AZ-500$^{Q\&As}$

Microsoft Azure Security Technologies

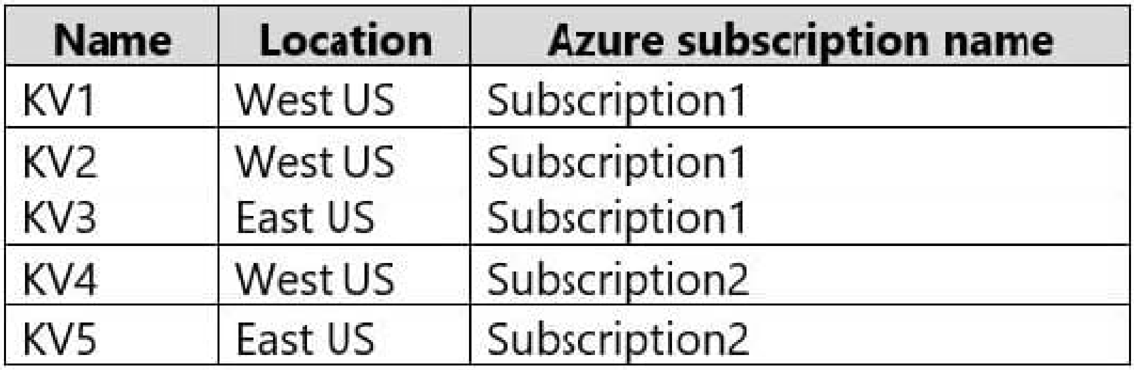
Pass Microsoft AZ-500 Exam with 100% Guarantee

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

QUESTION 1

HOTSPOT

You have the Azure key vaults shown in the following table.



Name	Location	Azure subscription name
KV1	West US	Subscription1
KV2	West US	Subscription1
KV3	East US	Subscription1
KV4	West US	Subscription2
KV5	East US	Subscription2

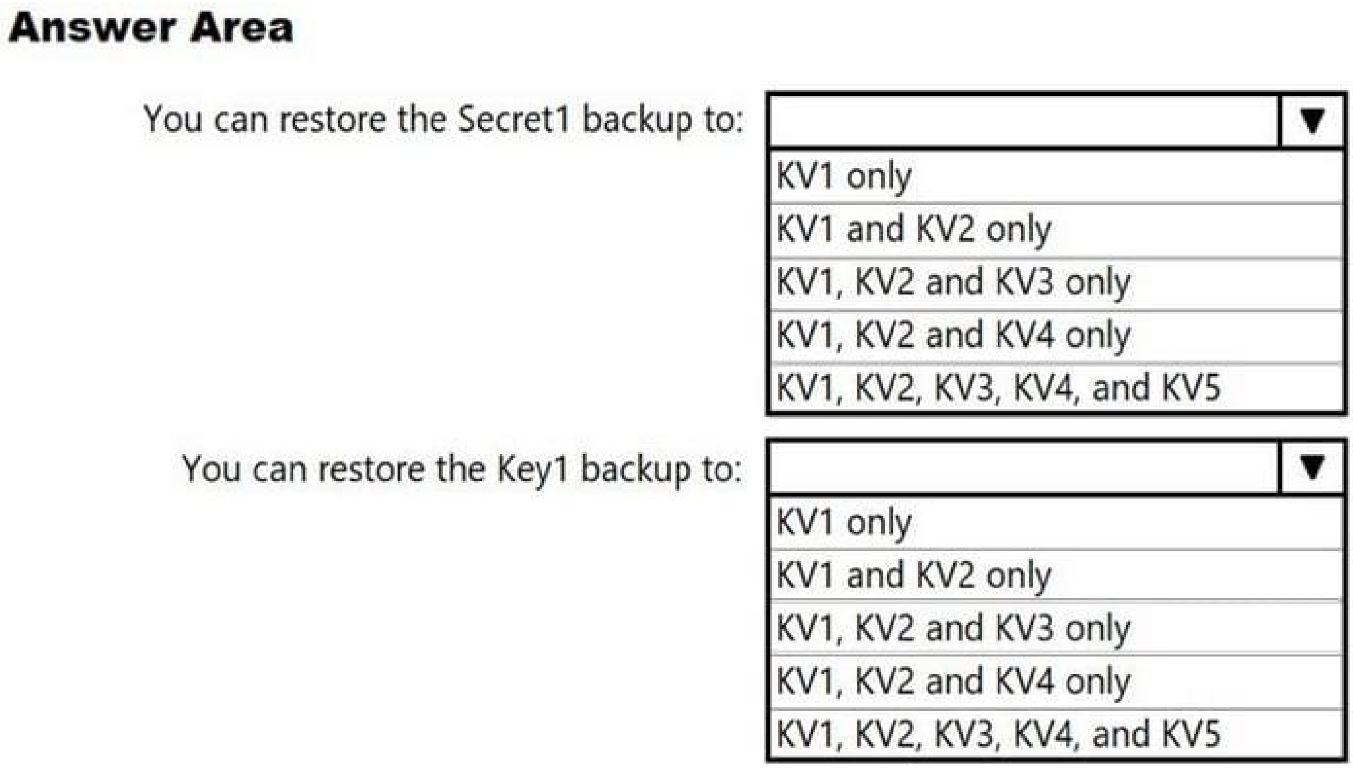
KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.

