

Latest Version: 11.0

Question: 1

You need to meet the authentication requirements for leaked credentials. What should you do?

- A. Enable federation with PingFederate in Azure AD Connect.
- B. Configure Azure AD Password Protection.
- C. Enable password hash synchronization in Azure AD Connect.
- D. Configure an authentication method policy in Azure AD.

Answer: C

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity>

Question: 2

You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements. What should you configure?

- A. named locations that have a private IP address range
- B. named locations that have a public IP address range
- C. trusted IPs that have a public IP address range
- D. trusted IPs that have a private IP address range

Answer: C

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>
Location offer your country set, IP ranges MFA trusted IP and corporate network VPN gateway IP address: This is the public IP address of the VPN device for your on-premises network. The VPN device requires an IPv4 public IP address. Specify a valid public IP address for the VPN device to which you want to connect. It must be reachable by Azure Client Address space: List the IP address ranges that you want routed to the local on-premises network through this gateway. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks your virtual network connects to, or with the address ranges of the virtual network itself.

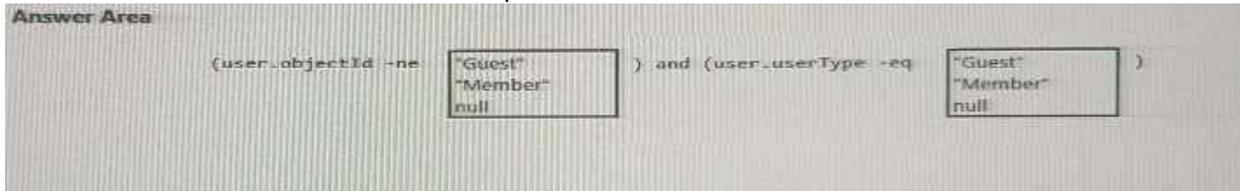
Question: 3

HOTSPOT

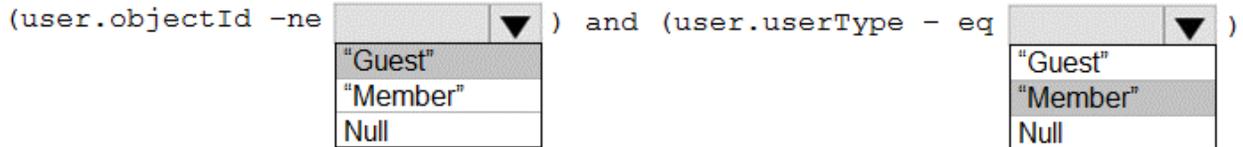
You need to create the LWGroup1 group to meet the management requirements.

How should you complete the dynamic membership rule? To answer, drag the appropriate values to the correct targets. Each value 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.



Answer:



Question: 4

You need to configure the detection of multi staged attacks to meet the monitoring requirements. What should you do?

- A. Customize the Azure Sentinel rule logic.
- B. Create a workbook.
- C. Add an Azure Sentinel playbook.
- D. Add Azure Sentinel data connectors.

Answer: D

Question: 5

HOTSPOT

You need to implement password restrictions to meet the authentication requirements.

You install the Azure AD password Protection DC agent on DC1.

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

NOTE: Each correct selection is worth one point.

Answer Area

Configure the Azure AD Password Protection proxy service on:

DC1
SERVER1
SERVER2

Configure the password list:

In Azure AD
On DC1
On SERVER1
On SERVER2

Answer:

Answer Area

Configure the Azure AD Password Protection proxy service on:

DC1
SERVER1
SERVER2

Configure the password list:

In Azure AD
On DC1
On SERVER1
On SERVER2