IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **SC-300**

Title : Microsoft Identity and Access Administrator

Version : DEMO

1. Topic 1, Litware, Inc

Overview
Litware, Inc. is a pharmaceutical company that has a subsidiary named fabrikam, inc Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled. Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection polices in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

On-premises Environment
The on-premises network contains the severs shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Delegation Requirements
Litware identifies the following delegation requirements:
* Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
* Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant-
* Use custom catalogs and custom programs for Identity Governance.
* Ensure that User1 can create enterprise applications in Azure AD. Use the principle of least privilege.

Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by
modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to Microsoft 365 group that he appropriate license assigned.

Management Requirement
Litware wants to create a group named LWGroup1 will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Authentication Requirements
Litware identifies the following authentication requirements:
• Implement multi-factor authentication (MFA) for all Litware users.
• Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
• Implement a banned password list for the litware.com forest.
• Enforce MFA when accessing on-premises applications.
• Automatically detect and remediate externally leaked credentials

Access Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

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

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: B

Explanation:

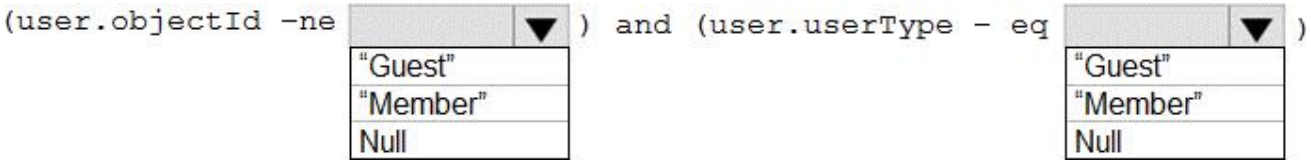
Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

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.

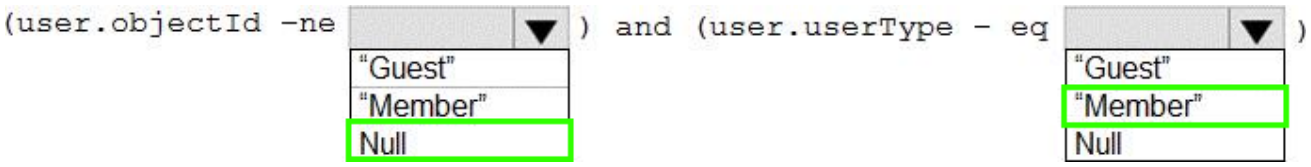
3.HOTSPOT

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 many need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Null

"Member"

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.

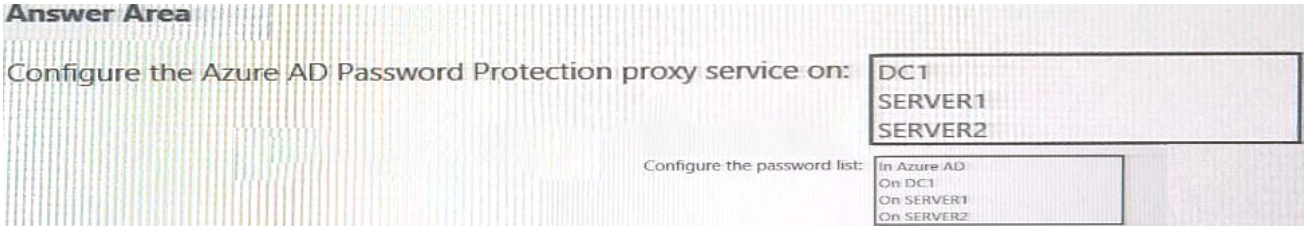
Answer: D

5.HOTSPOT

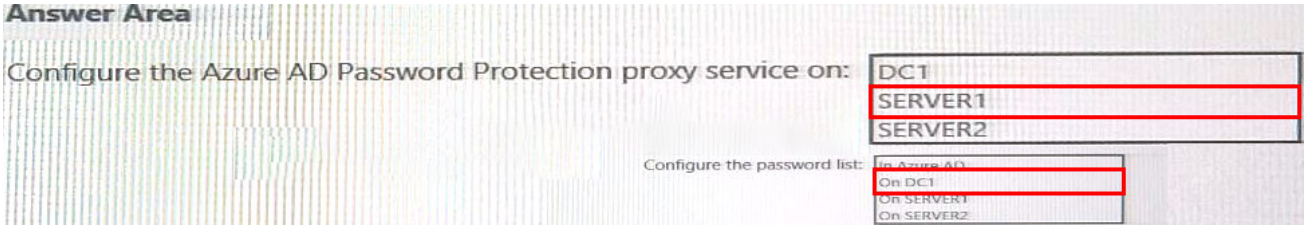
You need to implement password restrictions to meet the authentication requirements.

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:



Explanation:

Server1

On DC1