AZ-500 Q&As

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

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

https://www.pass2lead.com/az-500.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

SIMULATION

You need to create a new Azure Active Directory (Azure AD) directory named 10317806.onmicrosoft.com. The new directory must contain a user named user10317806 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

A. See the explanation below.

Correct Answer: A

To create a new Azure AD tenant:

1.

Browse to the Azure portal and sign in with an account that has an Azure subscription.

2.

Select the plus icon (+) and search for Azure Active Directory.

3.

Select Azure Active Directory in the search results.

4.

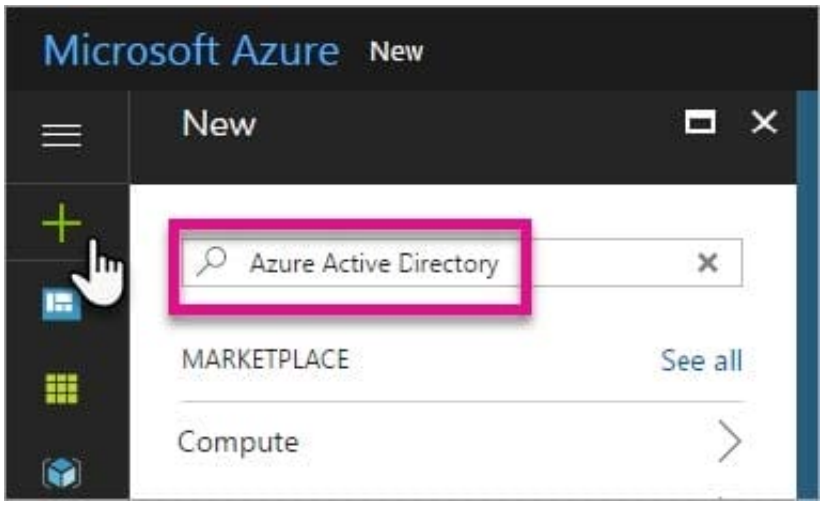
Select Create.

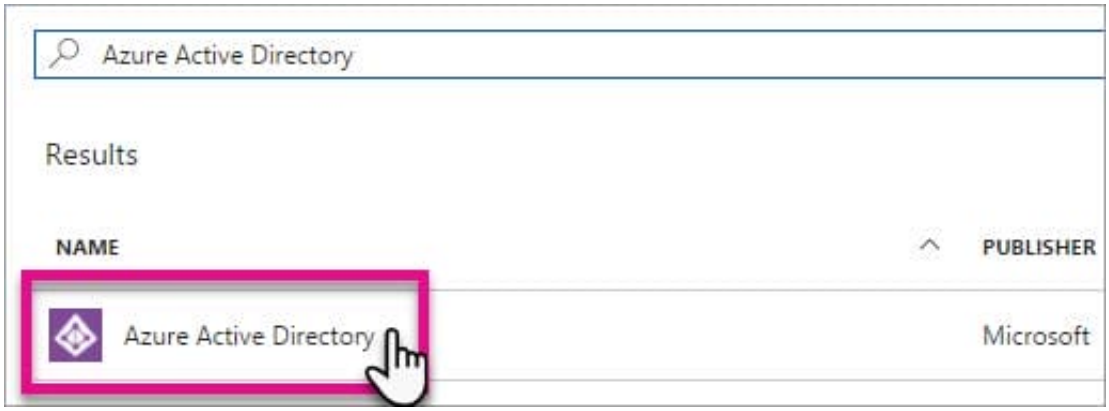
5.

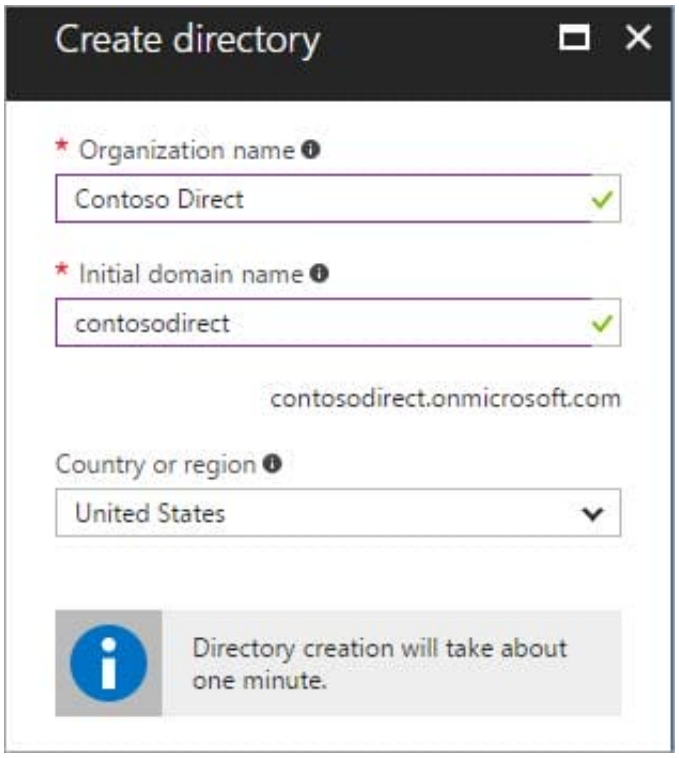
Provide an Organization name (10317806) and an Initial domain name (10317806). Then select Create. This will create the directory named 10317806.onmicrosoft.com.

