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

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

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

https://www.leads4pass.com/az-500.html

100% Passing Guarantee
100% Money Back Assurance

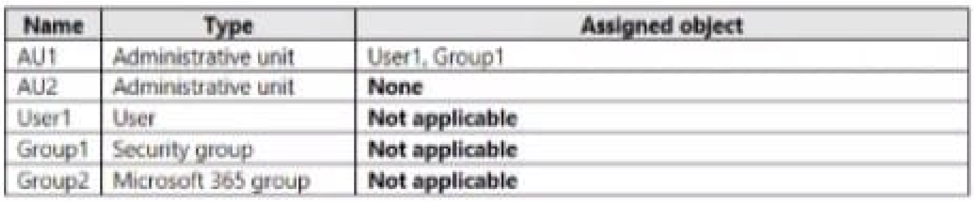
Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

HOTSPOT

You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.

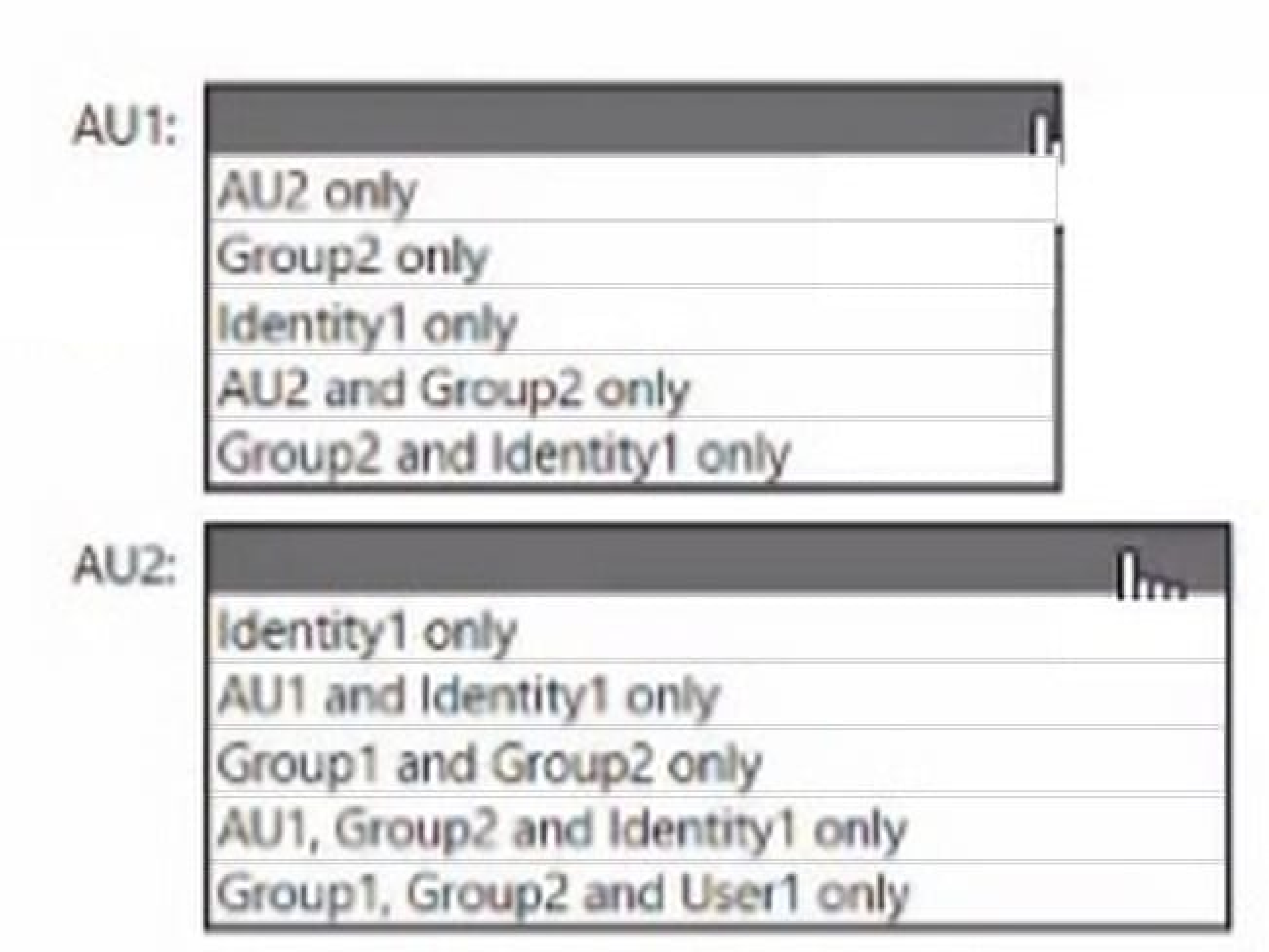
Which resources can be added to AUI and AU2? To answer, select the appropriate options in the answer area.



Name	Type	Assigned object
AU1	Administrative unit	User1, Group1
AU2	Administrative unit	None
User1	User	Not applicable
Group1	Security group	Not applicable
Group2	Microsoft 365 group	Not applicable

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

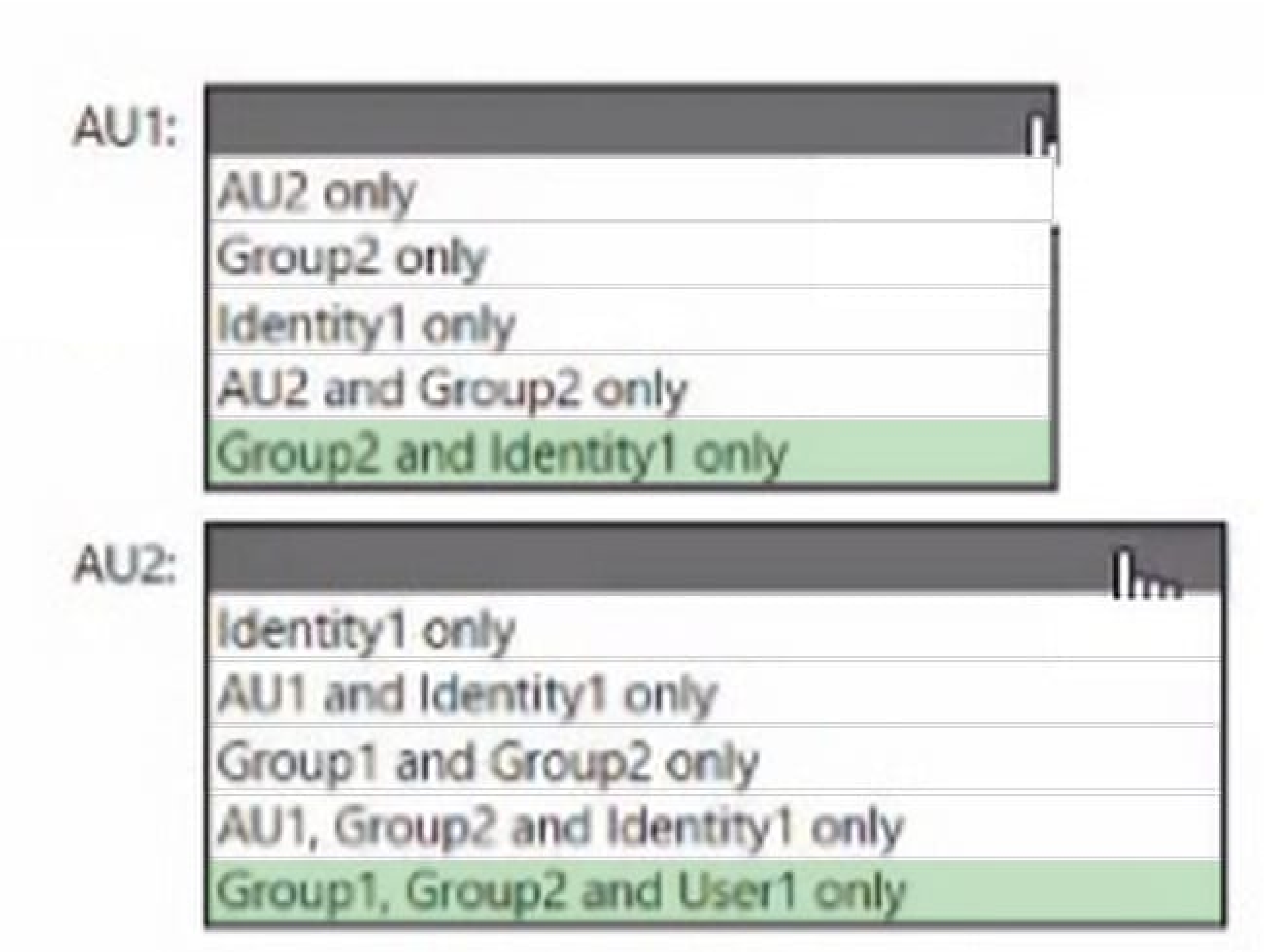
Hot Area:



AU1:
- AU2 only
- Group2 only
- Identity1 only
- AU2 and Group2 only
- Group2 and Identity1 only

AU2:
- Identity1 only
- AU1 and Identity1 only
- Group1 and Group2 only
- AU1, Group2 and Identity1 only
- Group1, Group2 and User1 only

Correct Answer:



AU1:

- AU2 only
- Group2 only
- Identity1 only
- AU2 and Group2 only
- [✓ Group2 and Identity1 only]

AU2:

- Identity1 only
- AU1 and Identity1 only
- Group1 and Group2 only
- AU1, Group2 and Identity1 only
- [✓ Group1, Group2 and User1 only]

QUESTION 2

You have an Azure subscription that contains an Azure Blob storage account bolb1.

You need to configure attribute-based access control (ABAC) for blob1.

Which attributes can you use in access conditions?

A. blob index tags only

B. blob index tags and container names only

C. file extensions and container names only

D. blob index tags, file extensions, and container names

Correct Answer: B

https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview

QUESTION 3

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.

You plan to publish several apps in the tenant.

You need to ensure that User1 can grant admin consent for the published apps.

Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Application developer

B. Security administrator

C. Application administrator

D. User administrator

E. Cloud application administrator

Correct Answer: CE

Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

QUESTION 4

SIMULATION

The developers at your company plan to publish an app named App11641655 to Azure.

You need to ensure that the app is registered to Azure Active Directory (Azure AD). The registration must use the sign-on URLs of https://app.contoso.com.

To complete this task, sign in to the Azure portal and modify the Azure resources.

A. See the explanation below.

Correct Answer: A

Step 1: Register the Application

1.

Sign in to your Azure Account through the Azure portal.

2.

Select Azure Active Directory.

3.

Select App registrations.

4.

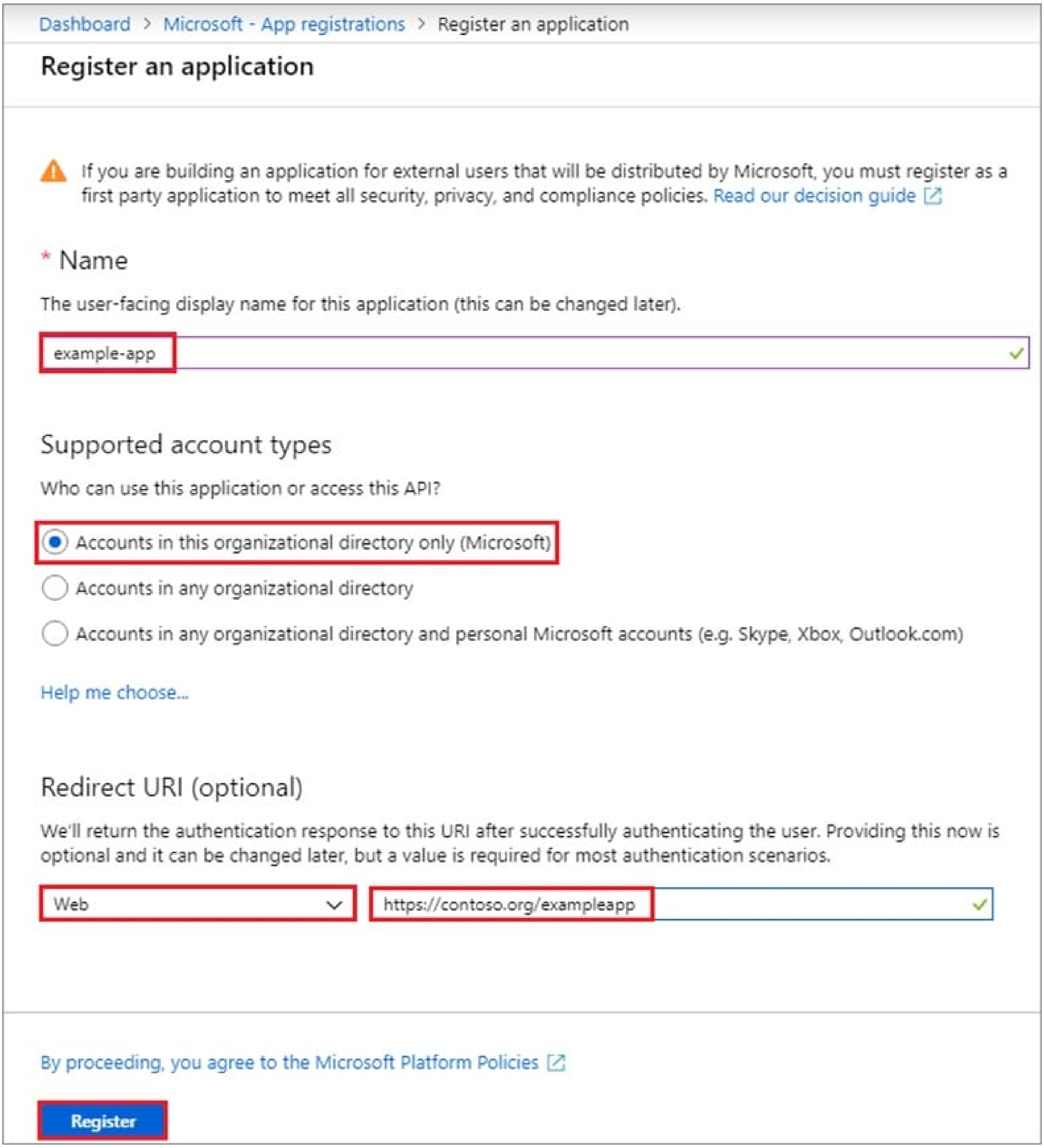
Select New registration.

5.

Name the application App11641655. Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: https://app.contoso.com, where the access token is sent to.

6.

