



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.geekcert.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

HOTSPOT

You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You plan to create an Azure file share that will contain folders and files.

Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Azure file share:

	▼
AD DS only	
Azure AD only	
AD DS and Azure AD	

Folders in the file share:

	▼
AD DS only	
Azure AD only	
AD DS and Azure AD	

Correct Answer:

Answer Area

Azure file share:

	▼
AD DS only	
Azure AD only	
AD DS and Azure AD	

Folders in the file share:

	▼
AD DS only	
Azure AD only	
AD DS and Azure AD	



Box1 and Box2: AD DS Only

Azure Files supports identity-based authentication for Windows file shares over Server Message Block (SMB) using the Kerberos authentication protocol through the following three methods:

1.

On-premises Active Directory Domain Services (AD DS)

2.

Azure Active Directory Domain Services (Azure AD DS)

3.

Azure Active Directory (Azure AD) Kerberos for hybrid user identities

Note Azure Files supports authentication for Azure AD DS with full or partial (scoped) synchronization with Azure AD. For environments with scoped synchronization present, administrators should be aware that Azure Files only honors Azure RBAC role assignments granted to principals that are synchronized. Role assignments granted to identities not synchronized from Azure AD to Azure AD DS will be ignored by the Azure Files service.

QUESTION 2

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has Azure subscription linked to their Azure Active Directory (Azure AD) tenant.

As a Global administrator for the tenant, part of your responsibilities involves managing Azure Security Center settings.

You are currently preparing to create a custom sensitivity label.

Solution: You start by creating a custom sensitive information type.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: A

Reference: <https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type>

QUESTION 3

You have an Azure subscription.

You plan to deploy a new Conditional Access policy named CAPolicy1.

You need to use the What if tool to evaluate how CAPolicy1 will affect users. The solution must minimize the impact of



CAPolicy1 on the users.

To what should you set the Enable policy setting for CAPolicy1?

- A. Off
- B. On
- C. Report only

Correct Answer: C

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

Conditional Access policies can be enabled in report-only mode, this is not applicable with the "User Actions" scope.

During sign-in, policies in report-only mode are evaluated but not enforced.

Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.

Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only>

QUESTION 4

HOTSPOT

You have an Azure subscription that contains an Azure Sentinel workspace.

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.

You need to identify which Azure Sentinel components to configure to meet the following requirements:

1.

When Azure Sentinel identifies a threat, an incident must be created.

2.

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

Which component should you identify 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

When Azure Sentinel identifies a threat, an incident must be created:

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

Correct Answer:

Answer Area

When Azure Sentinel identifies a threat, an incident must be created:

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts> <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

QUESTION 5

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 do not have access



Access denied

You do not have access

You don't have permission to register applications in the sk200510outlook (Default Directory) directory. To request access, contact your administrator.

Summary



Session ID

f8e55e67d10141b4bf0c7ac5115b3be7

Resource ID

Not available

Extension

Microsoft_AAD_RegisteredApps

Content

CreateApplicationBlade

Error code

403

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>



VCE & PDF

GeekCert.com

<https://www.geekcert.com/az-500.html>

2024 Latest geekcert AZ-500 PDF and VCE dumps Download

[Latest AZ-500 Dumps](#)

[AZ-500 Practice Test](#)

[AZ-500 Braindumps](#)