You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

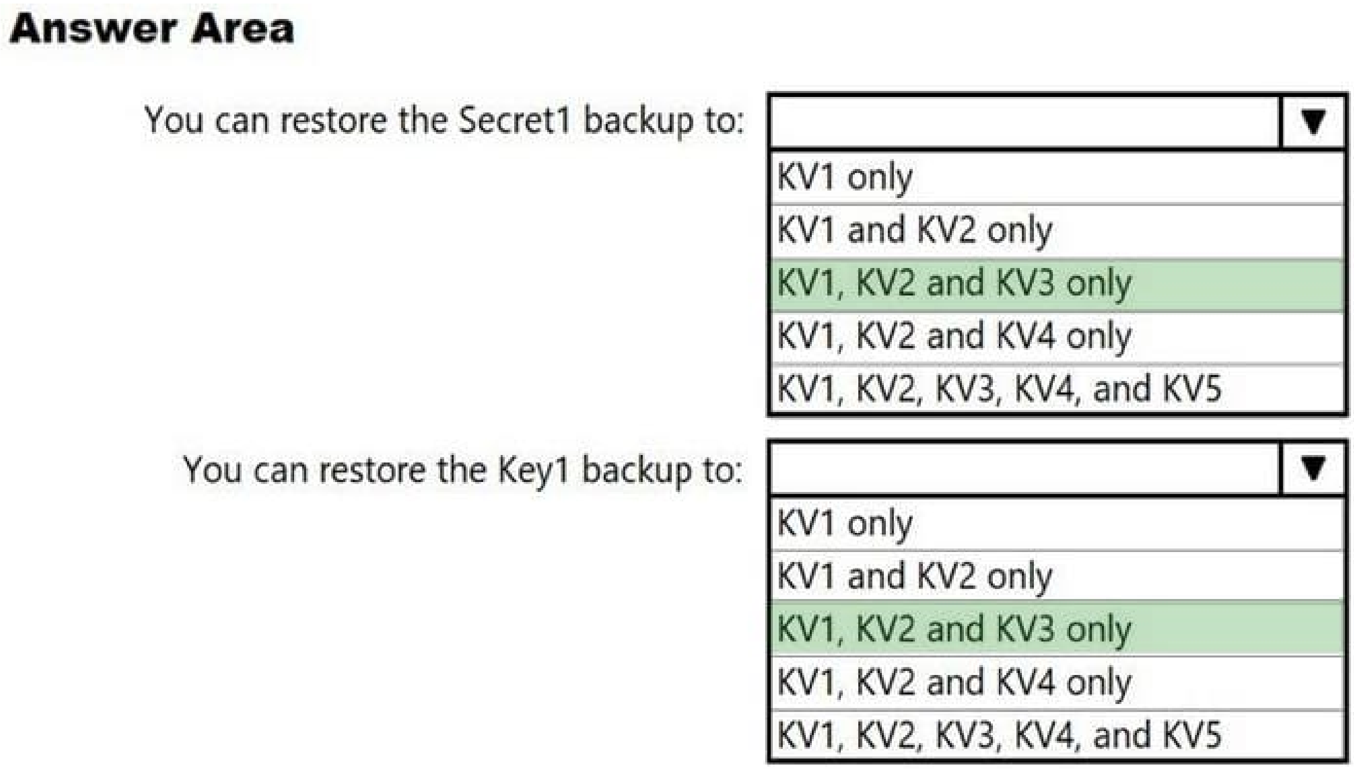
You can restore the Secret1 backup to: ▼

- KV1 only
- KV1 and KV2 only
- KV1, KV2 and KV3 only
- KV1, KV2 and KV4 only
- KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to: ▼

- KV1 only
- KV1 and KV2 only
- KV1, KV2 and KV3 only
- KV1, KV2 and KV4 only
- KV1, KV2, KV3, KV4, and KV5

Correct Answer:



Answer Area

You can restore the Secret1 backup to:

KV1 only
KV1 and KV2 only
[✓ KV1, KV2 and KV3 only]
KV1, KV2 and KV4 only
KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to:

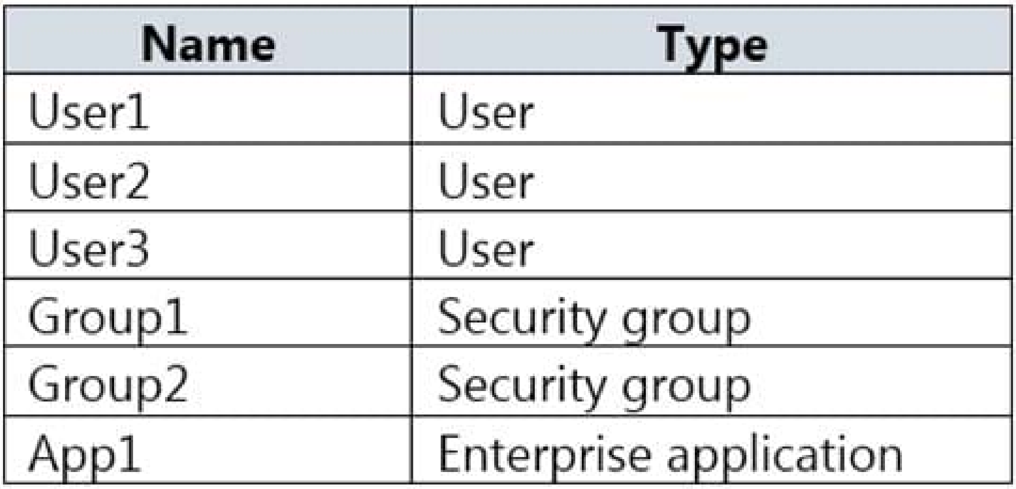
KV1 only
KV1 and KV2 only
[✓ KV1, KV2 and KV3 only]
KV1, KV2 and KV4 only
KV1, KV2, KV3, KV4, and KV5

The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.