6.

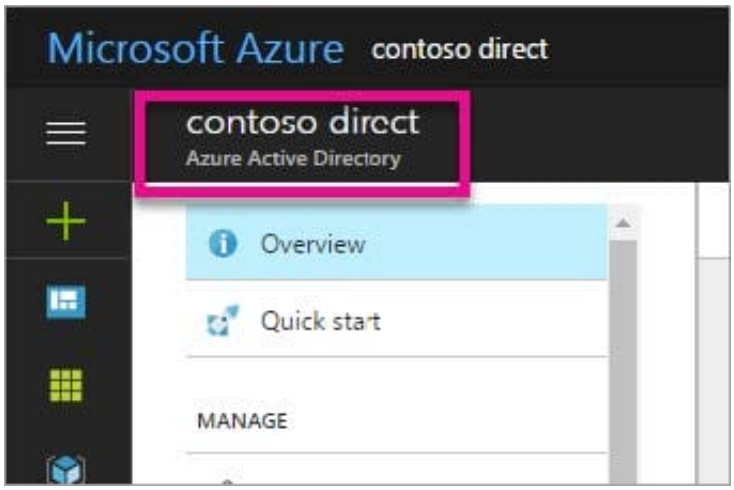
After directory creation is complete, select the information box to manage your new directory. To create the user:







1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.

2.

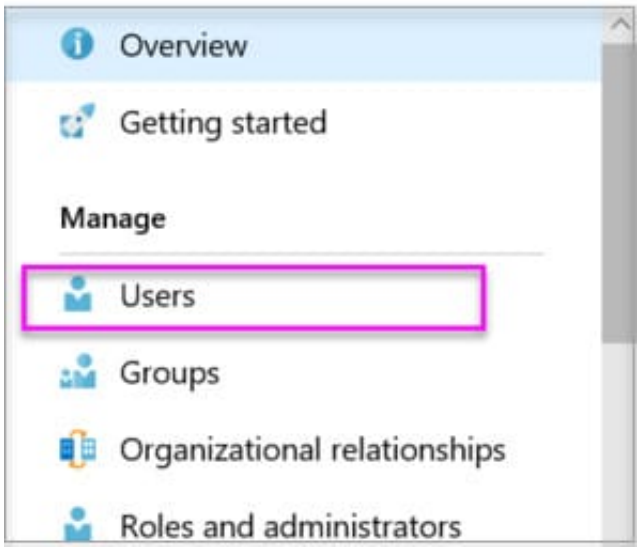
Under Manage, select Users.

3.

Select All users and then select + New user.

4.

Provide a Name and User name (user10317806) for the user. When you\\'re done, select Create.



To enable MFA:

1.

In the Azure portal, make sure you are on the Azure Active Directory fly out.

2.

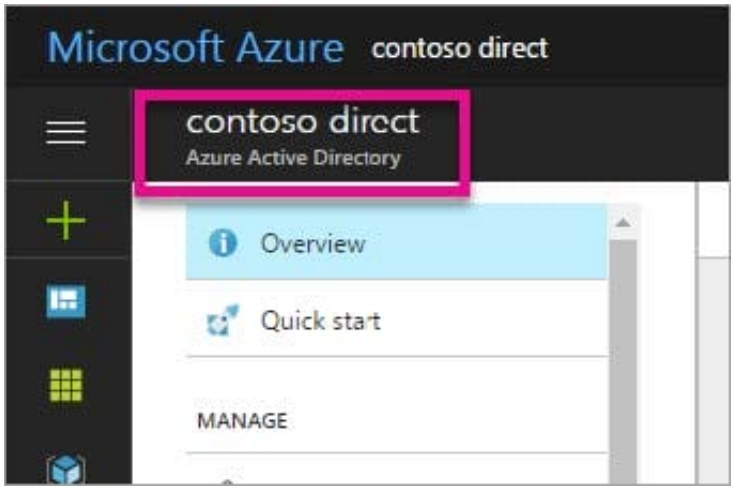
Under Manage, select Users.

