Dumps Planet

Your Partner in Success

Microsoft

AZ-500 EXAM

Microsoft Azure Security Technologies (beta)

Product: Demo File

For More Information:

https://www.dumpsplanet.com/AZ-500-dumps

QUESTION: 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies. You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.

Solution: You create a new stored access policy. Does this meet the goal?

A. Yes
B. No

Answer(s): A

Explanation:
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.

References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored- Access-Policy

QUESTION: 2

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy the On-premises data gateway to the on-premises network. Does this meet the goal?

A. Yes
B. No

Answer(s): B

Explanation:
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you

must perform the following actions: Create Azure Virtual Network.
Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server.

References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises- network

QUESTION: 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.
Solution: You create a site-to-site VPN between the virtual network and the on-premises network.
Does this meet the goal?

A. Yes
B. No

Answer(s): A

Explanation:
You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: Create Azure Virtual Network.
Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server.
References:https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises- network

QUESTION: 4

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.
You need to recommend an integration solution that meets the following requirements:

Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?

A. federated identity with Active Directory Federation Services (AD FS)

B. password hash synchronization with seamless single sign-on (SSO)
C. pass-through authentication with seamless single sign-on (SSO)

Answer(s): B

Explanation:

Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes.

Incorrect Answers:
A: 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.

C: For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.

Pass-through Authentication requires unconstrained network access to domain controllers. All network traffic is encrypted and limited to authentication requests.
References:https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

QUESTION: 5

Your network contains an on-premises Active Directory domain named corp.contoso.com.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You sync all on-premises identities to Azure AD.
You need to prevent users who have a given Name attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort. What should you use?

A. Synchronization Rules Editor
B. Web Service Configuration Tool
C. the Azure AD Connect wizard
D. Active Directory Users and Computers

Answer(s): A

Explanation:
Use the Synchronization Rules Editor and write attribute-based filtering rule.

References:https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

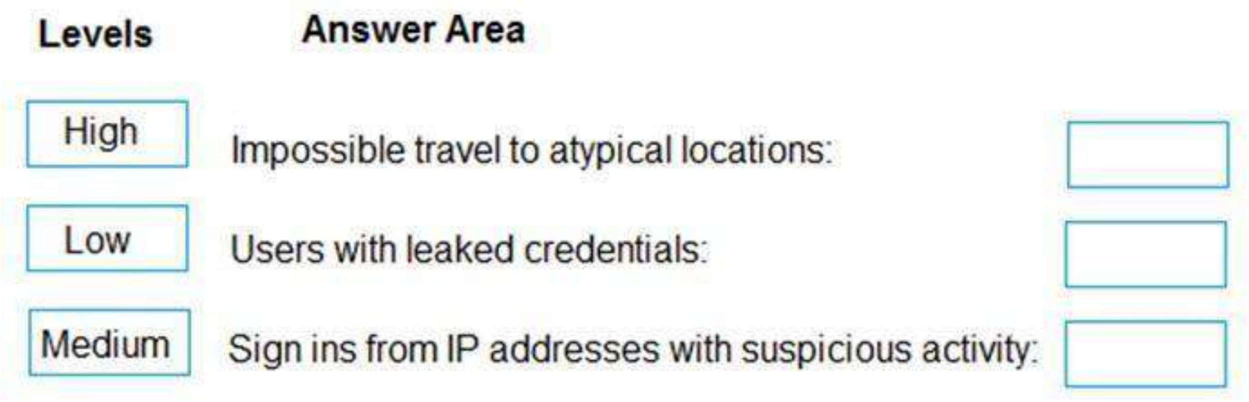
QUESTION: 6

DRAG DROP
You are implementing conditional access policies.
You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies. You need to identify the risk level of the following risk events:

- Users with leaked credentials

- Impossible travel to atypical locations
- Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.
Select and Place:



Levels

High

Low

Medium

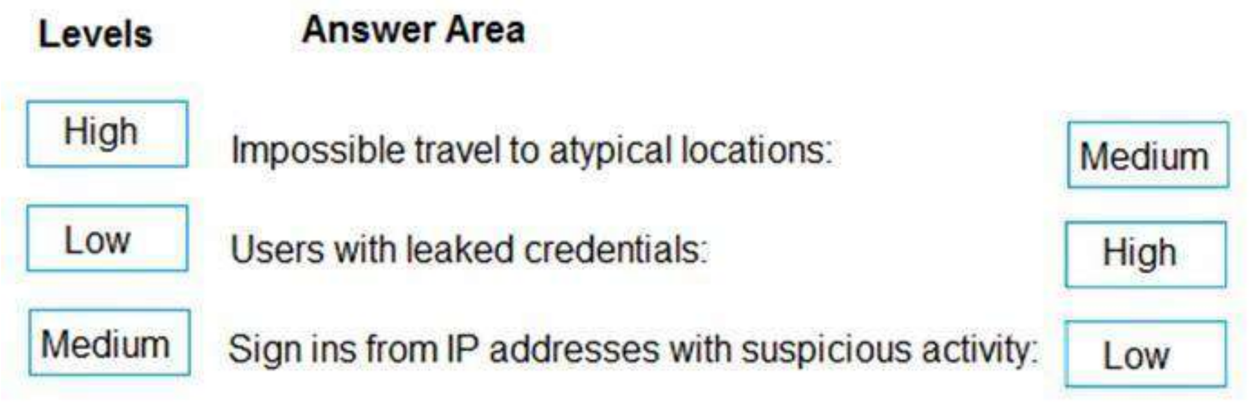
Answer Area

Impossible travel to atypical locations:

Users with leaked credentials:

Sign ins from IP addresses with suspicious activity:

Answer(s):



Levels

High

Low

Medium

Answer Area

Impossible travel to atypical locations: Medium

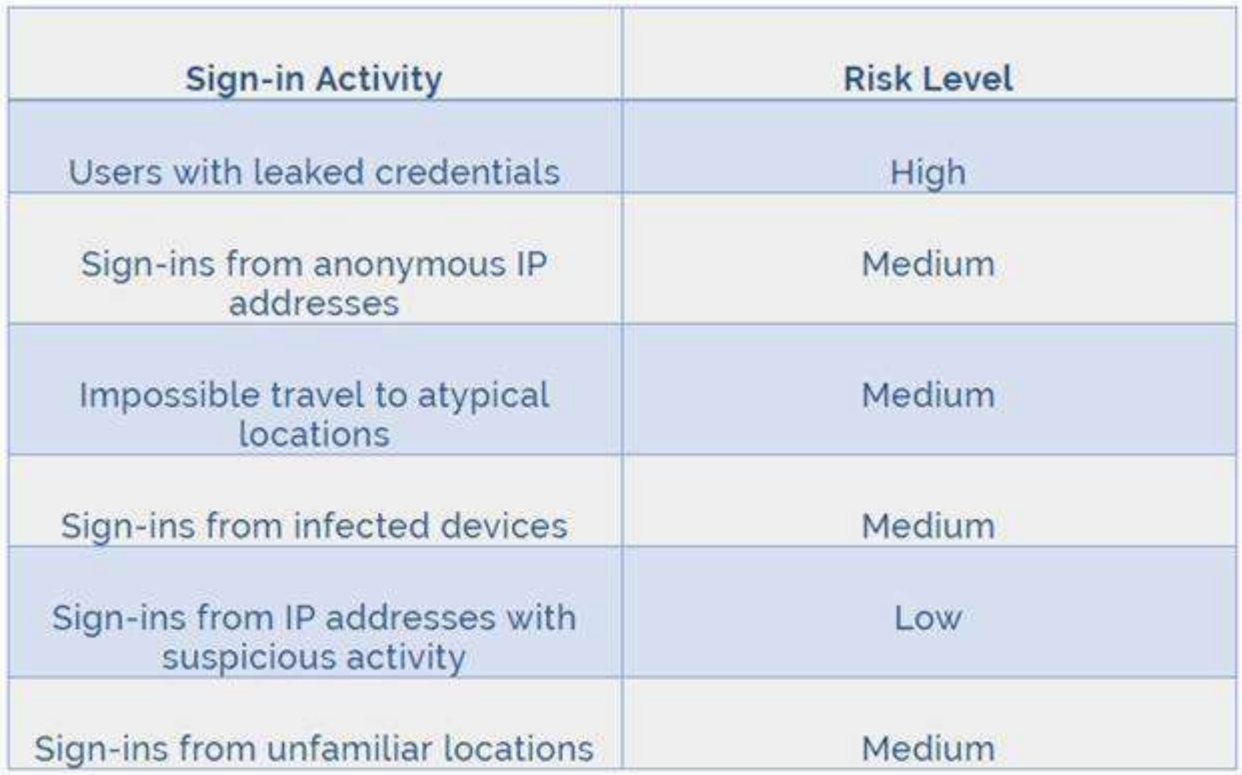
Users with leaked credentials: High

Sign ins from IP addresses with suspicious activity: Low

Explanation:
Azure AD Identity protection can detect six types of suspicious sign-in activities:

- Users with leaked credentials
- Sign-ins from anonymous IP addresses
- Impossible travel to atypical locations
- Sign-ins from infected devices
- Sign-ins from IP addresses with suspicious activity
- Sign-ins from unfamiliar locations

These six types of events are categorized in to 3 levels of risks – High, Medium & Low:

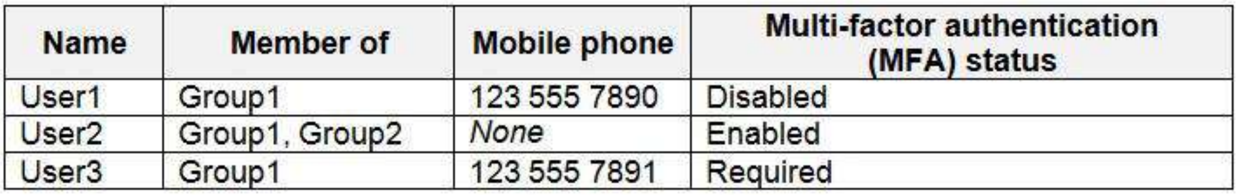


Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

QUESTION: 7

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

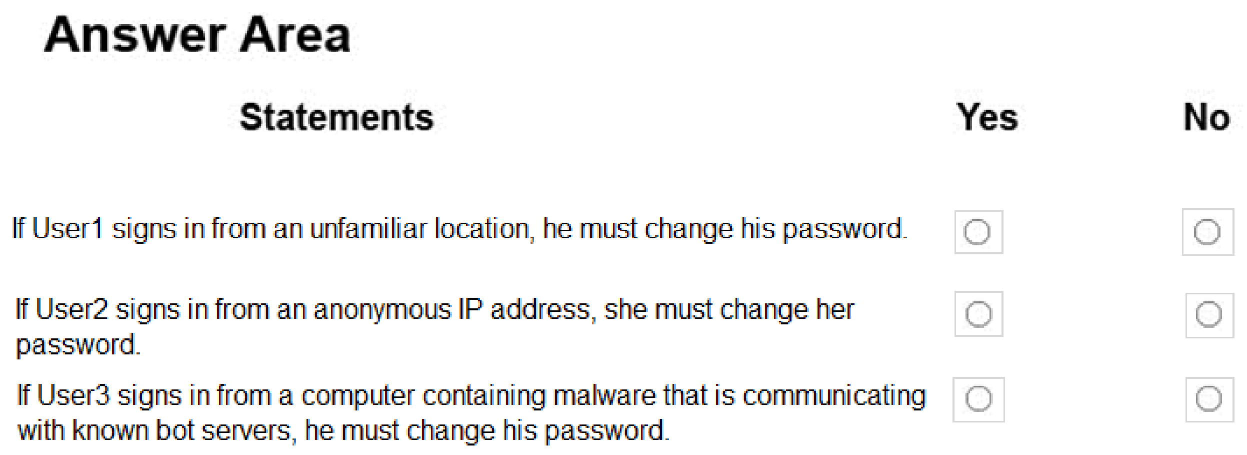


Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	*None*	Enabled
User3	Group1	123 555 7891	Required

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

- Assignment: Include Group1, Exclude Group2
- Conditions: Sign-in risk of Medium and above
- Access: Allow access, Require password change