QUESTION 2

HOTSPOT

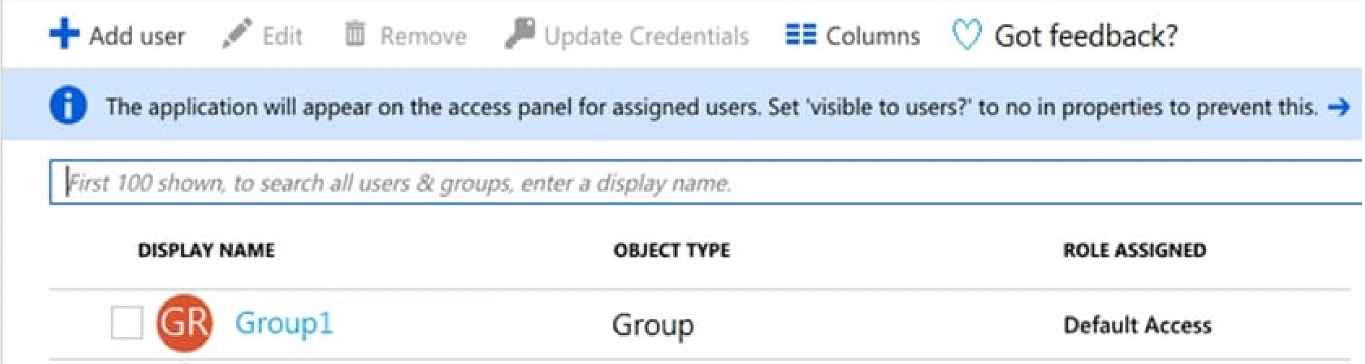
You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.



Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

User2 is the owner of Group2.

The user and group settings for App1 are configured as shown in the following exhibit.

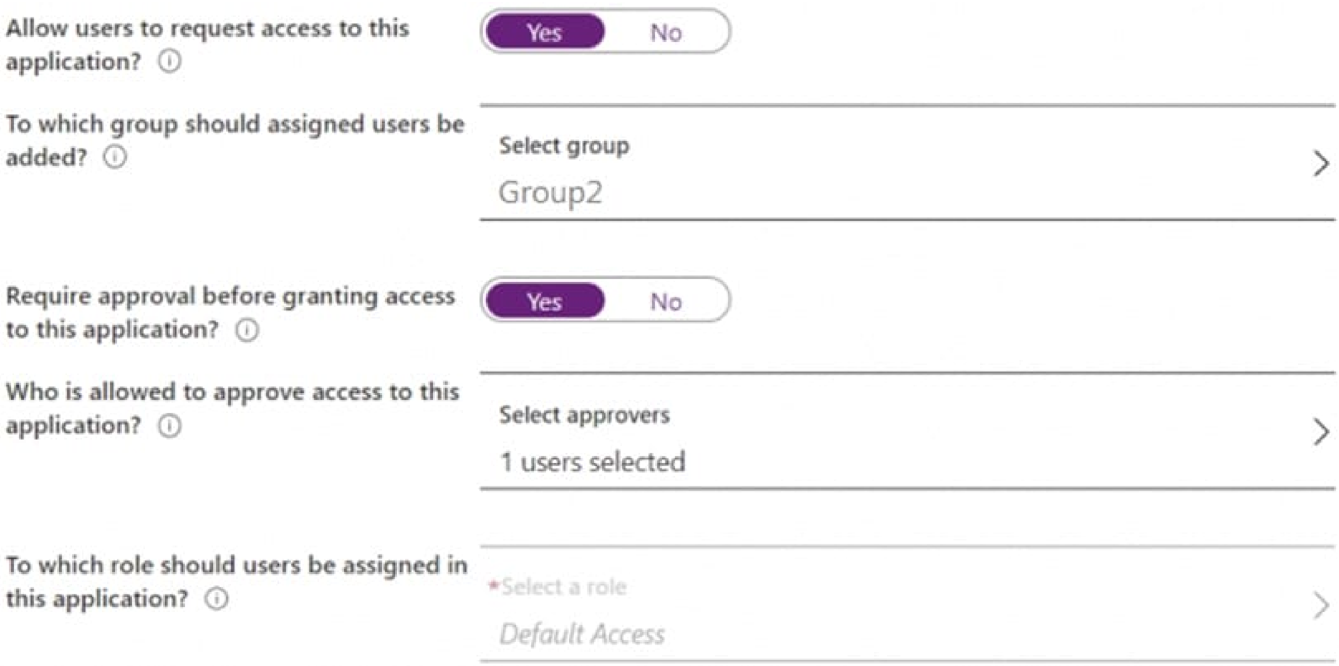


The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.

First 100 shown, to search all users & groups, enter a display name.

	DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
□	GR Group1	Group	Default Access

You enable self-service application access for App1 as shown in the following exhibit.