3.

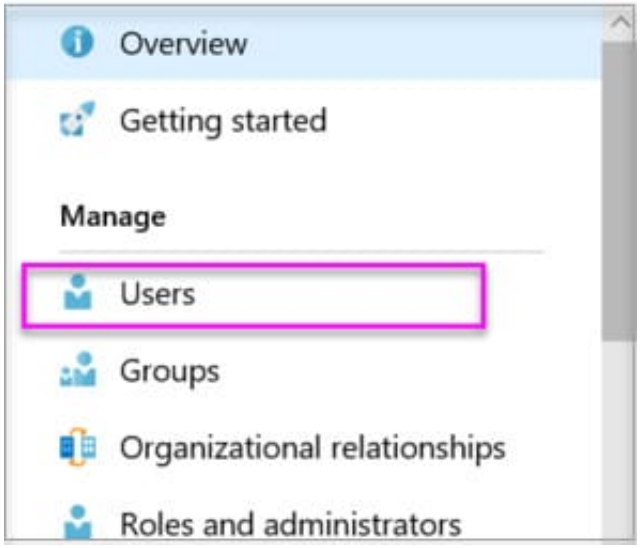
Click on the Multi-Factor Authentication link.

4.

Tick the checkbox next to the user\\'s name and click the Enable link.



If not, select the Azure Active Directory icon from the left services navigation.



Reference: https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

QUESTION 2

HOTSPOT

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.

Query1 returns a subset of security events generated by Azure AD.

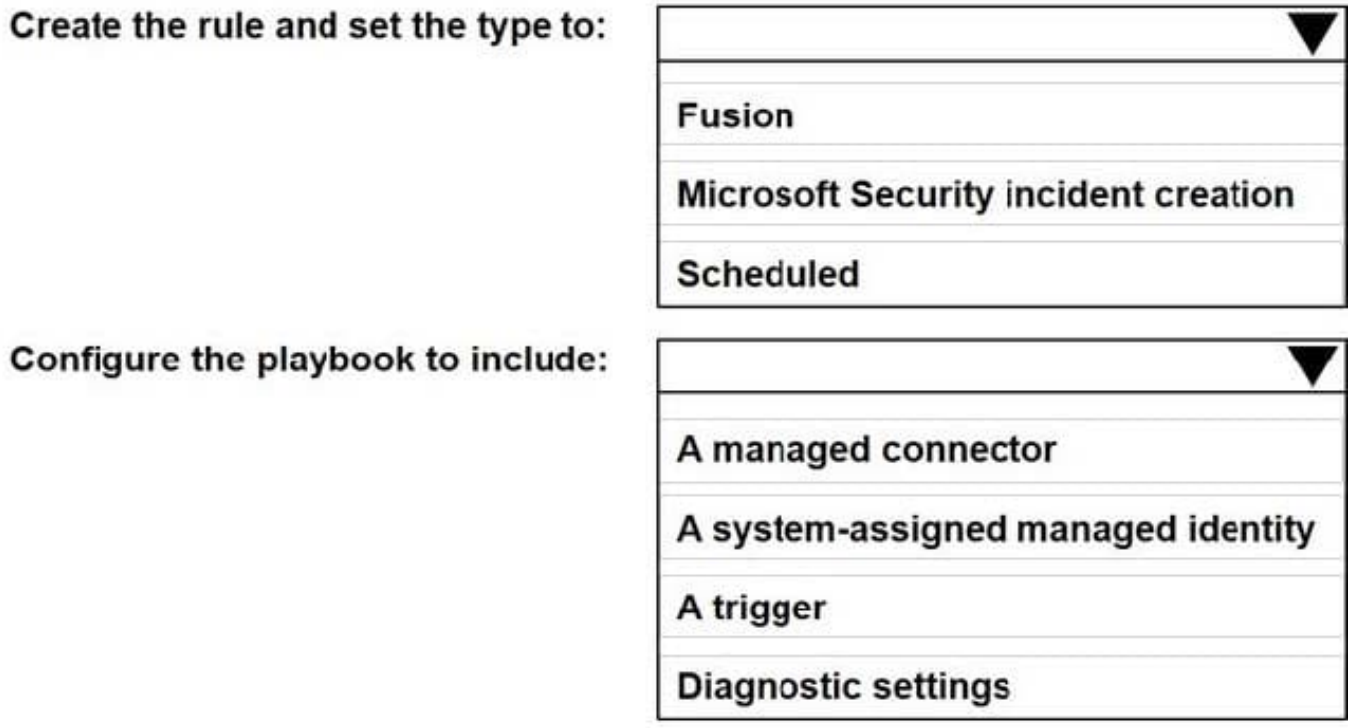
You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1.