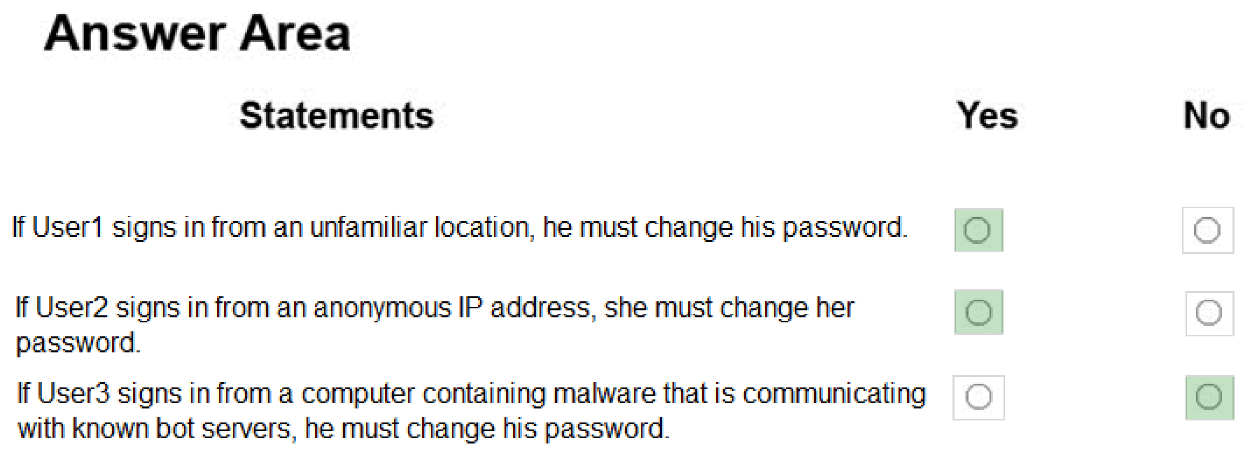
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	○	○
If User2 signs in from an anonymous IP address, she must change her password.	○	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	○

Answer(s):



Answer Area

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	[✓ ○]	○
If User2 signs in from an anonymous IP address, she must change her password.	[✓ ○]	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	[✓ ○]

Explanation:

Box 1: Yes
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.

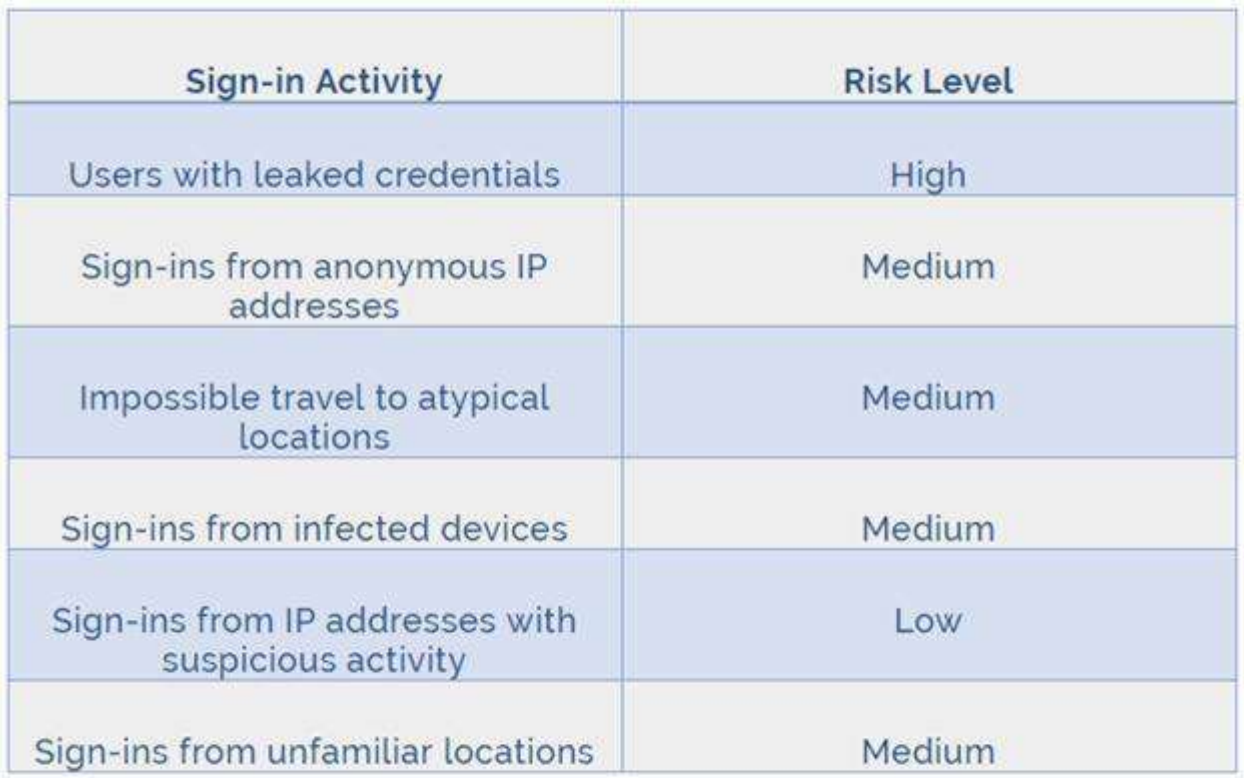
Box 2: Yes
User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.

Box 3: No
Sign-ins from IP addresses with suspicious activity is low. Note:

Azure AD Identity protection can detect six types of suspicious sign-in activities:

- Users with leaked credentials
- Sign-ins from anonymous IP addresses
- Impossible travel to atypical locations
- Sign-ins from infected devices
- Sign-ins from IP addresses with suspicious activity
- Sign-ins from unfamiliar locations

These six types of events are categorized in to 3 levels of risks – High, Medium & Low:

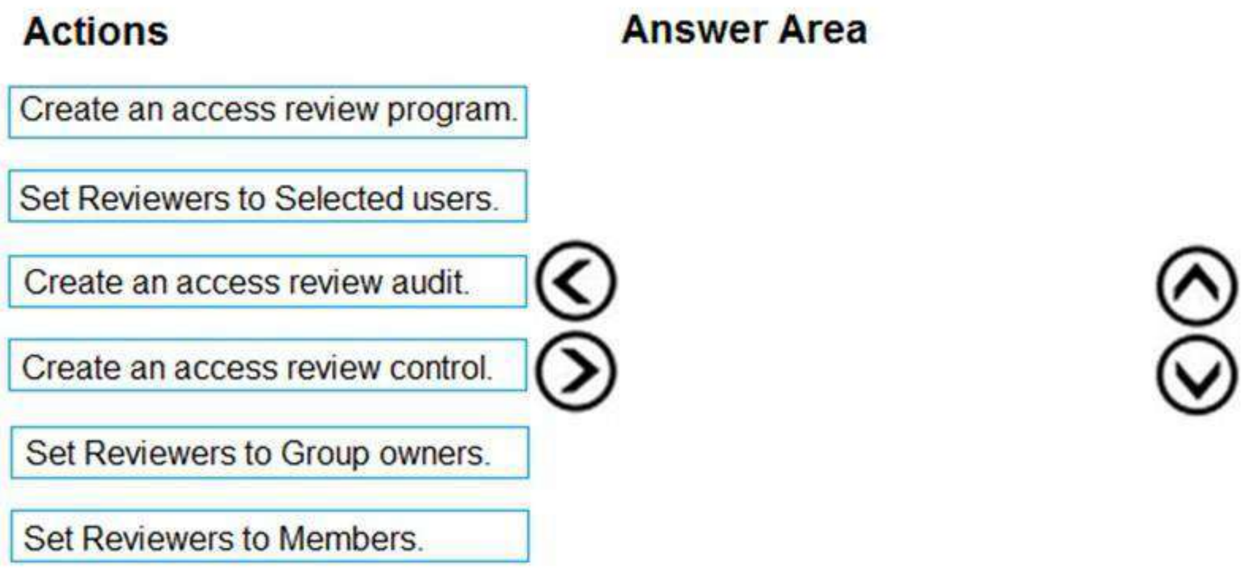


Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

References:http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

QUESTION: 8
DRAG DROP
You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:

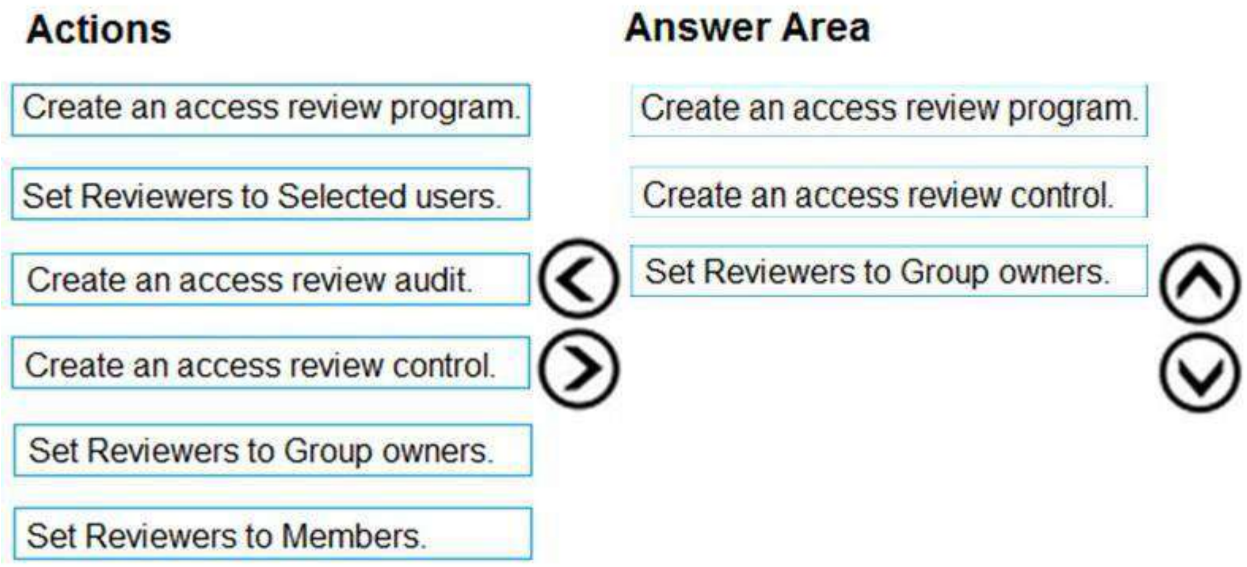


Actions

- Create an access review program.
- Set Reviewers to Selected users.
- Create an access review audit.
- Create an access review control.
- Set Reviewers to Group owners.
- Set Reviewers to Members.

Answer Area

Answer(s):



Actions

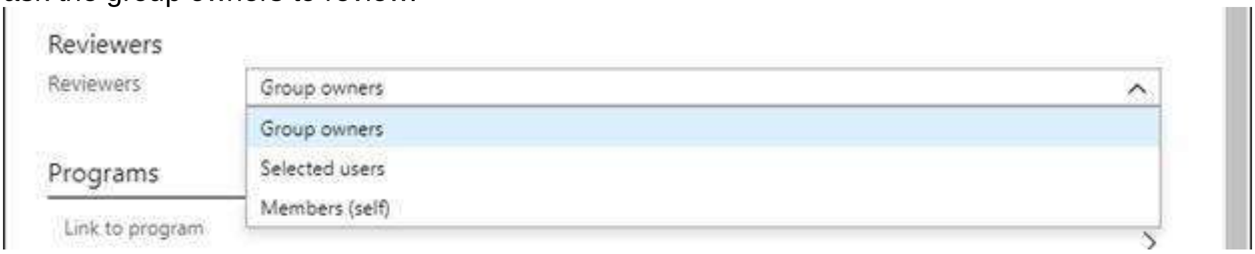
- Create an access review program.
- Set Reviewers to Selected users.
- Create an access review audit.
- Create an access review control.
- Set Reviewers to Group owners.
- Set Reviewers to Members.

Answer Area

- Create an access review program.
- Create an access review control.
- Set Reviewers to Group owners.

Explanation:
Step 1: Create an access review program
Step 2: Create an access review control Step 3: Set Reviewers to Group owners

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



Reviewers

Reviewers: Group owners

- Group owners
- Selected users
- Members (self)

Programs

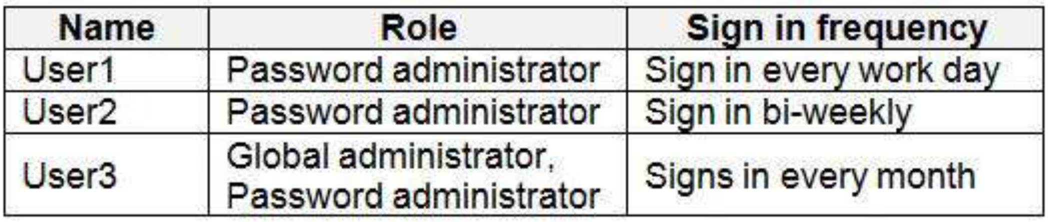
Link to program

References:https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

QUESTION: 9

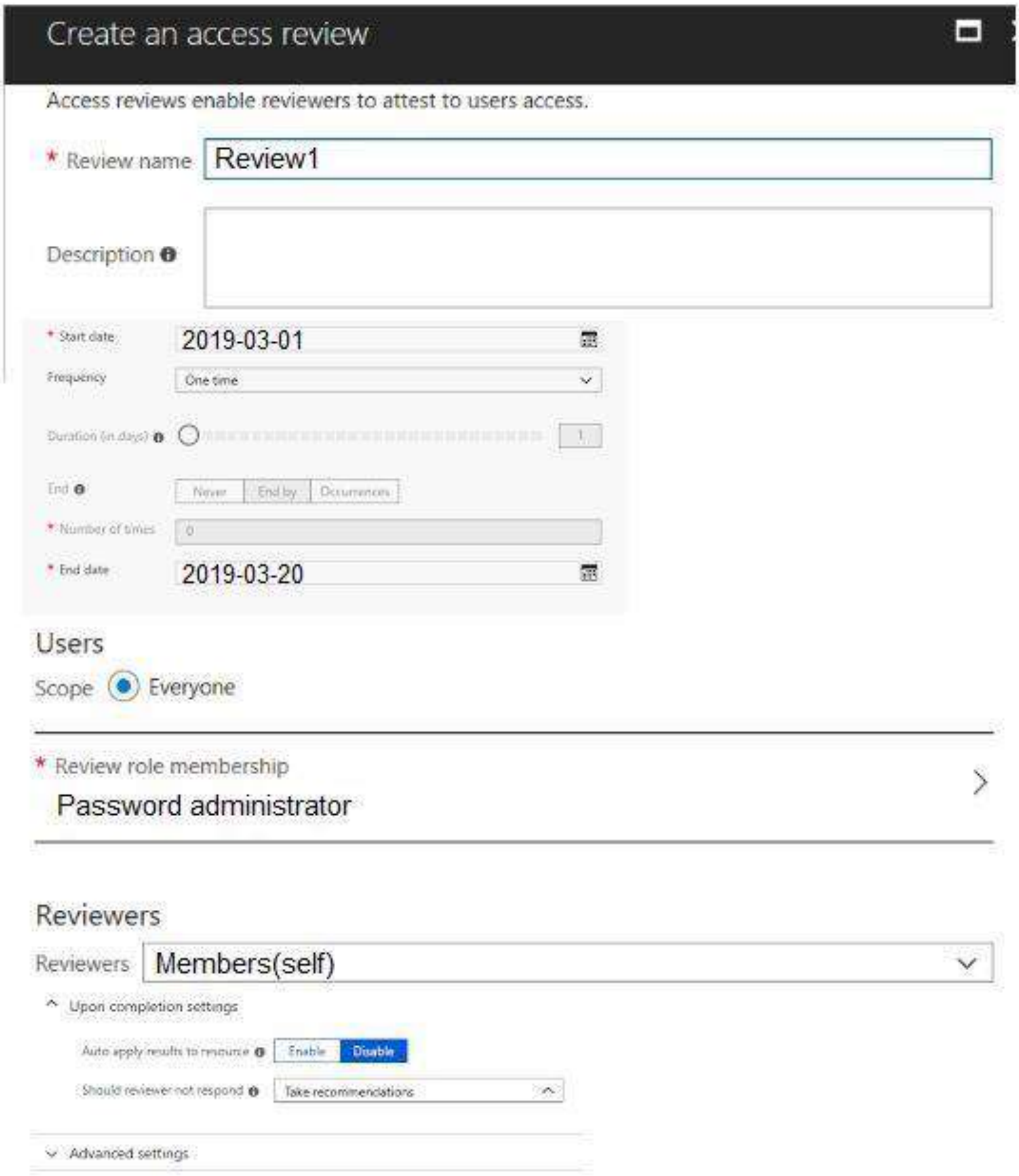
HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Role	Sign in frequency
User1	Password administrator	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

You configure an access review named Review1 as shown in the following exhibit.