Allow users to request access to this application? ⓘ [✓ Yes] No

To which group should assigned users be added? ⓘ Select group: Group2

Require approval before granting access to this application? ⓘ [✓ Yes] No

Who is allowed to approve access to this application? ⓘ Select approvers: 1 users selected

To which role should users be assigned in this application? ⓘ *Select a role: Default Access

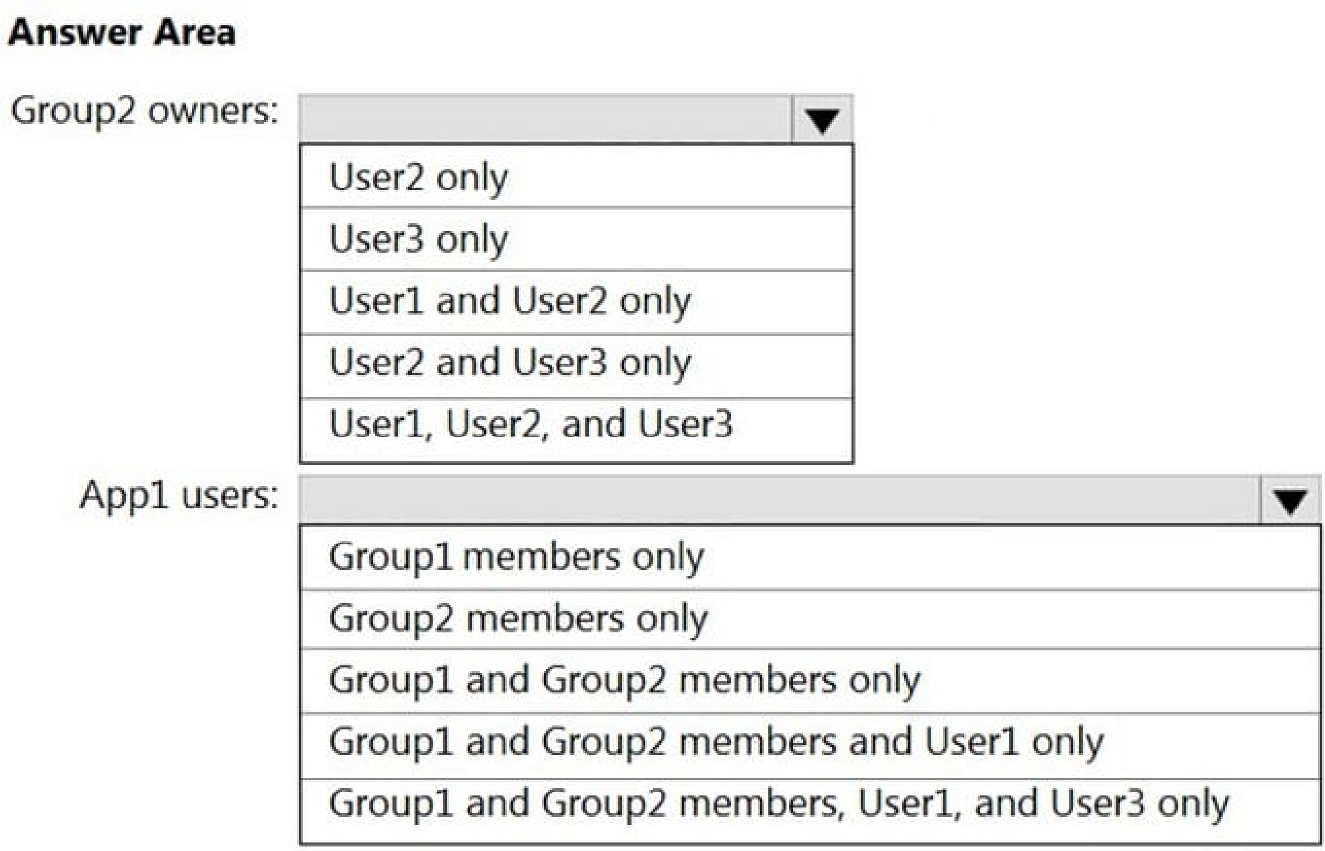
User3 is configured to approve access to Appl.

You need to identify the owners of Group2 and the users of Appl.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