Click Register



Dashboard > Microsoft - App registrations > Register an application

Register an application

If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. Read our decision guide

* Name

The user-facing display name for this application (this can be changed later).

example-app ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Microsoft)

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://contoso.org/exampleapp ✓

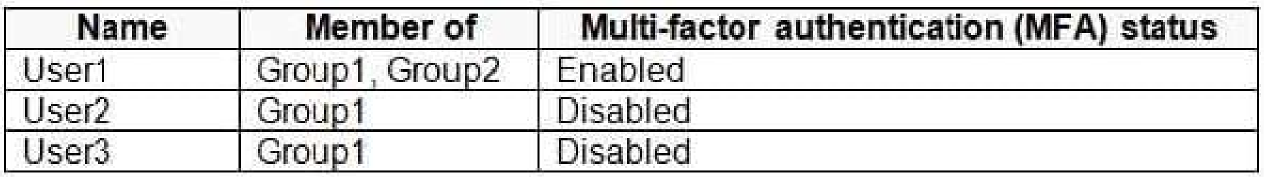
By proceeding, you agree to the Microsoft Platform Policies

Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

QUESTION 5

HOTSPOT

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



Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

1.

Assignments: Include Group1, exclude Group2

2.

Conditions: Sign-in risk level: Medium and above

3.

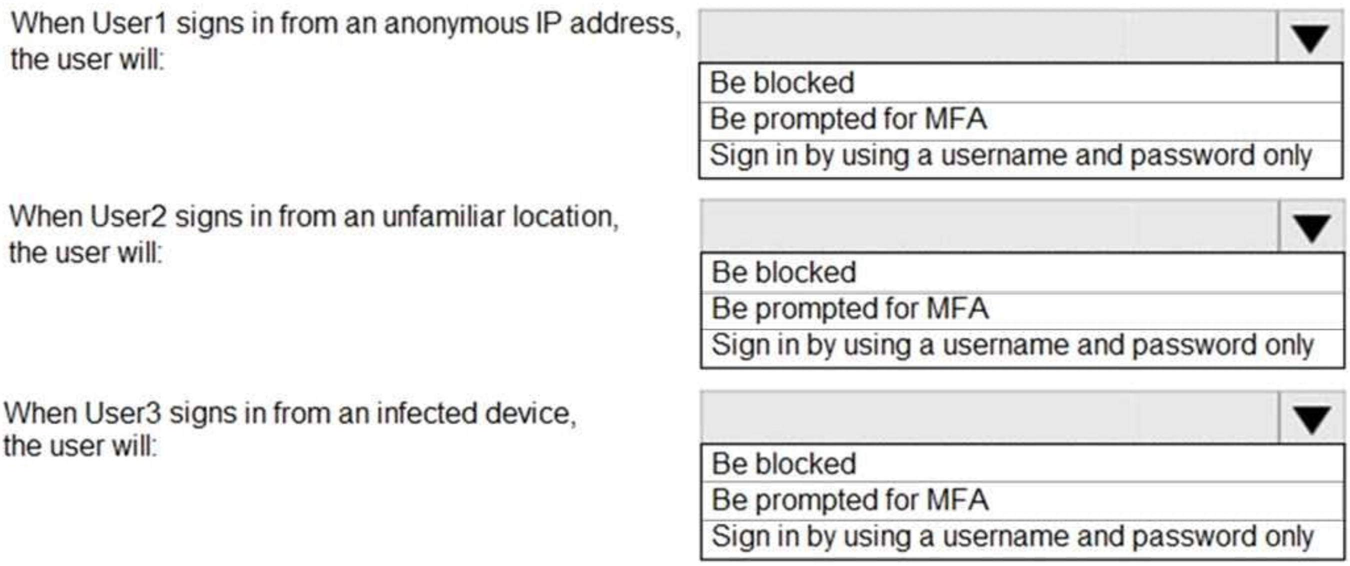
Access Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

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

NOTE: Each correct selection is worth one point.

Hot Area:



When User1 signs in from an anonymous IP address, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

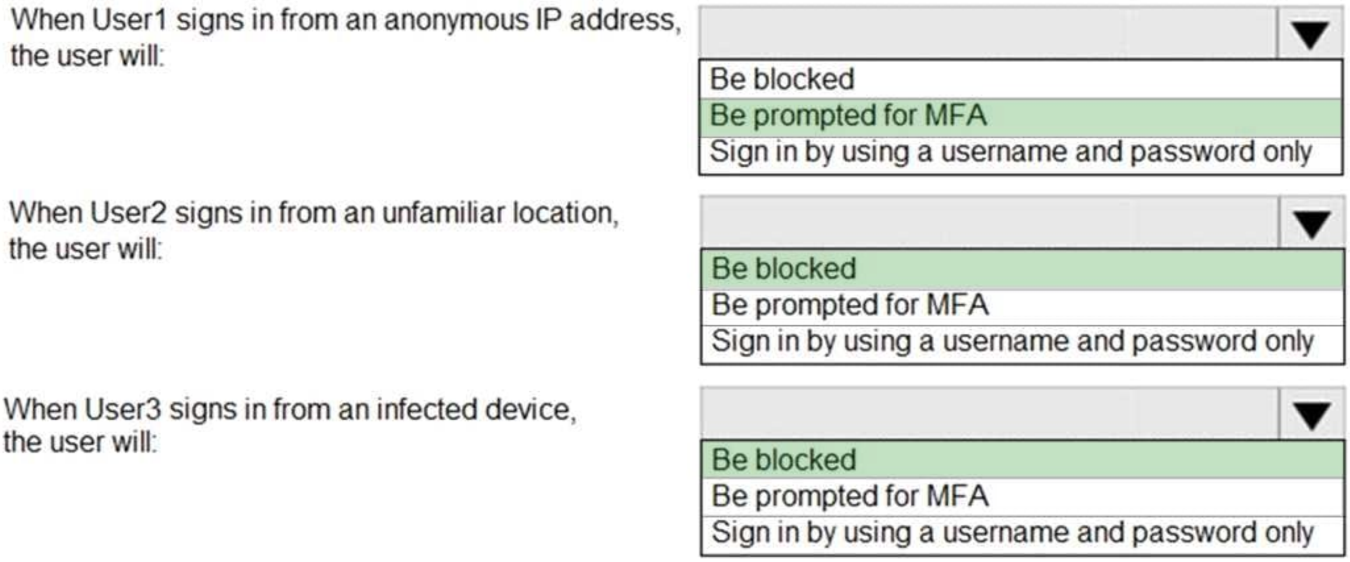
When User2 signs in from an unfamiliar location, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

Correct Answer:



When User1 signs in from an anonymous IP address, the user will:

- Be blocked
- [✓ Be prompted for MFA]
- Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:

- [✓ Be blocked]
- Be prompted for MFA
- Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

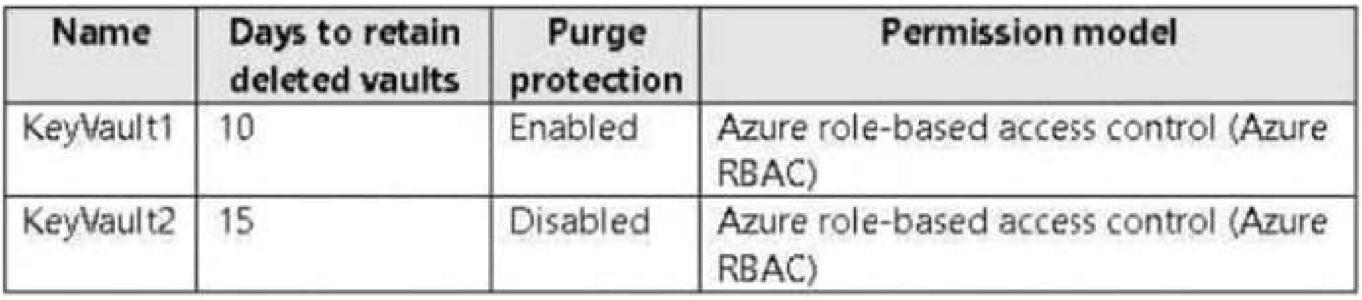
- [✓ Be blocked]
- Be prompted for MFA
- Sign in by using a username and password only

References: http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditionalaccess-policies/ https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identityprotection-policies https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identityprotection-risks

QUESTION 6

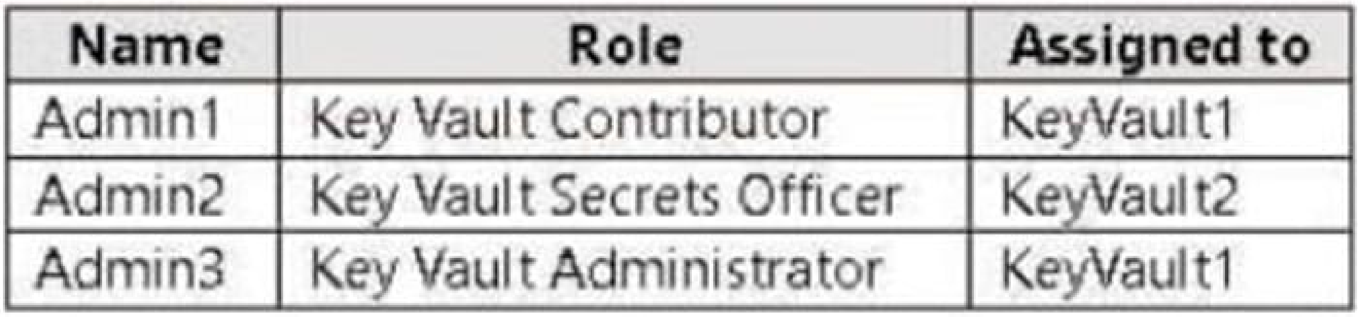
HOTSPOT

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



Name	Days to retain deleted vaults	Purge protection	Permission model
KeyVault1	10	Enabled	Azure role-based access control (Azure RBAC)
KeyVault2	15	Disabled	Azure role-based access control (Azure RBAC)

The subscription contains the users shown in the following table.



Name	Role	Assigned to
Admin1	Key Vault Contributor	KeyVault1
Admin2	Key Vault Secrets Officer	KeyVault2
Admin3	Key Vault Administrator	KeyVault1

On June 1, you perform the following actions:

1.

Delete a key named key1 from KeyVault1.

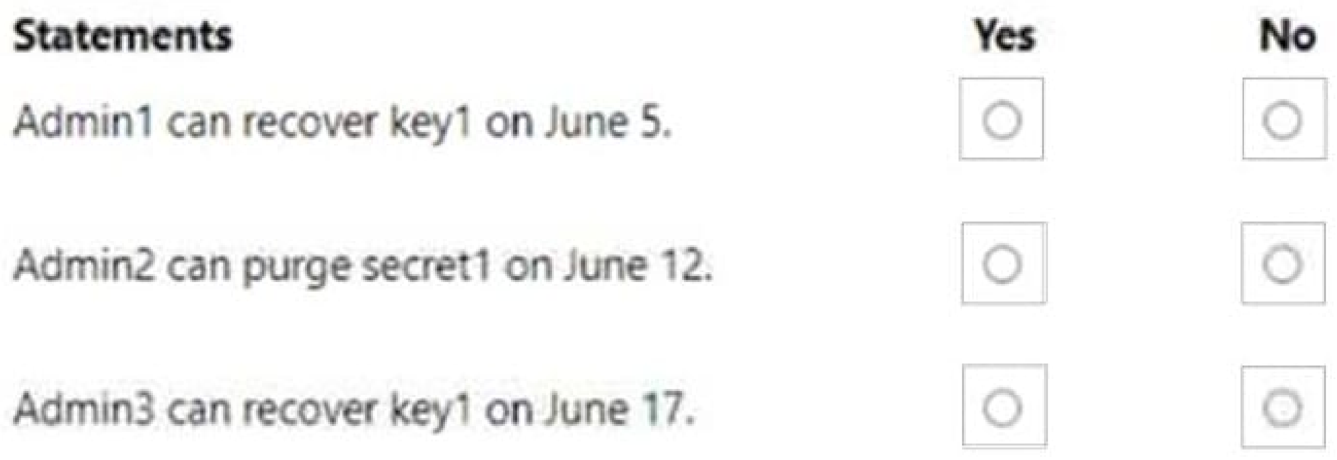
2.

Delete a secret named secret1 from KeyVault2.

For each of the following statements, select Yes If the statement is true. Otherwise, select No.

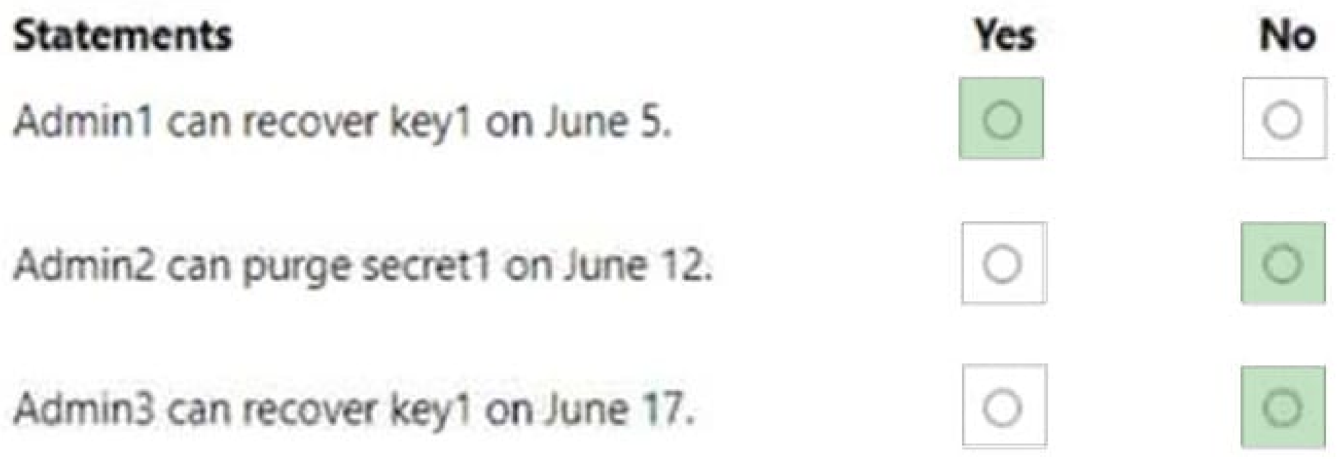
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
Admin1 can recover key1 on June 5.	○	○
Admin2 can purge secret1 on June 12.	○	○
Admin3 can recover key1 on June 17.	○	○

Correct Answer:



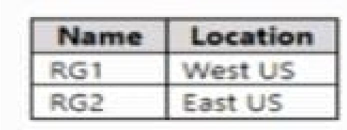
Statements	Yes	No
Admin1 can recover key1 on June 5.	[✓ ○]	○
Admin2 can purge secret1 on June 12.	○	[✓ ○]
Admin3 can recover key1 on June 17.	○	[✓ ○]

Y - within 10 days N - purge protection enabled so no, also Secrets officer has not enough permission N - more than 15 days have passed, so already deleted and not possible to recover anymore

QUESTION 7

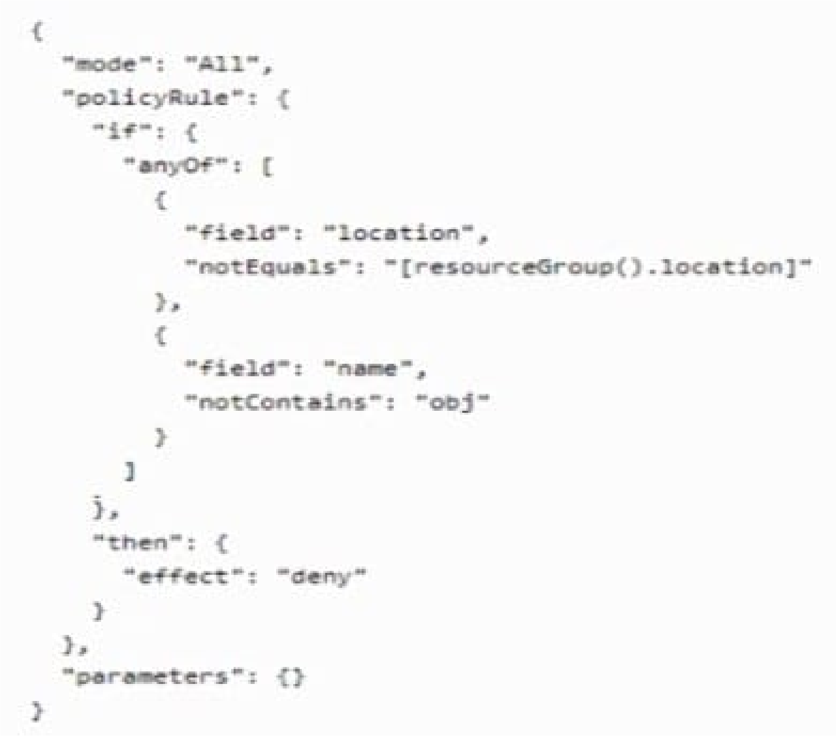
HOTSPOT

You have an Azure subscription named Sub1 that contains the resource groups shown in the following table.



Name	Location
RG1	West US
RG2	East US

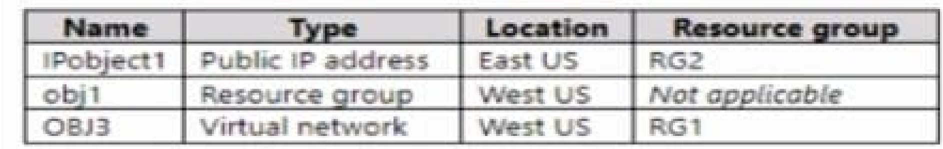
You create the Azure Policy definition shown in the following exhibit.



```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "anyOf": [
        {
          "field": "location",
          "notEquals": "[resourceGroup().location]"
        },
        {
          "field": "name",
          "notContains": "obj"
        }
      ]
    },
    "then": {
      "effect": "deny"
    }
  },
  "parameters": {}
}
```

You assign the policy to Sub1.

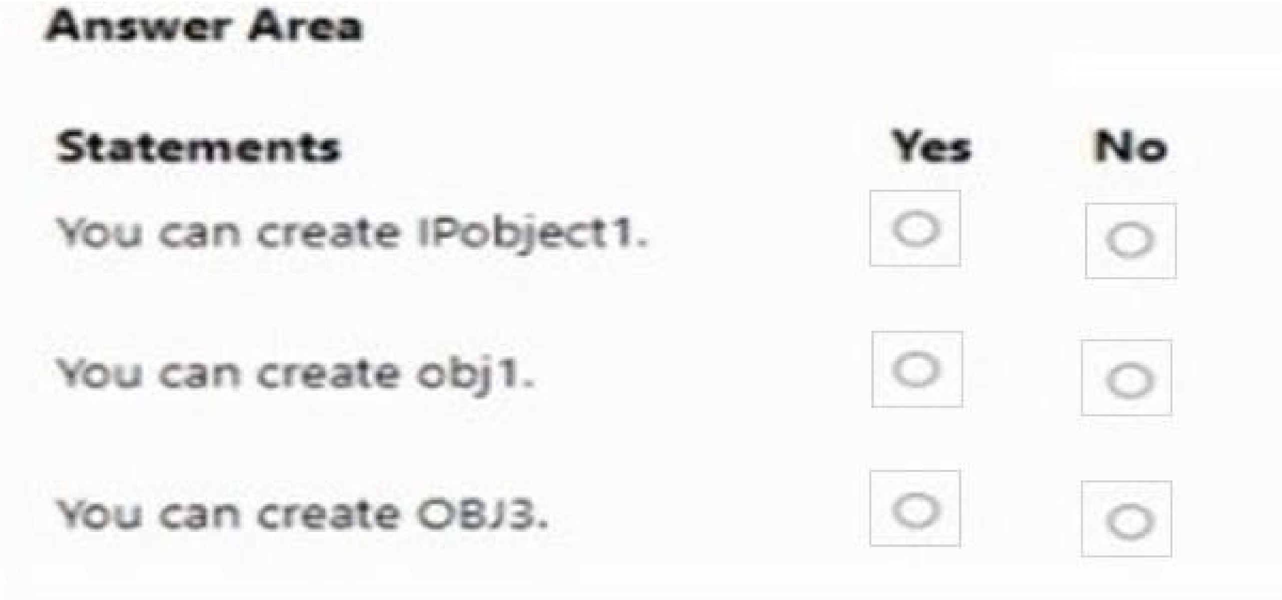
You plan to create the resources shown in the following table.



Name	Type	Location	Resource group
IPobject1	Public IP address	East US	RG2
obj1	Resource group	West US	*Not applicable*
OBJ3	Virtual network	West US	RG1

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

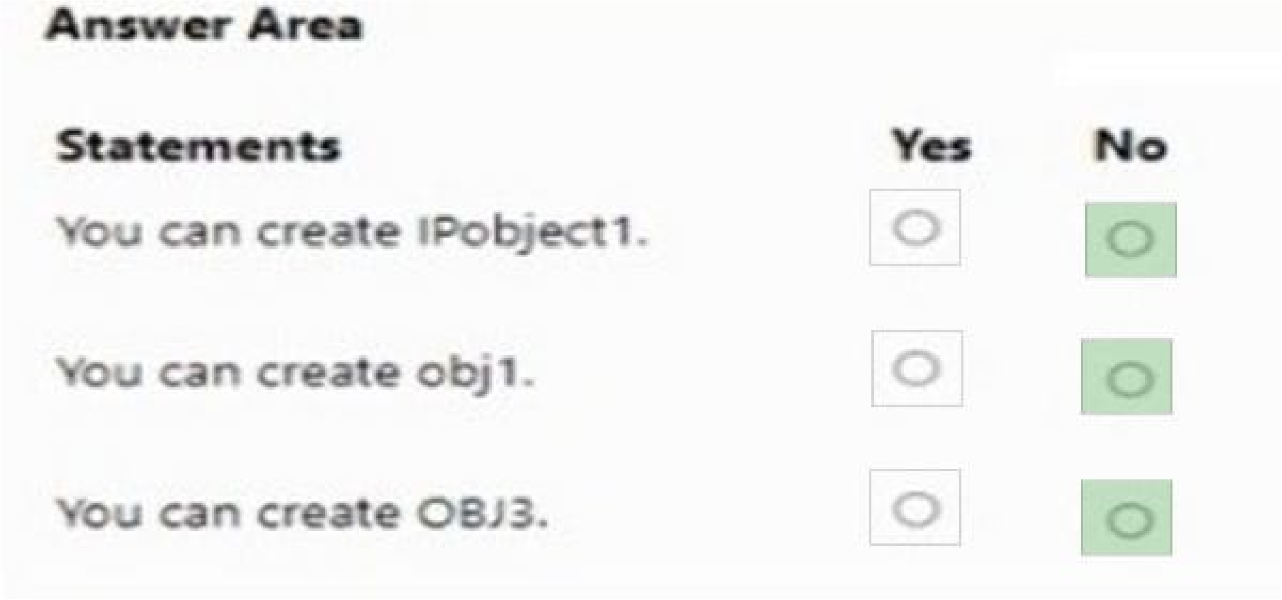
Hot Area:



Answer Area

Statements	Yes	No
You can create IPobject1.	○	○
You can create obj1.	○	○
You can create OBJ3.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
You can create IPobject1.	○	[✓ ○]
You can create obj1.	○	[✓ ○]
You can create OBJ3.	○	[✓ ○]

QUESTION 8

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 an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of password hash synchronization and seamless SSO.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 9

You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contoso.com and a resource group named RG1.

You create a custom role named Role1 for contoso.com.

You need to identify where you can use Role1 for permission delegation.

What should you identify?

A. contoso.com only

B. contoso.com and RGT only

C. contoso.com and Subscription1 only

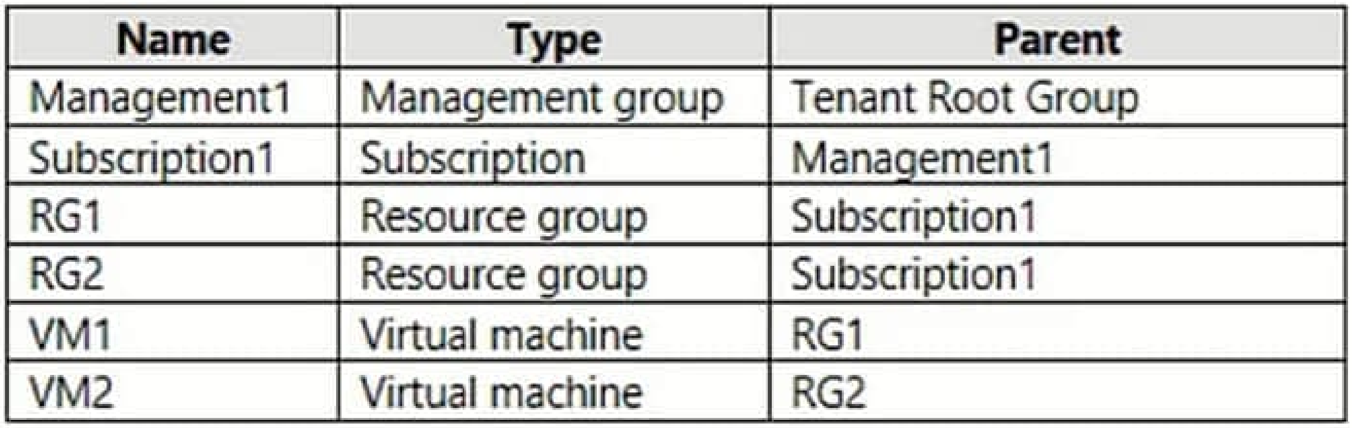
D. contoso.com, RG1, and Subcription1

Correct Answer: A

https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

QUESTION 10

You have the Azure resource shown in the following table.



Name	Type	Parent
Management1	Management group	Tenant Root Group
Subscription1	Subscription	Management1
RG1	Resource group	Subscription1
RG2	Resource group	Subscription1
VM1	Virtual machine	RG1
VM2	Virtual machine	RG2

You need to meet the following requirements:

1.

Internet-facing virtual machines must be protected by using network security groups (NSGs).

2.

All the virtual machines must have disk encryption enabled.

What is the minimum number of security that you should create in Azure Security Center?

A. 1

B. 2

C. 3

D. 4

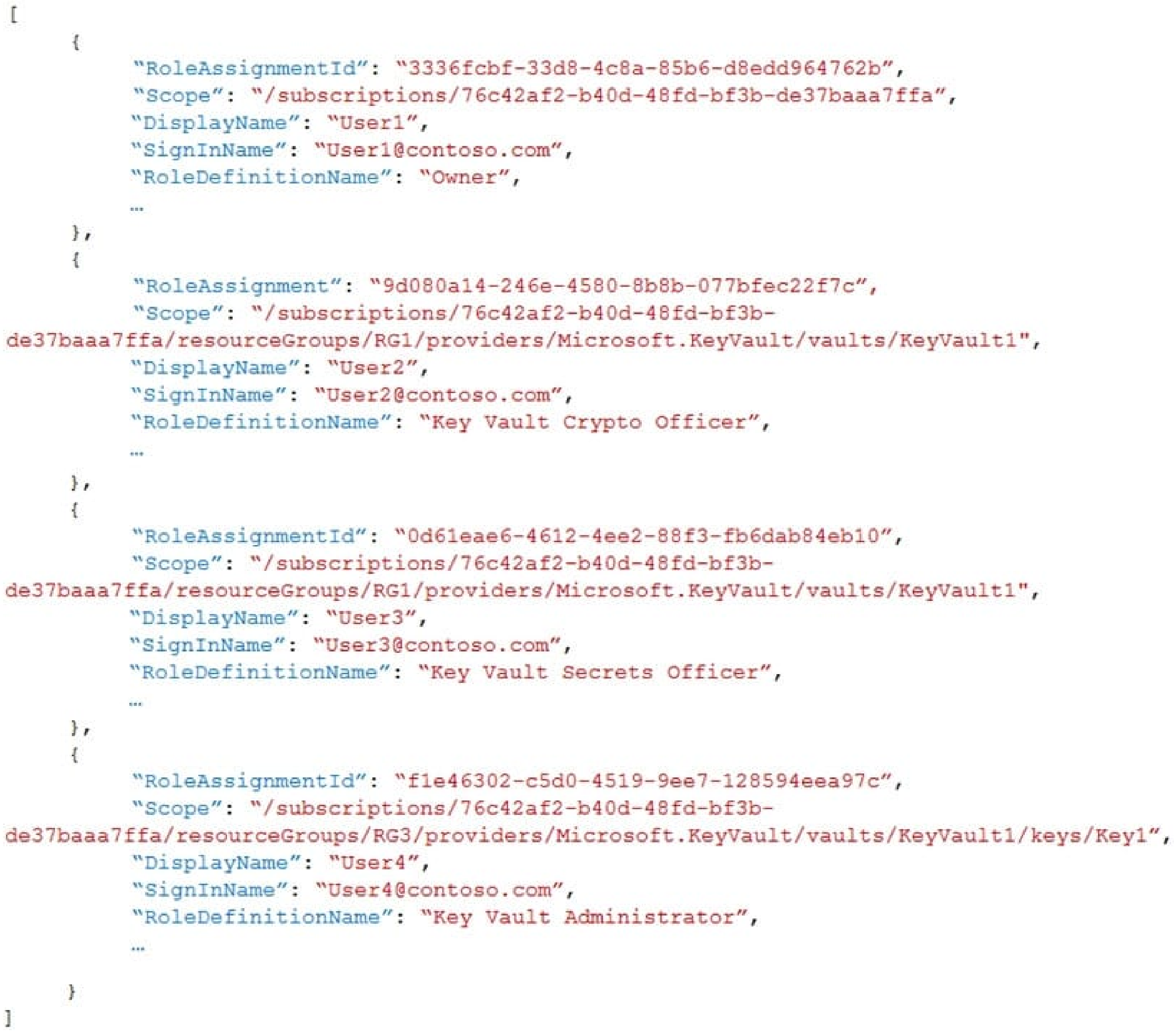
Correct Answer: B

https://learn.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept#what-is-a-security-policy An Azure Policy definition, created in Azure Policy, is a rule about specific security conditions that you want controlled. Built in definitions include things like controlling what type of resources can be deployed or enforcing the use of tags on all resources. You can also create your own custom policy definitions.

QUESTION 11

HOTSPOT

You have an Azure subscription that contains an Azure key vault. The role assignments for the key vault are shown in the following exhibit.

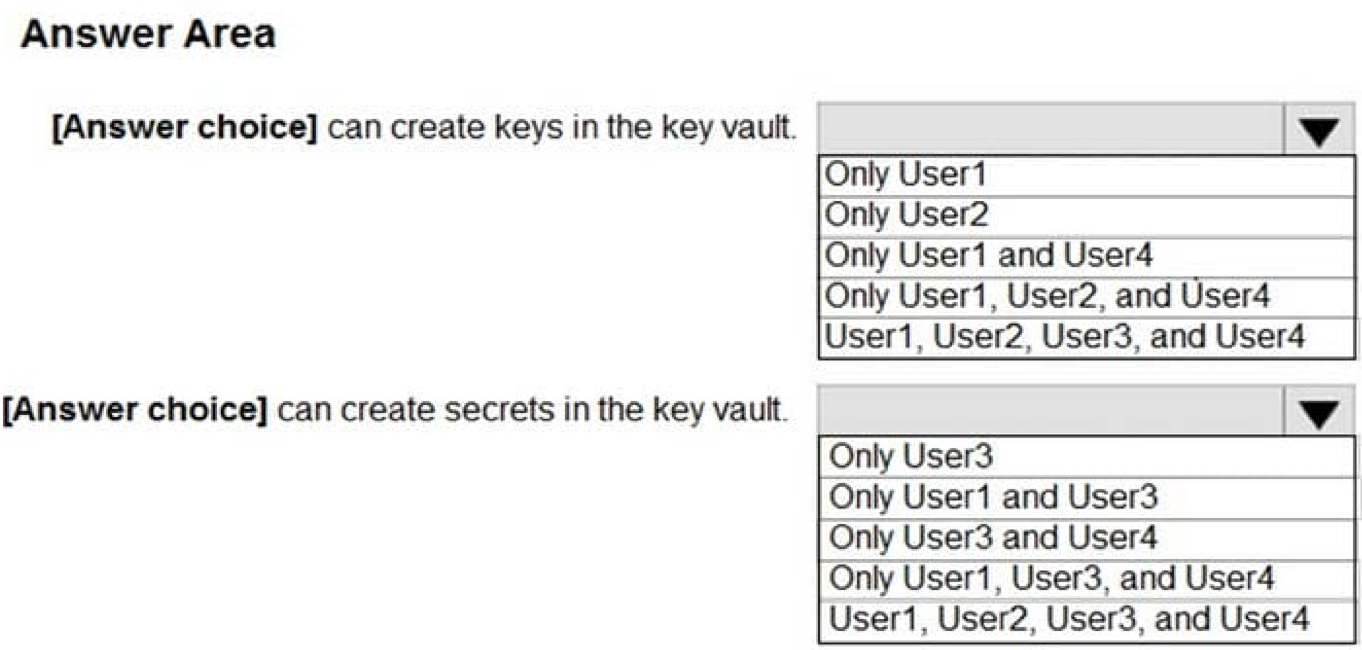


```
[
      {
            “RoleAssignmentId”: “3336fcbf-33d8-4c8a-85b6-d8edd964762b”,
            “Scope”: “/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa”,
            “DisplayName”: “User1”,
            “SignInName”: “User1@contoso.com”,
            “RoleDefinitionName”: “Owner”,
            …
      },
      {
            “RoleAssignment”: “9d080a14-246e-4580-8b8b-077bfec22f7c”,
            “Scope”: “/subscriptions/76c42af2-b40d-48fd-bf3b-
de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
            “DisplayName”: “User2”,
            “SignInName”: “User2@contoso.com”,
            “RoleDefinitionName”: “Key Vault Crypto Officer”,
            …
      },
      {
            “RoleAssignmentId”: “0d61eae6-4612-4ee2-88f3-fb6dab84eb10”,
            “Scope”: “/subscriptions/76c42af2-b40d-48fd-bf3b-
de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
            “DisplayName”: “User3”,
            “SignInName”: “User3@contoso.com”,
            “RoleDefinitionName”: “Key Vault Secrets Officer”,
            …
      },
      {
            “RoleAssignmentId”: “f1e46302-c5d0-4519-9ee7-128594eea97c”,
            “Scope”: “/subscriptions/76c42af2-b40d-48fd-bf3b-
de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1”,
            “DisplayName”: “User4”,
            “SignInName”: “User4@contoso.com”,
            “RoleDefinitionName”: “Key Vault Administrator”,
            …

      }
]
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

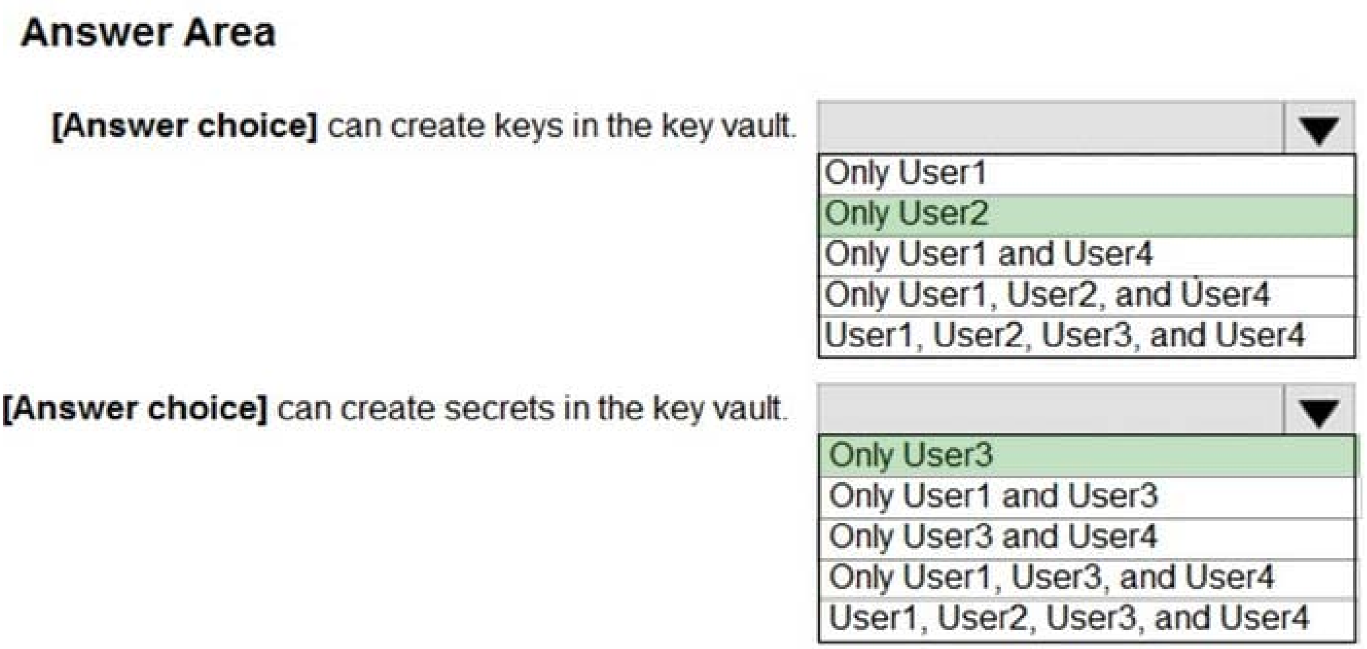
[Answer choice] can create keys in the key vault.

- Only User1
- Only User2
- Only User1 and User4
- Only User1, User2, and User4
- User1, User2, User3, and User4

[Answer choice] can create secrets in the key vault.

- Only User3
- Only User1 and User3
- Only User3 and User4
- Only User1, User3, and User4
- User1, User2, User3, and User4

Correct Answer:



Answer Area

[Answer choice] can create keys in the key vault.

- Only User1
- [✓ Only User2]
- Only User1 and User4
- Only User1, User2, and User4
- User1, User2, User3, and User4

[Answer choice] can create secrets in the key vault.

- [✓ Only User3]
- Only User1 and User3
- Only User3 and User4
- Only User1, User3, and User4
- User1, User2, User3, and User4

User1 - has ownership at subscription level therefore has access to the control plane of the key vault but not to the data plane. therefore User1 can manage RBAC permissions but cannot create/access keys or secrets (unless bthey can grant themself \\'Key Administrator\\' access and do this, which again does not show up in this RBACs listed so we cannot assume that)

-Therefore User1 has not access to the keys or secrets in this vault

User2 - Is a Key VAult Crypto officer for the KeyVault1. so according to this:https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli#azure-built-in-roles-for-key-vault-data-plane-operations , they can manage keys

(but not access secrets or manage permissions)

User3 - Is a Secrets officer for the KeyVault1 scope. they can access secrets data in this key vault

User4 - Here\\'s a tricky one. while they are indeed given \\'Key Vault Administrator\\', notice the scope is set to "../KeyVault1/Keys/Key1". So they should only be able to work with that key.

QUESTION 12

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 an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of federation with Active Directory Federation Services (AD FS).

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It\\'s up to the organization by using the federated system to make sure it\\'s deployed securely and can handle the authentication load.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

QUESTION 13

SIMULATION

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.

To complete this task, sign in to the Azure portal.

A. See the explanation below.

Correct Answer: A

To enable the RDP port in an NSG, follow these steps:

1.

Sign in to the Azure portal.

2.

In Virtual Machines, select VM1

3.

In Settings, select Networking.

4.

In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:

Priority: 300 Name: Port_3389 Port(Destination): 3389 Protocol: TCP Source: Any Destinations: Any Action: Allow

Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem

---

QUESTION 14

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 15

SIMULATION

You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

To complete this task, sign in to the Azure portal.

A. See the explanation below.

Correct Answer: A

Create an alert rule on a metric with the Azure portal

1.

In the portal, locate the resource, here VM1, you are interested in monitoring and select it.

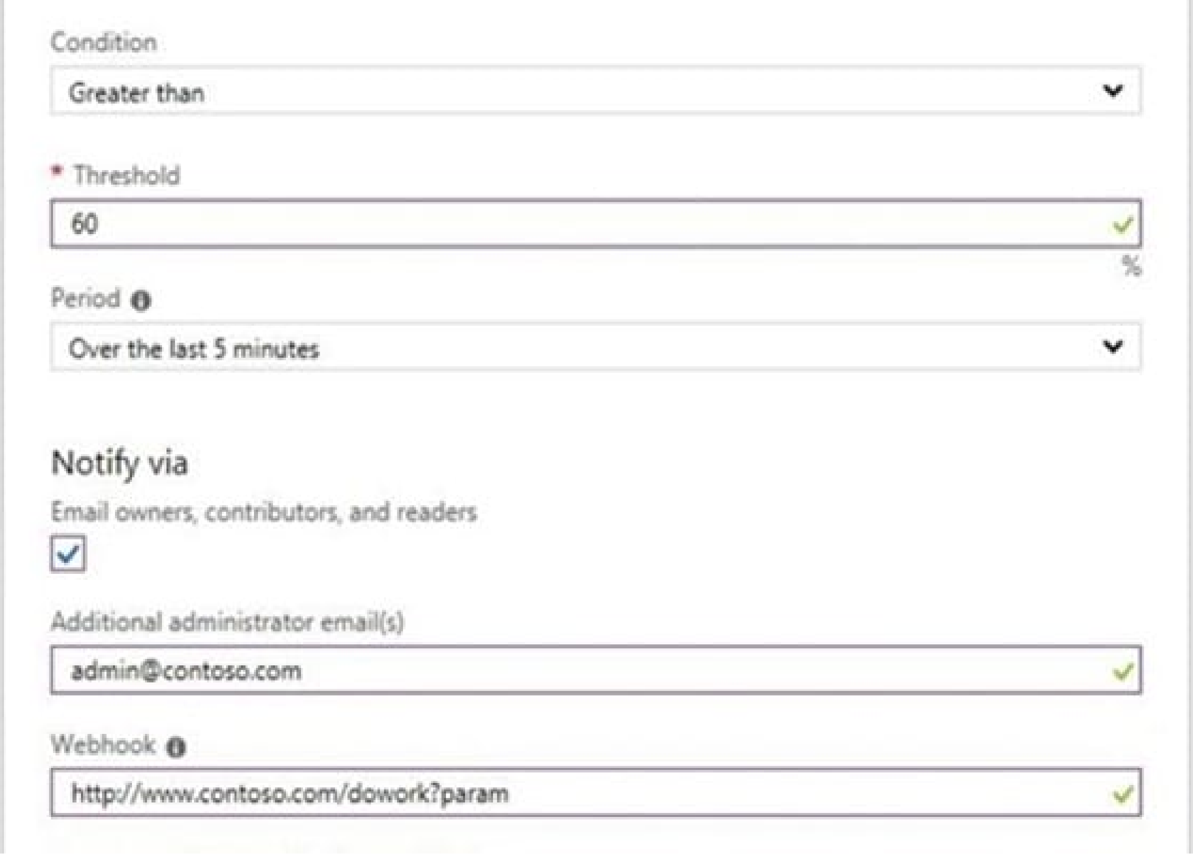
2.

Select Alerts (Classic) under the MONITORING section. The text and icon may vary slightly for different resources.

3.

Select the Add metric alert (classic) button and fill in the fields as per below, and click OK.

Metric: CPU Percentage Condition: Greater than Period: Over last 15 minutes Notify via: email Additional administrator email(s): admin1@contoso.com



Condition

Greater than

* Threshold

60 %

Period

Over the last 5 minutes

Notify via

Email owners, contributors, and readers

☑

Additional administrator email(s)

admin@contoso.com

Webhook

http://www.contoso.com/dowork?param

Reference: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-insights-alerts-portal

AZ-500 PDF Dumps AZ-500 VCE Dumps AZ-500 Practice Test