Create an access review

Access reviews enable reviewers to attest to users access.

* Review name: Review1

Description:

* Start date: 2019-03-01

Frequency: One time

Duration (in days): 1

End: Never | End by | Occurrences

* Number of times: 0

* End date: 2019-03-20

Users

Scope ● Everyone

* Review role membership

Password administrator

Reviewers

Reviewers: Members(self)

Upon completion settings

Auto apply results to resource: Enable | Disable

Should reviewer not respond: Take recommendations

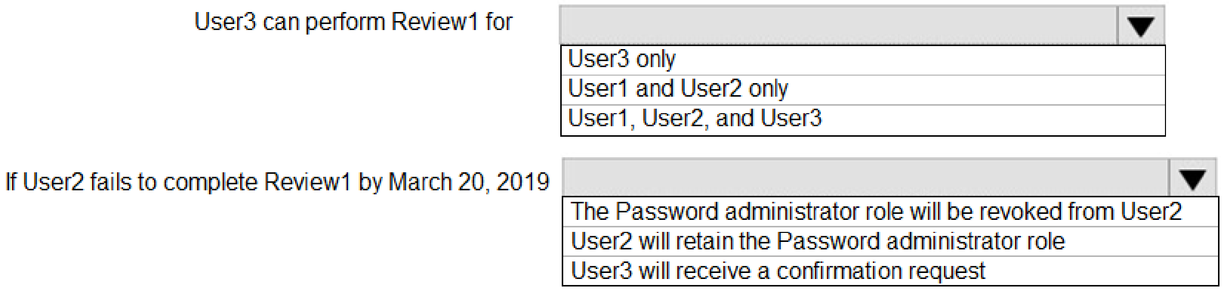
Advanced settings

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:

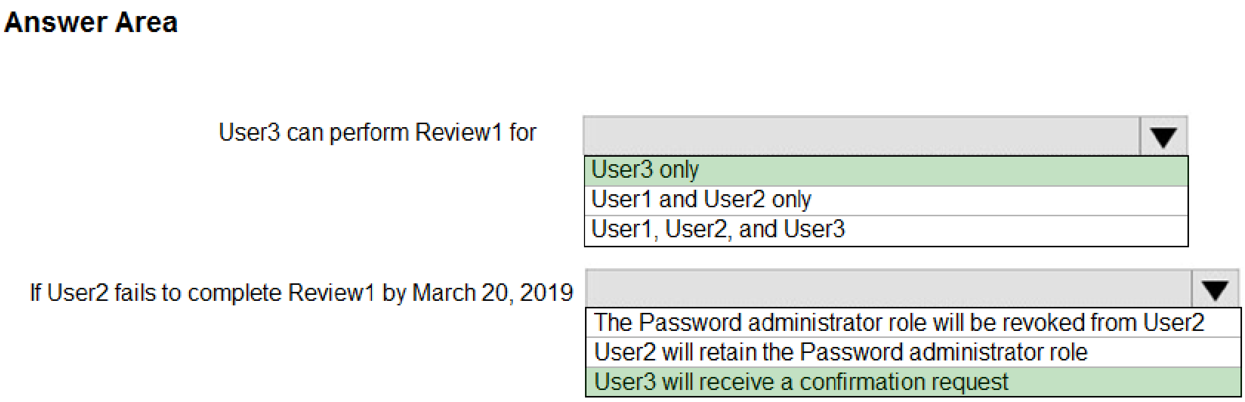
Answer Area



User3 can perform Review1 for ▼
- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019 ▼
- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

Answer(s):



Answer Area

User3 can perform Review1 for ▼

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

If User2 fails to complete Review1 by March 20, 2019 ▼

The Password administrator role will be revoked from User2
User2 will retain the Password administrator role
[✓ User3 will receive a confirmation request]

Explanation:
Box 1: User3 only
Use the Members (self) option to have the users review their own role assignments.

Thank You for Trying Our Product

Our Certification Exam Features:

★ More than **99,900 Satisfied Customers**Worldwide

★ Average **99.9%**Success Rate

★**Free Update**to match latest and real exam scenarios

★**Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF format.**

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**

★**100%** Guaranteed Success.

★ Fast, helpful support 24x7

View Certification Exam page for Full Product:

https://www.dumpsplanet.com/AZ-500-dumps