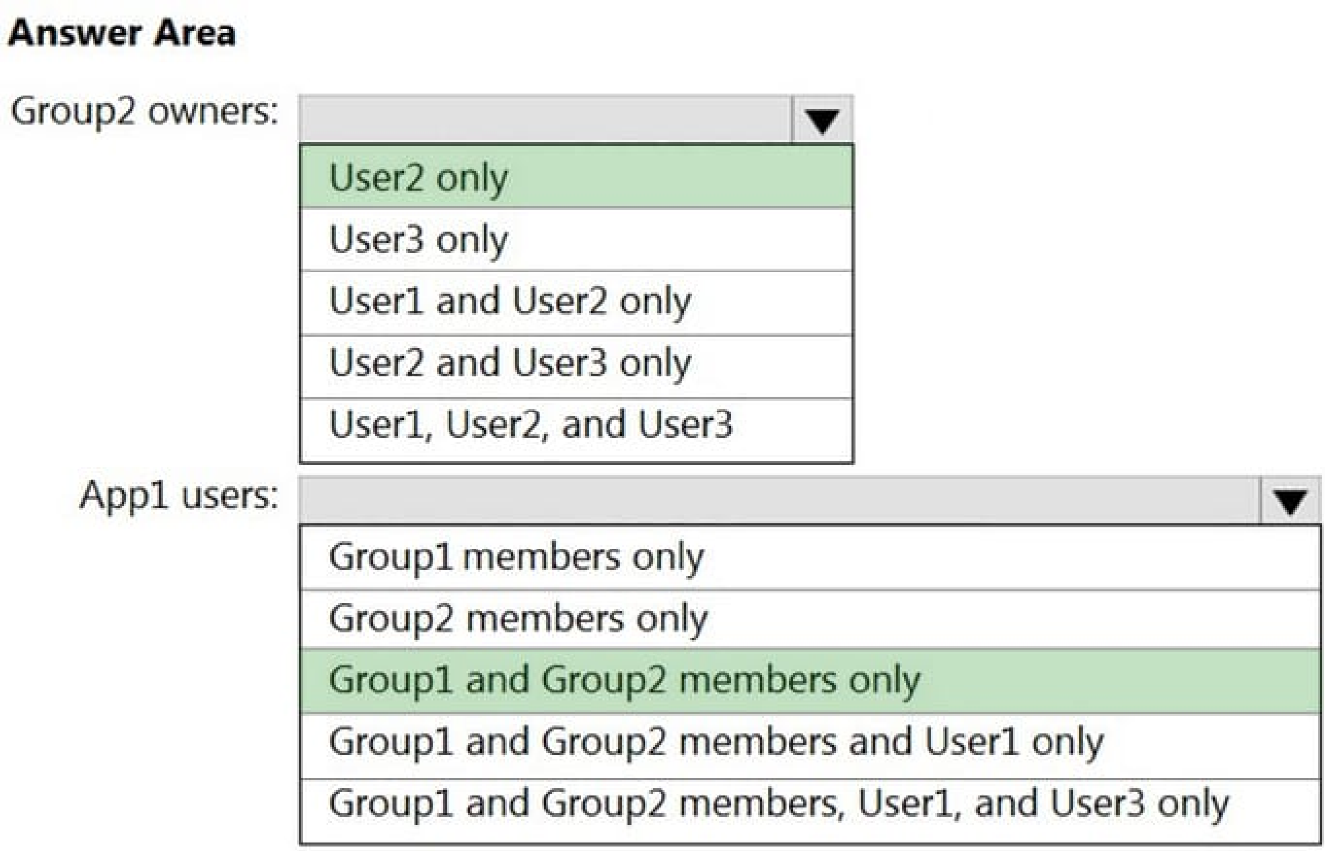
Group2 owners:

- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users:

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Correct Answer:



Answer Area

Group2 owners:

- [✓ User2 only]
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users:

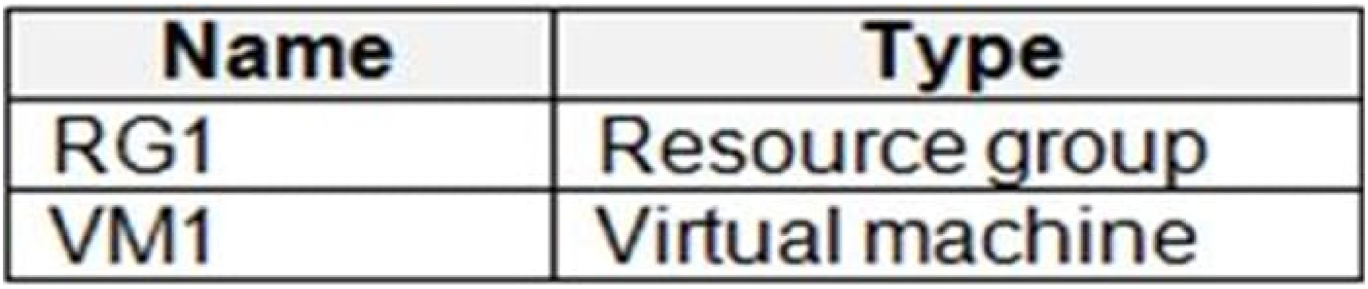
- Group1 members only
- Group2 members only
- [✓ Group1 and Group2 members only]
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

QUESTION 3

HOTSPOT

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



Name	Type
RG1	Resource group
VM1	Virtual machine

You perform the following tasks:

Create a managed identity named Managed1.

Create a Microsoft 365 group named Group1.

Register an enterprise application named App1.

