Microsoft

SC-300

Microsoft Identity and Access Administrator

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 26.9

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

Explanation:
Explanation:
In SC-300, Azure AD Identity Protection is the prescribed control to “automatically detect and remediate externally leaked credentials.” That specific user risk—Leaked credentials—relies on Microsoft comparing known breached username/password pairs with what Azure AD can evaluate. The study materials explain that Identity Protection “detects leaked credentials when Microsoft finds a match with the user’s current credentials,” and also note that password hash synchronization (PHS) can be enabled even if your sign-in method is Pass-through Authentication or federation. A common exam call-out is that without PHS, Azure AD has no hash to compare, so the leaked-credential signal is unavailable. Enabling PHS (you can keep PTA as the active sign-in method) allows Identity Protection to raise user risk and enforce policy actions such as require password change or block access. By contrast, Azure AD Password Protection addresses banned/weak passwords at change time, not breached-credential telemetry; federation choices (e.g., PingFederate) don’t deliver the leaked-credential signal; and authentication method policy controls how users perform MFA (e.g., methods) rather than whether leaked credentials are detected. Therefore, to meet the requirement to “automatically detect and remediate externally leaked credentials,” the minimum correct step is to enable password hash synchronization while retaining PTA—exactly as recommended in SC-300 guidance.

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

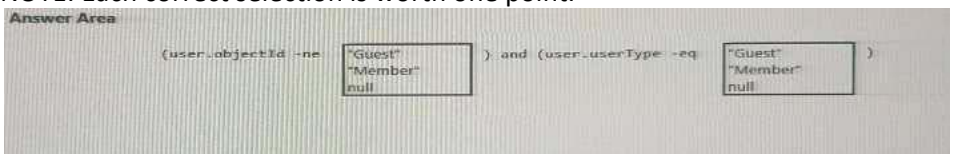
C. trusted IPs that have a public IP address range
D. trusted IPs that have a private IP address range

Answer: B

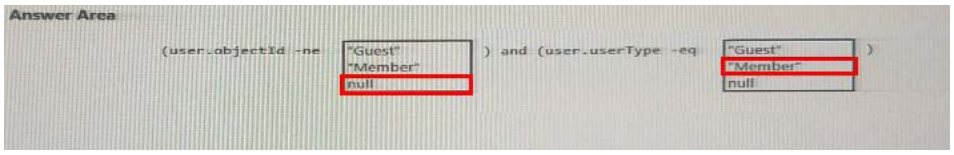
Explanation:
SC-300 emphasizes using Conditional Access with named locations to scope MFA—especially to exclude trusted corporate egress IPs. The materials state that administrators can define named locations by public IP ranges and "mark them as trusted" for policy exceptions. This aligns with the requirement: enforce MFA for all users, but exempt users authenticating from the Boston office. Because Azure AD evaluates the client's public egress address, private RFC1918 ranges are never seen by Azure AD on the internet, so defining private IP ranges would not work. Likewise, the legacy "Trusted IPs" setting belongs to the old per-user MFA service settings; SC-300 guidance prefers Conditional Access named locations for modern MFA deployments and for combining with other conditions (apps, platforms, user risk, locations). Implementing the Boston office as a named location using its public egress IP range(s), and marking it trusted, lets you exclude that location from the tenant-wide MFA policy while still meeting the broader requirement to enforce MFA for everyone else and for on-prem apps published via Azure AD Application Proxy. In short: define Boston's public IP as a named location and use it in your Conditional Access policy exclusion to satisfy the exemption precisely and securely.

