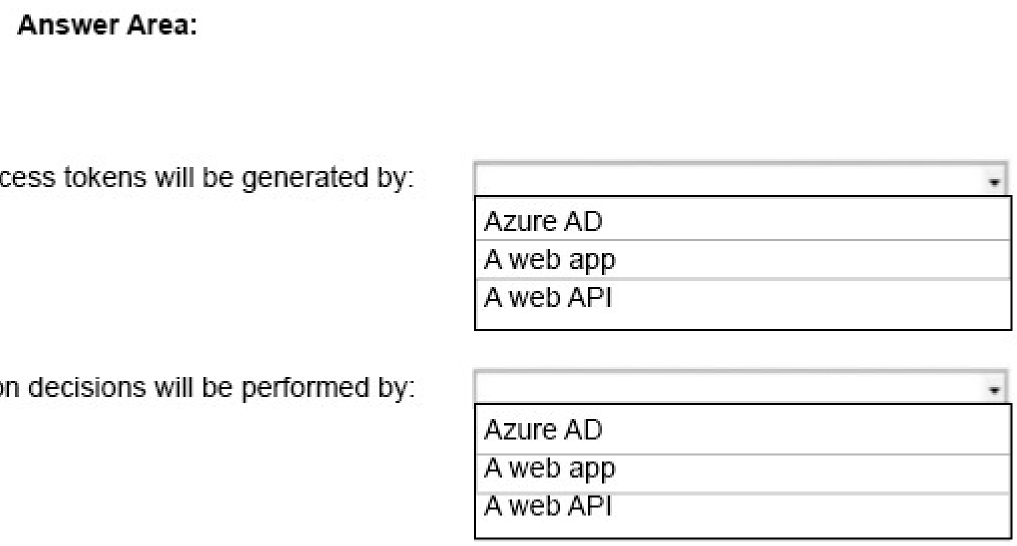
Question #13 *Topic 2*

HOTSPOT -

You are designing a software as a service (SaaS) application that will enable Azure Active Directory (Azure AD) users to create and publish surveys. The SaaS application will have a front-end web app and a back-end web API. The web app will rely on the web API to handle updates to customer surveys.

You need to design an authorization flow for the SaaS application. The solution must meet the following requirements:

✑ To access the back-end web API, the web app must authenticate by using OAuth 2 bearer tokens.
✑ The web app must authenticate by using the identities of individual users.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

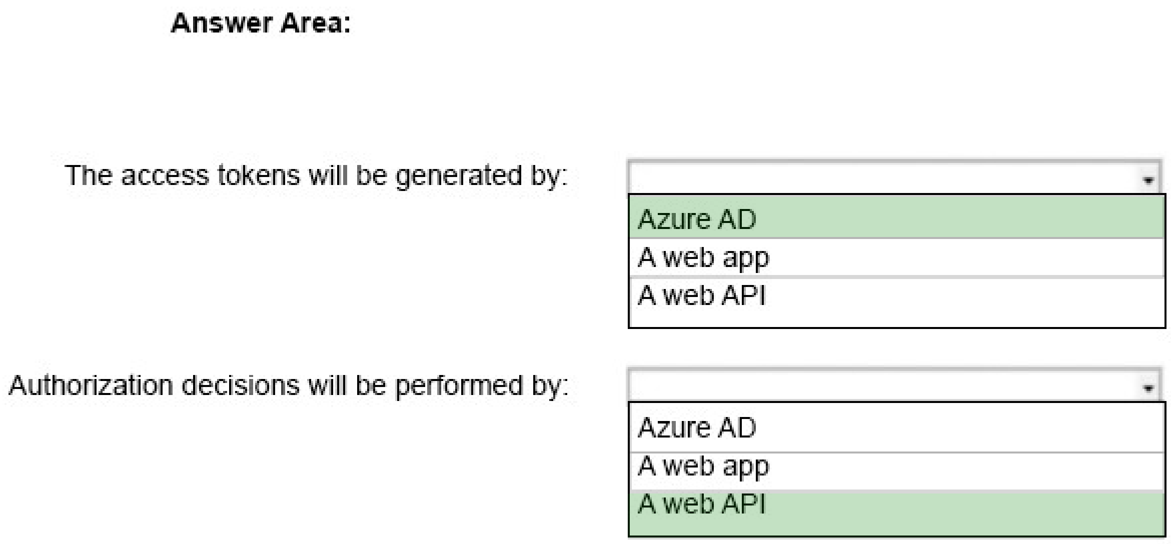


Answer Area:

The access tokens will be generated by:
- Azure AD
- A web app
- A web API

Authorization decisions will be performed by:
- Azure AD
- A web app
- A web API

Correct Answer:



Answer Area:

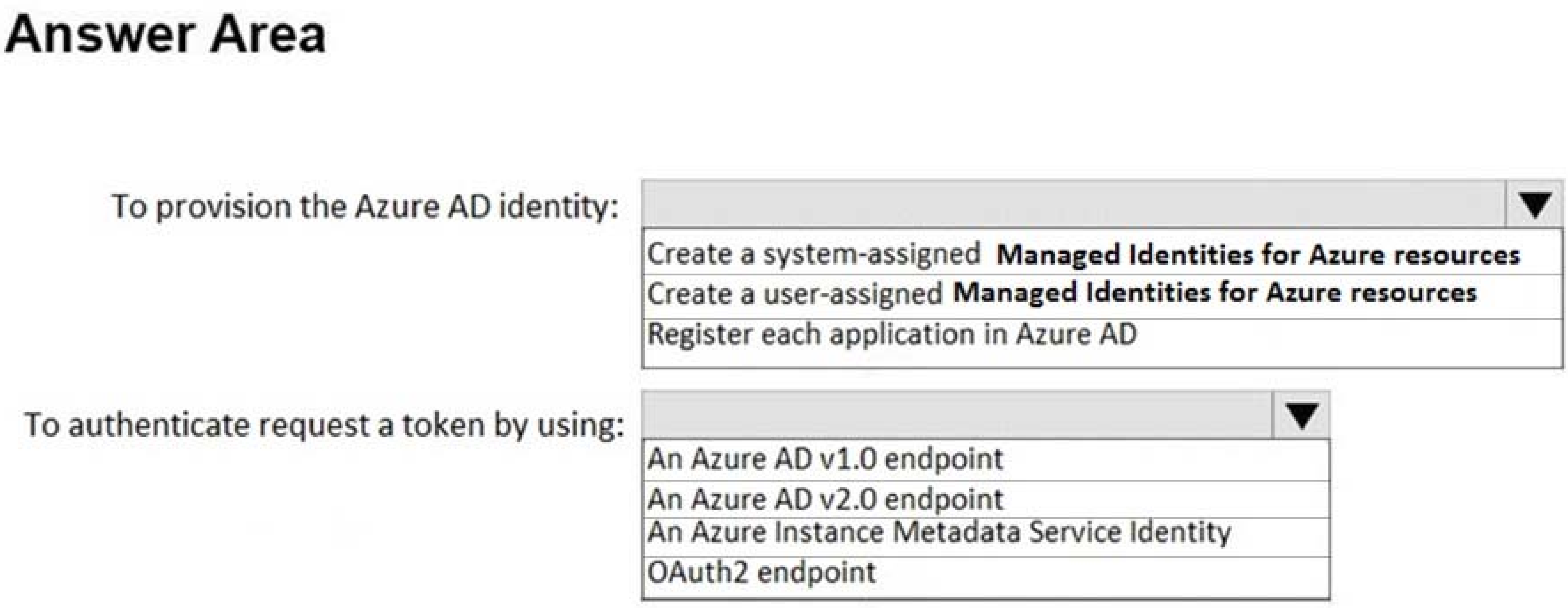
The access tokens will be generated by:
- [✓ Azure AD]
- A web app
- A web API

Authorization decisions will be performed by:
- Azure AD
- A web app
- [✓ A web API]

References:
https://docs.microsoft.com/lb-lu/azure/architecture/multitenant-identity/web-api https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v1-dotnet-webapi

Question #14 *Topic 2*

HOTSPOT -
You have five .NET Core applications that run on 10 Azure virtual machines in the same subscription.
You need to recommend a solution to ensure that the applications can authenticate by using the same Azure Active Directory (Azure AD) identity.
The solution must meet the following requirements:
✑ Ensure that the applications can authenticate only when running on the 10 virtual machines.
✑ Minimize administrative effort.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

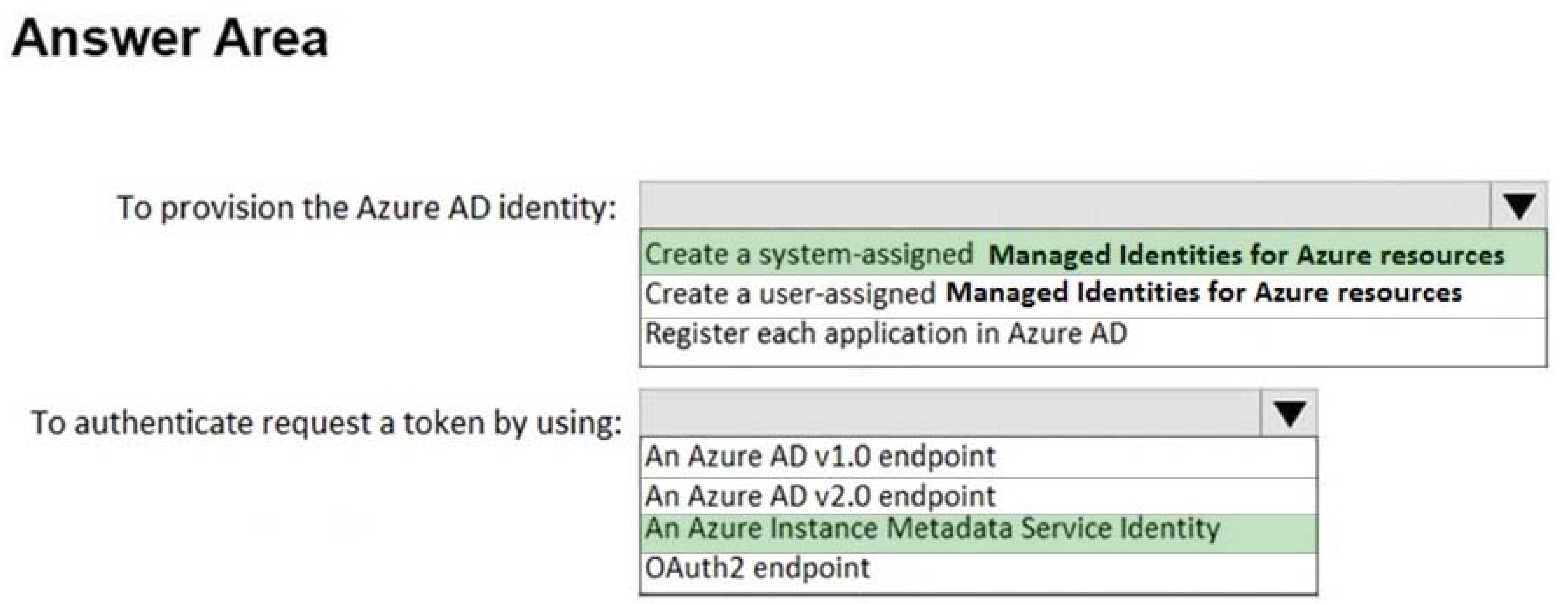


Answer Area

To provision the Azure AD identity:
- Create a system-assigned **Managed Identities for Azure resources**
- Create a user-assigned **Managed Identities for Azure resources**
- Register each application in Azure AD

To authenticate request a token by using:
- An Azure AD v1.0 endpoint
- An Azure AD v2.0 endpoint
- An Azure Instance Metadata Service Identity
- OAuth2 endpoint

Correct Answer:



Answer Area

To provision the Azure AD identity: ▼

- [✓ Create a system-assigned **Managed Identities for Azure resources**]
- Create a user-assigned **Managed Identities for Azure resources**
- Register each application in Azure AD

To authenticate request a token by using: ▼

- An Azure AD v1.0 endpoint
- An Azure AD v2.0 endpoint
- [✓ An Azure Instance Metadata Service Identity]
- OAuth2 endpoint

← Previous Questions

Next Questions →