You need to ensure that you can add Playbook1 to the new rule.

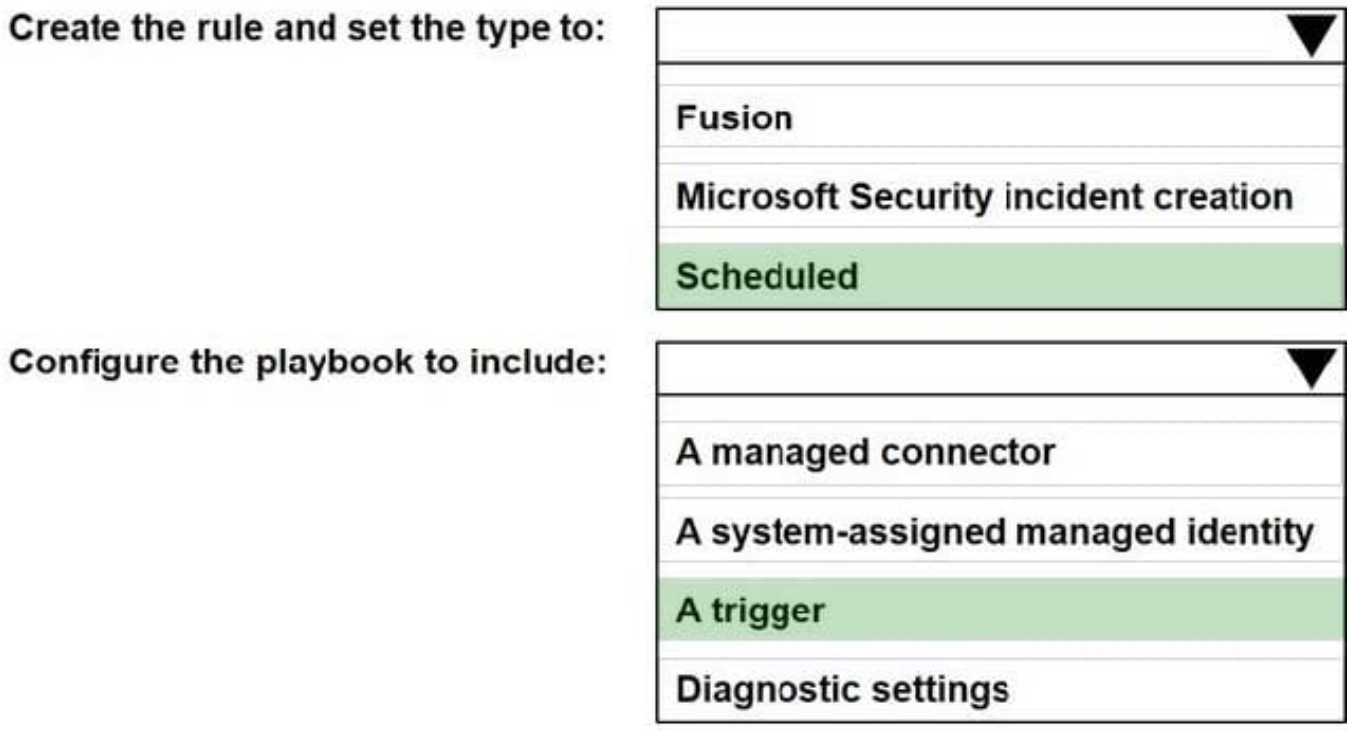
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 3

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
LB1	Azure Standard Load Balancer
VM1	Virtual machine
SQL1	Azure SQL Database
VMSS1	Virtual machine scale set

You plan to deploy an Azure Private Link service named APL1. Which resource must you reference during the creation of APL1?