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



Answer:



Explanation:
According to the Microsoft Identity and Access Administrator (SC-300) Exam Ref and the Azure AD Dynamic Membership Rules documentation, when you create a dynamic group in Azure Active

Directory (now Entra ID), you define rules that automatically add or remove users based on their attributes.
The scenario requires a group named LWGroup1 that contains all Azure AD user accounts for Litware but excludes all guest accounts. In Azure AD, internal users created within the tenant are designated with the attribute user.userType = "Member", while external or guest accounts from partner organizations have user.userType = "Guest".
To ensure only internal (Litware) users are included, the membership rule must:
Ensure the user object exists — by checking (user.objectId -ne null) which confirms that the rule only applies to valid user objects.
Include only members, excluding guests — by filtering with (user.userType -eq "Member").
Hence, the dynamic rule that satisfies these conditions is:
(user.objectId -ne null) and (user.userType -eq "Member")
This rule guarantees that LWGroup1 dynamically includes all internal users from litware.com and excludes all external users or guest accounts (such as Fabrikam users).
This logic aligns precisely with the Microsoft Learn module “Manage groups in Azure Active Directory” and SC-300 study guide section “Implement and manage dynamic membership rules”, which states:
“Use user.userType to distinguish between internal members and external guests when configuring membership rules for dynamic groups.”
 Correct Answe r:
(user.objectId -ne null) and (user.userType -eq "Member")

Question: 4

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

Azure AD Password Protection has two components: the DC agent (installed on domain controllers) and the proxy service (installed on one or more member servers). The SC-300 materials and Microsoft Identity Governance guidance explain that the proxy service is required when domain controllers do not have direct internet access. The proxy retrieves the password protection policy and custom banned password list from Azure AD over outbound HTTPS and makes it available to DC agents. The documentation further states that you should deploy at least one proxy per forest and two for high availability, and that domain controllers do not need internet connectivity when a proxy is deployed. In this scenario, DCs are explicitly blocked from internet access, so the proxy must be placed on member servers. Both SERVER1 (Application Proxy connector) and SERVER2 (Azure AD Connect) are domain-joined member servers with internet connectivity and are appropriate locations for the AzureADPasswordProtectionProxy service; selecting both provides the recommended redundancy. The custom banned password list is configured in Azure AD at the tenant level (as part of Azure AD Password Protection settings), not on individual servers. Once configured, the policy and list are downloaded by the proxy and enforced by the DC agent during password set or change operations, satisfying the requirement to implement a banned password list for the litware.com forest.

Question: 5

HOTSPOT
You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE:Each correct selection is worth one point.

Azure AD Connect settings to modify:
- Directory Extensions
- Domain Filtering
- Optional Features

Assign Azure AD licenses to:
- An Azure Active Directory group that has only nested groups
- An Azure Active Directory group that has the Assigned membership type
- An Azure Active Directory group that has the Dynamic User membership type

Answer:

Azure AD Connect settings to modify:
- **Directory Extensions**
- Domain Filtering
- Optional Features

Assign Azure AD licenses to:
- An Azure Active Directory group that has only nested groups
- An Azure Active Directory group that has the Assigned membership type
- **An Azure Active Directory group that has the Dynamic User membership type**

Explanation:

In the SC-300 coverage of Azure AD Connect and Identity Governance, Microsoft explains that to surface a custom on-premises attribute in Azure AD you must enable Directory extensions in Azure AD Connect. The guide states that “Directory extensions lets you synchronize additional attributes from on-premises Active Directory to Azure AD so they are available in the cloud directory for apps and policy.” This is the supported way to bring a custom attribute (here, LWLicenses) from the litware.com forest into Azure AD so it can be referenced by cloud features such as dynamic group rules. Domain filtering or optional features do not expose a new attribute to Azure AD; directory extensions does.

For license automation, the SC-300 materials on group-based licensing and dynamic groups emphasize that “licenses can be assigned to Azure AD groups; group members then inherit the licenses, and when membership changes, licenses are added or removed automatically.” They further note that “dynamic user groups evaluate rules against user attributes to add or remove users without manual effort,” and that “nested groups are not supported for license inheritance—only direct members receive licenses.” Using the synced LWLicenses attribute in a Dynamic User group rule (for example, user.extensionAttribute… -eq "E5") ensures users are automatically added to the correct group and therefore receive the specified licenses without administrative intervention, fully meeting Litware’s requirement to “manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute.”

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/