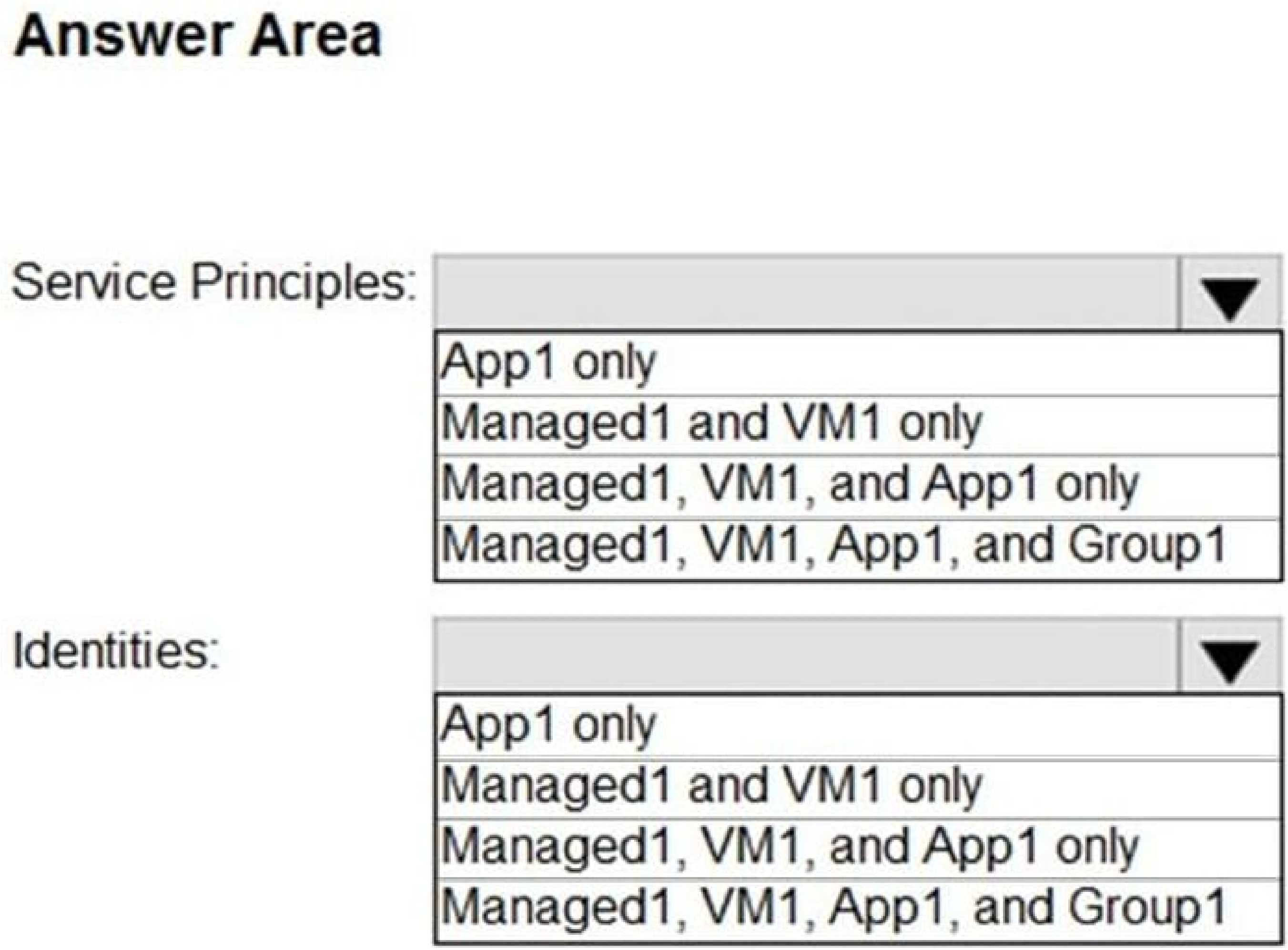
Enable a system-assigned managed identity for VM1.

You need to identify which service principals were created and which identities can be assigned the Reader role for RG1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