A. VMSS1

B. VM1

C. SQL

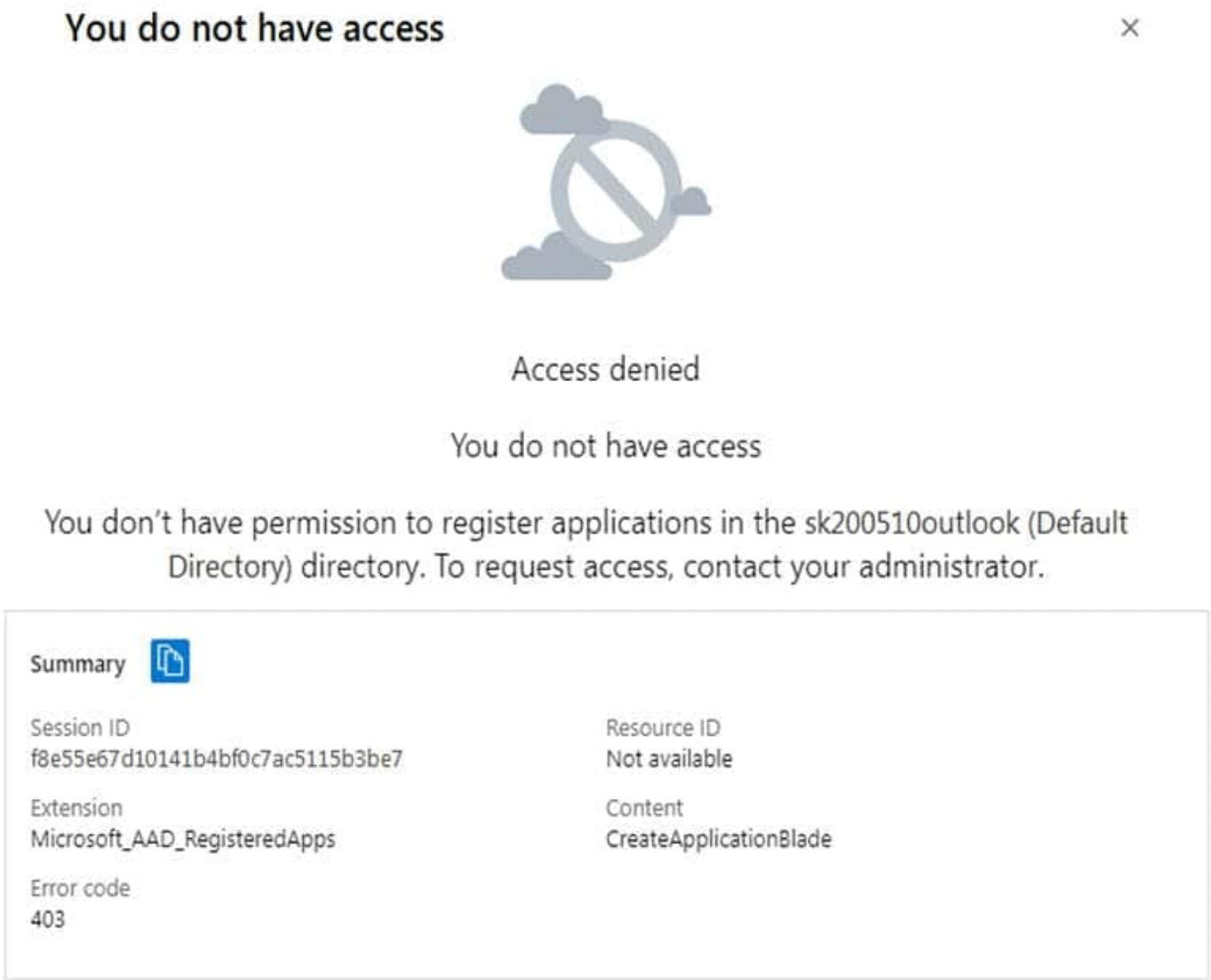
D. LB1

Correct Answer: D

QUESTION 4

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.

When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.



You need to ensure that the developer can register App1 in the tenant. What should you do for the tenant?

A. Modify the User settings

B. Set Enable Security default to Yes.

C. Modify the Directory properties.

D. Configure the Consent and permissions settings for enterprise applications.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

QUESTION 5

You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant.

You plan to implement Azure Active Directory (Azure AD) Identity Protection.

You need to ensure that you can configure a user risk policy and a sign-in risk policy.

What should you do first?

A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.

B. Register all users for Azure Multi-Factor Authentication (MFA).

C. Enable security defaults for Azure AD.

D. Upgrade Azure Security Center to the standard tier.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa