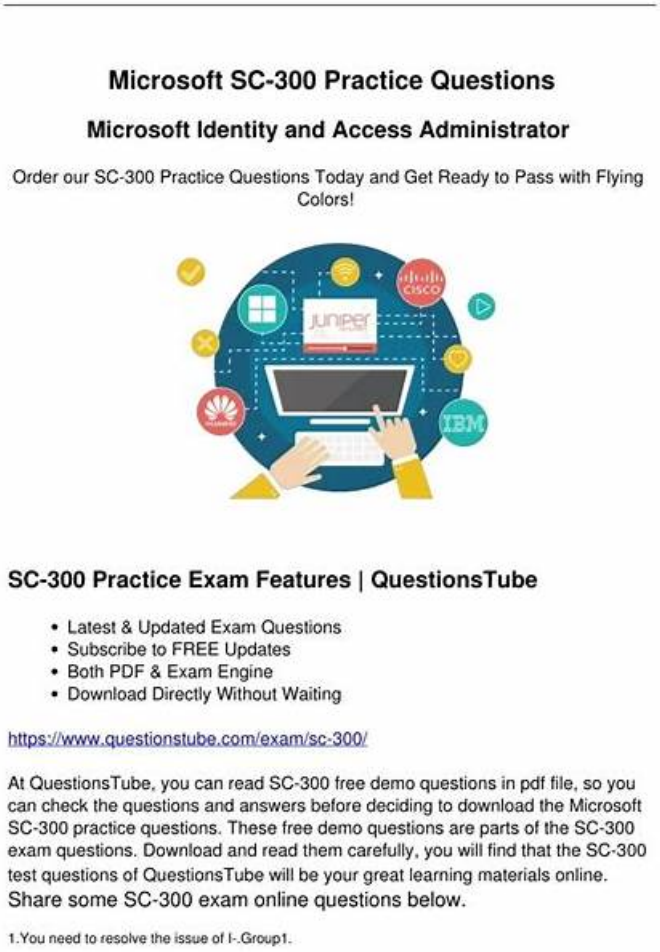
Free PDF Quiz High Pass-Rate Microsoft - Latest SC-300 Study Notes



DOWNLOAD the newest DumpsReview SC-300 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=16Fgq7Mc_iAScfLY6ade6xoBmpA009cUp

To pass the Microsoft Identity and Access Administrator (SC-300) certification exam you need to prepare well with the help of top-notch SC-300 exam questions which you can download from DumpsReview platform. On this platform, you will get valid, updated, and real DumpsReview SC-300 Dumps for quick exam preparation.

DumpsReview has built customizable Microsoft SC-300 practice exams (desktop software & web-based) for our customers. Users can customize the time and SC-300 questions of Microsoft SC-300 Practice Tests according to their needs. You can give more than one test and track the progress of your previous attempts to improve your marks on the next try.

>> Latest SC-300 Study Notes <<

DumpsReview Offers Valid and Real SC-300 Microsoft Identity and Access Administrator Exam Questions

Learning with our SC-300 learning guide is quiet a simple thing, but some problems might emerge during your process of SC-300 exam materials or buying. Considering that our customers are from different countries, there is a time difference between us, but we still provide the most thoughtful online after-sale service twenty four hours a day, seven days a week, so just feel free to contact with

us through email anywhere at any time. Our commitment of helping you to Pass SC-300 Exam will never change. Considerate 24/7 service shows our attitudes, we always consider our candidates' benefits and we guarantee that our SC-300 test questions are the most excellent path for you to pass the exam.

The SC-300 certification exam is intended for IT professionals who have experience working with Microsoft identity and access management technologies. It is recommended that candidates have at least one year of experience working with Microsoft Azure Active Directory or Microsoft identity technologies. Additionally, candidates should have a solid understanding of networking concepts, as well as experience working with Windows Server and Active Directory.

Microsoft SC-300 (Microsoft Identity and Access Administrator) Certification Exam is designed to test the skills and knowledge of IT professionals regarding managing identity and access in Microsoft Azure Active Directory (AAD) and Microsoft 365. SC-300 exam is intended for those who are responsible for managing identities and access in their organizations, such as administrators or security professionals. Microsoft Identity and Access Administrator certification is a valuable asset for IT professionals who want to demonstrate their expertise in identity and access management in Microsoft environments.

Microsoft SC-300 Exam is an essential certification for individuals who want to enhance their skills and knowledge in managing and securing identity and access solutions in Microsoft Azure and other Microsoft cloud services. By passing SC-300 exam and earning the certification, candidates can demonstrate their proficiency to potential employers and advance their careers in the IT and security industry.

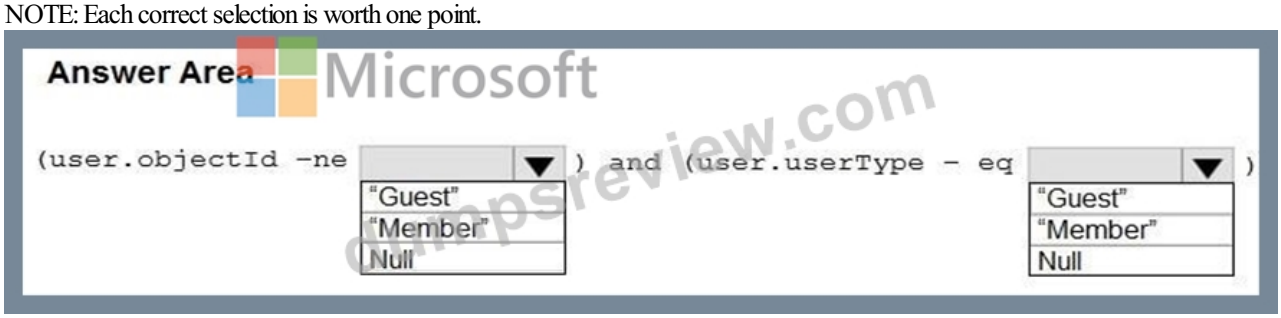
Microsoft Identity and Access Administrator Sample Questions (Q31-Q36):

NEW QUESTION # 31
Case Study 2 - 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.
Existing Environment. Identify 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.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies 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.
Existing Environment. On-premises Environment
The on-premises network contains the servers 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.
Requirements. 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.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicensesto the litware.com Active Directory forest. Litware wants to

manage the assignment of Azure AD licenses by modifying the value of the LWLicensesattribute. Users who have the appropriate value for LWLicensesmust be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management 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.
Requirements. 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.
Requirements. Access Requirements
Litware identifies the following access requirements:
* Control all access to all Azure resources and Azure AD applications by using conditional access policies.
* Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
* Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.
Hotspot Question
You need to create the LWGroup1 group to meet the management requirements.
How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

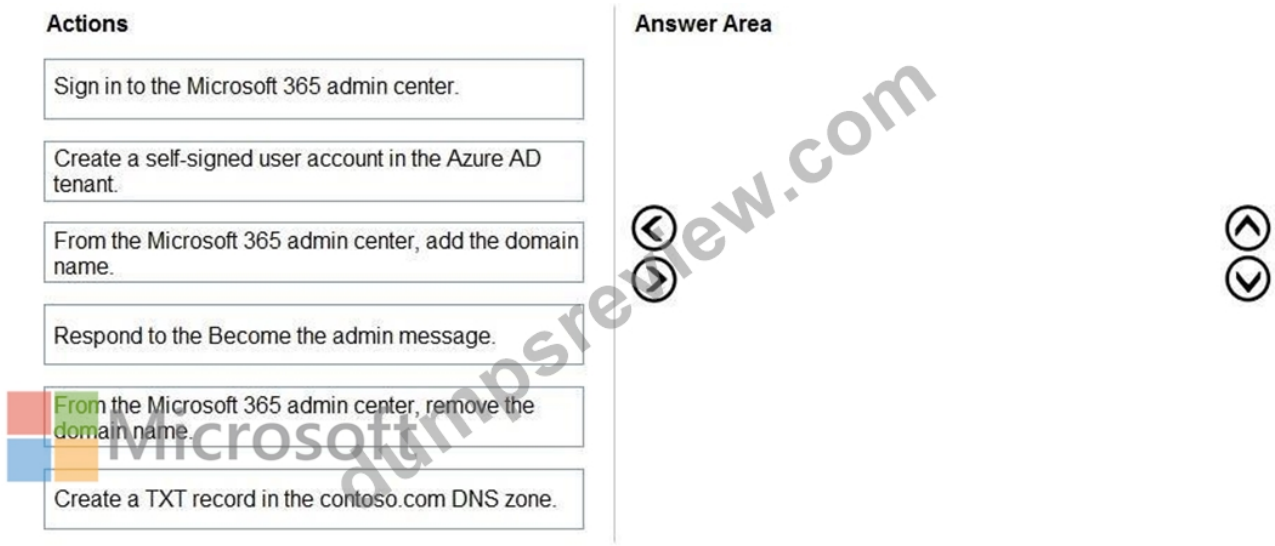


Answer:

Explanation:

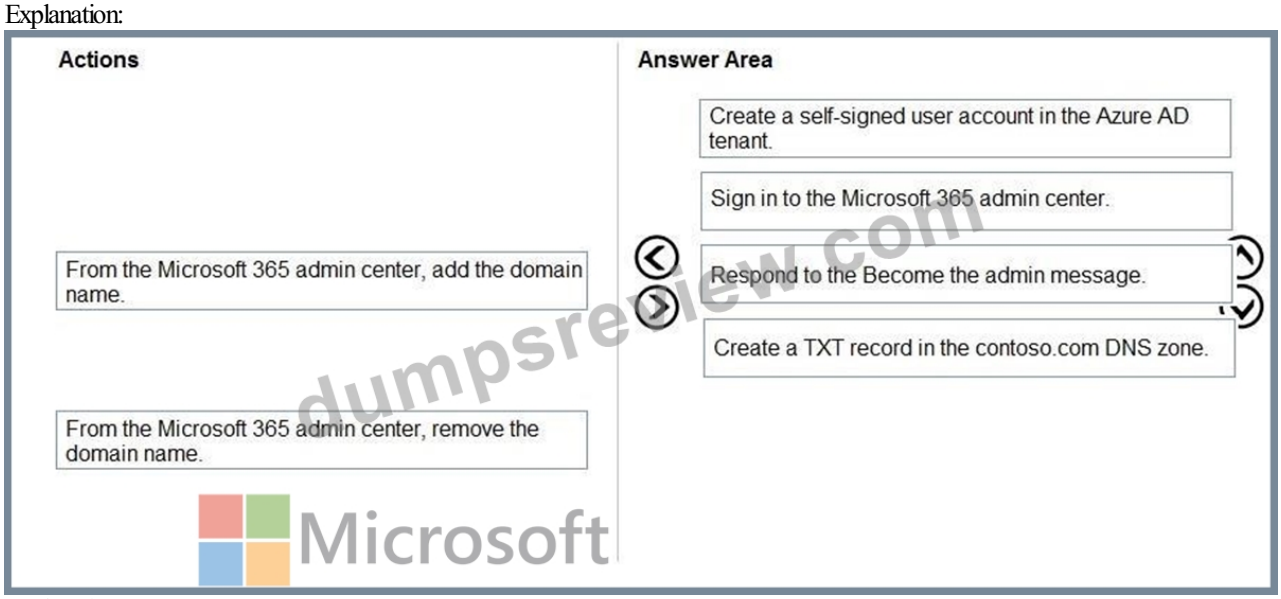
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/use-dynamic-groups#creating-a-group-of-members-only

NEW QUESTION # 32
Drag and Drop Question
You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com.
You discover that users use their email address for self-service sign-up to Microsoft 365 services.
You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed users.
Which four 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.



Answer:

Explanation:



Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover

NEW QUESTION # 33
Case Study 2 - 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.
Existing Environment. Identify 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.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies 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.

Existing Environment. On-premises Environment

The on-premises network contains the servers 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.

Requirements. 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.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicensesto the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicensesattribute. Users who have the appropriate value for LWLicensesmust be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management 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.

Requirements. 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.

Requirements. Access Requirements

Litware identifies the following access requirements:

* Control all access to all Azure resources and Azure AD applications by using conditional access policies.
* Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
* Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

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

Hotspot Question

You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.

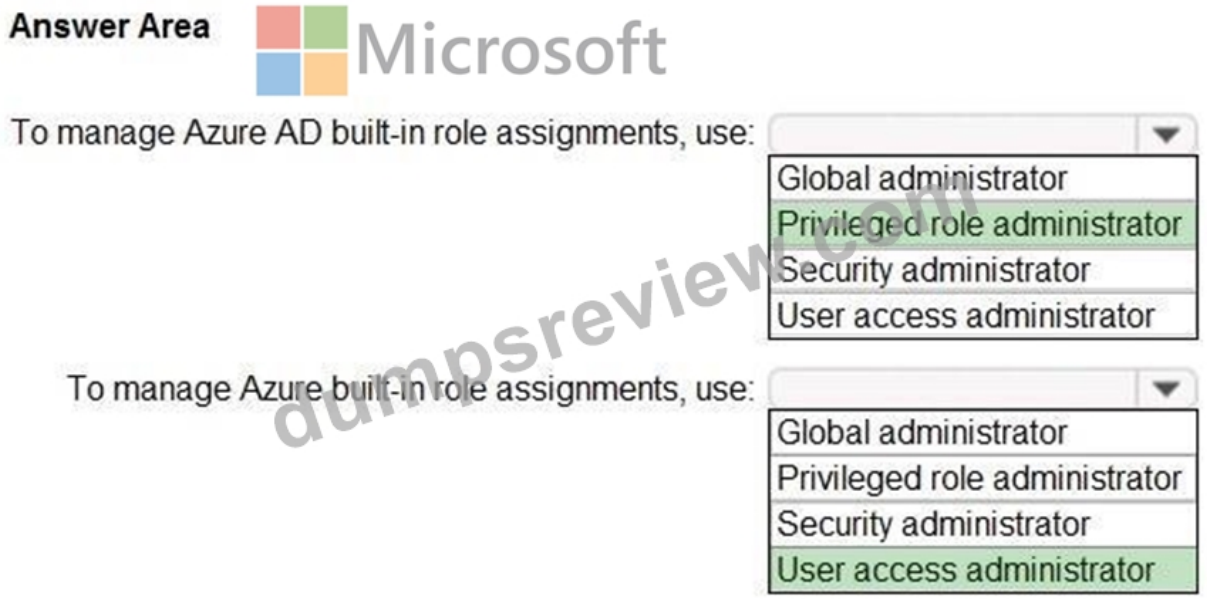
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

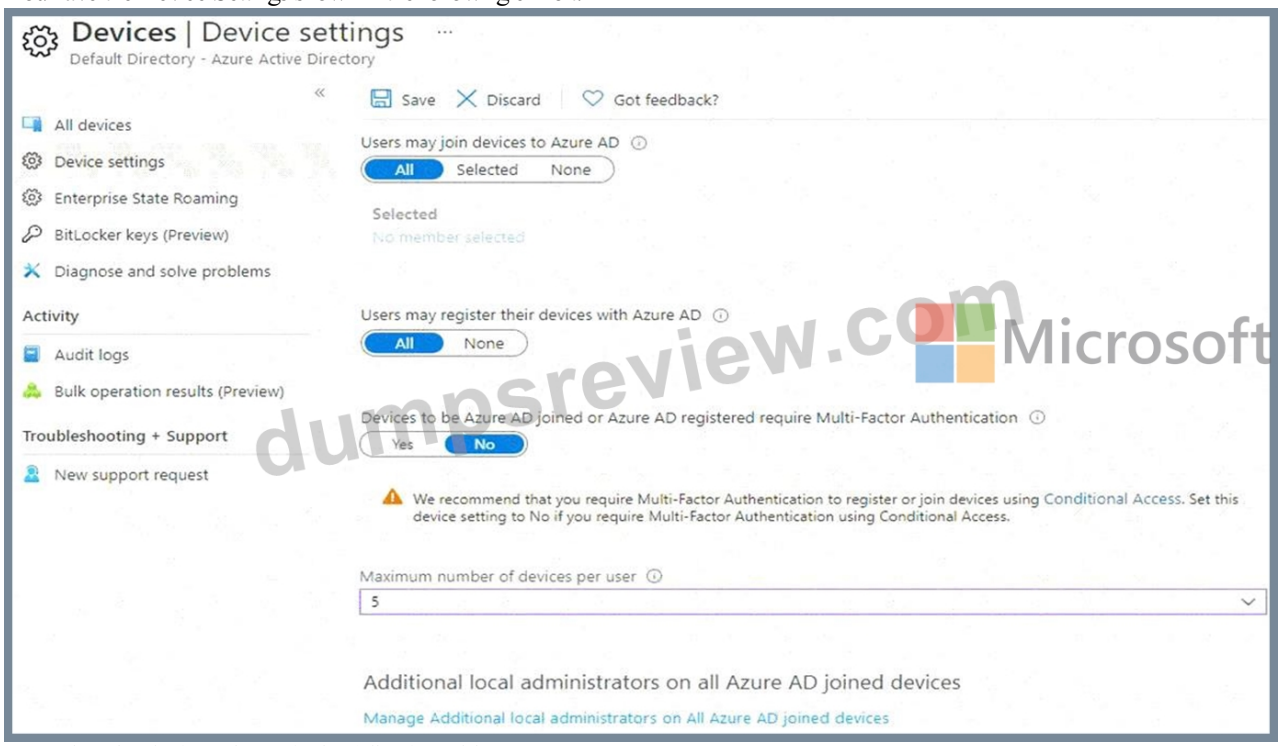


Explanation:
For Azure AD roles in Privileged Identity Management, only a user who is in the Privileged Role Administrator or Global Administrator role can manage assignments for other administrators.
Global Administrators, Security Administrators, Global Readers, and Security Readers can also view assignments to Azure AD roles in Privileged Identity Management.
For Azure resource roles in Privileged Identity Management, only a subscription administrator, a resource Owner, or a resource User Access administrator can manage assignments for other administrators. Users who are Privileged Role Administrators, Security Administrators, or Security Readers do not by default have access to view assignments to Azure resource roles in Privileged Identity Management.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- configure

NEW QUESTION # 34
You have an Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium Plan 2 license. The tenant contains the users shown in the following table.

Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	None

You have the Device Settings shown in the following exhibit.



User1 has the devices shown in the following table.

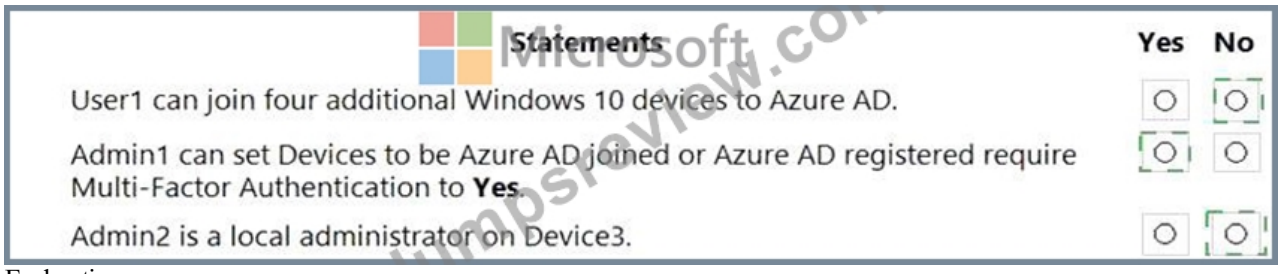
Name	Operating system	Device identity
Device1	Windows 10	Azure AD joined
Device2	iOS	Azure AD registered
Device3	Windows 10	Azure AD registered
Device4	Android	Azure AD registered

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

Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	○	○
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Answer:

Explanation:



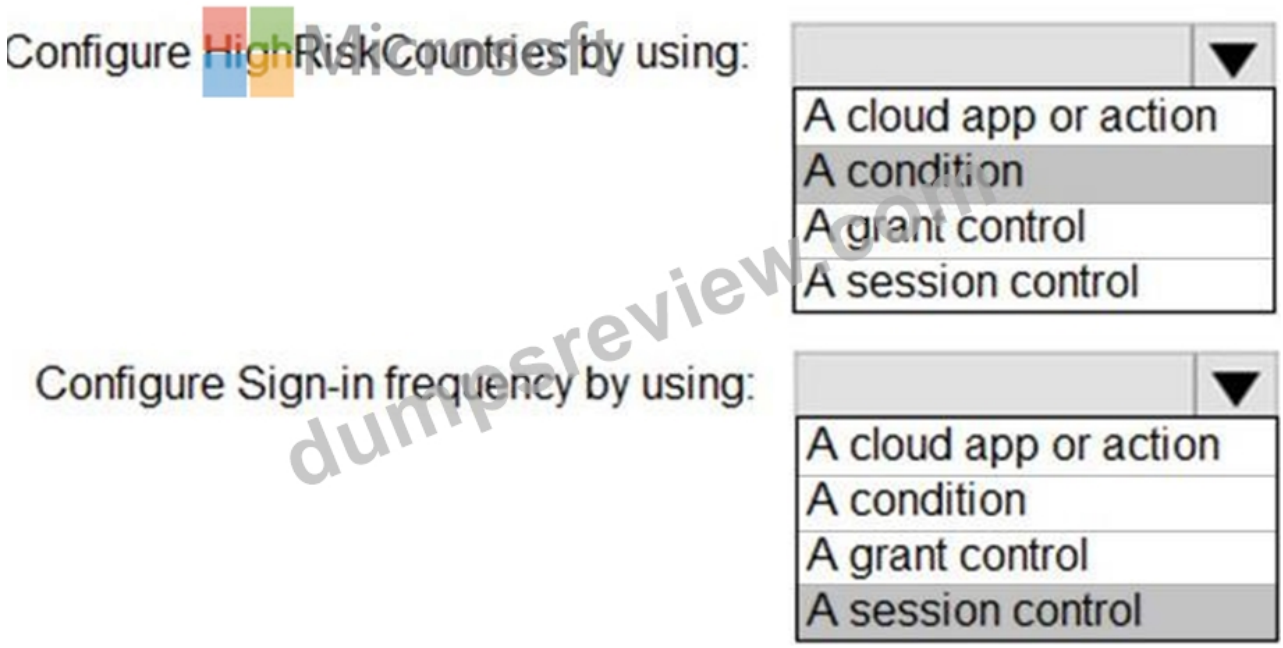
Explanation:
< User1 can join four additional Windows 10 devices to Azure AD. # No
2## Admin1 can set "Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication" to Yes. # Yes
3## Admin2 is a local administrator on Device3. # No
This scenario draws from Module: Manage device identities in Azure Active Directory in the Microsoft SC-300 Official Study Guide and Microsoft Learn content.
In the Device Settings, the "Maximum number of devices per user" is configured as 5. User1 already has one Azure AD joined device (Device1) and three Azure AD registered devices (Device2, Device3, Device4).
Since both Azure AD joined and Azure AD registered devices count toward the same limit, User1 has already registered 4 devices. This means they can add only one more, not four additional Windows 10 devices.
Therefore, the statement is No.
Microsoft documentation states: "The maximum number of devices per user setting applies collectively to all Azure AD-joined and Azure AD-registered devices." The Cloud Device Administrator role (Admin1's role) has the delegated permissions to manage device settings in Azure AD, including enforcing MFA requirements for device registration and join operations. The role allows management of the Azure AD device configuration blade, including toggling settings like MFA for join/register, join limits, and device ownership policies. Therefore, Admin1 can enable the MFA requirement for device join/registration.
As per Microsoft Learn: "Cloud Device Administrator can manage all aspects of device settings, including device join and registration MFA requirements." Admin2 holds the Device Administrator role. However, per Microsoft's documentation, only Azure AD- joined Windows 10 devices grant local administrator rights to users in the Device Administrator role. Azure AD-registered devices (such as Device3) are personal devices that do not have local administrator assignment through Azure AD roles. Since Device3 is Azure AD registered, not joined, Admin2 is not a local admin on it.
Microsoft guidance clarifies: "Users assigned to the Device Administrator role are added as local administrators only on Azure AD-joined devices, not on Azure AD-registered or hybrid devices."

NEW QUESTION # 35
You have a Microsoft 36S tenant.
You create a named location named HighRiskCountries that contains a list of high-risk countries.
You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country.
What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation
Graphical user interface, text, application Description automatically generated



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

NEW QUESTION # 36
.....

If you have been very panic sitting in the examination room, our SC-300 actual exam allows you to pass the exam more calmly and calmly. After you use our products, our SC-300 study materials will provide you with a real test environment before the SC-300 Exam. After the simulation, you will have a clearer understanding of the exam environment, examination process, and exam outline. And our SC-300 learning guide will be your best choice.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, building.lv, shortcourses.russellcollege.edu.au, qiyue.net, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, pct.edu.pk, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of DumpsReview SC-300 dumps from Cloud Storage: https://drive.google.com/open?id=16Fgq7Mc_iAScfLY6ade6xoBmpA009cUp