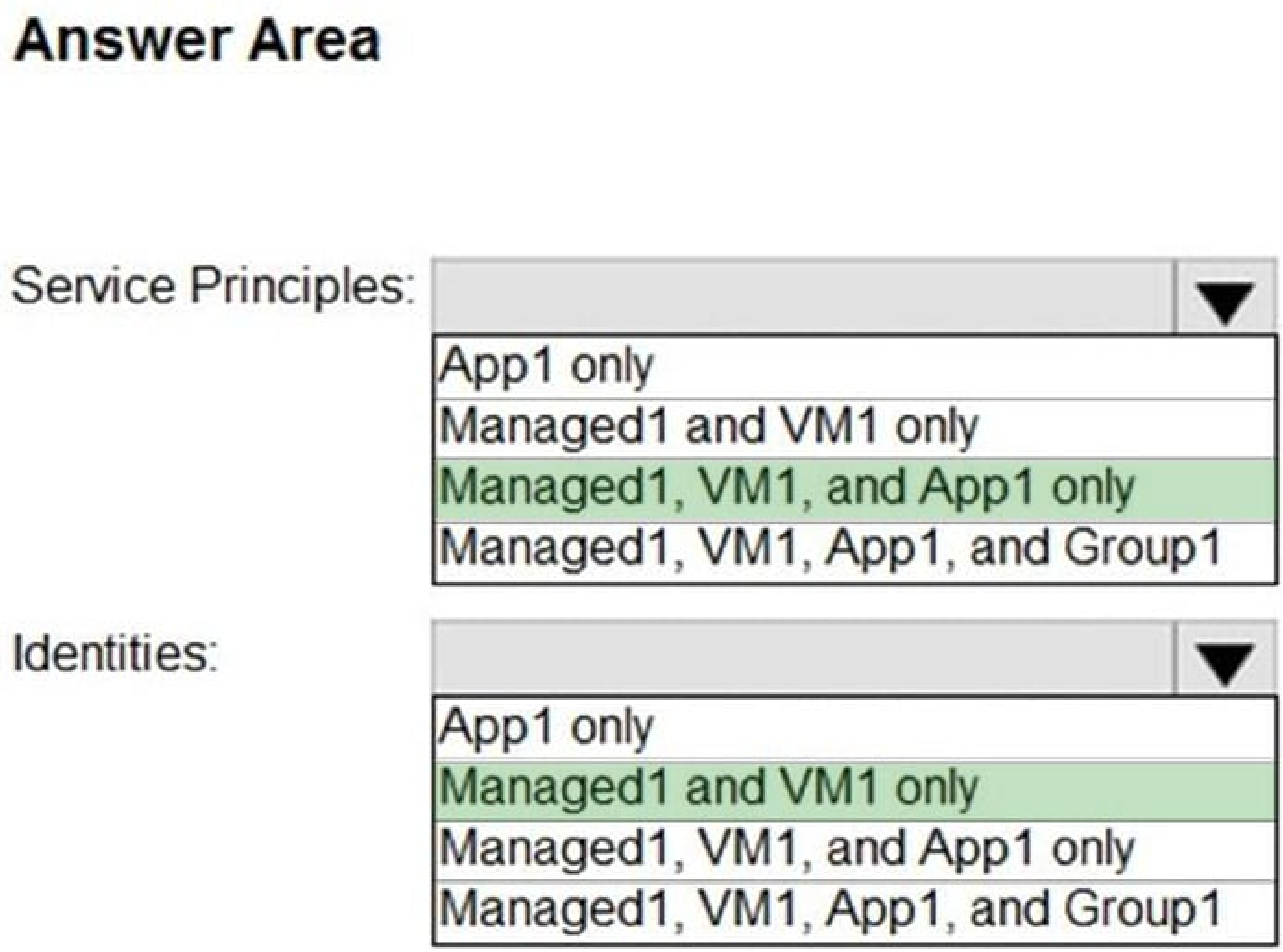


Answer Area

Service Principles: ▼
- App1 only
- Managed1 and VM1 only
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

Identities: ▼
- App1 only
- Managed1 and VM1 only
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

Correct Answer:



Answer Area

Service Principles:

- App1 only
- Managed1 and VM1 only
- [✓ Managed1, VM1, and App1 only]
- Managed1, VM1, App1, and Group1

Identities:

- App1 only
- [✓ Managed1 and VM1 only]
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

QUESTION 4

HOTSPOT

You have an Azure Sentinel workspace that has the following data connectors:

1.

Azure Active Directory Identity Protection

2.

Common Event Format (CEF)

3.

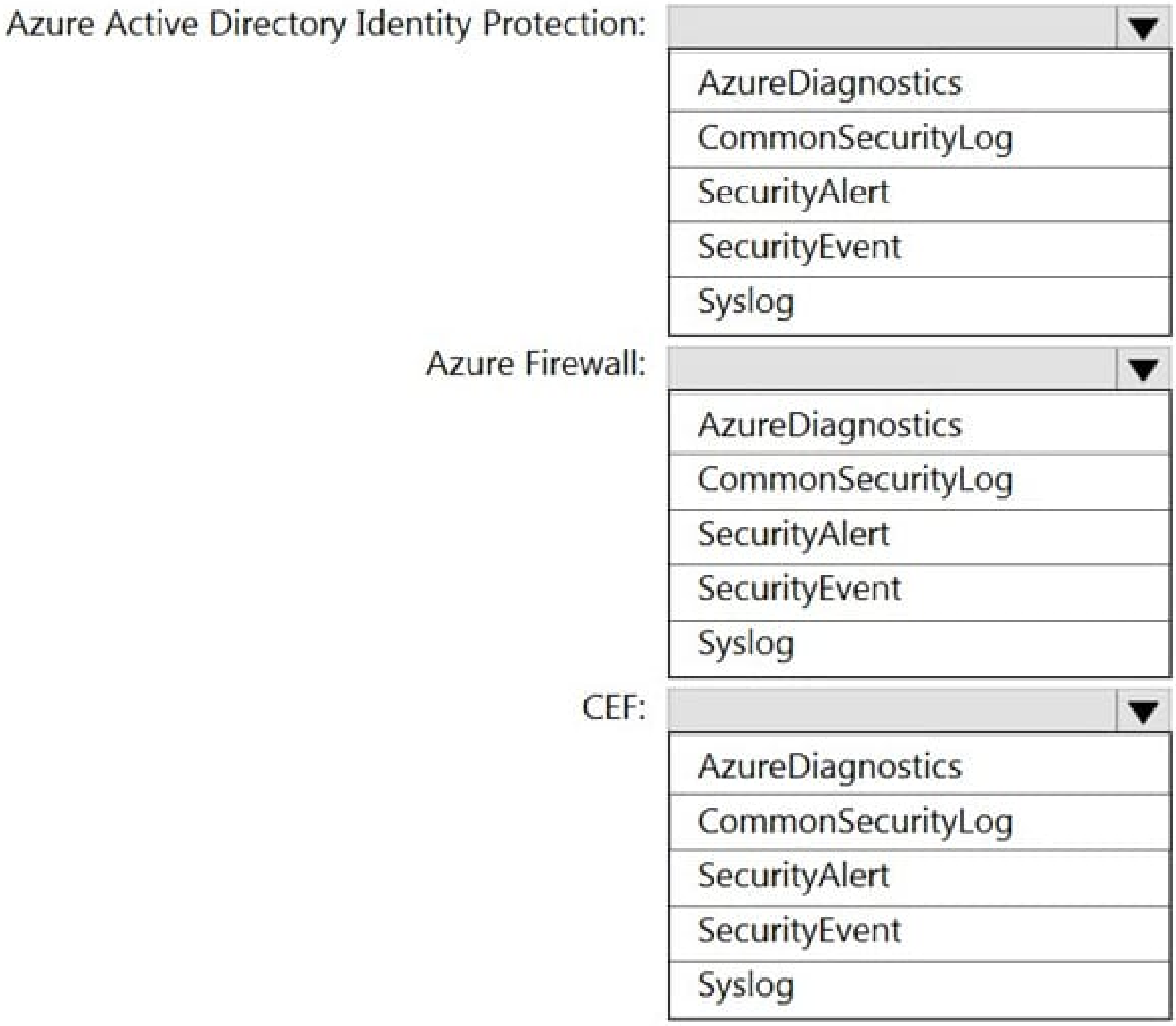
Azure Firewall

You need to ensure that data is being ingested from each connector.

From the Logs query window, which table should you query for each connector? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Azure Active Directory Identity Protection: ▼

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

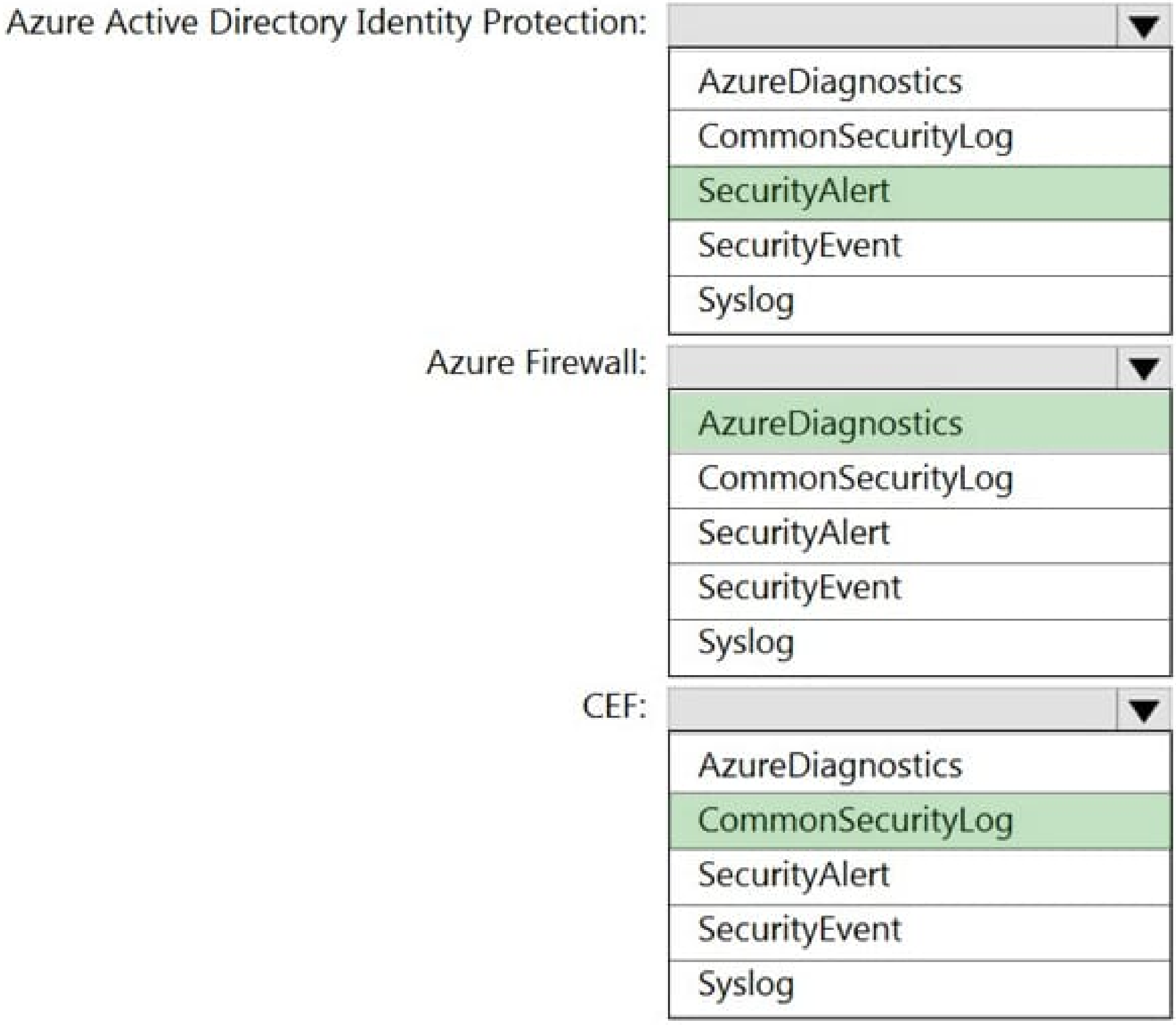
Azure Firewall: ▼

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

CEF: ▼

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

Correct Answer:



Azure Active Directory Identity Protection:

- AzureDiagnostics
- CommonSecurityLog
- [✓ SecurityAlert]
- SecurityEvent
- Syslog

Azure Firewall:

- [✓ AzureDiagnostics]
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

CEF:

- AzureDiagnostics
- [✓ CommonSecurityLog]
- SecurityAlert
- SecurityEvent
- Syslog

Reference: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-firewall https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

QUESTION 5

You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant. The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.

You create a new Azure subscription.

You discover that the synced on-premises user accounts cannot be assigned roles in the new subscription.

You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts.

What should you do fist?

A. Configure the Azure AD tenant used by the new subscription to use pass-through authentication.

B. Configure the Azure AD tenant used by the new subscription to use federated authentication.

C. Change the Azure AD tenant used by the new subscription.

D. Configure a second instance of Azure AD Connect.

Correct Answer: C

You create a new Azure subscription. Hence you need to assign. These questions something are tricky. Go over every answer and try to backtrack if it triggers an earlier statement.