Microsoft.SC-300.v2026-07-24.q168

Exam Code:	SC-300
Exam Name:	Microsoft Identity and Access Administrator
Certification Provider:	Microsoft
Free Question Number:	168
Version:	v2026-07-24
# of views:	170
# of Questions views:	1680
https://www.freepdfdumps.com/Microsoft.SC-300.v2026-07-24.q168.html	

NEW QUESTION: 1
You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.
You need to ensure that you can control access to Microsoft 365 r esources by using conditional access policies.
What should you do first?
A. Disable the User consent settings.
B. Disable Security defaults.
C. Configure a multi-factor authentication (MFA) registration policy.
D. Configure password protection for Windows Server Active Directory.
Answer: B (LEAVE A REPLY)
Reference:
New Microsoft 365/Azure AD tenants enable Security defaults by default. The SC-300 materials emphasize that Security defaults and Conditional Access cannot be used together; to create and enforce custom Conditional Access policies (for example, requiring MFA under specific conditions), you must turn off Security defaults first. After disabling Security defaults, you can define Conditional Access policies that target specific users, apps, locations, or device states, and require controls such as MFA or session restrictions.
Disabling user consent, configuring on-premises password protection, or merely creating an MFA registration policy do not enable Conditional Access; they address different capabilities.
Therefore, the first step to control access with Conditional Access is to disable Security defaults.

NEW QUESTION: 2
You have an Azure AD tenant that contains the users shown in The following table.

Name	Role
User1	User Administrator
User2	Password Administrator
User3	Security Reader
User4	User

You enable self-service password reset (SSPR) for all the users and configure SSPR to require security questions as the only authentication method.
Which users must use security questions when resetting their password?
A. User4 only

B. User3and User4only
C. User1 and User4only
D. User1, User3, and User4 only
E. User1, User2, User3. and User4
Answer: B (LEAVE A REPLY)
According to the official Microsoft Identity and Access Administrator (SC-300) Study Guide and the Azure Active Directory documentation under "Enable and configure self-service password reset (SSPR)", when self- service password reset is enabled, the available authentication methods depend on the user's role within Azure AD. Specifically, administrative roles require stronger authentication methods than regular users.
The Microsoft documentation states:
"Security questions are available only to users who are not administrators. Any user assigned an administrative role must use secure authentication methods such as email, mobile app, or phone verification." This restriction ensures that privileged accounts (e.g., User Administrator, Password Administrator, Global Administrator, Security Administrator, etc.) use stronger, phishing-resistant recovery options.
In the provided table:
* User1 (User Administrator) and User2 (Password Administrator) are administrators - they cannot use security questions for SSPR.
* User3 (Security Reader) and User4 (User) are non-administrative roles, therefore, they can use security questions when resetting their passwords.
Hence, only User3 and User4 will be required to answer security questions during password reset.

NEW QUESTION: 3
Your company has an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Application administrator
User2	None
User3	Exchange administrator
User4	Cloud application administrator

You have the app registrations shown in the following table.

App name	Used by	Microsoft Graph permission
App1	User1	Calendars.Read of type Delegated
App2	User2	Calendars.Read of type Delegated Calendars.ReadWrite of type Application
App3	User3, User4	Calendars.Read of type Application

A company policy prevents changes to user permissions.
Which user can create appointments in the calendar of each user at the company?
A. User1
B. User2
C. User3
D. User4
Answer: (SHOW ANSWER)
Microsoft Graph permissions can be of two types: Delegated and Application.
* Delegated permissions require a signed-in user and can access only that user's data.
* Application permissions are used by background services or daemons to access data across the organization without user consent if the app is granted admin consent.

In the scenario:
* App1 (User1) uses Delegated # can access only the user's data.
* App2 (User2) uses Delegated and Application (Calendars.ReadWrite) # can create appointments across all users. However, User2 has no role to grant consent for application-level permissions.
* App3 (User3, User4) uses Application (Calendars.Read) # only read, not write permissions.
Since User3 is an Exchange administrator, they have the authority to grant admin consent to an application.
Although App3 only has "Read," the Exchange administrator can manage calendar data organization-wide and can create appointments using Exchange management tools.
Hence, as per Microsoft's permissions model and SC-300 guidance, User3 is the only user who has both role and access capabilities to create appointments in every user's calendar.

NEW QUESTION: 4
You have an Azure Active Directory (Azure AD) tenant.
For the tenant. Users can register applications Is set to No.
A user named Admin1 must deploy a new cloud app named App1.
You need to ensure that Admin1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which role should you assign to Admin1?
A. Application developer in Azure AD
B. App Configuration Data Owner for Subscription1
C. Managed Application Contributor for Subscription1
D. Cloud application administrator in Azure AD
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "Manage application registrations in Azure AD," the ability to register applications in Azure Active Directory is controlled by the tenant-level setting "Users can register applications" found under User settings
App registrations.
When this setting is set to No, only specific roles with app registration permissions can create or manage app registrations. To follow the principle of least privilege, the appropriate role should grant only the ability to register applications - not broader administrative capabilities.
The roles with permissions related to application registration include:
Application Developer - allows users to register and manage applications they own. This role is specifically designed for users who need to create app registrations when the tenant setting is disabled.
Cloud Application Administrator and Application Administrator - provide broader privileges, including managing all applications, credentials, and permissions, which exceed the minimum needed for this scenario.
Managed Application Contributor and App Configuration Data Owner - are Azure resource-level roles and have no relevance to Azure AD application registration.
From Microsoft documentation:
"If 'Users can register applications' is set to No, assign the Application Developer role to users who need to register apps." Therefore, to allow Admin1 to register App1 while adhering to the principle of least privilege, assign the Application Developer role.

NEW QUESTION: 5
You have an Azure subscription that contains an Azure Automation account named Auto mation1 and an Azure key vault named Vault1. Vault1 contains a secret named Secret 1.
You enable a system-assigned managed identity for Automation1.
You need to ensure that Automation! can read the contents of Secret1. The solution must meet the following requirements:

* Prevent Automation1 from accessing other secrets stored in Vault1.
* Follow the principle of least privilege.
What should you do?
A. From Vault1, configure the Access control (1AM) settings.
B. From Automation1, configure the Identity setti ngs.
C. From Secret1, configure the Access control (1AM) settings
D. From Automation1, configure the Run as accounts settings.
Answer: C (LEAVE A REPLY)
As per the Microsoft SC-300 Study Guide and Azure Key Vault documentation , when you enable a system- assigned managed identity for a resource (in this case, Automation1), that identity can be granted permissions to specific Key Vault resources using Azure role-based access control (RBAC) .
Since the requirement states that Automation1 must be able t o read only one secret (Secret1) and not other secrets in the vault, you must assign permissions at the Secret level - not at the vault level. Assigning permissions at the Vault1 level (option A) would potentially allow access to all secrets, violating the principle of least privilege .
Therefore, you must go to Secret1 # Access control (IAM) and assign the Key Vault Secrets User role (or similar least-privileged role) to the system-assigned identity of Automation1 .
This aligns with Microsoft's documentation :
"To restrict access to individual secrets or keys, use Azure role assignments at the specific secret, key, or certificate level rather than the vault level."

NEW QUESTION: 6
You have an Azure subscription.
You are evaluating enterprise software as a service (SaaS) apps.
You need to ensure that the apps support automatic provisioning of Microsoft Entra users.
Which specification should the apps support?
A. WS-Fed
B. SCIM 2.0
C. LDAP3
D. OAuth 2.0
Answer: B (LEAVE A REPLY)
The SC-300 Exam Ref and official Microsoft Learn module "Plan and implement user provisioning" confirm that automatic user provisioning between Microsoft Entra ID (formerly Azure AD) and external SaaS applications uses the System for Cross-domain Identity Management (SCIM) 2.0 protocol.
SCIM 2.0 is an op en standard that simplifies identity lifecycle management - enabling automatic creation, update, and removal of user accounts within connected SaaS applications. When a SaaS app supports SCIM
2.0, Entra ID can automatically synchronize user identities and attributes based on defined mappings.
Other protocols listed, such as WS-Fed , LDAP , or OAuth 2.0 , serve different purposes - authentication and directory access rather than provisioning. WS-Fed is used for federated authentication; LDAP provides directory querying; OAuth 2.0 handles delegated authorization for resource access.
Thus, any enterprise SaaS app that supports automatic provisioning from Entra ID must implement SCIM
2.0 as per Microsoft's integration requirements.

NEW QUESTION: 7
You have a Microsoft 365 E5 subscription that contains a user named User1.
You need to ensure that User1 can create access reviews for Microsoft Entra roles. The solution must use the principle of least privilege.
Which role should you assign to User1?
A. Privileged Role Administrator

B. User Administrator
C. User Access Administrator
D. Identity Governance Administrator
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.
Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.
You plan to manage access to external applications by using Azure AD.
You need to use th e firewall logs to create a list of unmanaged external applications and the users who access them.
What should you use to gather the information?
A. Application Insights in Azure Monitor
B. access reviews in Azure AD
C. Cloud App Discovery in Microsoft Cl oud App Security
D. enterprise applications in Azure AD
Answer: C (LEAVE A REPLY)
According to the Microsoft SC-300: Identity and Access Administrator study materials and Microsoft Learn modules under "Implement and manage Cloud App Security (Microsoft Defender for Cloud Apps)", the Cloud App Discovery feature in Microsoft Cloud App Security (now called Microsoft Defender for Cloud Apps) is designed to identify and analyze the use of shadow IT - unmanaged or unsanctioned applications accessed by users within the organization.
Cloud App Discovery collects logs from network appliances such as firewalls, proxies, or Secure Web Gateways (SWGs). Administrators upload these logs into Cloud App Security or configure continuous log collection through automatic log uploaders. The service then parses and analyzes the data to detect which external applications are being accessed and which users are using them.
In this scenario, since users authenticate to the firewall with their on-premises Active Directory credentials, the firewall logs will contain user information and the external applications being accessed. By importing these logs into Cloud App Discovery, administrators can generate a detailed list of unmanaged (unsanctioned) external applications and identify the specific users connecting to them.
Microsoft documentation explicitly states:
"Cloud App Discovery analyzes traffic logs to identify all cloud applications used in your organization. It provides information about app usage, users, IP addresses, and risk levels to help you assess shadow IT." Hence, the correct and verified answer - based on official SC-300 curriculum and Azure AD Identity Governance content - is Cloud App Discovery in Microsoft Cloud App Securit

NEW QUESTION: 9
You have a Microsoft 365 E5 subscription.
You need to be able to create a Microsoft Defender for Cloud Apps session policy.
What should you do first?
A. From the Microsoft Defender portal, select User monitoring.
B. From the Microsoft Entra admin center, create a Conditional Access policy.
C. From the Microsoft Defender portal, select App onboarding/maintenance
D. From the Microsoft Defender portal, create a continuous report.
Answer: B (LEAVE A REPLY)

Before you can create a session policy in Microsoft Defender for Cloud Apps (MCAS), you must enable real-time session control integration through Conditional Access. This is achieved by creating a Conditional Access policy that uses the "Use Conditional Access App Control" session control option.
As explained in SC-300's "Manage Cloud App Security integration" module, Conditional Access policies are the gateway for routing session traffic through Defender for Cloud Apps for monitoring or control.
Options A, C, and D in the question represent post-deployment or reporting tasks, not the initial configuration step needed to enable session control.
Correct Answer: B. From the Microsoft Entra admin center, create a Conditional Access policy.

NEW QUESTION: 10
You have an Azure Active Directory (Azure AD) tenant that contains the objects shown in the following table.

Name	Type	Directly assigned license
User1	User	*None*
User2	User	Microsoft Office 365 Enterprise E5
Group1	Security group	Microsoft Office 365 Enterprise E5
Group2	Microsoft 365 group	*None*
Group3	Mail-enabled security group	*None*

Which objects can you add as members to Group3?
A. User2 and Group2 only
B. User2, Group1, and Group2 only
C. User1, User2, Group1 and Group2
D. User1 and User2 only
E. User2 only
Answer: D (LEAVE A REPLY)
Azure AD supports several group types with different membership rules. For Microsoft 365 groups, "group nesting isn't supported; only user identities can be members." For mail-enabled security groups used in Azure AD/Exchange Online, the SC-300 materials emphasize that only user objects are supported as members when managed in Azure AD, while "Microsoft 365 groups can't be added to other groups." Security groups are commonly nestable for access scenarios, but the mail-enabled security group membership experience in Azure AD limits member selection to users; thus you cannot add Group1 (security group) or Group2 (Microsoft 365 group) as members of Group3 (mail-enabled security group). Licensing assignments shown in the table are irrelevant to membership eligibility. Consequently, the only valid members you can add to Group3 are the user objects - User1 and User2.

NEW QUESTION: 11
You have an Azure subscription that contains the key vaults shown in the following table.

Name	In resource group	Number of days to retain deleted key vaults	Purge protection
KeyVault1	RG1	15	Enabled
KeyVault2	RG1	10	Disabled

The subscription contains the users shown in the following table.

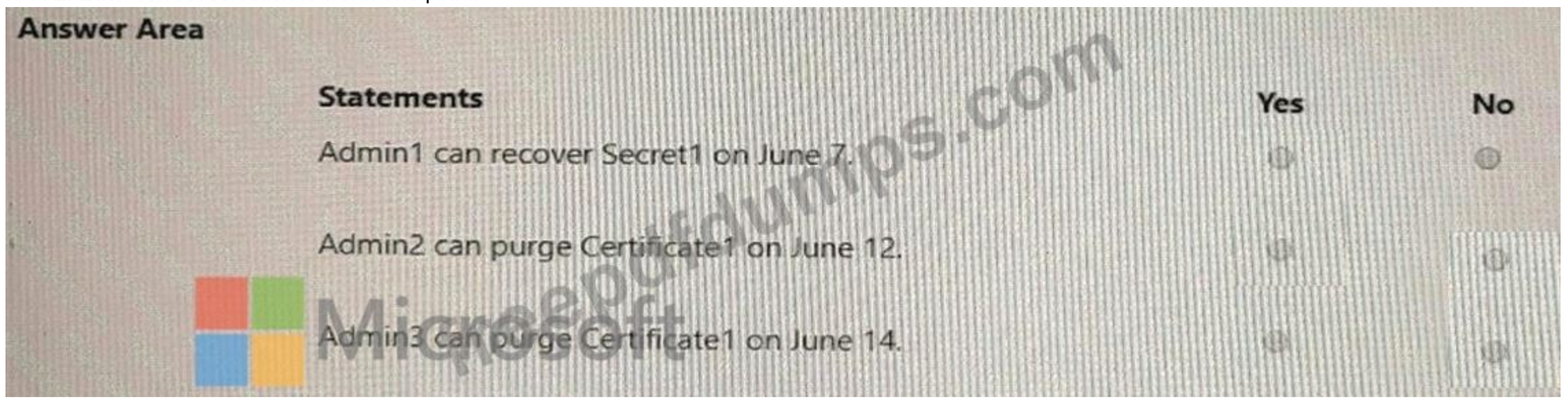
Name	Role
Admin1	Key Vault Administrator
Admin2	Key Vault Contributor
Admin3	Key Vault Certificates Officer
Admin4	Owner

On June1, Admin4 performs the following actions:

* Deletes a certificate named Certificate! from Key Vault1
* Deletes a secret named Secret1 from Key Vault2

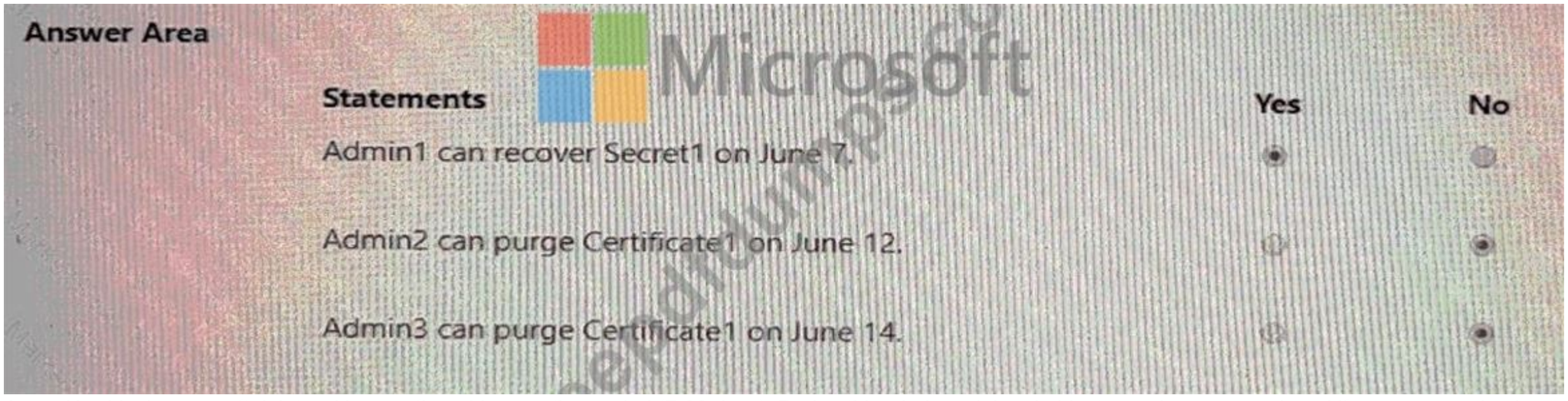
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Azure Key Vault uses soft delete with a configurable retention period (7-90 days). During this window, deleted objects can be recovered, and if purge protection is enabled, they cannot be purged until the retention period expires. The SC-300 materials describe: "Soft-delete retains keys, secrets, and certificates for the configured retention days. When purge protection is enabled, even users with purge pe rmission cannot permanently delete objects before the retention period ends; objects remain recoverable until expiry." The Key Vault RBAC data-plane roles further clarify capabilities. The guide states: "Key Vault Administrator has full data actions, inclu ding recover and purge across keys, secrets, and certificates. Key Vault Contributor manages the vault resource and settings but does not have data-plane permissions to read, delete, purge, or recover objects. Certificates Officer can manage and recover ce rtificates but is not granted purge." Applying this:

* Secret1 was deleted on June 1 from KeyVault2 (retention 10 days, purge protection Disabled). If it hasn' t been purged, it is recoverable any time through June 11. Admin1 (Key Vault Administrator) therefore can recover on June 7.
* Certificate1 was deleted on June 1 from KeyVault1 (retention 15 days, purge protection Enabled).

Purge is blocked until June 16 regardless of role. Additionally, Admin2 (Key Vault Contributor) lacks data-plane purge rights. Hence cannot purge on June 12.

* Admin3 (Key Vault Certificates Officer) also lacks purge permission; with purge protection still in effect, cannot purge on June 14.

NEW QUESTION: 12

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 o ne 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 Microsoft 365 E5 subscriptio n.

You create a user named User1.

You need to ensure that User1 can update the status of identity Secure Score improvement actions.

Solution: You assign the SharePoint Administrator role to User1

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed Explanation: =

According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the official Microsoft Learn documentation on Microsoft Secure Score , only specific roles in Azure AD and Microsoft 365 can view and update Secure Score improvement actions .

The SharePoint Administrator role allows managing SharePoint Online sites, permissions, and sharing policies, but it does not grant access to Microsoft Secure Score functionalities or security-related impro vement actions.

Microsoft defines the following roles as being able to update and manage Secure Score:
* Global Administrator
* Security Administrator
* Security Reader (read-only view)
Therefore, assigning the SharePoint Administrator role does not meet the requirement.

NEW QUESTION: 13
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You need to ensure that users can request access to Site. the solution must meet the following requirements.
* Automatically approve requests from users based on their group membership.
* Autom atically remove the access after 30 days
What should you do?
A. Create a Conditional Access policy.
B. Create an access package.
C. Configure Role settings in Azure AD Privileged Identity Management.
D. Create a Microsoft Defender for Cloud Apps access pol icy.
Answer: B (LEAVE A REPLY)
This scenario describes the need for users to request access, have access automatically approved based on group membership, and automatically expire after 30 days.
These are exactly the features provided by Azure AD Entitlement Management access packages under Identity Governance.
* Access packages allow users to request access to resources (such as SharePoint sites, apps, or groups).
* Policies within an access package can automatically approve requests based on group membership or manager approval.
* You can also configure access expiration, automatically removing access after a set duration (e.g., 30 days).
Conditional Access, PIM, and Defender for Cloud Apps do not provide automatic access expiration tied to request workflows.

NEW QUESTION: 14
You have an Azure Active Directory (Azure AD) tenant that uses conditional access policies.
You plan to use third-party security information and event management (SIEM) to analyze conditional access usage.
You need to download the Azure AD log that contains conditional access policy data.
What should you export from Azure AD?
A. sign-ins in JSON format
B. sign-ins in CSV format
C. audit logs in JSON format
D. audit logs in CSV format
Answer: (SHOW ANSWER)
As per the Microsoft SC-300: Identity and Access Administrator Study Guide and official Microsoft Learn content under "Monitor and troubleshoot Azure AD using reports and logs" , Conditional Access policy data is captured in the Sign-ins log within Azure Active Directory. Each sign-in record contains detailed information about the authentication process, including which co nditional access policies were evaluated, the policies applied, and their enforcement results (e.g., "Grant access," "Block," or "Require MFA").
The Audit logs in Azure AD, on the other hand, track directory-level changes such as policy creation, modificat ion, or administrative actions - they do not include user authentication or conditional access evaluation data. Therefore, to analyze Conditional Access activity in an external SIEM system, you must export Sign-in logs , which contain the conditional access evaluation details.

Microsoft documentation specifies that exporting in JSON format is preferred for integration with third-party SIEM systems because JSON preserves nested policy evaluation data structures that CSV format cannot fully represent. CSV expo rts omit detailed conditional access results (e.g., policy IDs and results per policy), making them unsuitable for automated parsing and deep analysis.
Thus, based on official Microsoft documentation:
"Conditional Access policy evaluation results are only available in Sign-in logs and should be exported in JSON format for SIEM integration."
Correct Answer: A. sign-ins in JSON format

NEW QUESTION: 15
You have a Microsoft Entra tenant that contains an administrative unit named AU1. AU1 is configured for assigned membership.
The tenant contains the users shown in the following table.

Name	Department	Administrative unit
User1	HR	*None*
User2	IT	AU1

The tenant contains the groups shown in the following table.

Name	Members	Administrative unit
HR	User1	AU1
IT	User2	AU1

For AU1, yo u update the following configurations:
. Membership type: Dynamic User
Dynamic membership rule: (user.department -eq " hr ")
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
HR is a member of AU1.	○	○
User1 is a member of AU1.	○	○
User2 is a member of AU1.	○	○

Answer:

Statements	Yes	No
HR is a member of AU1.	○	○
User1 is a member of AU1.	○	○
User2 is a member of AU1.	○	○

Explanation:
HR is a member of AU1: No
User1 is a member of AU1: Yes
User2 is a member of AU1: No
Let's break this down step by step based on Microsoft Entra ID dynamic membership rules, administrative units, and group membership, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Administrative Units and Dynamic Me mbership in Microsoft Entra ID:
Administrative Units (AUs):Administrative Units in Microsoft Entra ID are used to delegate administrative tasks to a subset of users, groups, or devices. They allow you to scope administrative roles (e.g., User Administrator) to specific users or groups within the AU.
Membership Types for AUs:
Assigned Membership:Members (users, groups, or devices) are manually added to the AU by an administrator.
Dynamic Membership:Members are automatically added or removed based on a dynami c membership rule, similar to dynamic groups. Dynamic membership for AUs can be applied to users or devices (but not groups directly).
The question states that AU1 is initially configured for assigned membership but is then updated to useDynamic Usermember ship with the rule (user.department -eq " HR ").
Dynamic Membership Rule:The rule (user.department -eq " HR ") means that AU1 will automatically include all users whose department attribute in Microsoft Entra ID is set to " HR " .
This rule applies to users, not groups or devices, because the membership type is " Dynamic User. " Impact of Changing AU1 to Dynamic Membership:
When AU1's membership type is changed from assigned to dynamic, the existing assigned memberships (e.
g., User2, HR group, IT group) are no longe r relevant. Thedynamic rule takes over, and AU1's membership is determined solely by the rule (user.department -eq " HR ").
Dynamic User Membership:Only users whose attributes match the rule will be members of AU1. Groups (like HR and IT) are not evaluated b y this rule because the membership type is " Dynamic User, " not " Dynamic Group. " Let's evaluate the users based on the rule:
User1:Department = " HR " . The rule (user.department -eq " HR ") matches, so User1 will be dynamically added to AU1.
User2:Department = " IT " . The rule does not match, so User2 will not be a member of AU1, even though they were previously assigned to AU1 and are a member of the IT group.
Groups (HR and IT):The dynamic membership rule for AU1 applies to users, not groups. Therefore, groups l ike HR and IT are not directly evaluated by the rule. However, we need toconsider whether group membership in AU1 affects the statements.
Statement 1: HR is a member of AU1:
Analysis:
The HR group is listed in the second table with AU1 as its administrative unit, indicating that it was initially assigned to AU1 when AU1 used assigned membership.
However, AU1's membership type has been updated to " Dynamic User " with the rule (user.department -eq " HR "). Dynamic User membership applies to users, n ot groups.
In Microsoft Entra ID, administrative units with dynamic user membership do not include groups as members unless the AU's membership type is explicitly set to " Dynamic Group " (which is not the case here).

When AU1 was changed to dynamic membersh ip, the HR group would no longer be considered a member of AU1 because the dynamic rule only evaluates users. Groups are not dynamically added to AUs based on user attributes.
Conclusion:The HR group is not a member of AU1 after the change to dynamic membe rship. Therefore, this statement isNo.
Statement 2: User1 is a member of AU1:
Analysis:
User1 has the department attribute set to " HR " (from the first table).
The dynamic membership rule for AU1 is (user.department -eq " HR "), which matches User1's departme nt.
Therefore, User1 will be automatically added to AU1 as a member based on the dynamic rule.
Additionally, User1 is a member of the HR group, which was initially assigned to AU1. However, since AU1 now uses dynamic membership, the HR group's assignment to AU1 is irrelevant. User1's membership in AU1 is determined solely by the dynamic rule, not their group membership.
Conclusion:User1 is a member of AU1 because their department matches the dynamic rule. Therefore, this statement isYes.
Statement 3: User2 is a member of AU1:
Analysis:
User2 has the department attribute set to " IT " (from the first table).
The dynamic membership rule for AU1 is (user.department -eq " HR "), which does not match User2's department.
User2 was initially assigned to AU1 (as shown in the first table) and is a member of the IT group, which was also assigned to AU1. However, when AU1's membership type was changed to " Dynamic User, " the assigned memberships (including User2 and the IT group) are no longer relevant.
The dynamic rule onl y includes users with the department " HR, " so User2 is not added to AU1.
Conclusion:User2 is not a member of AU1 because their department does not match the dynamic rule.
Therefore, this statement isNo.
Additional Considerations:
If AU1's membership type w ere " Dynamic Group " instead of " Dynamic User, " we would evaluate whether the HR and IT groups match a group-based rule. However, the question specifies " Dynamic User, " so the rule applies to user attributes only.
The initial assigned memberships (e.g., Use r2, HR group, IT group) are overridden by the dynamic membership rule. Microsoft Entra ID does not retain assigned memberships when an AU or group is converted to dynamic membership.
The HR and IT groups being assigned to AU1 initially does not affect the dynamic membership of users, but it might be relevant for administrative scoping (e.g., if an admin role is scoped to AU1). However, the statements are about membership, not administrative roles.
Conclusion:Based on the dynamic membership rule (user.depart ment -eq " HR ") for AU1:
HR group:Not a member of AU1 because dynamic user membership does not apply to groups.
User1:A member of AU1 because their department is " HR, " matching the rule.
User2:Not a member of AU1 because their department is " IT, " which does not match the rule.Therefore, the answers are:
HR is a member of AU1:No
User1 is a member of AU1:Yes
User2 is a member of AU1:No
References:
Microsoft Entra ID documentation: " Dynamic membership rules for groups and administrative units " (Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership) Microsoft Entra ID documentation: " Manage administrative units " (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-uni ts) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers dynamic membership rules and administrative units in Microsoft Entra ID.

NEW QUESTION: 16

You have an Azure AD tenant that con tains the users shown in the following table.

Name	Role
User1	None
User2	None
Admin1	Application administrator
Admin2	Authentication administrator

The User settings for enterprise applications have the following configuration.
* Users can consent to apps accessing company data on their behalf:
* Users can consent to apps accessing company data for the g roups they
* Users can request admin consent to apps they are unable to consent to: Yes
* Who can review admin consent requests: Admin2, User2
User1 attempts to add an app that requires consent to access company data.
Which user can provide consent?
A. Use r1
B. User2
C. Admin1
D. Admin2
Answer: D (LEAVE A REPLY)
In Azure AD, user consent and admin consent workflows control which users or administrators can approve access to organizational data requested by applications.
The question states:
* "Users can request admin consent to apps they are unable to consent to: Yes"
* "Who can review admin consent requests: Admin2, User2"
When User1 attempts to add an app that requires consent to access company data, and if that app requires admin consent, the request is routed to those designated as admin consent reviewers. In this case, Admin2 and User2 are listed, but only one has the administrative capability to approve the request.
Based on Microsoft documentation:
"Only users who hold an administrative role such as Global Administrator, Cloud Application Administrator, or Authentication Administrator and are designated as reviewers can grant consent on behalf of the organization." Here, Admin2 holds the Authentication Administrator role - an Azure AD admin-level role - while User2 has no administrative privileges. Thus, Admin2 is the only eligible user to approve the admin consent request.

NEW QUESTION: 17
You have an Azure subscription. The subscription contains a virtual machine named VM1 that runs Linux.
You need to configure enhanced security for VM1. The solution must meet the following requirements:
* Ensure that users can sign in to VM1 by using their Microsoft Entra credentials
* Ensure That users authenticate by using multi-factor out-of-band
* Prevent users from signing in to VM1 by using passwords.

Which two authentication methods can you include in the solution? Each correct answer presents a complete solution. NOTE: Each correct selection Is worth one point.

A. the Microsoft Authenticator app

B. Windows Hello for Business

C. Passkey(FID02)

D. Temporary Access Pass

E. SMS

Answer: (SHOW ANSWER)

The requirement specifies that:

* Users must sign in using Microsoft Entra credentials,
* Multi-factor authentication must be out-of-band,
* Password sign-ins must be prevented.

According to Microsoft Learn: "Configure passwordless authentication in Microsoft Entra ID" and the SC-300 Exam Ref , the two supported passwordless and MFA-capable authentication methods that satisfy these conditions are:

* Microsoft Authenticator app - Supports passwordless sign-in using push notifications, providing both identity verification and multi-factor authentication in a single step.
* FIDO2 Passkey - Enables secure passwordless authentication through hardware security keys or device-bound passkeys that rely on public key cryptography and satisfy MFA requirements when configured properly.

Both methods eliminate password usage entirely and integrate with Microsoft Entra for strong identity assurance.

Windows Hello for Business is passwordless but limited to Windows devices (VM1 is Linux). Temporary Access Pass (TAP) is a bootstrap mechanism for enrolling in passwordless sign-in, not a long-term solution.

SMS authentication, while MFA-capable, still requires passwords for primary authentication and doesn't meet the passwordless requirement.

NEW QUESTION: 18

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

All the users work remotely.

Azure AD Connect is configured in Azure AD as shown in the following exhibit.

Connectivity from the on-premises domain to the internet is lost.

Which users can sign in to Azure AD?

A. User1 and User3 only

B. User1 only

C. User1, User2, and User3

D. User1 and User2 only

Answer: (SHOW ANSWER)

The exhibit shows Password Hash Synchronization (PHS) enabled and Pass-through Authentication (PTA) enabled. The SC-300 materials clarify that when both PTA and PHS are enabled, Azure AD can fall back to PHS if PTA agents become unavailable. The guidance states that PHS can serve as a backup sign-in method to ensure continuity during on-premises connectivity failures. In this scenario, on-premises connectivity to the internet is lost, so PTA agents cannot process sign-ins. Because PHS is enabled, synchronized users can still authenticate in Azure AD using their synced password hashes.

* User1 is a cloud-only user and authenticates directly in Azure AD-unaffected by on-premises outages.
* User2 is directory-synced; with PTA down, sign-in falls back to PHS, allowing access as long as the hash is present.
* User3 is a guest; guests authenticate in their home directory/IdP, independent of your on-premises environment, so they can still sign in.Therefore, during the outage, all three users (User1, User2, and User3) can sign in to Azure AD, satisfying the behavior described in the SC-300 documentation regarding PHS backup for PTA and guest sign-in independence.

NEW QUESTION: 19

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You have a user risk policy that has the following settings:

* Assignments:

o Include: Group1

o Exclude: Group2
* Sign-in risk Medium and above
* Access controls:
o Grant access: Require password change
When the users attempt to sign in. user risk levels are detected as shown in the following table.

User	Risk level
User1	High
User2	Medium
User3	High

For each of the following statements, select Y es if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
User1 must change their password during sign in.	○	○
User2 must change their password during sign in.	○	○
User3 must change their password during sign in.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 must change their password during sign in.	○	○
User2 must change their password during sign in.	○	○
User3 must change their password during sign in.	○	○

Explanation:

Answer Area

Statements	Yes	No
User1 must change their password during sign in.	●	○
User2 must change their password during sign in.	○	●
User3 must change their password during sign in.	○	●

This scenario is based on the Microsoft Entra (Azure AD) Identity Protection feature, which is a major topic in the SC-300: Microsoft Identity and Access Administrator exam. According to the official study guide and Microsoft documentation:
"A user risk pol icy in Microsoft Entra ID is used to detect when a user account is at risk and to enforce remediation actions, such as requiring the user to change their password on the next sign-in."
* Assignments:
* Include: Group1
* Exclude: Group2
* Sign-in risk: Medium and above
* Access control: Require password change

Given Policy Settings: User Details: User
Group Membership
Risk Level
User1
Group1
High
User2
Group2
Medium
User3
Group1, Group2
High
* User1:
* Included in Group1 (policy applies).
* Not a member of Group2 (not excluded).
* Risk level = High, which is # Medium, meeting policy threshold. # User1 must change their password.
* User2:
* Member of Group2 (excluded).
* Even though their risk level is Medium, exclusion overrides inclusion. # User2 will not be prompted to change their password.
* User3:
* Member of both Group1 (included) and Group2 (excluded).
* Exclusion always takes precedence in Microsoft Entra conditional access and risk policies. # User3 will not be required to change their password.
Analysis:
Official Microsoft SC-300 Source Excerpt: From the Microsoft Identity and Access Administrator Study Guide (Exam Ref SC-300) and Microsoft Learn ("Configure and manage user risk policies"):
"When a user is included in both the include and exclude assignments of a pol icy, the exclude setting takes precedence. Risk policies can enforce password change for users with detected risk levels that meet or exceed the configured threshold."

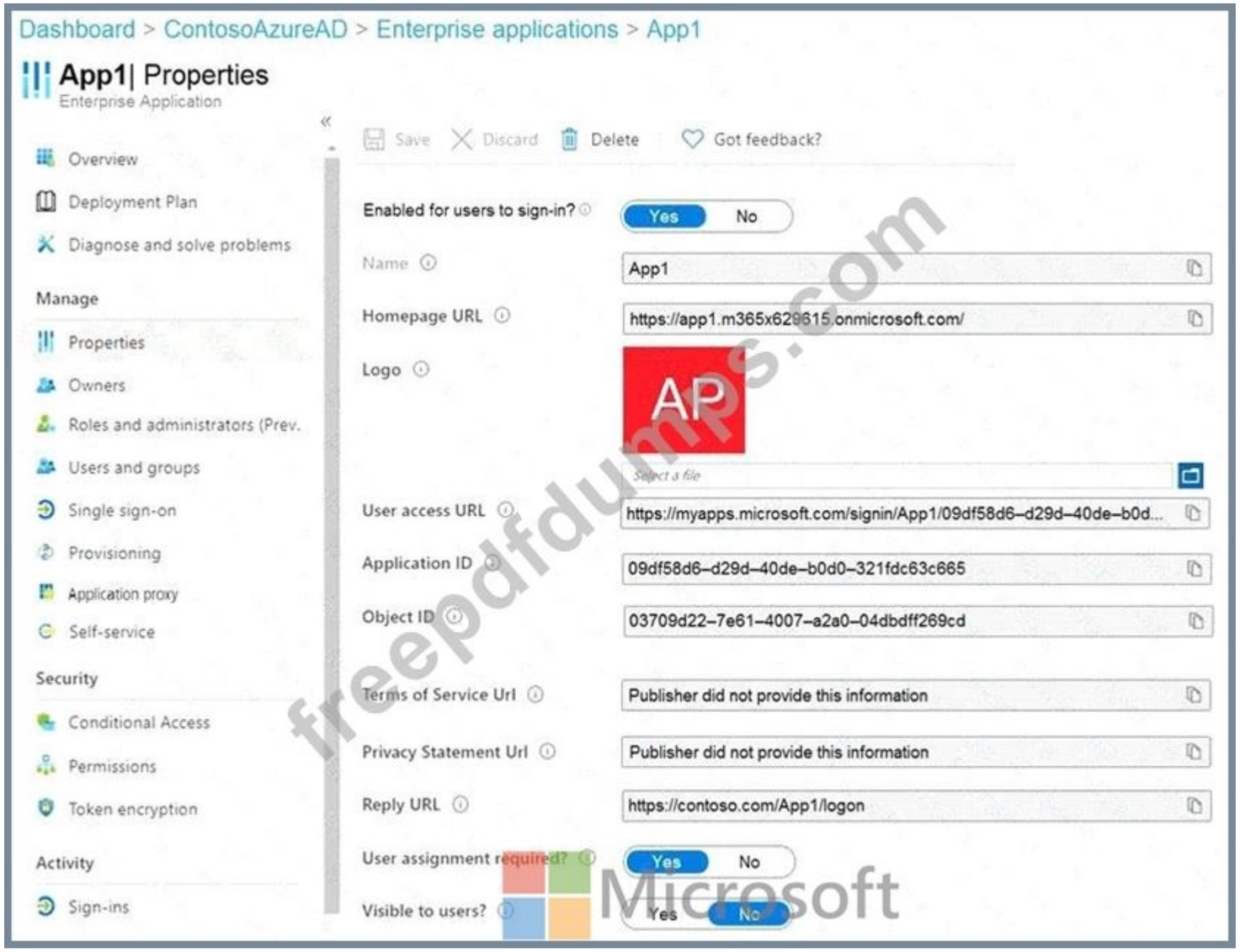
NEW QUESTION: 20
You need to implement the planned changes for litware.com. What should you configure?
A. Azure AD Connect cloud sync between the Azure AD tenant and litware.com
B. Azure AD Connect to include the litware.com domain
C. staging mode in Azure AD Connect for t he litware.com domain
Answer: (SHOW ANSWER)
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "Implement and manage synchronization for Azure AD" , Azure AD Connect Cloud Sync is the preferred solution when you need to synchronize objects from multiple Active Directory (AD DS) forests without establishing forest trusts .
The scenario specifies that trust relationships must NOT be established between adatum.com and litware.
com , but A. Datum must still sync the AD DS users and groups of litware.com to their existing Azure AD tenant (adatum.com).
The SC-300 training materials clarify:

"Azure AD Connect cloud sync enables syncing from multiple AD forests to a single Azure AD tenant without the need f or forest trusts or a full Azure AD Connect installation in each forest." Unlike staging mode (which provides a standby sync server for failover) or extending the same Azure AD Connect instance to another domain (which requires trust relationships and netw ork connectivity between forests), Azure AD Connect Cloud Sync uses lightweight agents and does not depend on forest trust.
Therefore, to meet the requirement of syncing Litware's AD DS to A. Datum's Azure AD tenant without creating a trust , the correct ch oice is to configure Azure AD Connect Cloud Sync between the Azure AD tenant and the litware.com domain.

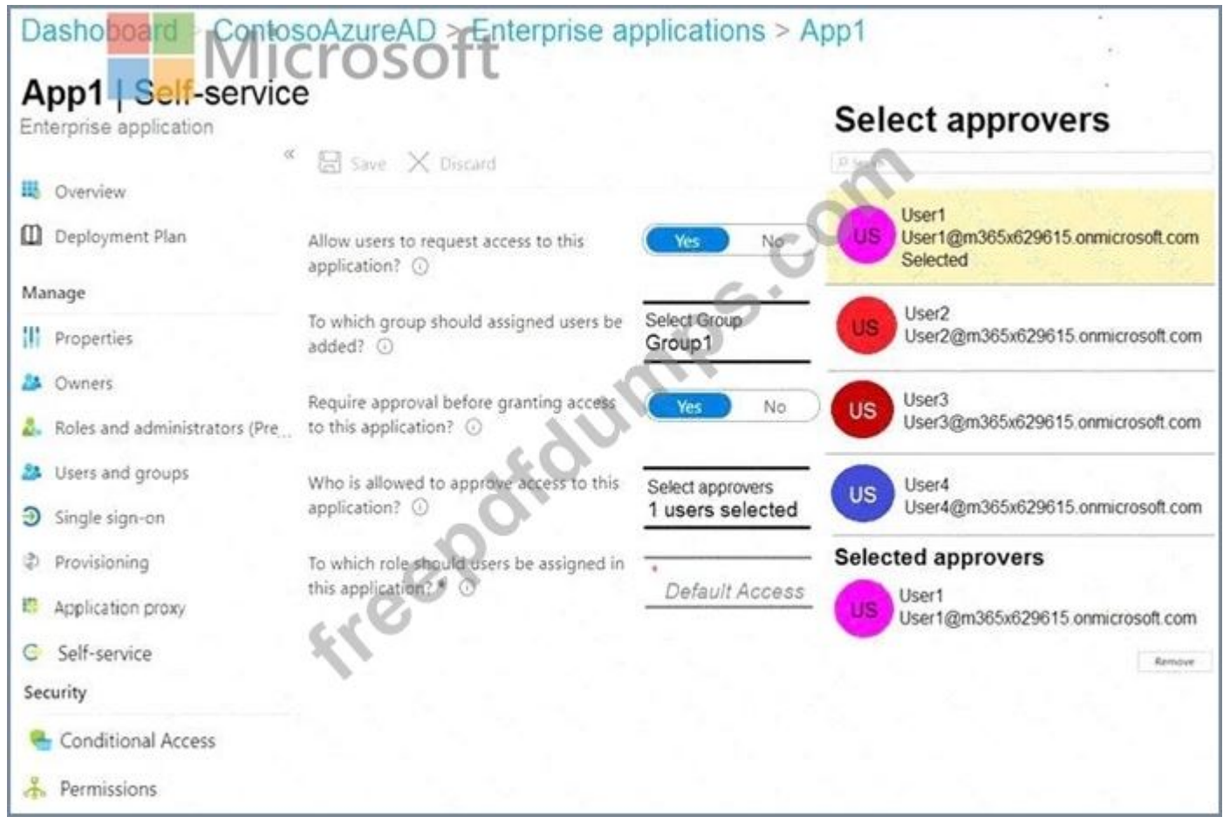
NEW QUESTION: 21
You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit. (Click theGroup1tab.)

```
PS C:\> Get-AzureADGroup -searchstring "group1" | Get-AzureADGroupowner

ObjectId                             DisplayName   UserPrincipalName                UserType
--------                             -----------   -----------------                --------
a7f7d405-636f-4493-b971-5c2b7a131b1c Admin         admin@M365x629615.onmicrosoft.com Member

PS C:\> Get-AzureADGroup -searchstring "group1" | GetAzureADGroupMember | ft displayname

DisplayName
-----------
User1
User4
Group3
```


You create an enterprise application named App1 as shown in the App1 Properties exhibit. (Click theApp1 Propertiestab.)



You configure self-service for App1 as shown in the App1 Self-service exhibit. (Click theApp1Self- servicetab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE:Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Answer:

Explanation:

No

No

Yes

a) When you assign a group to an application, only users in the group will have access. The assignment does not cascade to nested groups.

b) Tested in lab, existing owners will be replaced. Also direct assignment (resource owner) is path of least privilege. (replicated in test) c) Application setting 'visible to users' is set to No, then no users see this application on their My Apps portal and O365 launcher.

Reference

According to the Microsoft SC-300: Identity and Access Administrator Study Guide, Azure AD Enterprise Application Self-service configuration determines how users can request access, who approves it, and whether access is automatically granted. Let's analyze each statement based on the exhibits:

* Members of Group3 can access App1 without approval from User1 - NOIn the Group1 exhibit, Group1 contains User1, User4, and Group3. In the App1 Self-Service exhibit, it shows that "Require approval before granting access" is set to Yes, and User1 is designated as the approver. Therefore, even though Group3 members might indirectly be part of Group1, access requests to App1 must still be approved by User1 before being granted.

* After configuring self-service, the owner of Group1 is User1 - NOThe PowerShell command Get- AzureADGroupOwner clearly shows that Admin (not User1) is the owner of Group1. Configuring self- service for an application does not change group ownership; it only defines how access requests are handled. Ownership of Group1 remains with Admin.

* App1 appears in the Microsoft 365 app launcher of User4 - YESIn the App1 Properties exhibit, the

"User assignment required" setting is set to Yes. This means only assigned users (directly or via groups) can see and access the application. Since Group1 is configured as the target group for user assignment and User4 is a member of Group1, User4 will see App1 in their Office 365 app launcher after assignment approval.

This logic follows Microsoft Learn documentation:

"When a user is assigned to an enterprise application (either directly or through group membership), the application appears in the user's Office 365 app launcher once access is granted."

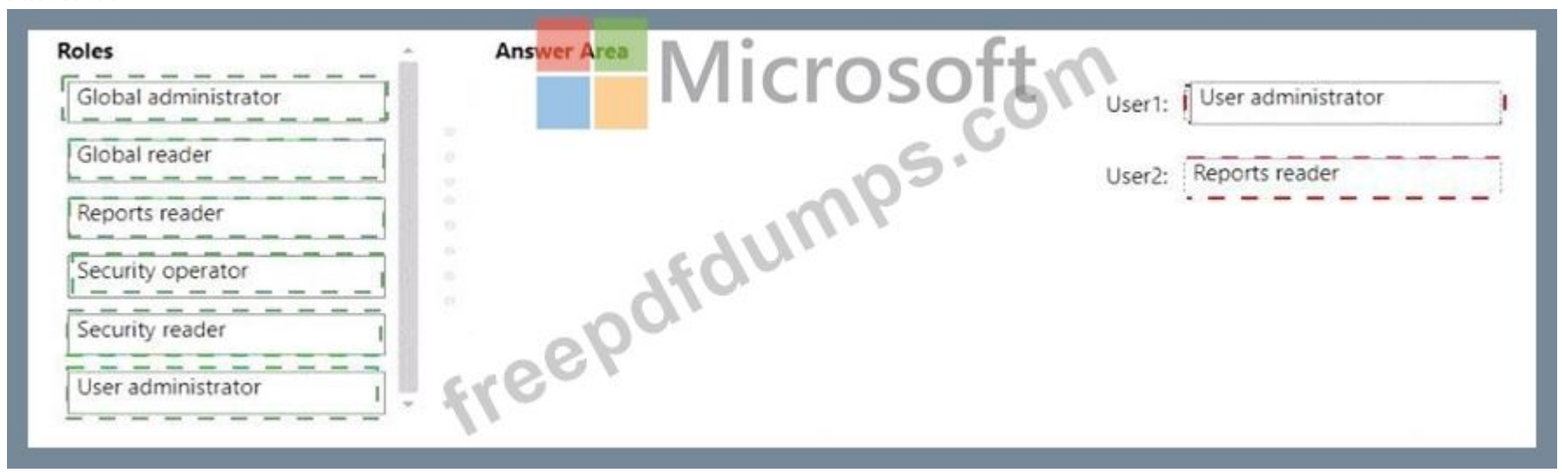
NEW QUESTION: 22

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You need to ensure that User1 can create access reviews for groups, and that User2 can review the history report for all the completed access reviews. The solution must use the principle ofleast privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag th e split bar between panes or scroll to view content NOTE: Each correct selection is worth one point.

Answer:



Explanation:

< User1: User administrator

User2: Reports reader

According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Exam Ref SC-300: Microsoft Identity and Access Administrator , Azure AD includes several predefined roles that control delegated administrative permissions in the directory. Access reviews in Azure AD (part of Identity Governance) can be created and managed by specific roles, dependi ng on their intended task.

The User administrator role is designed for managing users and groups. It allows the user to create and manage access reviews for groups and applications within the organization. This includes the ability to start new reviews, mo dify existing ones, and manage reviewers. Therefore, User1 , who must create access reviews, requires this role.

On the other hand, the Reports reader role is a read-only administrative role that allows viewing of all audit logs, sign-in logs, and reports, including access review history reports . This role cannot create or modify reviews but can access and review the outcomes of completed reviews. Therefore, User2 , who needs to review historical access review reports, should be assigned the Reports reader ro le.

Microsoft Learn's "Manage access reviews in Azure AD Identity Governance" module and the SC-300 Learning Path confirm:

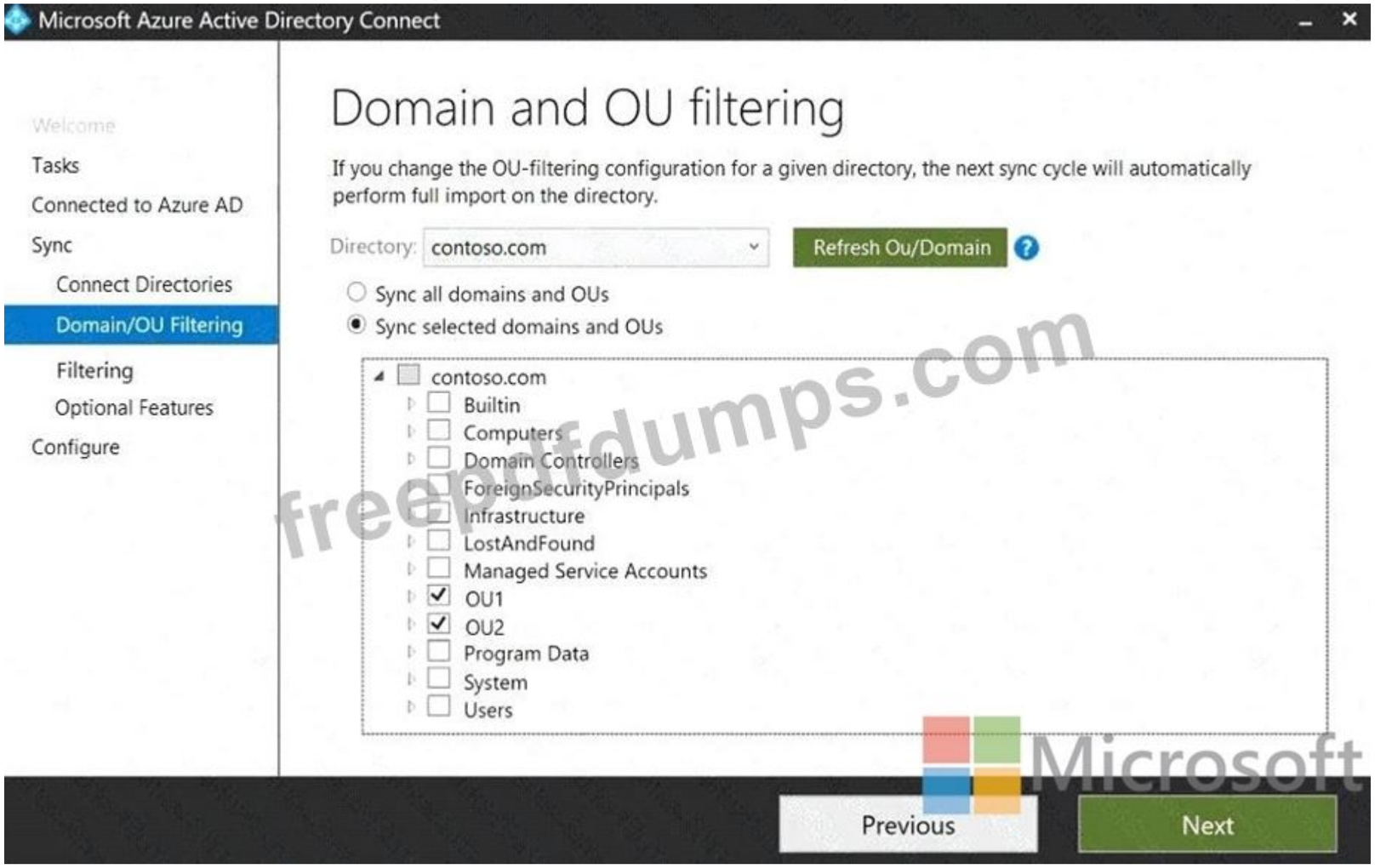
"User administrators can create and manage access reviews for users, groups, and applications. Reports readers can view the access re view results and history reports but cannot create or modify them

NEW QUESTION: 23

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)	Description
User1	User	OU1	User1 is a member of Group1.
User2	User	OU1	User2 is not a member of any groups.
Group1	Security group	OU2	User1 and Group2 are members of Group1.
Group2	Security group	OU1	Group2 is a member of Group1.

You install Azure AD Connect. You configure the Domain and OU filtering settings as shown in the Domain and OU Filtering ex hibit. (Click theDomain and OU Filteringtab.)



You configure the Filter users and devices settings as shown in the Filter Users and Devices exhibit. (Click theFilter Users and Devicestab.)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer:

Explanation:

User1 syncs to Azure AD: # Yes

* User2 syncs to Azure AD: # No

* Group2 syncs to Azure AD: # No

This scenario is directly covered in the Microsoft SC-300: Identity and Access Administrator exam section "Implement Azure AD Connect synchronization" and detailed in Microsoft documentation: "Azure AD Connect: Configure filtering" .

Azure AD Connect supports multiple filtering mechanisms:

* Domain and Organizational Unit (OU) filtering - only objects in selected OUs are synchronized.

* Group-based filtering (Pilot sync) - when enabled, only members of the specified security group (and required dependency objects) are synchronized. Nested groups are not supported.

* OU Filtering:

* Both OU1 and OU2 are selected.

* Therefore, objects in both OUs are eligible for synchronization (if other filters allow).

* Group-based filtering:

* The selected filter group is Group1, located in OU2.

* Azure AD Connect synchronizes only direct members of Group1 (users, groups, or devices).

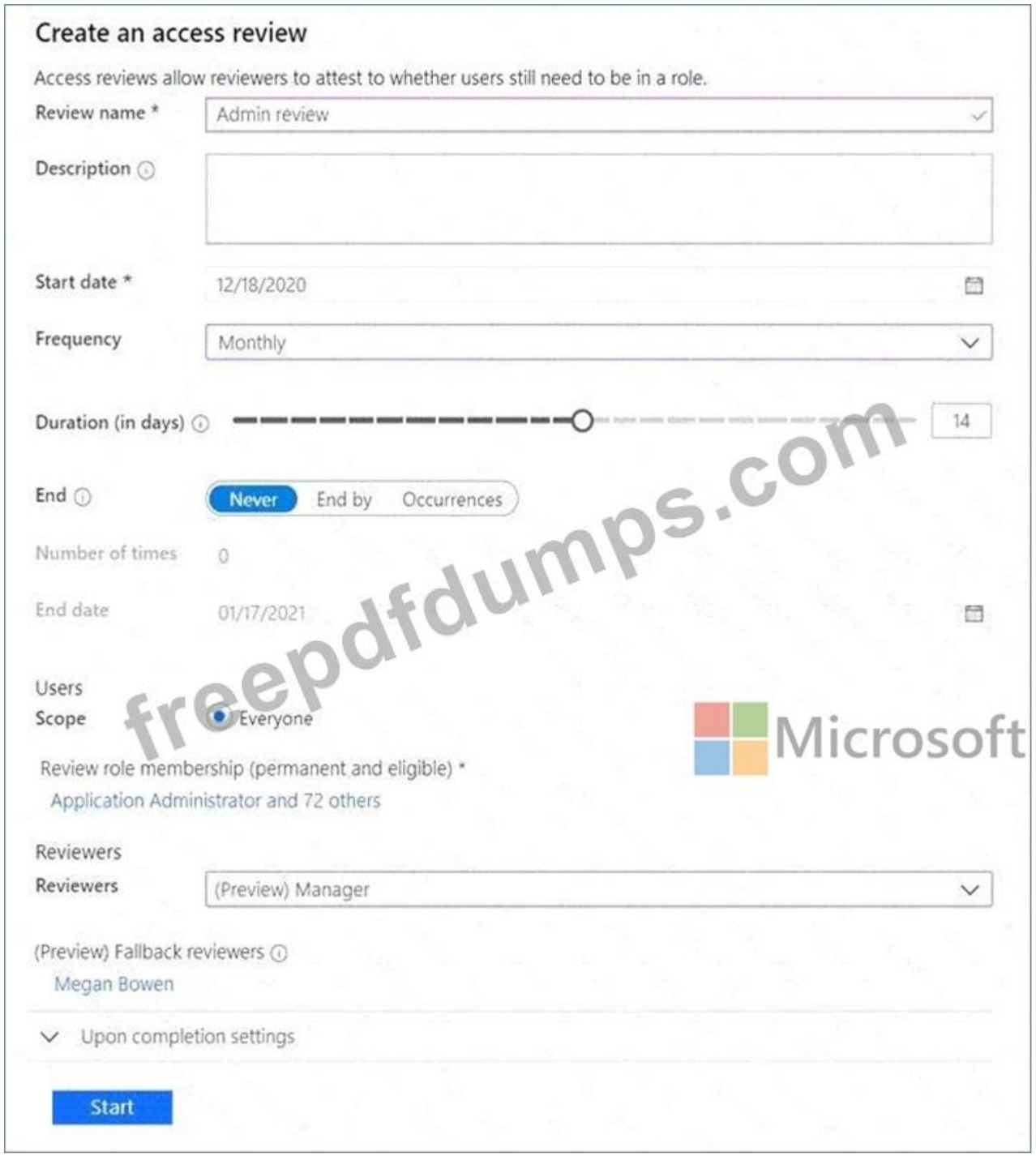
* Nested groups are ignored - their members are not recursively synchronized .

* User1:

* Is a direct member of Group1 (in OU1).

* Since User1 is directly in Group1, and OU1 is included, User1 will sync to Azure AD. # User1 syncs to Azure AD = Yes
* User2:
* Is not a member of any group.
* The Group1-based filtering excludes non-members, even though OU1 is selected. # User2 syncs to Azure AD = No
* Group2:
* Is a member of Group1, but nested groups are ignored in Azure AD Connect group-based filtering.
* Thus, Group2 itself and its members will not be synchronized. # Group2 syncs to Azure AD = No Based on the exhibits: Evaluating Each Object: Supporting Microsoft Documentation (from SC-300 material):
"When you use group-based filtering, only objects that are direct members of the specified group are synchronized. Nested group memberships are ignored."
"If you select specific OUs for synchronization, objects must meet both the OU filtering and the group filtering criteria to be included in the sync."

NEW QUESTION: 24
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 Microsoft 365 tenant.
You have 100 IT admin istrators who are organized into 10 departments.
You create the access review shown in the exhibit. (Click theExhibittab.)



You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You create a separate access review for each role.

Does this meet the goal?

A. Yes

B. NoD18912E1457D5D1DDCBD40AB3BF70D5D

Answer: (SHOW ANSWER)

In this scenario, all access review notifications are going to Megan Bowen, the fallback reviewer, instead of department managers. Creating a separate access review for each role does not meet the requirement because the issue lies in the reviewer selection, not the number of reviews.
Microsoft documentation clarifies:
"To have reviews sent to each user's manager, the reviewer type must be set to 'Manager'. The system uses the 'manager' attribute from Azure AD user properties." Thus, you don't need separate reviews for each role; you need to configure the reviewer type to Manager or update user account manager attributes. Therefore, the proposed solution (creating separate reviews) does not meet the goal.

NEW QUESTION: 25
You have a Microsoft Entra tenant that contains the groups shown in the following exhibit.

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.

Answer Area

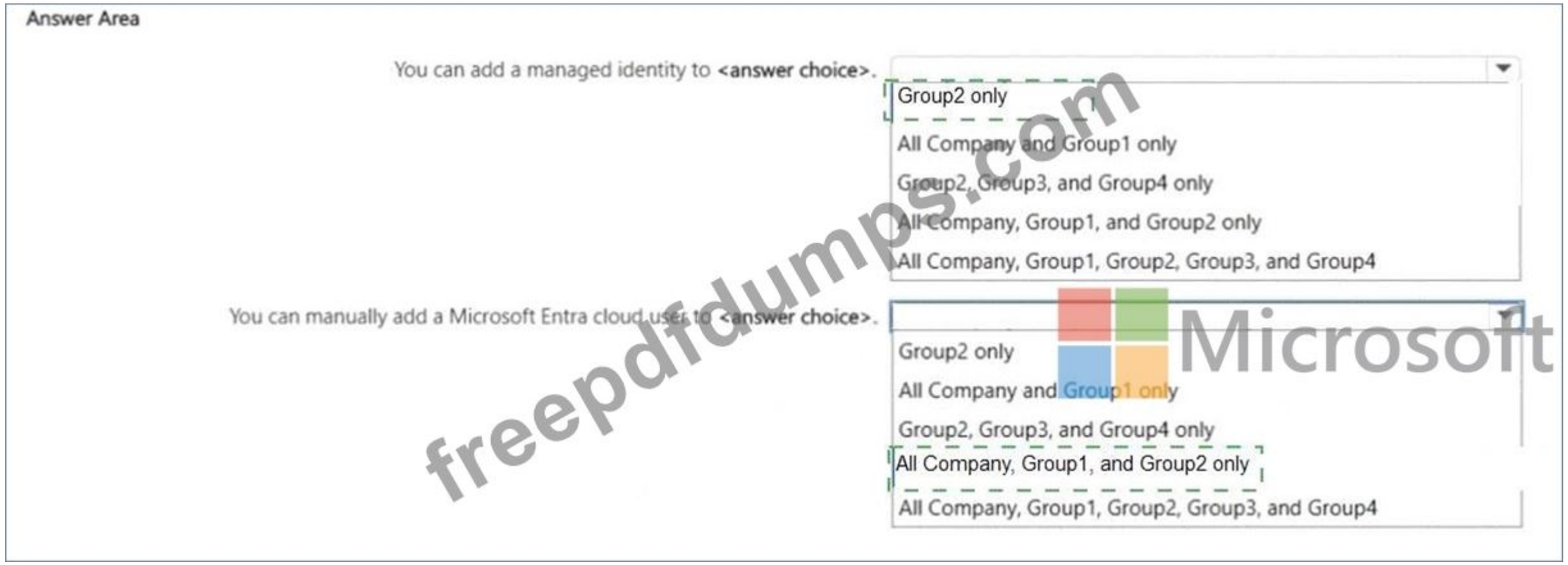
You can add a managed identity to <answer choice>.

- Group2 only
- All Company and Group1 only
- Group2, Group3, and Group4 only
- All Company, Group1, and Group2 only
- All Company, Group1, Group2, Group3, and Group4

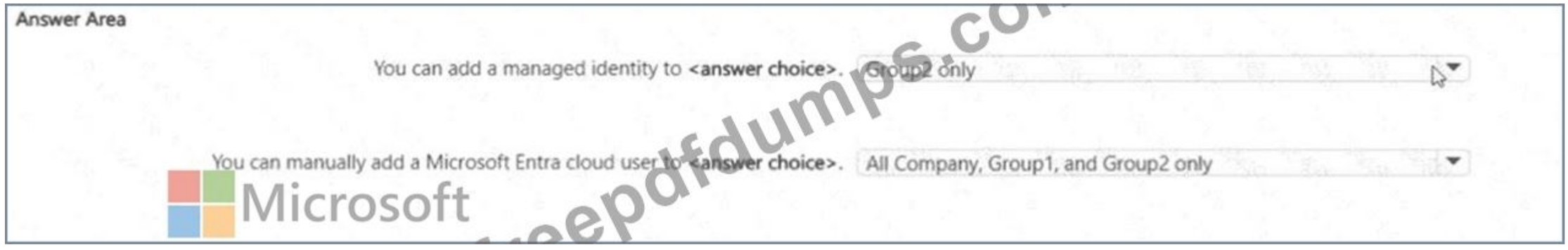
You can manually add a Microsoft Entra cloud user to <answer choice>.

- Group2 only
- All Company and Group1 only
- Group2, Group3, and Group4 only
- All Company, Group1, and Group2 only
- All Company, Group1, Group2, Group3, and Group4

Answer:

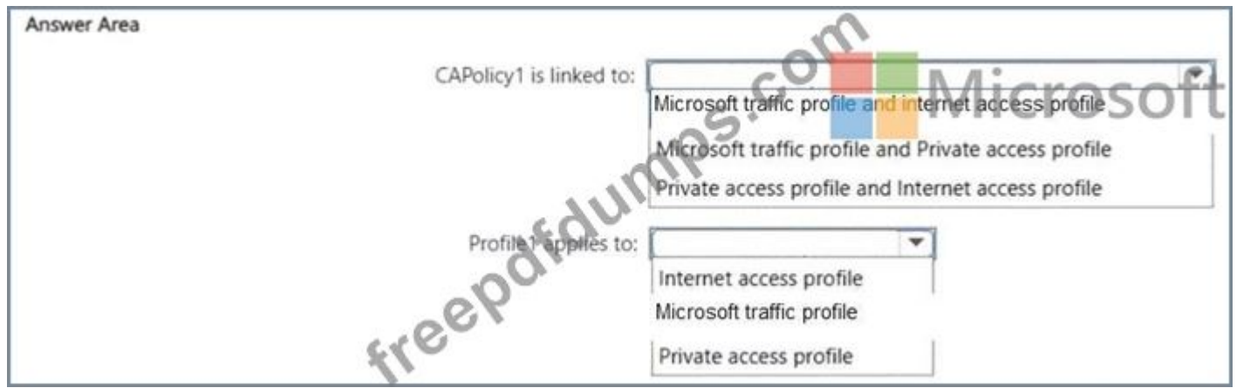


Explanation:

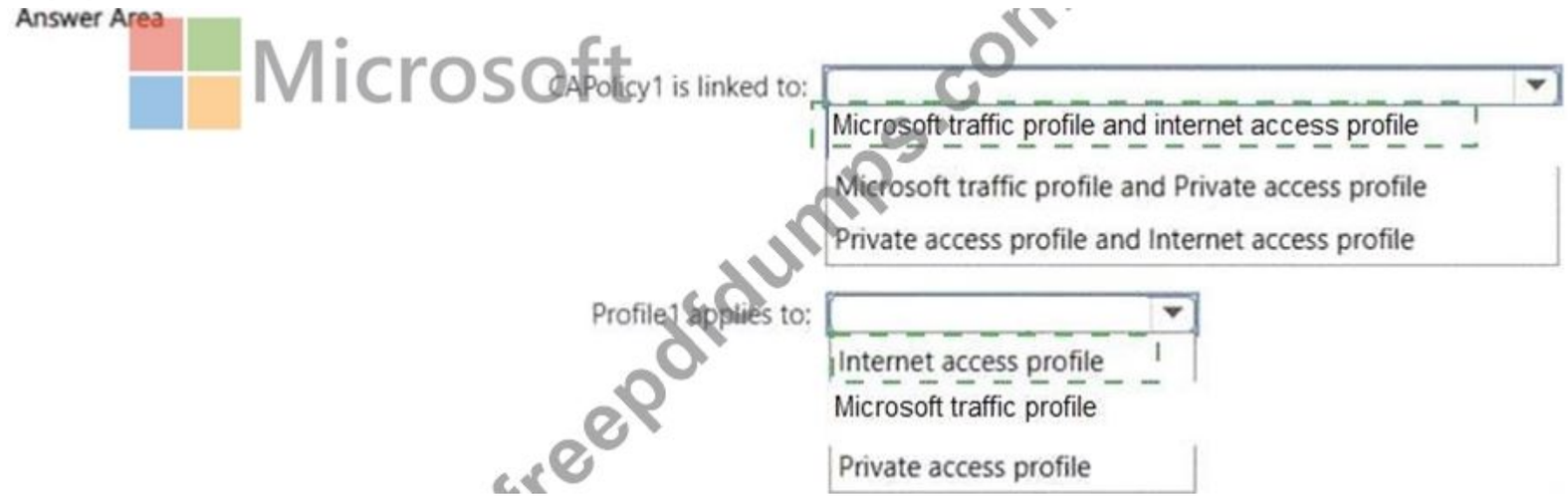


NEW QUESTION: 26
You have an Azure subscription named Sub1 that contains a resource group named RG1. RG1 contains an Azure Cosmos DB database named DB1 and an Azure Kubernetes Service (AKS) cluster named AKS1.
AKS1 uses a managed identity.
You need to ensure that AKS1 can access DB1. The solution must meet the following requirements:
* Ensure that AKS1 uses the managed identity to access DB1.
* Follow the principle of least privilege.
Which role should you assign to the managed identity of AKS1.
A. For R61, assign the Azure Cosmos DB Data Reader Role role.
B. For Sub1. assign the Owner role.
C. For RG1, assign the Reader role.
D. For DB1, assign the Azure Cosmos DB Account Reader Role role.
Answer: D (LEAVE A REPLY)
When enabling an Azure Kubernetes Service (AKS) cluster with a managed identity to access Azure Cosmos DB, you should assign the least privileged role required for the operation directly on the

NEW QUESTION: 27
You have a Microsoft Entra tenant that contains 1,000 users. The users are assigned Microsoft Entra Suite licenses. You perform the following actions:
* Deploy Global Secure Access.
* Create a Global Secure Access security profile named Profile1.
* Create the following Conditional Access policies:
o Name: CApolicy1
o Target resources: All internet resources with Global Secure Access
o Name: CApolicy2 o Session:
* Use Global Secure Access security profile: Profile1
To which Global Secure Access traffic forwarding profiles is CAPolicy1 linked, and to which profile does Profile1 apply? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

NEW QUESTION: 28

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps.

You have multiple third-party apps that access the resources in the subscription.

You need to monitor the access of the third-party apps.

What should you create?

A. an OAuth app policy

B. an endpoint protection policy

C. an app permission policy

D. an access policy

Answer: A (LEAVE A REPLY)

In Micr osoft Defender for Cloud Apps, OAuth app policies monitor and control third-party applications that have OAuth permissions to your Microsoft 365 environment. They allow administrators to review app permissions, detect over-privileged apps, and revoke acces s where needed.

This aligns with the SC-300 topic "Monitor and manage app permissions in Defender for Cloud Apps" , which states:

"OAuth app policies allow you to detect risky applications connected via OAuth authorization and monitor app access to your org anizational data."

NEW QUESTION: 29

You have an Azure AD tenant.

You perform the tasks shown in the following table.

Date	Task
March 1	Register four enterprise applications named App1, App2, App3, and App4.
March 15	From the tenant, update the following settings for App1: App roles, Users and groups, Client secret, and Self-service.
March 20	From the tenant, update the following settings for App2: App roles, Users and groups, Client secret, and Self-service.
March 25	From the tenant, update the following settings for App3: App roles, Users and groups, Client secret, and Self-service.
March 30	From the tenant, update the following settings for App4: App roles, Users and groups, Client secret, and Self-service.

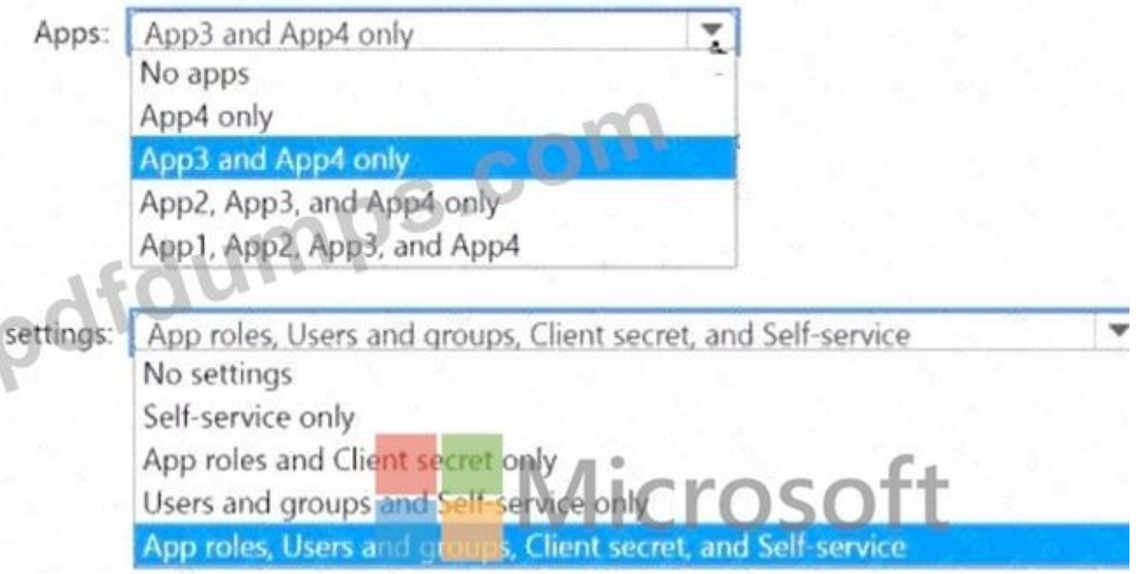
On April 5, an administrator deletes App1, App2, App3, and App4.

You need to restore the apps and the settings.

Which apps can you restore on April 16, and which settings can you restore for App4 on April 16? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Microsoft Entra ID (Azure AD) supports soft-delete for application objects for 30 days after deletion. The SC-
300 materials explain that administrators can recover deleted applications within 30 days; objects deleted beyond that window become non-recoverable. The guide also distinguishes between the application (app registration) and the service principal (enterprise application): the app registration contains credentials (client secrets/certificates) and app role definitions, while the tenant's service principal contains tenant- specific settings such as assignments and self-service configuration. The study content states that recovery operations restore the deleted application object and its schema (including defined app roles and credentials) if performed within the retention window, whereas tenant-scoped assignments and end-user self-service settings are not guaranteed to be recovered because they are specific to the service principal in the tenant.
Applying this: the apps were deleted April 5 and restoration is attempted April 16, which is inside the 30-day window. However, the exam scenario emphasizes the timing of tenant-side updates in March; App1's updates are older than 30 days by April 16, so it falls outside the reliable recovery period for those settings, while App2-App4 remain within it. For App4, the restorability applies to the application object contents- app roles and the client secret-not the tenant-specific Users and groups assignments or Self-service configuration. Hence: Apps = App2, App3, and App4 only; App4 settings = App roles and Client secret only.

NEW QUESTION: 30
You have an Azure AD tenant that contains a user named User1 and a registered app named App1.
User1 deletes the app registration of Appl.
You need to restore the app registration.
What is the maximum number of days you have to restore the app registration from when it was deleted?
A. 14
B. 30
C. 60
D. 180
Answer: B (LEAVE A REPLY)
As per Microsoft documentation and the SC-300 course objective "Manage application registrations" , when an app registration or enterprise app is deleted in Azure AD, it enters a soft-deleted state . You can restore the app registration within 30 days from the dat e of deletion using the Azure portal, PowerShell, or Microsoft Graph API.
After 30 days, the app registration and its associated service principal are permanently deleted and cannot be recovered.

NEW QUESTION: 31
You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Pr otection policies enforced.
You create an Azure Sentinel instance and configure the Azure Active Directory connector.
You need to ensure that Azure Sentinel can generate incidents based on the risk alerts raised by Azure AD Identity Protection.
What should you do first?
A. Add an Azure Sentinel data connector.
B. Configure the Notify settings in Azure AD Identity Protection.
C. Create an Azure Sentinel playbook.
D. Modify the Diagnostics settings in Azure AD.
Answer: D (LEAVE A REPLY)
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and Microsoft Learn module "Integrate Azure AD Identity Protection with Azure Sentinel" , Azure Sentinel (now part of Microsoft Defender XDR) can collect and analyze Azure AD Identity Protection (AIP) alerts to generate incidents and automated responses. However, Sentinel cannot directly pull these alerts until diagnostic logging is enabled in Azure AD.
By default, Azure AD does not send Identity Protection data (such as User risk detections , S ign-in risk detections , and Risky users) to Sentinel. To integrate them, you must first enable diagnostic settings to send these logs to a Log Analytics workspace that Sentinel uses. Once logs are being streamed, Sentinel can correlate and generate incidents from these risk alerts using its built-in analytics rules or custom playbooks.

The official Microsoft documentation states:
"To surface Azure AD Identity Protection alerts in Azure Sentinel, you must first enable Azure AD diagnostic logs and send them to a Log Analytics workspace connected to Sentinel."
* Modify Azure AD diagnostic settings # Enable log categories:
* AuditLogs
* SignInLogs
* RiskyUsers
* RiskDetections
* Stream these logs to the Log Analytics workspace linked to Azure Sentinel.
* Azure Sentinel can now use data connectors and analytic rules to trigger incidents or automation playbooks based on risk events.
* A. Add an Azure Sentinel data connector: You do that after diagnostic settings are configured and logs are available in Log Analytics.
* B. Configure Notify settings in Azure AD Identity Protection: This only controls email notifications to administrators - it does not forward alerts to Sentinel.
* C. Create an Azure Sentinel playbook: Playbooks are for automated responses, not for collecting data.
Step-by-step reasoning: Why not the other options:

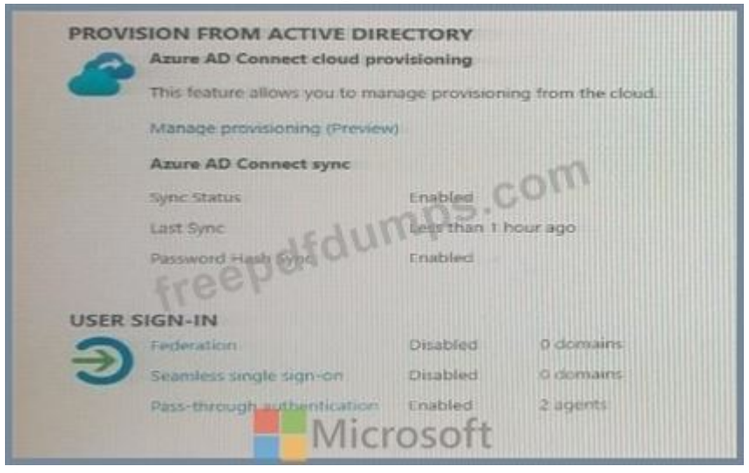
NEW QUESTION: 32
You configure a new Microsoft 36S tenant to use a default domain name of contosso.com.
You need to ensure that you can control access to Microsoft 365 resource-, by using conditional access policy.
What should you do first?
A. Disable the User consent settings.
B. Disable Security defaults.
C. Configur e a multi-factor authentication (Ml A) registration policy1.
D. Configure password protection for Windows Server Active Directory.
Answer: B (LEAVE A REPLY)
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Microsoft Learn module "Plan and implement Conditional Access policies" , enabling or customizing Conditional Access policies requires that Security Defaults in Azure AD be disabled .
Security defaults provide a basic level of protection, such as enforcing M FA for all users and blocking legacy authentication. However, when Security Defaults are enabled, custom Conditional Access policies cannot be created because both features manage sign-in risk and access control.
From the Microsoft documentation:
"To use C onditional Access policies, you must disable security defaults. Conditional Access policies provide more granularity and flexibility than security defaults." Therefore, before you can control access to Microsoft 365 resources through Conditional Access, th e first step is to disable Security Defaults in the Azure AD tenant.

NEW QUESTION: 33
Your network contains an on-premises Active Directory domain that sync to an Azure Active Directory (Azure AD) tenant. The tenant contains the shown in the following table.

Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

All the users work remotely.

Azur e AD Connect is configured in Azure as shown in the following exhibit.



Connectivity from the on-premises domain to the internet is lost.

Which user can sign in to Azure AD?

A. User1 only

B. User1 and User 3 only

C. User1, and User2 only

D. User1, User2, and User3

Answer: C (LEAVE A REPLY)

The exhibit shows Pass-through authentication (PTA) enabled with two agents and Password Hash Sync (PHS) enabled. SC-300 materials state that when both PTA and PHS are enabled, Azure AD can fall back to password hash verification if PTA agents are unavailable. With connectivity from on-premises to the Internet lost , PTA agents cannot validate passwords; however, PHS continues to allow cloud authentication for synchronized users. Therefore:

* User1 (cloud-only) authenticates in Azure AD directly, unaffected by on-prem connectivity.
* User2 (directory-synced) can still sign in because PHS is enabled and provides backup authentication when PTA is unreachable.
* User3 (guest) authenticates in the home tenant, which is independent of your on-prem connectivity; the host tenant simply relies on the external identity.

SC-300 explicitly teaches that enabling PHS alongside PTA provides resiliency for sign-in and is a recommended best practice. Consequently, all three users can sign in under the described outage.

NEW QUESTION: 34

You have a Microsoft Entra tenant that has a Microsoft Entta ID P2 license. You create a Log Analytics workspace.

You need to ensure that you can view Microsoft Entra ID audit log information by using Azure Monitor.

What should you do first?

A. Create an Microsoft Entra ID workbook.

B. Modify the Diagnostics settings for Microsoft Entra ID.

C. Runtheupdate-ngoomaincmdlet.

D. Run the update-Mgorganization cmdlet

Answer: B (LEAVE A REPLY)
According to the Microsoft SC-300 Study Guide and Microsoft Learn module: "Monitor and troubleshoot Microsoft Entra ID", in order to view Microsoft Entra ID audit log information in Azure Monitor (and thereby in a Log Analytics workspace), you must first configure diagnostic settings for Microsoft Entra ID.
By default, Entra ID audit logs are retained within the Microsoft Entra portal for 30 days (for P1) or 180 days (for P2). To integrate these logs into Azure Monitor for advanced analysis, alerting, and retention, administrators must explicitly enable and direct log export through Diagnostic settings.
Steps include:
* In the Microsoft Entra admin center, navigate to Monitoring # Diagnostic settings.
* Select Audit Logs (and optionally, Sign-in Logs).
* Choose Send to Log Analytics workspace and select the desired workspace.
This configuration allows continuous streaming of Entra ID audit data into Azure Monitor, where it can be queried with Kusto Query Language (KQL).
Other options such as creating a workbook or running PowerShell cmdlets (update-MgOrganization or update- ngoomain) do not initiate log forwarding.

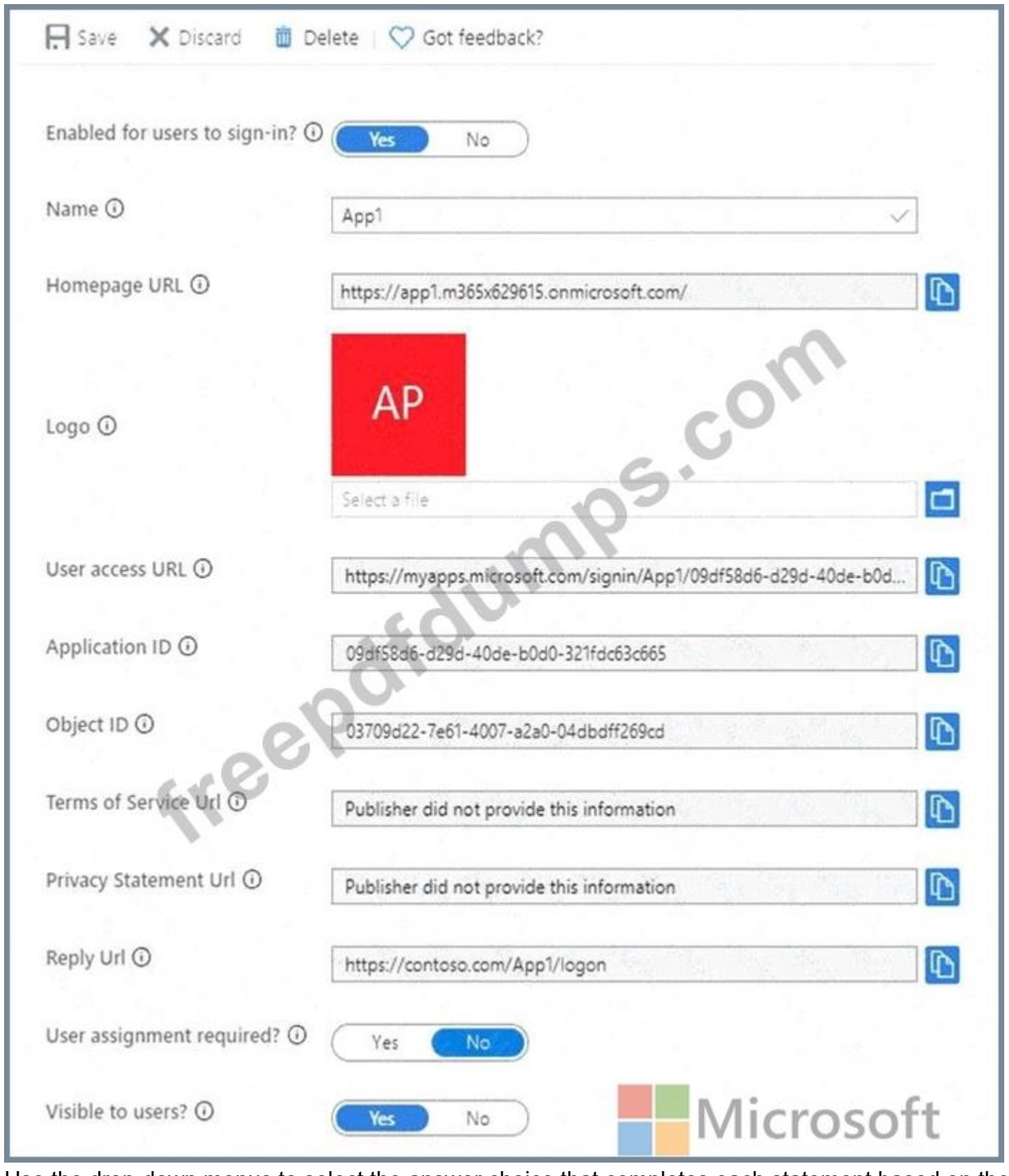
NEW QUESTION: 35
You have an Azure AD tenant.
You deploy a new enterprise application named App1.
When users attempt to provide App1 with access to the tenant, the attempt fails.
You need to ensure that the users can request admin consent for App1. The solution must follow the principle of least privilege.
What should you do first?
A. Enable admin consent requests for the tenant.
B. Designate a reviewer of admin consent requests for the tenant.
C. From the Permissions settings of App1, grant App1 admin consent for the tenant
D. Create a Conditional Access policy for Appl.
Answer: A (LEAVE A REPLY)
Azure AD (Entra ID) allows administrators to control how users request permission for applications that require admin consent. By default, only administrators can grant such consent.
According to the SC-300 Study Guide (Identity Management & Governance) and Microsoft Entra Documentation, the least privileged and compliant method to enable user-driven admin consent requests is to:
* Enable admin consent requests in the tenant.
* Designate one or more reviewers (optional) to handle these requests.
Once enabled, users who encounter an app that needs admin consent can submit a request for approval instead of being blocked. This ensures controlled delegation without globally granting broad permissions to all apps.
"Enable admin consent requests in Azure AD to allow users to request approval for apps that need tenant- wide permissions, ensuring least privilege and administrator oversight."

NEW QUESTION: 36
You have a Microsoft 365 tenant that has 5,000 users. One hundred of the users are executives. The executives have a dedicated support team.
You need to ensure that the support team can reset passwords and manage multi-factorauthentication (MFA) settings for only the executives. The solution must use the principle of least privilege.
Which object type and Azure Active Directory (Azure AD) role should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Object type: An administrative unit
Role: Authentication administrator
In Azure AD Identity and Access Administration, Administrative units (AUs) let you scope delegated admin privileges to a subset of users. The study materials describe AUs as a way to "delegate administration to a subset of users by using administrative units," ensuring the support team's privileges apply only to the executives and not tenant-wide. You would place the 100 executives in a dedicated AU and then assign the support team a suitable role scoped to that AU, satisfying least-privilege principles.
For the required tasks-reset passwords and manage MFA settings-the correct least-privileged role is Authentication administrator. The role capabilities are documented as allowing you to "view, set, and reset authentication method information for non-administrators" and to "require users to re-register for MFA," which covers managing MFA settings for the executives. By contrast, Password administrator is limited to
"reset passwords for non-administrators" and does not include managing authentication methods/MFA, and Helpdesk administrator focuses on basic user help tasks and password resets without full MFA method management. Therefore, assigning Authentication administrator scoped to an Administrative unit containing only the executives meets the scenario and adheres to least privilege.

NEW QUESTION: 37
You have a custom cloud app named App1 that is registered in Azure Active Directory (Azure AD).
App1 is configured as shown in the following exhibit.



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.

[answer choice] can access App1 from the homepage URL.

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for **[answer choice]**.

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade

Answer:

[answer choice] can access App1 from the homepage URL.

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for **[answer choice]**.

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade

Explanation:

< [answer choice] can access App1 from the homepage URL: # Only users listed on the Users and groups blade App1 will appear in the Microsoft Office 365 app launcher for [answer choice]: # Only users listed on the Users and groups blade

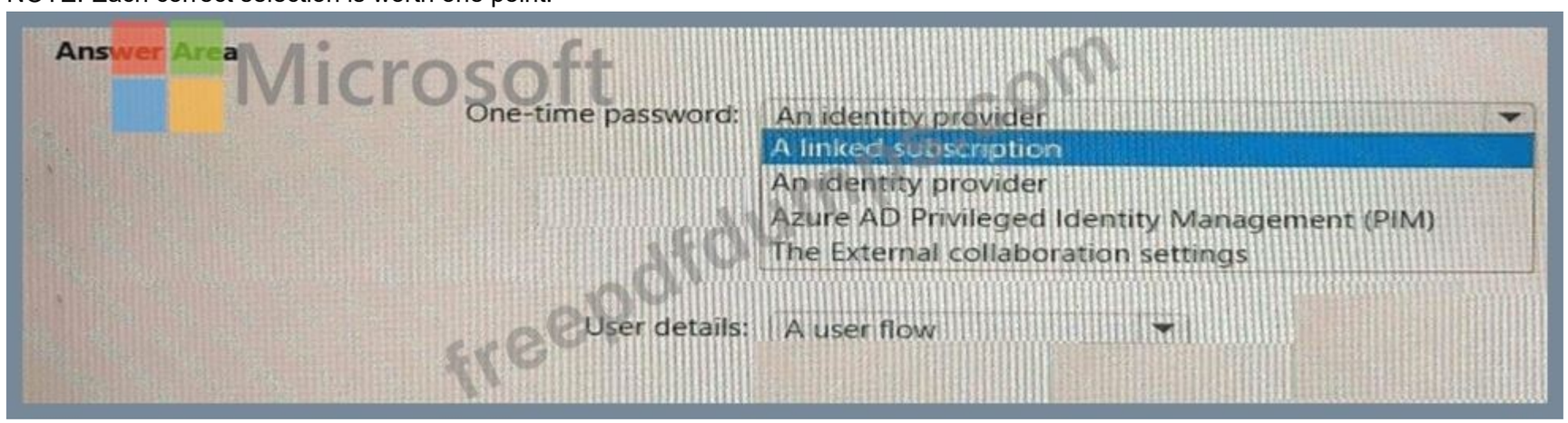
According to Microsoft's official documentation and the SC-300: Microsoft Identity and Access Administrator study guide, when you register and configure an enterprise application in Azure Active Directory, two specific settings directly influence user visibility and access:
* User assignment required?
* If this option is set to Yes, Azure AD requires users to be explicitly assigned to the app before they can sign in.
* Only users or groups listed on the Users and groups blade (app assignments) will have access.
* This means that even if the application is visible in Azure AD, users not assigned to it cannot authenticate or launch it.
* Visible to users?
* If set to Yes, the app appears in the Microsoft 365 app launcher (also known as the My Apps portal).
* However, when "User assignment required" is Yes, the visibility is limited only to those who are assigned to the app.
From the exhibit:
* "User assignment required?" = Yes
* "Visible to users?" = Yes
This configuration implies:
* Only assigned users (those listed on the Users and groups blade) can sign in to App1 via the homepage URL.
* App1 will appear in the Microsoft 365 app launcher (My Apps portal) only for those same assigned users.
As per Microsoft Learn documentation ("Manage enterprise apps in Azure AD"):
"When User assignment required is set to Yes, only users assigned to the application can access it. If Visible to users is also Yes, the application will appear in My Apps for those assigned users."

NEW QUESTION: 38
You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.
What should you do firs t?
A. Modify the User consent settings for the enterprise applications.
B. Create a catalog.
C. Create a program.
D. Modify the Admin consent requests settings for the enterprise applications.
Answer: B (LEAVE A REPLY)
In Azure AD Identity Governance, application access granted through Entitlement management is organized around catalogs and access packages. The SC-300 study materials explain that "a catalog is a container for resources and access packages" and that you must add your enterprise applications (or the groups tied to those apps) to a catalog before you can build access packages that users can request. Creating the catalog first enables you to place only the required resources in scope and to delegate day-to-day ownership: "catalog owners can manage the resources and access packages within their catalog without being tenant-wide admins," satisfying the delegation requirement to use custom catalogs and least privilege. After the catalog exists, you create one or more access packages that include the application (or groups) and policies that control who can request, how they are approved, and for how long. Identity Governance then lets you track access package assignments and review who has the app over time. By contrast, programs are used to group and report on governance initiatives (for example, collections of access reviews) rather than to onboard application resources; and modifying user/admin consent settings affects app consent behavior, not the lifecycle tracking of assignments. Therefore, the correct first step to track application access assignments while meeting the delegation requirements is to create a catalog.

NEW QUESTION: 39
You have an Azure subscription that contains a virtual machine named VM1. VM1 has the following configurations:
* Priva te IP address: 172.16.1.5
* Public IP address 10fl.143.16U5
* System-assigned managed identity status: On

You install an app named App1 on VM1.
You need to configure App1 to request a managed identity app-only access token. Which IP address should App1 use for the request?
A. 108.143.161.25
B. 127.0.0.1
C. 169.254.169.254
D. 172.1615
Answer: (SHOW ANSWER)
When an application running on an Azure VM needs to authenticate using its system-assigned managed identity, it must request a token from the Azure Instance Metadata Service (IMDS).
This service is accessible via a non-routable IP address - 169.254.169.254 .
The correct request URI pattern is:
http://169.254.169.254/metadata/identity/oauth2/token
This IP is used exclusively by Azure VMs to securely obtain tokens for managed identities without requiring credentials in the code.
Microsoft's documentation specifies:
"Applications running on Azure resources can request tokens from the Azure Instance Metadata Service (IMDS) endpoint at 169.254.169.254." Other options:
* 127.0.0.1 - loopback address (not used for IMDS)
* 108.143.161.25 - external public IP (irrelevant)
* 172.16.1.5 - private VM IP, not used for token requests

NEW QUESTION: 40
You have an Azure AD tenant and an Azure web app named App1.
You need to provide guest use rs with self-service sign-up for App1. The solution must meet the following requirements:
* Guest users must be able to sign up by using a one-time password.
* The users must provide their first name, last name, city, and email address during the sign-up p rocess.
What should you configure in the Azure Active Directory admin center for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:
One-time password: The External collaboration settings
User details: A user flow
According to Microsoft's official documentation and the Microsoft Identity and Access Administrator (SC-

300) Study Guide , when configuring self-service sign-up for guest users in Azure Active Directory (Azure AD) External Identities, there are two separate configuration areas that govern how users authenticate and what information they must provide:
One-time password requirement To allow guest users who do not have Azure AD, Microsoft, or Google accounts to authenticate using a one-time passcode (OTP) sent to their email, you must enable this feature under External collaboration settings.
This configuration is found in the Azure AD admin center under:
Azure Active Directory # External Identities # External collaboration settings # One-time passcode for guests.
Microsoft documentation states:
"The one-time passcode feature in External collaboration settings enables guest users to authenticate by using a temporary code emailed to them when they sign in." Therefore, for the requirement "Guest users must be able to sign up by using a one-time password," you must configure The External collaboration settings.
User details requirement To collect specific user attributes such as first name, last name, city, and email address during self-service sign-up, you configure a user flow (also known as a sign-up/sign-in flow) under Azure AD B2C or External Identities user flows.
In the Azure AD admin center, navigate to:
Azure AD # External Identities # User flows # New user flow # Sign-up flow.
Within the flow, you define the attributes (like name, city, and email) that must be collected at registration.
Microsoft's official Identity and Access Administrator materials explain:
"User flows in External Identities determine the user experience during sign-up and sign-in and allow administrators to collect custom attributes such as name, location, or other organization-specific details."

NEW QUESTION: 41
You have a Microsoft Entra tenant.
You need to query risky user activity for the tenant.
How long will the logs of risky user activity be retained?
A. 30 days
B. 60 days
C. 90 days
D. 180 days
Answer: C (LEAVE A REPLY)
According to the Microsoft Entra ID Protection section of the SC-300 Study Guide and the official Microsoft documentation on risk detections and retention, Microsoft Entra ID stores risky user activity and detections for 90 days. This includes logs of risky users, risky sign-ins, and risk detections identified by machine learning models and heuristic signals.
The retention period of 90 days ensures administrators can analyze user risk patterns, investigate compromised accounts, and implement mitigations such as Conditional Access or user risk policies. After 90 days, these logs are automatically purged unless exported to a SIEM such as Microsoft Sentinel for extended retention.
Microsoft Learn states:
"Identity Protection retains data for 90 days. Administrators can view risk detections, risky users, and risky sign-ins in the portal or query them using Microsoft Graph."

NEW QUESTION: 42
You have an Azure subscription that contains a user named User1. You onboard Microsoft Entra Permissions Management. You need to perform the following tasks:
* Identify all the accounts that are assigned the Global Administrator role permanently.
* Review the Permission Creep Index (PCI) of User1.
Which tab in Permissions Management should you use for each task? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

Explanation:

Identify all the accounts that are assigned the Global Administrator role permanently: Microsoft Entra Insights Review the PCI of User1: Analytics In Microsoft Entra Permissions Management, the Microsoft Entra Insights tab provides role-focused visibility into directory privileges. The SC-300 materials describe it as the place to surface "standing privileges for Microsoft Entra roles" and to identify accounts with high-risk assignments such as Global Administrator. The insights view surfaces who has those roles and whether they're permanent (standing) versus eligible or time-bound, enabling you to quickly "identify high-impact directory roles and users with persistent assignments." The Analytics tab is centered on identities, resources, and actions, featuring risk and usage metrics, including the Permission Creep Index (PCI). The study content explains that Analytics lets you "drill into an identity' s effective permissions and risk score (PCI) to compare granted vs. used permissions." For a specific user (e.

g., User1), you navigate to Analytics # Identities, search/select the user, and view the PCI card and detailed breakdown of unused vs. used permissions.

Accordingly: to find permanent Global Administrator assignments, use Microsoft Entra Insights; to review User1's PCI, use Analytics.

NEW QUESTION: 43

You have an on-premises datacente r that contains the hosts shown in the following table.

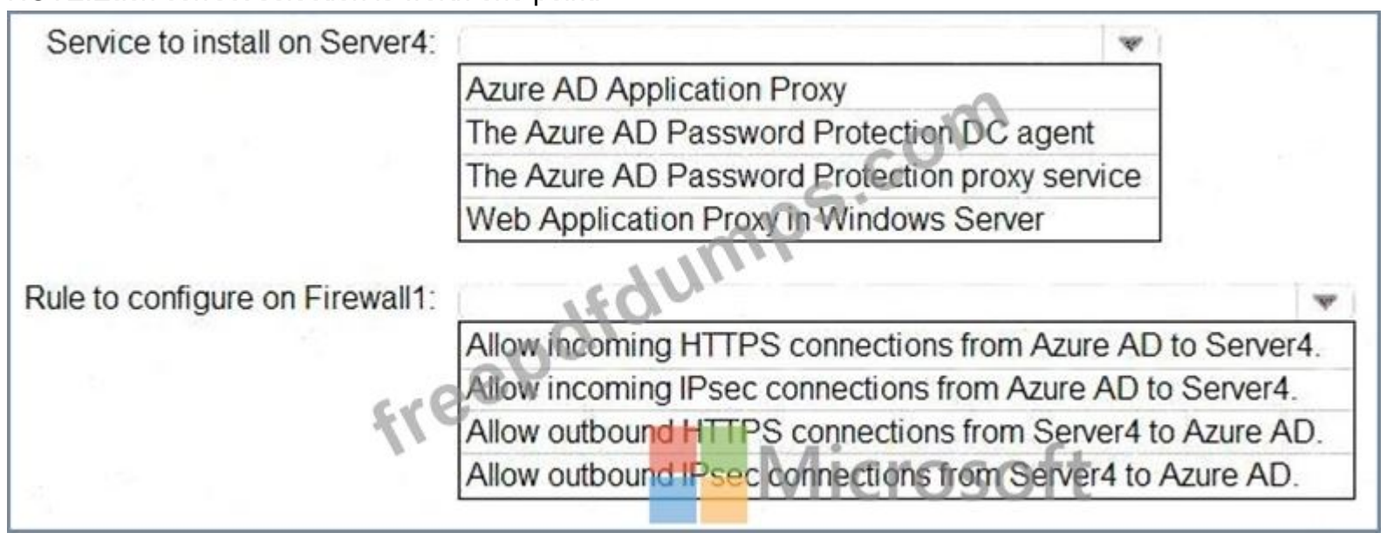
Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows Server 2019
Firewall1	Hardware firewall connected to the internet that blocks all traffic unless explicitly allowed

You have an Azure Active Directory (Azure AD) tenant that syncs to the Active Directory forest. Multi-factor authentication (MFA) is enforced for Azure AD.

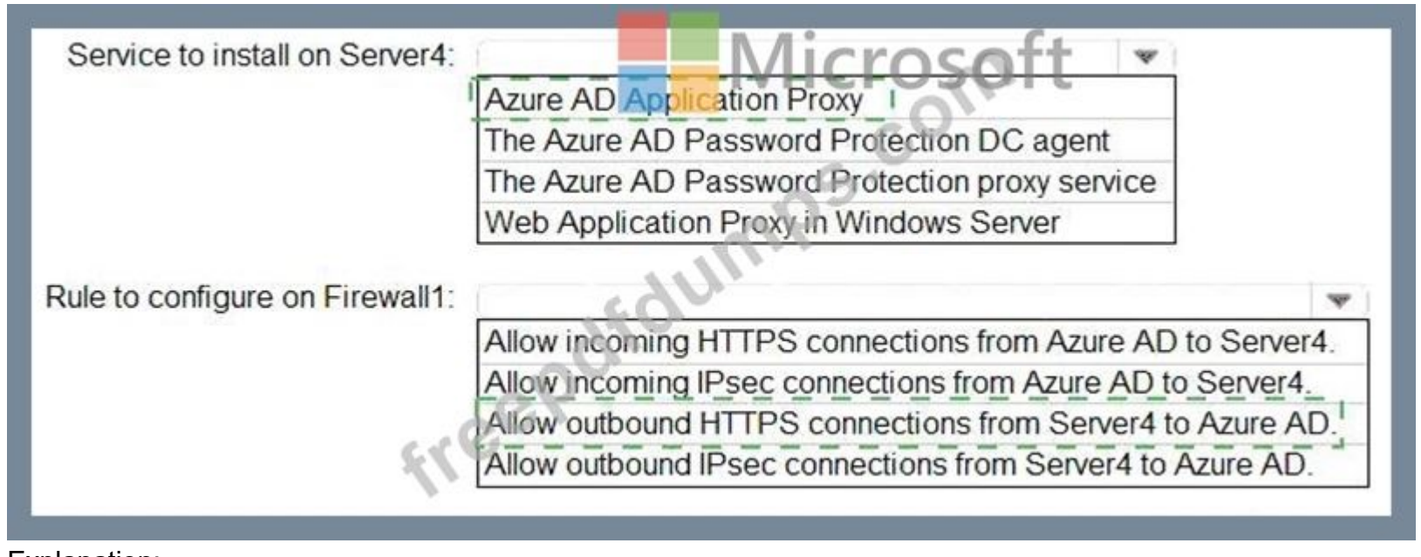
You need to ensure that you can publish App1 to Azure AD users.

What should you configure on Server and Firewall1? To answer, select the appropriate options in the answer area.

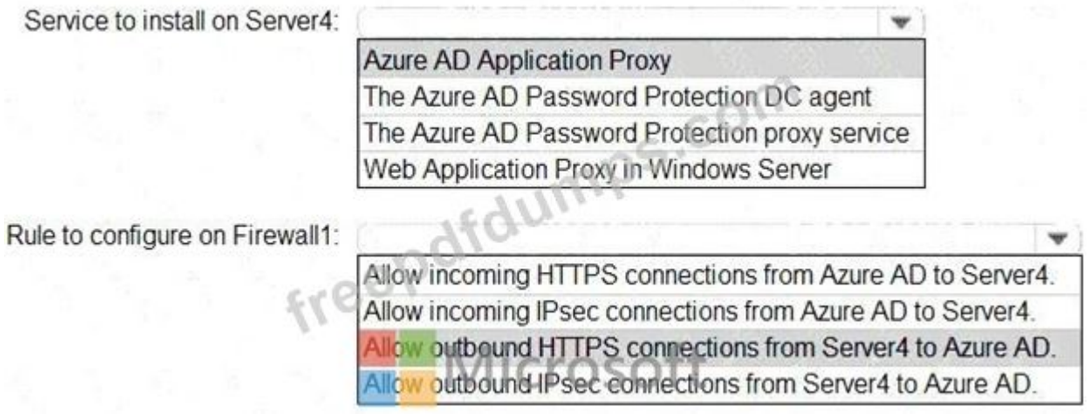
NOTE:Each correct selection is worth one point.



Answer:



Explanation:



In SC-300, publishing an on-premises web app to Azure AD users is performed with Azure AD Application Proxy. The exam materials and Microsoft curriculum explain that you deploy an Application Proxy connector on a Windows Server joined to your on-premises network, which brokers requests to internal apps such as an ASP.NET site. The connector is designed for perimeter-friendly deployments: "Application Proxy connectors only make outbound connections to the Application Proxy service" and "no inbound ports need to be opened in the firewall." Because the connector initiates the session to Azure over TLS, the firewall requirement is simply to permit the connector's outbound HTTPS to the service endpoints. This aligns with the least- exposure pattern emphasized in Identity Governance: you avoid publishing inbound listener rules and still support Azure AD features like Conditional Access and MFA at the cloud edge. Alternatives in the list do not meet the publishing requirement: the Password Protection DC agent and Password Protection proxy service are for banned-password enforcement, and Web Application Proxy in Windows Server is a different reverse- proxy technology not required when using Azure AD Application Proxy. Therefore, to publish App1 securely to Azure AD users, install Azure AD Application Proxy on Server4 and allow outbound HTTPS from Server4 through Firewall1.

NEW QUESTION: 44

You need to meet the planned changes for the User administrator role.

What should you do?

A. Create an access review.

B. Modify Role settings

C. Create an administrator unit.

D. Modify Active Assignments.

Answer: B (LEAVE A REPLY)

In Azure AD Privileged Identity Management (PIM) for Azure AD roles, the exam materials describe that you tailor how a role (for example, User administrator) is used by editing its Role settings. These settings control activation behavior, including require multi-factor authentication, justification, approval, assignment /activation durations, and notifications . The guide states that administrators can "configure activation requirements and time-bound eligibility on a per-role basis" and "enforce approval workflows and MFA at activation." Access reviews are used to periodically verify who still needs a role , but they do not implement the operational changes to how the role is activated. Active assignments simply shows and changes who currently holds active/eligible assignments; it does not set policy for the role's activation behavior. Administrative units scope certain directory tasks, but they are not how you change PIM activation/approval /MFA requirements. Therefore, to meet planned changes for the User administrator role (such as least privilege activation with approval, justification, and MFA), you update PIM # Azure AD roles # User administrator # Role settings. This aligns with the SC-300 objective to "configure PIM settings and policies for Azure AD roles," ensuring governance by policy rather than ad-hoc assignment.

NEW QUESTION: 45

You have an Azure AD tenant that has multi-factor authentication (MFA) enforced and self-service password reset (SSPR) enabled.

You enable combined registration in interrupt mode.

You create a new user named User1.

Which two authentication methods ca n User1 use to complete the combined registration process? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. a FID02 security key
B. a hardware token
C. a one-time passcode email
D. Windows Hello for Business
E. the Microsoft Authenticator app
Answer: C,E (LEAVE A REPLY)
To Answer this question accurately, we must analyze the Combined Security Information Registration experience in Interrupt Mode for a new user within an Azure AD (Microsoft Entra ID) tenant where both MFA and SSPR are enabled.
1. Understanding Combined Registration in Interrupt Mode: According to Microsoft documentation on Combined security information registration , this feature allows users to register their security methods for both Azure AD Multi-Factor Authentication (MFA) and Self-Service Password Reset (SSPR) in a single, unified step.
* Interrupt Mode triggers when a user signs in and a policy (like Identity Protection or Conditional Access) requires them to register security infor mation immediately.
* Because the question states SSPR is enabled and MFA is enforced , the user is required to register methods that satisfy both policies.
2. Validating the Methods (Options Analysis):
* Option E: The Microsoft Authenticator app (Correct): The Microsoft Authenticator app is the primary and most recommended method in the combined registration flow. It satisfies the strong authentication requirement for MFA and can also be used for SSPR . Microsoft documentation explicitly lists the Microsoft Auth enticator app as a supported method that users can register during the combined experience.
* Option C: A one-time passcode email (Correct): While Email is not a valid method for Azure AD MFA (primary authentication), it is a supported and common method for SSPR .
* Documentation Extract: " Users can register the following methods... Email (SSPR only). "
* Since the question specifies that SSPR is enabled , the combined registration wizard requires the user to register SSPR methods in addition to MFA methods. Therefo re, registering an email address to receive a one-time passcode is a valid step User1 can take to complete the portion of the combined registration process related to SSPR.
* Option A: A FIDO2 security key (Incorrect for Initial Registration):
* Documentation Extract: " User registration of FIDO2 security keys... relies on the combined registration experience. Users must have already registered at least one Azure AD Multi-Factor Authentication method. "
* Because User1 is a new user (and likely does not have a Temporary Access Pass specified), they cannot use a FIDO2 key to complete the initial registration interrupt. They must first register a standard MFA method (like the Authenticator app) before they can add a FIDO2 key via the " Manage " mode (Security Info p age).
* Option B: A hardware token (Incorrect): Hardware OATH tokens are not self-registered by the user in the combined registration portal. They must be uploaded and assigned by an administrator via a CSV file. Therefore, User1 cannot " use " this method to complete the self-service registration process.
* Option D: Windows Hello for Business (Incorrect): Windows Hello for Business (WHfB) is provisioned at the device level (via Windows Settings or OOBE), not through the web-based Combined Registration interrupt wizard. Additionally, WHfB typically requires the user to have already completed MFA registration to provision the credential.
Conclusion: The only two methods from the list that a new user can actively register and use to complete the web-based Combined Registration interrupt wizard (satisfying both MFA and SSPR requirements) are the Microsoft Authenticator app (for MFA/SSPR) and Email (for SSPR).

NEW QUESTION: 46
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to identify which users access Facebook from their devices and browsers. The solution must minimize admini strative effort.
What should you do first?
A. From the Microsoft Defender for Cloud Apps portal, unsanctioned Facebook.
B. Create an app configuration policy in Microsoft Endpoint Manager.
C. Create a Defender for Cloud Apps access policy.

D. Create a Cond itional Access policy.

Answer: C (LEAVE A REPLY)

The question asks how to identify which users access Facebook from their devices and browsers using Microsoft Defender for Cloud Apps (MCAS) , with minimal administrative effort.

Here's the breakdown:

* Objective: Identify users who access Facebook (a cloud app).
* Tool: Microsoft Defender for Cloud Apps.
* Requirement: Visibility, not control - i.e., detect and report.

To achieve this, the appropriate first step is to create an Access Policy in Defender for Cloud Apps.

An Access Policy allows you to monitor and control real-time session access to cloud apps based on user, device, location, and app usage. It can:

* Detect when a user signs into or uses specific apps (like Facebook).
* Log and alert administrators automatically.
* Require no endpoint or Conditional Access configuration - satisfying the "minimize administrative effort" requirement.

From Microsoft Defender for Cloud Apps documentation:

"Access policies enable monitoring of app access patterns and can tr igger alerts when users sign in to or access specific sanctioned or unsanctioned cloud applications." Other options explained:

* (A) Unsanctioning Facebook marks it as disallowed, but does not identify users accessing it.
* (B) App configuration policies in In tune control mobile device settings, not cloud app access.
* (D) Conditional Access policies can block or require conditions for Facebook access but do not report who accessed it .

NEW QUESTION: 47

You have a Microsoft Entra tenant named contoso.com that contains an administrative unit named AU1 and two users named User1 and User2. User1 is a member of AU1.

You need to perform the following role assignments:

* User1: Security Administrator
* User2: User Administrator

For which scopes can each user be assigned the role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

Explanation:

According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and Microsoft Entra documentation , role assignments in Entra ID (formerly Azure AD) can be scoped at directory (tenant- wide) or administrative unit (AU) levels.

An Administrative Unit (AU) is a logical grouping of Azure AD resources (users, groups, devices) that allows administrators to delegate management responsibilities. When you assign roles scoped to an AU, the permissions of the role apply only to objects within that AU.

From Microsoft's "Manage role-based access control (RBAC) with administrative units" module:

"You can assign directory roles to users either at the tenant level or scoped to an administrative unit. Only users who are members of the AU can be assigned roles scoped to that AU."

Applying this to the scenario:

* User1 is a member of AU1. Therefore, User1 is eligible for a role assignment scoped to AU1 and/or tenant-wide (contoso.com). User1 can have the Security Administrator role assigned at both AU1 and contoso.com.
* User2 is not a member of AU1. Users who are not members of an administrative unit cannot be assigned roles scoped to that AU. Thus, User2's User Administrator role can be assigned only at the tenant-wide (contoso.com) level.

This aligns with the Microsoft Learn reference:

"Only members of an administrative unit can be assigned directory roles scoped to that administrative unit.

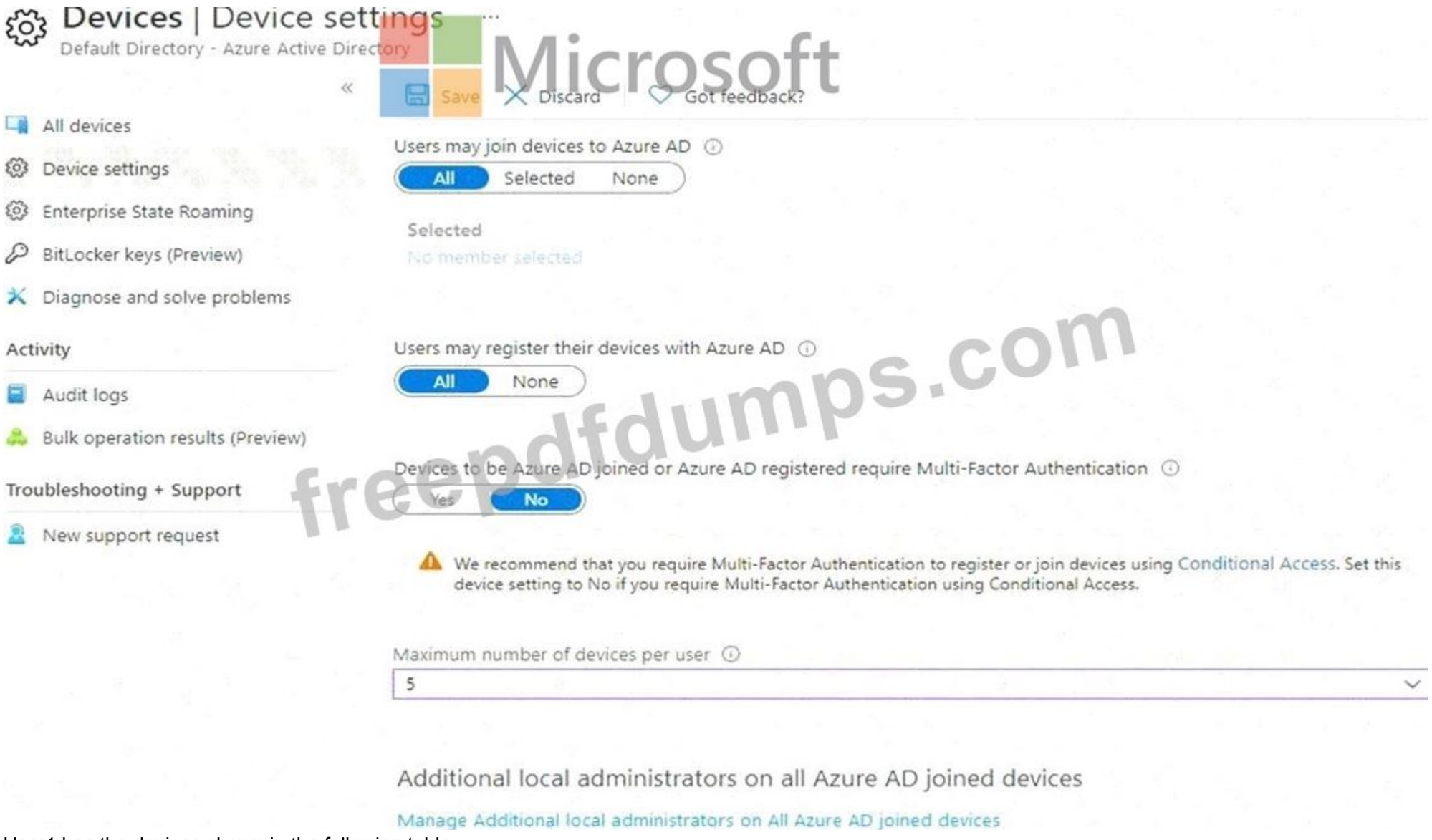
Roles can always be assigned at the organization level regardless of AU membership."

NEW QUESTION: 48

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.



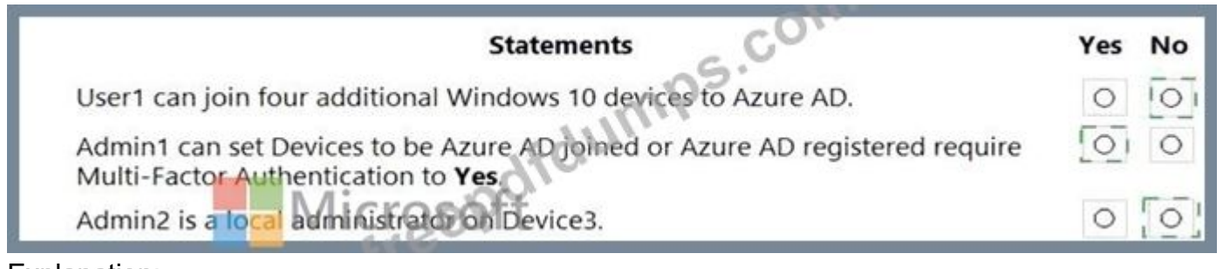
User1 has the devices shown in the following table.

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.

Answer:



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.

Statement 1: User1 can join four additional Windows 10 devices to Azure AD - NO 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." Statement 2: Admin1 can set Devices to be Azure AD joined or Azure AD registered require MFA to Yes - YES 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." Statement 3: Admin2 is a local administrator on Device3 - NO 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."

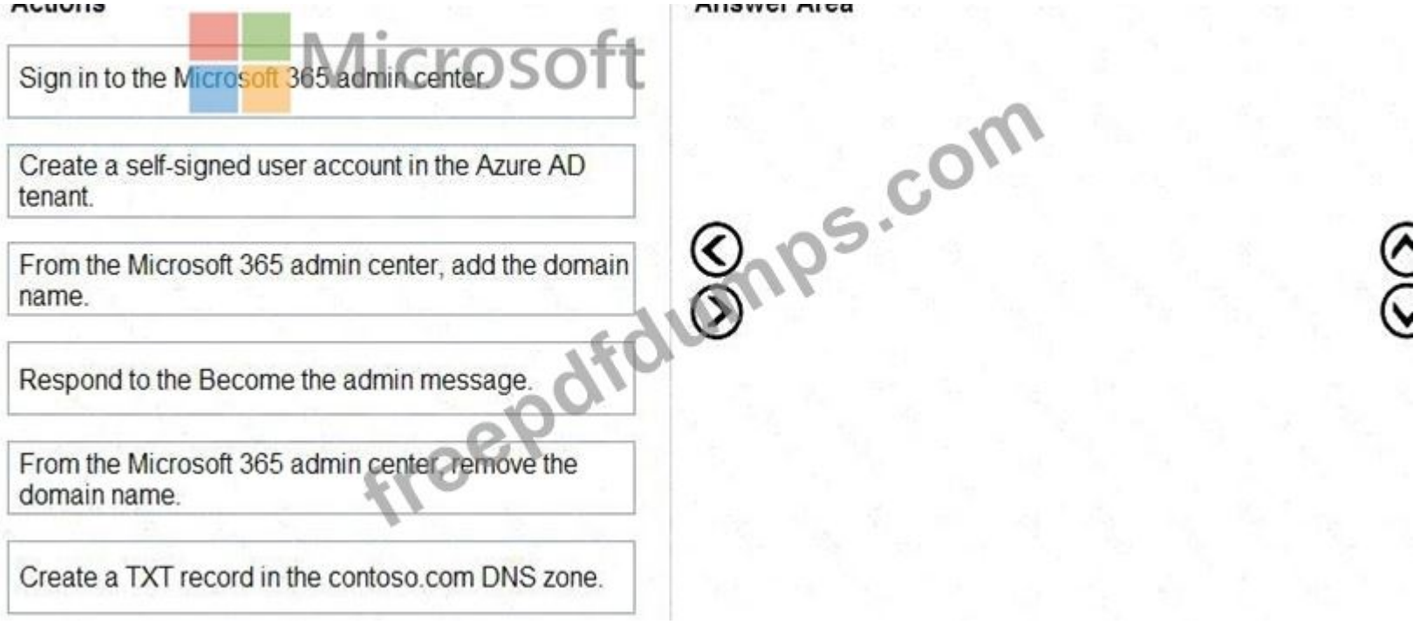
NEW QUESTION: 49

You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com.

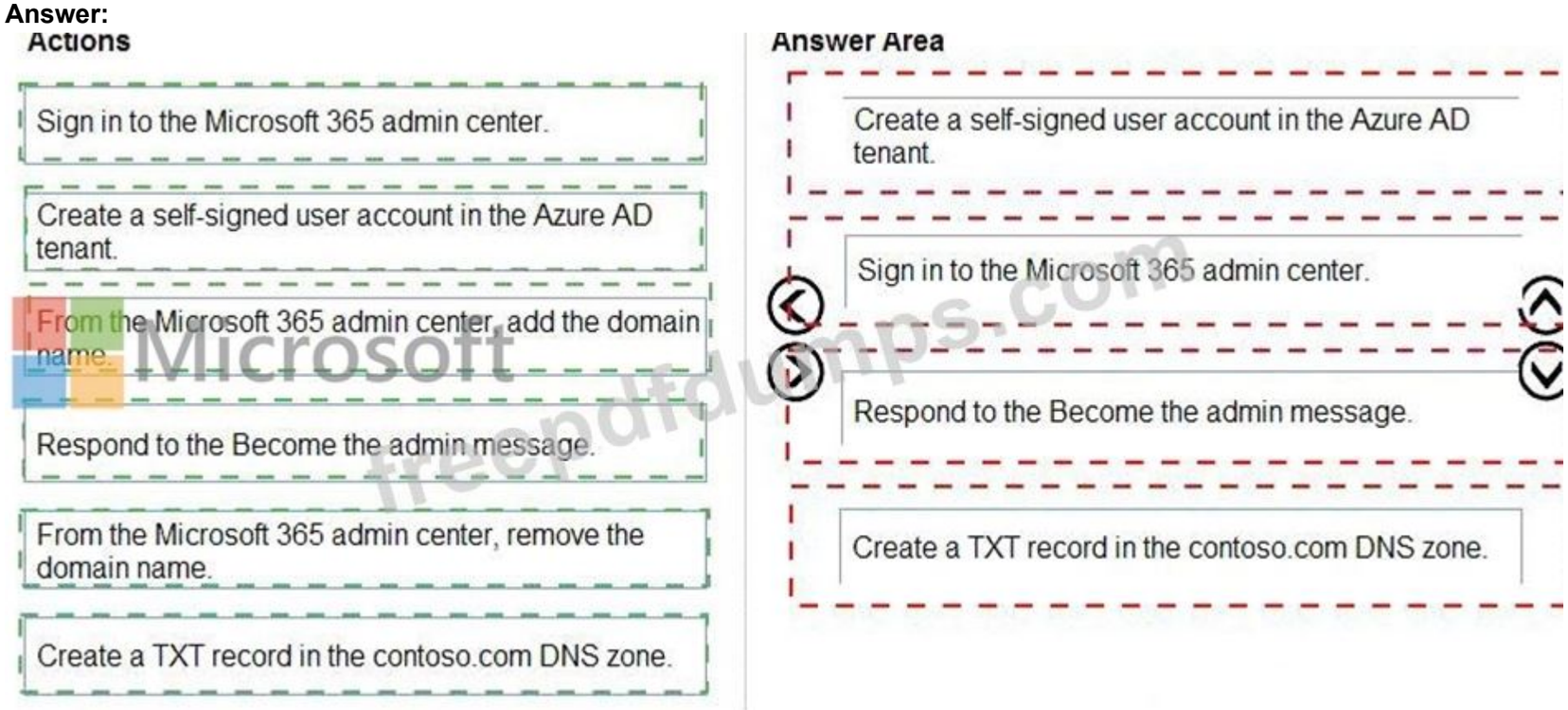
You discover that users use their email address for self-service sign-up to Microsoft 365 services.

You need to gain global administrator privileges to th e 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:

In SC-300, Microsoft describes taking control of an unmanaged (self-service created) Azure AD tenant by performing an admin takeover. The process begins in the Microsoft 365 admin center where you attempt to add the domain that users used for self-service sign-up. When the domain is already in use in an unmanaged directory, the portal surfaces the "Become the admin" option, enabling an internal admin takeover. The study material states that admins must "verify ownership of the domain by creating a DNS TXT record" and that, after verification, "the account that completes the takeover is promoted to Global Admi nistrator of the unmanaged tenant." It also emphasizes that the TXT record step comes after selecting the takeover option because the wizard provides the exact TXT value to publish. Unrelated actions-such as creating a "self- signed user account" in Azure AD or removing the domain-are not part of the takeover sequence. Thus, the correct order is: sign in # add the domain # select Become the admin # publish the TXT record to prove domain ownership, which completes the takeover and grants Global Administrator privileges to manage the tenant created by self-service sign-ups. takeover

NEW QUESTION: 50

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1 and the groups shown in the following table.

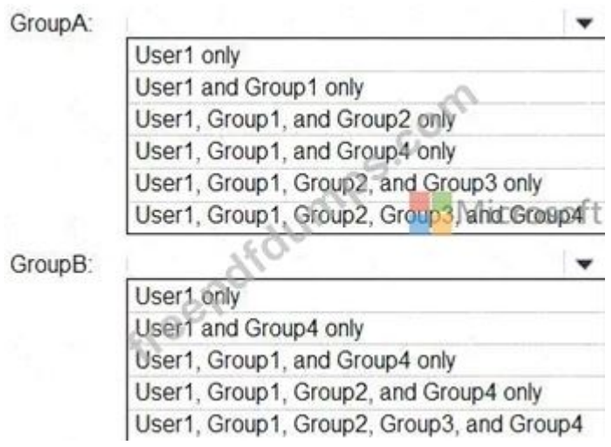
Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

In the tenant, you create the groups shown in the following table.

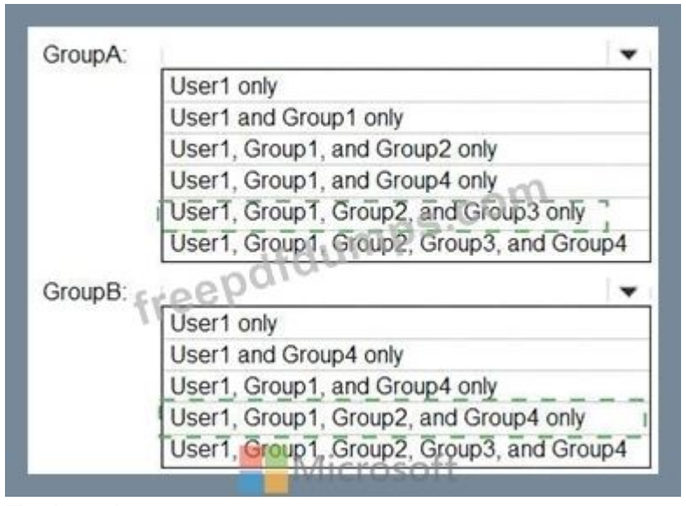
Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

Which members can you add to GroupA and GroupB? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one poin t.



Answer:



Explanation:

< GroupA: # User1, Group1, Group2, and Group3 only

GroupB: # User1, Group1, Group2, and Group4 only

According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and the Microsoft Learn module "Manage groups in Azure Active Directory" , group nesting rules in Azure AD depend on group type and membership type .

* GroupA is a Secur ity group with an Assigned membership type.
* In Azure AD, security groups (whether assigned, dynamic user, or dynamic device) can contain users , devices , and other security groups as members.
* However, Microsoft 365 groups cannot be added to a security group because Microsoft 365 groups include collaborative services (SharePoint, Teams, Planner) that rely on unique membership and ownership models.

Therefore, GroupA (security group) can include:

* User1 (user) #
* Group1 (security - assigned) #
* Group2 (security - dynamic user) #
* Group3 (security - dynamic device) #
* # Group4 (Microsoft 365 group) - not allowed in a security group.

Correct composition for GroupA: User1, Group1, Group2, and Group3 only.

* GroupB is a Microsoft 365 group with an Assigned membership type.
* Microsoft 365 groups can include users and security groups as members, but cannot include other Microsoft 365 groups (nested Microsoft 365 groups are not supported).
* So GroupB can include:
* User1 (user) #
* Group1 (security - assigned) #
* Group2 (securit y - dynamic user) #
* # Group3 (dynamic device) - device groups can't be members of M365 groups.
* Group4 (Microsoft 365 group) # - nesting M365 groups is not supported.

Correct composition for GroupB: User1, Group1, Group2, and Group4 only.

NEW QUESTION: 51

You have an Azure subscription that contains a virtual machine named VM1 and an Azure key vault named Vault1. VM1 has a system-assigned managed identity. You need to ensure that VM1 can retrieve the values of secrets stored in Vault 1. The solution must minimize administrative effort. What should you do first?

A. Configure the Resource access settings for Vault1.
B. C onfigure the permissions model for Vault1
C. Add a user-assigned managed identity to VM1.
D. Assign an Azure role to VM1.
Answer: D (LEAVE A REPLY)
To ensure VM1 can retrieve the values of secrets stored in Vault1 while minimizing administrative effort, you should assign an Azure role to VM1 .
1. Managed Identities and Key Vault Access: VM1 has a system-assigned managed identity . This identity acts as a Service Principal in Microsoft Entra ID (formerly Azure AD). To access Key Vault secrets, this identity must be granted permissions on the Key Vault.
2. Permission Models (RBAC vs. Access Policies): Azure Key Vault supports two permission models:
* Azure role-based access control (Azure RBAC): The recommended, modern authorization system. It allows you to mana ge access to Key Vault keys, secrets, and certificates centrally using Azure IAM (Identity and Access Management), just like other Azure resources. It provides fine-grained access control and integrates with PIM (Privileged Identity Management).
* Vault acce ss policy: The legacy model where permissions are defined within the Key Vault ' s own " Access policies " blade.
3. Why " Assign an Azure role " (Option D) is the Correct First Step:
* Minimizing Administrative Effort: Using Azure RBAC is the recommended best pra ctice for minimizing effort because it unifies access management across Azure resources.
* The Action: To grant the required access (reading secrets) under the RBAC model, you must assign a specific role to the managed identity. The appropriate role is Key V ault Secrets User , which grants permission to read secret contents (Get and List operations) without granting administrative privileges (adhering to Least Privilege).
* Scenario Analysis: While older Key Vaults defaulted to Access Policies, new vaults and th e " minimize effort " requirement point towards the RBAC model. Option A (" Configure the Resource access settings ") is vague and likely refers to the " Access configuration " or " Access policies " blade, but " Assign an Azure role " is the definitive action to gr ant access in the modern RBAC workflow. If the vault were in Access Policy mode, one would typically " Add an access policy, " but that specific option is not listed, reinforcing that RBAC (Option D) is the intended path.
Documentation Extract:
" Azure RBAC is an authorization system built on Azure Resource Manager that provides centralized access management of Azure resources... The Azure RBAC model allows users to set permissions on different scope levels... To grant access to a specific user, group, or app lication... assign a role. For example, the Key Vault Secrets User role allows a user to read secret contents. " (Source: Microsoft Learn - Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control)

NEW QUESTION: 52
You have a Microsoft 365 E5 subscription that contains three gr oups named Groups1, Group2, and Group3, and the users shown in the following table.

Name	Role	Member of
User1	Global Administrator	Group1
User2	*None*	Group2
User3	Global Reader	Group2, Group3

You create a Conditional Access policy named CAT that has the following settings:
* Users
* Include
#Users and groups: Group1
o Exclude
#Users and groups: Group2
#Directory roles: Global Administrator
o Target resources
#Include: All cloud apps
o Access controls

#Grant: Require multifactor authentication
You create a Conditional Access policy named CA2 that has the following settings:
* Users
* Include
#Users and g roups: Group2
o Exclude
#Users and groups: Group3
o Target resources
#Include: All cloud apps
o Access controls
#Grant: Block access
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selecti on is worth one point.

Answer:

Explanation:

SC-300 materials explain that Conditional Access (CA) evaluates assignments (who/what) and conditions /exclusions before applying grant controls. Policy CA1 targets Group1 and requires MFA, but explicitly excludes Global Administrator and Group2. User1 is in Group1 and holds the Global Administrator role, so the directory-role exclusion means CA1 does not apply and no other policy targets User1 # no MFA prompt.
Policy CA2 targets Group2 and blocks access to all cloud apps, with an exclusion for Group3. User2 is in Group2 and not in Group3, so CA2 applies and blocks SharePoint Online sign-in. User3 is in Group2 and Group3; because Group3 is excluded from CA2, the block does not apply. User3 is not in Group1, so CA1 doesn't apply either; therefore, User3 can sign in normally. The SC-300 guidance also notes that exclusions take precedence over inclusions, and block access is an enforcing control when a matching policy applies, while policies are evaluated independently with the most restrictive applicable outcome applied per user and sign-in.

NEW QUESTION: 53
You have a Microsoft 365 E5 subscription that has a Conditional Access policy named Policy1. You need to perform the following actions:
* Create a Conditional Access App Control custom policy named Custom1.
* Configure Policy! to use Custom1
What should you use to create Custom1, and in which settings of Policy! should you enable Conditional Access App Control? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

Explanation:

NEW QUESTION: 54
You have a Microsoft 365 tenant.
You have an Active Dire ctory domain that syncs to the Azure Active Directory {Azure AD) tenant.
Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.
You plan to manage acce ss to external applications by using Azure AD.
You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.
What should you use to gather the information?
A. Cloud App Discovery in Microsoft Defender for Cloud Apps
B. enterprise applications in Azure AD
C. access reviews in Azure AD
D. Application Insights in Azure Monitor
Answer: A (LEAVE A REPLY)
The Cloud App Discovery feature in Microsoft Defender for Cloud Apps (formerly Cloud App Security) is designed to identify and analyze shadow IT-applications being accessed by users that are not managed by IT.
By importing firewall or proxy logs, Defender for Cloud Apps can automatically detect unmanaged external SaaS applications and the users accessing t hem. The study guide specifically states:
"Cloud App Discovery analyzes traffic logs from your firewalls and proxies to identify cloud applications used by your organization and provides visibility into usage and risk levels."
Therefore, to identify unmana ged external apps and the users accessing them using firewall logs, Cloud App Discovery is the correct Microsoft tool.

NEW QUESTION: 55
You have a Microsoft Entra tenant.
You configure self-service password reset (SSPR) with the following settings:
Require users to register when signing in: Yes
Number of methods required to reset: 1
What is a valid authentication method available to users?
A. A smartcard
B. A mobile app code
C. An FIDO2 security token
D. A Windows Hello PIN
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Microsoft Entra ID self-service password reset (SSPR) settings and the available authentication methods, as outlined in Microsoft Identity and Access Administrator documentation.

Understanding Self-Service Password Reset (SSPR) in Microsoft Entra ID:
Self-service password reset (SSPR) allows users to reset their passwords without administrator intervention, improving security and reducing helpdesk workload.
The settings provided are:
Require users to register when signing in: Yes- U sers must register their authentication methods (e.g., phone number, email, security questions) the first time they sign in. This ensures they have methods available for SSPR.
Number of methods required to reset: 1- Users must verify their identity using o ne authentication method to reset their password. This is the minimum number of methods required, meaning users must have at least one method registered, and they will use one method during the reset process.
Available Authentication Methods for SSPR:
Micr osoft Entra ID SSPR supports a specific set of authentication methods that users can use to verify their identity during a password reset. These methods are configured by the administrator in the Microsoft Entra admin center under " Password reset " settings .
The default authentication methods available for SSPR include:
Email:Users receive a code sent to an alternate email address.
Mobile phone (SMS):Users receive a code via SMS to their registered mobile phone.
Mobile app code:Users use a code generated by the Microsoft Authenticator app (or another compatible authenticator app).
Mobile app notification:Users receive a push notification in the Microsoft Authenticator app to approve the reset.
Security questions:Users answer predefined security questions they set up during registration.
Important Note:Methods like smartcards, FIDO2 security tokens, and Windows Hello are not supported for SSPR. These methods are typically used for authentication during sign-in (e.g., MFA or passwordless sign- in), not for the SS PR process.
Analysis of the Options:
A). A smartcard:
Smartcards are a form of certificate-based authentication often used for sign-in to Windows devices or VPNs.
They require a physical card and a reader, and they are typically used for primary authenticat ion, not for SSPR.
Microsoft Entra ID SSPR does not support smartcards as an authentication method for password reset.
Smartcards are not listed as an available method in the SSPR configuration settings.
Conclusion:This is incorrect.
B). A mobile app code:
A mobile app code refers to a time-based one-time password (TOTP) generated by an authenticator app, such as the Microsoft Authenticator app.
This is a supported method for SSPR in Microsoft Entra ID. Users can register the Microsoft Authenticator app (or another compatible app) and use the generated code to verify their identity during a password reset.
Since the setting " Number of methods required to reset: 1 " means only one method is needed, a mobile app code is a valid option if the user has registered it.
Conclusion:This is correct.
C). An FIDO2 security token:
FIDO2 security tokens (e.g., YubiKey) are hardware-based security keys that support passwordless authentication in Microsoft Entra ID. They are part of Microsoft's passwordless authentication stra tegy and can be used for sign-in.
However, FIDO2 security tokens are not supported for SSPR. The SSPR process does not allow users to verify their identity using a FIDO2 security key because the reset process is designed to work with simpler, more accessib le methods like email, SMS, or app-based codes.
Conclusion:This is incorrect.
D). A Windows Hello PIN:
Windows Hello PIN is a device-specific authentication method used to sign in to Windows devices. It is part of Windows Hello, which also includes biometric authentication (e.g., facial recognition, fingerprint).

Windows Hello PIN is not supported for SSPR in Microsoft Entra ID. The SSPR process occurs in a web- based portal (e.g., aka.ms/sspr) and does not integrate with device-specific authenticatio n methods like Windows Hello. Additionally, Windows Hello PIN is tied to a specific device, whereas SSPR is designed to be device-agnostic.
Conclusion:This is incorrect.
Additional Considerations:
The setting " Require users to register when signing in: Yes " ensures that users have at least one authentication method registered. However, the question does not specify which methods are enabled by the administrator. In Microsoft Entra ID, the default enabled methods for SSPR typically include email, mobile phon e (SMS), mobile app code, and mobile app notification. Security questions may also be enabled but are less common due to security concerns.
If the administrator has disabled certain methods (e.g., mobile app code), the answer could change. However, the que stion does not indicate any such restrictions, so we assume the default methods are available.
The " Number of methods required to reset: 1 " setting means users only need to use one method to reset their password, but they may have multiple methods registered. The question asks for a " valid authentication method available to users, " so we need to identify a method that SSPR supports.
Conclusion:Based on the SSPR settings and the supported authentication methods in Microsoft Entra ID:
A mobile app cod e (option B) is a valid authentication method for SSPR, as it is supported by default and aligns with the configuration.
Smartcards, FIDO2 security tokens, and Windows Hello PIN are not supported for SSPR.Therefore, the correct answer isB.
References:
Micr osoft Entra ID documentation: " Self-service password reset authentication methods " (Microsoft Learn:
https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#authentication- methods) Microsoft Entra ID documentation: " Configure self-service password reset " (Microsoft Learn:https://learn.
microsoft.com/en-us/entra/identity/authentication/howto-sspr-deployment) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers SSPR configuration and supported authe ntication methods.

NEW QUESTION: 56
You have a Microsoft Entra tenant that contains the users shown in the following table:

Name	User type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1 is the owner of Group1.
You create an access review that has the following settings:
What to review: Teams + Groups
Scope: All users
Group: Group1
Reviewers: Users review their own access
Which users can perform access reviews for User3?
A. User1 only

B. User3 only
C. User1 and User2 only
D. User1, User2, and User3
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on the Microsoft Entra access review settings and the principles outlined in Microsoft Identity and Access Administrator documentation.
Understanding the Access Review Settings:
What to review: Teams + GroupsThis indicates that the access review is evaluating memberships in Teams and Groups within the Microsoft Entra tenant. Since the group specified is Group1, the review focuses on Group1 membership.
Scope: All usersThe scope defines who is being reviewed. "All users" in this

NEW QUESTION: 57
You have an Azure subscription that contains an Azure Automation account named Automation1.
You need to grant Automation1 access to Azure resources. The solution must meet the following requirements:
* Ensure that any permissions granted to Automation1 are removed when the account is deleted.
* Minimize administrative effort.
What should you use?
A. a certificate
B. a client secret
C. a user-assigned managed identity
D. a system-assigned managed identity
Answer: D (LEAVE A REPLY)

NEW QUESTION: 58
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.
The users have the devices shown in the following table.
You create the following two Conditional Access policies:
* Name: CAPolicy1
* Assignments
o Users or workload identities: Group 1
o Cloud apps or actions: Office 365 SharePoint Online
o Conditions
#Fil ter for devices: Exclude filtered devices from the policy
#Rule syntax: device.displayName -starts With " Device* "
o Access controls
#Grant: Block access
#Session: 0 controls selected
o Enable policy: On
* Name: CAPolicy2
* Assignments
o Users or workload identities: Group2

o Cloud apps or actions: Office 365 SharePoint Online
o Conditions: 0 conditions selected
* Access controls
o Grant: Grant access
#Require multifactor authentication
o Session:
0 controls selected
* Enable policy: On
All users confirm th at they can successfully authenticate using MFA.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access Site1 from Device1.	○	○
User2 can access Site1 from Device2.	○	○
User3 can access Site1 from Device3.	○	○

Answer:

Answer Area

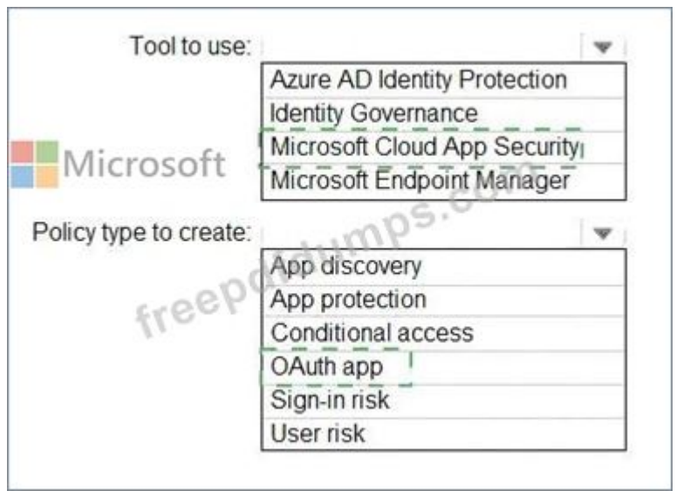
Statements	Yes	No
User1 can access Site1 from Device1.	○	○
User2 can access Site1 from Device2.	○	○
User3 can access Site1 from Device3.	○	○

Explanation:

NEW QUESTION: 59
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. You need to be notified if a user downloads more than 50 files in one minute from Site1.
Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?
A. session policy
B. anomaly detection policy
C. activity policy
D. file policy
Answer: C (LEAVE A REPLY)
To detect and get alerts when a user downloads a large number of files in a short period of time (for example, more than 50 files within one minute) in Microsoft SharePoint Online, you must configure an Activity policy in Microsoft Defender for Cloud Apps (MCAS).
* Activity policies monitor specific user actions (upload, download, delete, share, etc.) and can trigger alerts based on thresholds or frequency.
* Anomaly detection policies detect behavioral anomalies automatically (not threshold-based).
* Session policies apply real-time controls during sessions (e.g., block download).
* File policies monitor or classify files at rest.
From Microsoft's documentation:
"Activity policies let you monitor specific activities in your cloud apps and define actions or alerts when certain criteria are met, such as excessive downloads or mass deletions." Thus, for detecting a user who downloads more than 50 files in one minute - an Activity policy is required.

NEW QUESTION: 60
You have a Microsoft 365 tenant.
Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure Active Directory (Azure AD).
You need to receive an alert if a registered application gains read and write access to the users' email.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

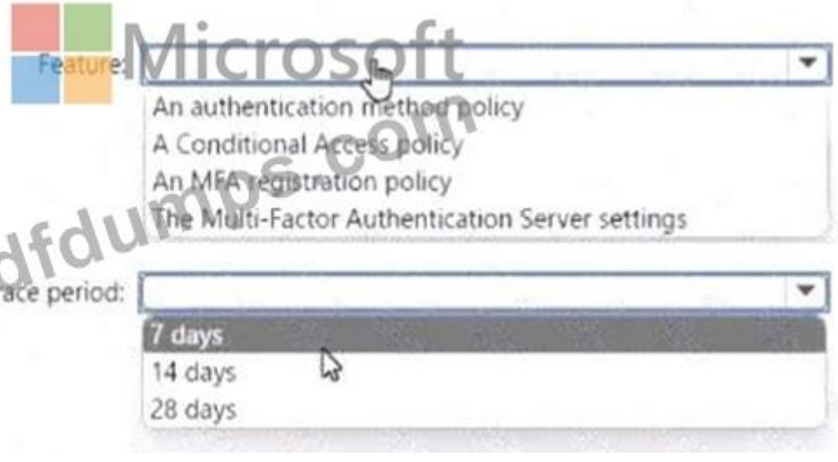


Explanation:

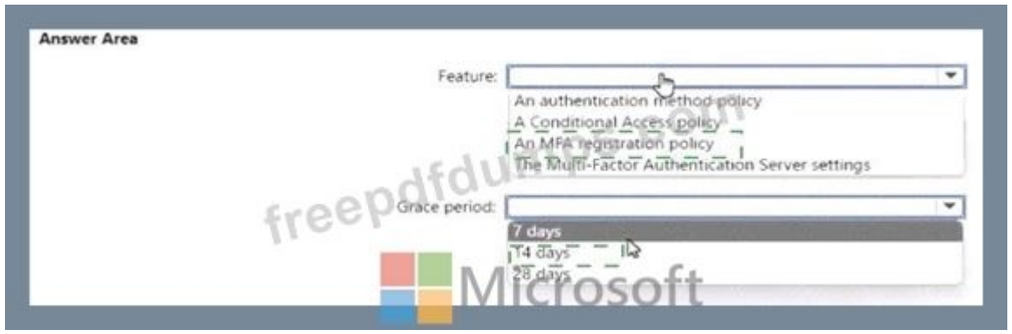
In the SC-300 curriculum, monitoring consented third-party apps is covered under Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security). The exam materials describe creating policies that watch OAuth-based applications users authorize against Azure AD and flag excessive permissions. The relevant guidance explains that you can configure a policy to alert when "an OAuth application is granted high-impact permissions," for example when a newly registered or consented app gains read and write access to mail (the Mail.ReadWrite permission). By contrast, Azure AD Identity Protection is focused on User risk and Sign-in risk policies for account compromise, not app consent. Identity Governance addresses access

packages and reviews, not OAuth permissions. Microsoft Endpoint Manager "app protection" policies are for MAM/MDM on client apps and do not monitor OAuth consent to Microsoft 365 data. The study path emphasizes using Defender for Cloud Apps to "detect and govern OAuth apps and their permissions," and to trigger alerts when scopes indicating data-write capability are granted. Therefore, to be notified if a user- registered app obtains read/write access to users' email, you configure an OAuth app policy in Microsoft Cloud App Security that matches the permission scope and raises an alert when detected.

NEW QUESTION: 61
You need to support the planned changes and meet the technical requirements for MFA.
Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area



Answer:



Explanation:
Feature: An MFA registration policy
Grace period: 14 days
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and Microsoft Learn documentation under "Plan, implem ent, and manage multifactor authentication (MFA)" , when an organization wants to require users to register for multi-factor authentication methods (such as Microsoft Authenticator, phone number, or email), this is managed through the MFA registration policy within Azure AD Identity Protection.
This feature is called "Combined security information registration" or MFA registration policy, and it allows administrators to enforce users to register for MFA and Self-Service Password Reset (SSPR). The policy defines which users are required to register and sets a grace period - the amount of time a user can postpone registration after first being prompted.
From the Microsoft official exam reference:
"The MFA registration policy allows users to postpone registration for a defined grace period. The default and maximum supported value is 14 days." During the grace period, users can skip the registration prompt but will be reminded every time they sign in until they complete registration or the grace period expires. Once the 14-day period ends, users must register their authentication methods before accessing resources.

Therefore, based on Microsoft's SC-300 study materials and Azure AD documentation:
* The correct feature used to enforce this is An MFA registration policy.
* The standard and maximum grace period before users must complete registration is 14 days.

NEW QUESTION: 62
Note: This question is part of a series of questi ons 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 q uestion 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 Active Directory (Azure AD) tenant that syncs to an Active Directory forest.
You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.
You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.
Solution: You configure pass-through authentication.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
Implementing Pass-through Authentication (PTA) ensures that Azure AD delegates the authentication process directly to the on-premises Active Directory in real-time. When a user signs in, Azure AD routes the authentication request through a secure channel to the on-premises Authentication Agent, which verifies credentials against AD.
If a user account is disabled in Active Directory, authentication immediately fails because the request is validated directly against the on-premises domain controllers - there's no delay or dependency on synchronization intervals.
From Microsoft documentation (SC-300 official guide):
"Pass-through Authentication provides real-time authentication directly against on-premises Active Directory.
If an account is disabled on-premises, authentication requests are denied immediately." Thus, enabling PTA satisfies the requirement for immediate blocking of disabled accounts.
Correct Answer: A. Yes

NEW QUESTION: 63
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."

NEW QUESTION: 64

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.

You need to configure the users as shown in the following table.

User	Configuration
User1	• User administrator role • Device Administrators role • Identity Governance Administrator role
User2	• Records Management role • Quarantine Administrator role group
User3	• Endpoint Security Manager role • Intune Role Administrator role

Which portal should you use to configure each user? To answer, drag the appropriate portals to t he correct users. Each portal 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.

Portals

- Azure Active Directory admin center
- Exchange admin center
- Microsoft 365 compliance center
- Microsoft Endpoint Manager admin center
- SharePoint admin center

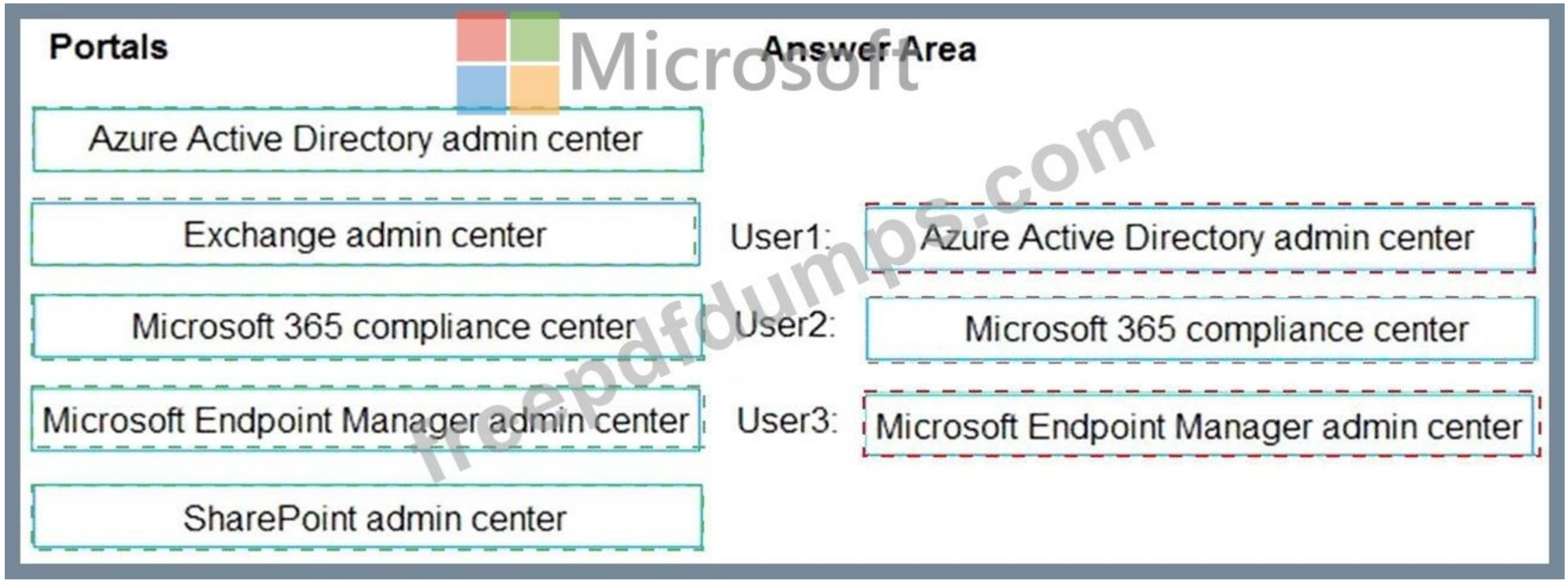
Answer Area

User1:

User2:

User3:

Answer:



Explanation:

User

Portal to Use

User1

Azure Active Directory admin center

User2

Microsoft 365 compliance center

User3

Microsoft Endpoint Manager admin center

This question tests your knowledge of Microsoft 365 administrative roles and their associated management portals, as defined in the Microsoft Identity and Access Administrator (SC-300) Exam Study Guide and Microsoft Learn's "Manage identity and access in Microsoft Entra ID and Microsoft 365" module.

Let's analyze each user and the roles assigned:

* Roles:
* User Administrator
* Device Administrator
* Identity Governance Administrator

User1 These are all Azure AD-based roles.

* The User Administrator role allows the management of users, groups, and password resets in Azure AD.
* The Device Administrator role applies to Azure AD joined devices.
* The Identity Governance Administrator manages Access Reviews, Entitlement Management, and Terms of Use, all of which are under Azure AD Identity Governance.

According to Microsoft documentation:

"User, Device, and Identity Governance Admin istrators perform their management tasks in the Azure Active Directory admin center." Portal: Azure Active Directory admin center
* Roles:
* Records Management
* Quarantine Administrator
User2 These are Microsoft Purview compliance roles, used for managing retention policies, data lifecycle management, and quarantine of messages/files.
Both are managed through the Microsoft 365 compliance center (previously known as the Security & Compliance Center). Microsoft documentation:
"Records Management and Quarantine A dministrator roles allow access to compliance features such as data retention, auditing, and message quarantine, all of which are configured from the Microsoft 365 compliance center." Portal: Microsoft 365 compliance center
* Roles:
* Endpoint Security Manager
* Intune Role Administrator
User3 These roles are directly tied to Microsoft Endpoint Manager (Intune).
* The Endpoint Security Manager configures device compliance, security baselines, and endpoint protection.
* The Intune Role Administrator manages Intune roles and permissions.
Microsoft documentation:
"Administrators managing Intune roles and endpoint security policies use the Microsoft Endpoint Manager admin center (https://endpoint.microsoft.com)." Portal: Microsoft Endpoint Manager admin center

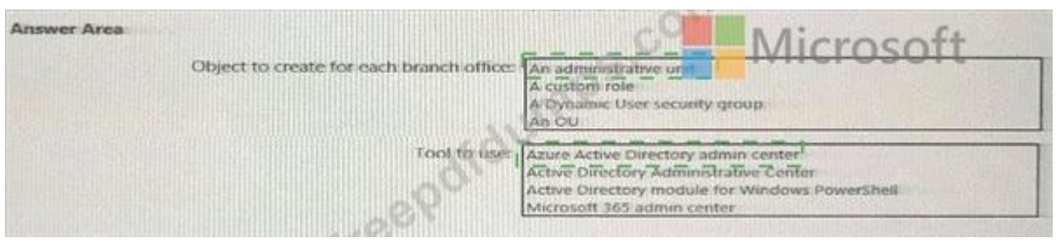
NEW QUESTION: 65
You have an Azure Active Directory (Azure AD) tenant.
You open the risk detections report.
Which risk detection type is classified as a user risk?
A. impossible travel
B. anonymous IP address
C. atypical travel
D. leaked credentials
Answer: (SHOW ANSWER)
SC-300 distinguishes user risk from sign-in risk. The text defines: "User risk is the probability that an identity is compromised," and lists its core detections, including " Leaked credentials detected on public or dark-web sources." By comparison, impossible/anomalous travel and anonymous IP are cited as sign-in risk detections:
"Sign-in r isk is calculated per authentication event using detections such as impossible travel, atypical travel, and anonymous IP address ." Therefore, among the options, only leaked credentials is a user risk detection type; the others are sign-in risk indicators used at authentication time. SC-300 also ties user risk to Identity Protection policies that can require password change or block access when a user's credentials are suspected to be compromised.

NEW QUESTION: 66
You have an Azure subscription that contains a user named User1. You need to meet the following requirements:
* Prevent User1 from being added as an owner of newly registered apps.
* Ensure that User1 can manage the application proxy settings.
* Ensure that User2 can register apps.
* Use the principle of least privilege.
Which role should you assign to User1?
A. Application developer

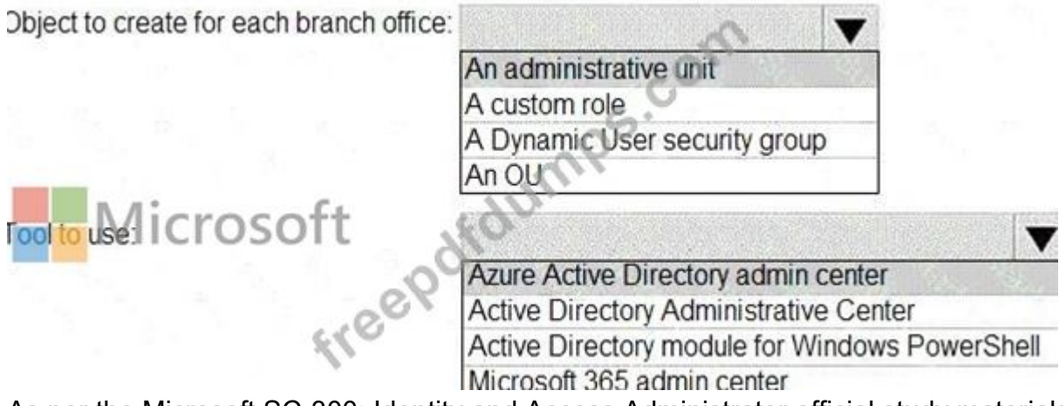
B. Cloud application administrator
C. Service support administrator
D. Application administrator
Answer: B (LEAVE A REPLY)
According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and Microsoft Learn documentation on Azure AD roles and permissions , the Cloud Application Administrator role provides privileges to manage applications while enforcing the principle of least privilege.
The scenario requires:
* Preventing User1 from being added as an owner of newly registered apps.
* Allowing User1 to manage Application Proxy settings (used for publishing on-premises apps through Azure AD).
* Allowing User2 to register new applications.
* Application Administrator: Can create and manage all app registrations and enterprise apps, and can add owners - too permissive for this requirement.
* Cloud Application Administrator: Can manage applications, including Application Proxy settings, but cannot assign application owners or grant broad permissions.
* Application Developer: Can only register and manage own applications.
* Service Support Administrator: Provides service health access - not relevant here.
Role Comparison (from Microsoft documentation): Thus, to let User1 manage Application Proxy and prevent assigning ownership of new apps, Cloud Application Administrator is the correct and least-privileged choice.

NEW QUESTION: 67
You need to meet the technical requirements for license management by the helpdesk administrators.
What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:



Explanation:



As per the Microsoft SC-300: Identity and Access Administrator official study materials and Microsoft Learn documentation on "Manage administrative units in Azure Active Directory" , Administrative Units (AUs) are designed to delegate administrative permissions within large organizations based on divisions such as geography or department. They provide scoped administrative control -allowing helpdesk or user administrators to manage users only within a specific subset of the directory, such as a branch office or department.

In this scenario, Contoso's technical requirement states:

"The helpdesk administrators must be able to manage licenses for only the users in their respective office." To fulfill this, you must create an administrative unit for each branch office (e.g., Montreal, London, Seattle) and assign helpdesk administrators scoped to those AUs. This ensures that each helpdesk admin can only manage licenses for the users within their respective office, enforcing the principle of least privilege.

The Azure Active Directory admin center is the correct tool for creating and managing administrative units.

SC-300 guidance clarifies that administrative units are Azure AD objects , not on-premises Active Directory objects like Organizational Units (OUs). Therefore, they are created and managed exclusively through the Azure portal , Microsoft Graph , or PowerShell for Azure AD , but the most straightforward interface for exam purposes is the Azure AD admin center .

NEW QUESTION: 68

You have an azure subscription that contains a resource group named RG1, RG1 contains tw o virtual machines named VM1 and VM2 that have Microsoft intra ID login enabled.

The subscription contains the users shown in the following, table.

Name	Role	Role scope
User1	Virtual Machine User Login	Subscription
User2	Virtual Machine Contributor	RG1
User3	Virtual Machine Administrator Login	VM1

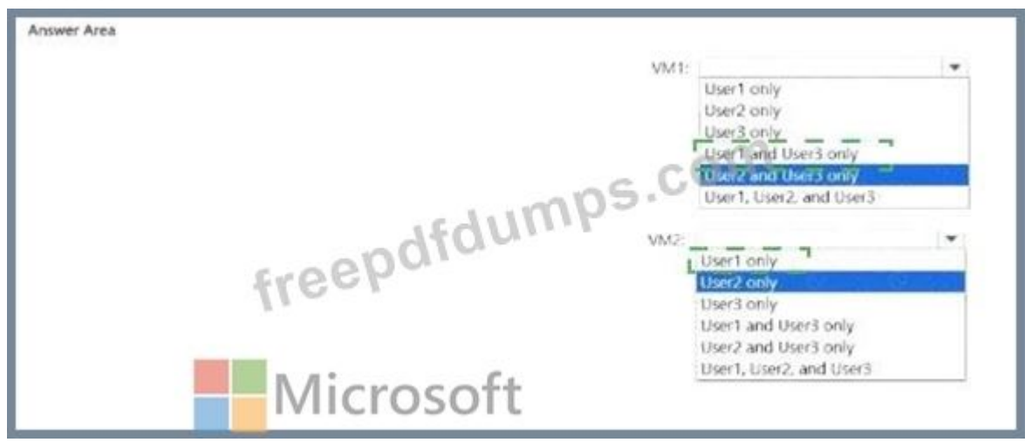
Which users can sign in to VM1. and which users can sign in to VM?? To answer, select the appropriate opti ons in the answer area. NOTE:

Each correct selection is worth one point.

Which users can sign in to VM1, and which users can sign in to VM2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:

In Microsoft Entra ID-based sign-in to Azure VMs, the right to sign in is granted by the Azure RBAC data- plane roles Virtual Machine User Login and Virtual Machine Administrator Login . The SC-300 study materials state that these roles are "used to log in to a virtual machine with Azure AD credentials" and that scope inheritance applies: "RBAC permissions assigned at a hi gher scope (subscription, resource group) flow down to child resources." The guidance further clarifies the difference: "Virtual Machine User Login allows standard user login" while "Virtual Machine Administrator Login allows administrator login." By contr ast, management roles such as Virtual Machine Contributor "manage virtual machines but do not grant sign-in rights." Applying this to the scenario: User1 has Virtual Machine User Login at the subscription scope , therefore the permission is inherited by RG1 , VM1 , and VM2 , allowing User1 to sign in to both VMs. User3 holds Virtual Machine Administrator Login scoped to VM1 , which authorizes sign-in only to VM1 (administrator level) and does not apply to VM2. User2 has Virtual Machine Contributor at RG1 ; this provides management capabilities (start/stop, configure) but no sign-in permission, so User2 cannot sign in to either VM.
Therefore, the correct selections are VM1: User1 and User3 only and VM2: User1 only .

NEW QUESTION: 69

You have a Microsoft 365 E5 subscription.

You deploy a third-party web gateway named Gateway1.

You need to integrate Gateway1 with Microsoft Defender for Cloud Apps. The solution must meet the following requirements:

Ensure that data flows automatically to Defender for Cloud Apps.
Minimize administrative effort.
What should you do first?
A. Add a data source
B. Create an app registration
C. Create a snapshot report
D. Add a log collector
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Microsoft Defender for Cloud Apps (MDCA)integration with third-party web gateways, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding the Scenario and Requirements:
Microsoft 365 E5 subscription:This subsc ription includes Microsoft Defender for Cloud Apps, which provides the necessary licensing for integrating with third-party web gateways.
Third-party web gateway named Gateway1:A web gateway (e.g., a Secure Web Gateway like Zscaler, Netskope, or Symantec) is deployed to manage and secure internet traffic. The question does not specify the vendor, but the process for integration with MDCA is generally the same for supported gateways.
Requirement:Integrate Gateway1 with Microsoft Defender for Cloud Apps to en sure that data (e.g., traffic logs, events) flows automatically to MDCA for analysis, visibility, and policy enforcement. The solution must also minimize administrative effort.
Microsoft Defender for Cloud Apps supports integration with third-party web gat eways to provide visibility into cloud app usage, detect shadow IT, and enforce security policies. This integration typically involves collecting logs from the gateway for analysis in MDCA.
How Microsoft Defender for Cloud Apps Integrates with Third-Party Web Gateways:
MDCA can integrate with third-party web gateways by collecting logs that contain traffic data (e.g., user activity, app usage, IP addresses). This allows MDCA to analyze the data and provide insights into cloud app usage, detect threats, and enforce policies.
The primary method for integrating a third-party web gateway with MDCA is toadd a log collector. This involves:
Configuring the web gateway to send logs to a log collector (e.g., via Syslog or FTP).
Setting up a log collector in MDCA to r eceive and process these logs.
Once configured, the log collector automatically pulls logs from the web gateway, ensuring that data flows to MDCA for analysis.
This method supports automatic data flow and minimizes administrative effort because, after the initial setup, the log collection process runs continuously without manual intervention.
Analyzing the Options:
A). Add a data source:
In Microsoft Defender for Cloud Apps, " data sources " typically refer to sources of user activity data, such as Microsoft E ntra ID audit logs, Microsoft 365 audit logs, or other Microsoft services. Adding a data source in MDCA is used to import user activity data for correlation with cloud app usage, but it is not the mechanism for integrating a third-party web gateway.
Third- party web gateways are not considered " data sources " in MDCA; instead, they are integrated via log collectors.
Conclusion:This option is incorrect because adding a data source does not facilitate integration with a third- party web gateway like Gateway1.
B). Create an app registration:
Creating an app registration in Microsoft Entra ID is typically used to integrate cloud apps with MDCA for session control (e.g., via Conditional Access App Control) or to enable API-based logcollection for supported apps (e.g. , Salesforce, Box).
However, a third-party web gateway like Gateway1 is not a cloud app that requires an app registration. Web gateways are network appliances or services that manage traffic, and their integration with MDCA involves log collection, not app registration.
Conclusion:This option is incorrect because creating an app registration is not relevant to integrating a web gateway with MDCA.
C). Create a snapshot report:

A snapshot report in MDCA is a manual process where an administrator uploads a log file (e.g., a CSV or JSON file) from a third-party service to analyze cloud app usage. This is a one-time, manual process used for discovery (e.g., to identify shadow IT).
The requirement specifies that data must flow " automatically " to Defender for Cloud Apps, and a snapshot report does not meet this requirement because it requires manual uploads each time. It also does not minimize administrative effort due to the ongoing manual intervention.
Conclusion:This option is incorrect because creating a snapshot report does not enable automatic data flow and increases administrative effort.
D). Add a log collector:
Adding a log collector in Microsoft Defender for Cloud Apps is the standard method for integrating third- party web gateways. MDCA supports log collecti on from many web gateways (e.g., Zscaler, Netskope, Symantec) via Syslog or FTP.
Process:
In the Microsoft Defender for Cloud Apps portal, navigate toSettings > Log collectors.
Add a new log collector, specifying the protocol (e.g., Syslog over TCP/UDP or FTP) and the details of the web gateway (e.g., IP address, port).
Configure Gateway1 to send logs to the log collector (this step is done on the Gateway1 side, typically by the network team).
Once set up, the log collector automatically collects logs from Gateway1 and processes them in MDCA for analysis.
Automatic Data Flow:The log collector ensures that data flows automatically to MDCA, meeting the first requirement.
Minimize Administrative Effort:After the initial setup, the log collector runs continuousl y without manual intervention, minimizing administrative effort.
Conclusion:This option is correct because adding a log collector is the first step to integrate Gateway1 with MDCA, ensuring automatic data flow and minimizing administrative effort.
Why " Add a log collector " is the First Step:
The question asks for the first step to integrate Gateway1 with Microsoft Defender for Cloud Apps. Adding a log collector is the initial action in MDCA to enable log collection from a third-party web gateway.
Subsequent steps (not asked in the question) would include configuring Gateway1 to send logs to the log collector, but this is done outside MDCA (e.g., in Gateway1's management console). The question focuses on the action in MDCA, making " Add a log collector " the co rrect first step.
Additional Considerations:
The question does not specify the vendor of Gateway1, but Microsoft Defender for Cloud Apps supports log collection from many third-party web gateways (e.g., Zscaler, Netskope, Symantec, Cisco Umbrella). The process is the same regardless of the vendor, as long as the gateway supports Syslog or FTP log export.
If Gateway1 were not a supported web gateway, additional steps (e.g., custom log parsing) might be required, but the question implies Gateway1 can be in tegrated using standard methods.
The Microsoft 365 E5 subscription includes Microsoft Defender for Cloud Apps, so no additional licensing is required.
Conclusion:To integrate Gateway1 with Microsoft Defender for Cloud Apps, ensuring that data flows automat ically and minimizing administrative effort, the first step is toadd a log collectorin MDCA. This sets up the infrastructure to receive logs from Gateway1, enabling automatic data flow for analysis. Therefore, the correct answer isD.
References:
Microsoft Defender for Cloud Apps documentation: " Integrate with a third-party web gateway " (Microsoft Learn:https://learn.microsoft.com/en-us/defender-cloud-apps/connect-third-party-gateway) Microsoft Defender for Cloud Apps documentation: " Set up a log collector " (Microsoft Learn:https://learn.
microsoft.com/en-us/defender-cloud-apps/log-collector)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers integrating Microsoft Defender for Cloud Apps with third-party services for cloud app visibility and control.

NEW QUESTION: 70
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant- Users sign in to computers that run Windows 10 and are joined to the domain.
You plan to implement Azure AD Seamless Single Sign-O n (Azure AD Seamless SSO).
You need to configure the computers for Azure AD Seamless SSO.

What should you do?
A. Enable Enterprise State Roaming.
B. Configure Sign-in options.
C. Install the Azure AD Connect Authentication Agent.
D. Modify the Intranet Zone settings.
Answer: D (LEAVE A REPLY)
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Microsoft Learn module "Plan and implement Azure AD Seamless Single Sign-On (SSO)", Azure AD Seamless SSO allows domain-joined Windows devices (that are not necessarily Azure AD-joined) to automatically sign in to Azure AD without requiring users to re-enter their credentials.
How Azure AD Seamless SSO Works: When a user tries to access an Azure AD-integrated application (like Microsoft 365, Teams, or SharePoint Online), Azure AD redirects the authentication request to the on- premises Active Directory. The Seamless SSO feature uses a computer account (AZUREADSSOACC) created in Active Directory to authenticate users through Kerberos tickets automatically.
For the Kerberos-based SSO to work properly in a browser or client, the service principal name (SPN) used by Azure AD must be treated as a trusted intranet site. This ensures that Integrated Windows Authentication (IWA) can pass the user's Kerberos ticket automatically - without prompting for credentials.
Configuration Required on Windows 10 Devices: To enable automatic SSO without credential prompts, you must:
* Add the following URLs to the Intranet Zone in Internet Explorer or Microsoft Edge (and by extension, Windows Authentication settings):
* https: //autologon.microsoftazuread-sso.com
* https: //aadg.windows.net.nsatc.net
* Ensure Automatic logon with current user name and password is enabled for the Intranet Zone.
From Microsoft Documentation: "For Azure AD Seamless SSO to work, the client machines must be on the corporate network and the URLs 'https://autologon.microsoftazuread-sso.com' and 'https://aadg.windows.net.
nsatc.net' must be added to the users ' Intranet zone settings."
Other options are not correct because:
* A. Enable Enterprise State Roaming - Manages user settings across devices, unrelated to SSO.
* B. Configure Sign-in options - User-level authentication preferences, not required for Seamless SSO.
* C. Install Azure AD Connect Authentication Agent - Used for Pass-through Authentication (PTA), not for Seamless SSO.

NEW QUESTION: 71
You have a Microsoft 365 E5 subscription.
You need to create a Microsoft Defender for Cloud Apps session policy.
What should you do first?
A. From the Microsoft Defender for Cloud Apps portal, select User monitoring.
B. From the Microsoft Defender for Cloud Apps portal, select App onboarding/maintenance
C. From the Azure Active Directory admin center, create a Conditional Access policy.
D. From the Microsoft Defender for Cloud Apps porta l, create a continuous report.
Answer: C (LEAVE A REPLY)
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide , Exam Ref SC-300
, and Microsoft Defender for Cloud Apps (MDCA) documentation , a session policy in Defender for Cloud Apps (formerly Microsoft Cloud App Security) is used to monitor and control user sessions in real time. These policies provide granular session-level access controls such as limiting downloads, blocking uploads, or monitoring user activity in SaaS applications integrated with Defender for Cloud Apps.

However, before a session policy can function, the Conditional Access App Control feature must be enabled. This integration connects Azure Active Directory (Azure AD) with Microsoft Defender for Cloud Apps , allowing session c ontrol to be enforced through Conditional Access policies .
The SC-300 official training content under "Implement and configure Microsoft Defender for Cloud Apps" states:
"To apply session controls using Microsoft Defender for Cloud Apps, you must first configure a Conditional Access policy in Azure AD that routes user sessions to Defender for Cloud Apps for inspection. Only after this step can you define a session policy within the Defender for Cloud Apps portal." Thus, the correct first step is to creat e a Conditional Access policy in Azure AD that uses the Use Conditional Access App Control option. This action establishes the required connection path so that session control policies in Defender for Cloud Apps can take effect.

NEW QUESTION: 72
You have the Azure resources show in the following table.

Name	Description
User1	User account
Group1	Security group that uses the Dynamic user membership type
VM1	Virtual machine with a system-assigned managed identity
App1	Enterprise application
RG1	Resource group

To Which identities can you assign the Contributor role for RG1?
A. User1 only
B. User1 and Group1 only
C. User1 and VW1 only
D. User1, VM1, and App1 only
E. User1, Group1, Vm1, and App1
Answer: E (LEAVE A REPLY)
Azure RBAC roles on a scope (subscription, resource group, resource) can be assigned to Azure AD security principals: users , groups , and service principals (which includes enterprise applications and managed identities). The SC-300 content states: "RBAC roles can be assigned to users, groups, and applications (service principals), including system-assigned managed identities created for Azure resources." In the table, User1 (user), Group1 (security group), VM1 (a VM with system-assigned managed identity), and App1 (an enterprise application service principal) are all valid principals. Therefore, all four can be assigned the Contributor role at the RG1 scope. This enables least-privilege delegation to workloads (VM1/App1) and to people (User1/Group1) without granting broader directory roles.

NEW QUESTION: 73
You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Group
User1	Group1
User2	Group1
User3	Group2
User4	Group2
User5	None

You have an administrative unit named Au1.Group1, User2, and User3are members of Au1.
User5 is assigned the User Administrator role for Au1.
For which users can User5 reset passwords?
A. User1 and User2 only
B. User2 and User3 only

C. User3 and User4 only
D. User1, User2, and User3
Answer: B (LEAVE A REPLY)
Per Microsoft SC-300: Manage administrative units and delegated roles , administrative units (AUs) allow scoping of administrative privileges to subsets of users or groups within a tenant.
In this case, User5 is assigned the User Administrator role for AU1. This means User5 can only manage users and groups that are members of AU1. From the given table, Group1, User2, and User3 are part of AU1.
Therefore, User5 can reset passwords for users who are either:
* Members of AU1 directly (User2, User3), or
* Members of groups that belong to AU1, if those groups' members fall under delegated scope.
However, User1 and User4 are not part of AU1, and User5 has no administrative control over them.

NEW QUESTION: 74
You have a Microsoft Entra tenant named contoso.com that contains a user named User1. User1 has the devices shown in the following table.

Name	Platform	Registered in contoso.com
Device1	Windows 11	Yes
Device2	Windows 11	No
Device3	iOS	Yes

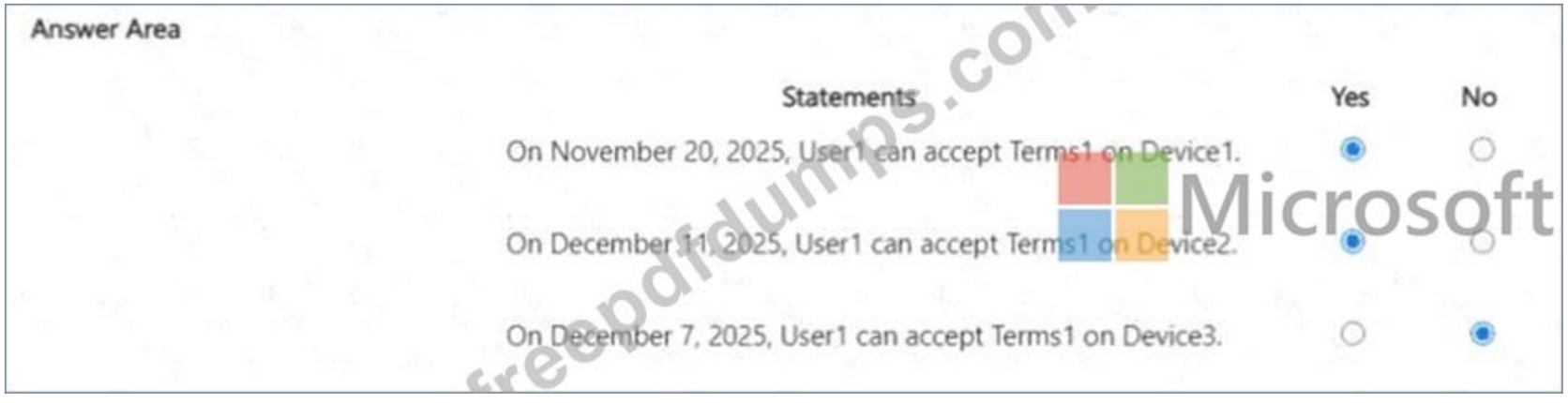
On November 5. 2025, you create and enforce terms of use in contoso.com that has the following settings:
* Name: Terms 1
* Display name: Contoso terms of use
* Require users to expand the terms of use: On
* Require users to consent on every device: On
* Expire consents: On
* Expire starting on: December 10,2025
* Frequency: Monthly
On November 15, 2025, User1 accepts Terms1 on Device3.
On November 15,2025, User1 accepts Terms1 on Device3.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE Each correct selection is worth one point.

Answer:

Answer Area

Statements	Yes	No
On November 20, 2025, User1 can accept Terms1 on Device1.	◉	○
On December 11, 2025, User1 can accept Terms1 on Device2.	◉	○
On December 7, 2025, User1 can accept Terms1 on Device3.	○	◉

Explanation:



NEW QUESTION: 75
You have a Microsoft 365 ES subscription that contains a user named User1. User1 is eligible for the Application a dministrator role.
User1 needs to configure a new connector group for an application proxy.
What should you to activate the role for User1?
A. the Microsoft Defender for Cloud Apps portal
B. the Microsoft 365 admin center
C. the Azure Active Directory admin center
D. the Microsoft 365 Defender portal
Answer: C (LEAVE A REPLY)
User1 is eligible for the Application Administrator role and needs to configure an Application Proxy connector group. Application Proxy is an Azure AD feature used to publish on-premises applications securely.
To activate the eligible role, User1 must perform a Privileged Identity Management (PIM) activation within the Azure AD admin center.
From Microsoft Documentation:
"Privileged Identity Management (PIM) role activations are performed in the Azure AD admin center under Azure AD # Privileged Identity Management # My roles." Activation steps are not available through Microsoft 365 or Defender portals.

NEW QUESTION: 76
Task 6
You need to implement additional security checks before the members of the Sg-Executive can access any company apps. The members must meet one of the following conditions:
* Connect by using a device that is marked as compliant by Microsoft Intune.

* Connect by using client apps that are protected by app protection policies.

Answer:

See the Explanation for the complete step by step solution.

Explanation:

To implement additional security checks for the Sg-Executive group members before they can access any company apps, you can use Conditional Access policies in Microsoft Entra.

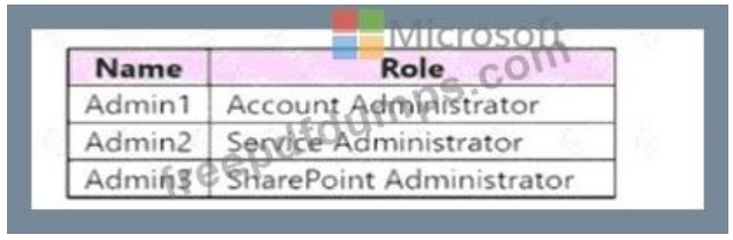
Here's a step-by-step guide:

* Sign in to the Microsoft Entra admin center:
* Ensure you have the role of Global Administrator or Security Administrator.
* Navigate to Conditional Access:
* Go to Security > Conditional Access.
* Create a new policy:
* Select + New policy.
* Name the policy appropriately, such as "Sg-Executive Security Checks".
* Assign the policy to the Sg-Executive group:
* Under Assignments, select Users and groups.
* Choose Select users and groups and then Groups.
* Search for and select the Sg-Executive group.
* Define the application control conditions:
* Under Cloud apps or actions, select All cloud apps to apply the policy to any company app.
* Set the device compliance requirement:
* Under Conditions > Device state, configure the policy to include devices marked as compliant by Microsoft Intune.
* Set the app protection policy requirement:
* Under Conditions > Client apps, configure the policy to include client apps that are protected by app protection policies.
* Configure the access controls:
* Under Access controls > Grant, select Grant access.
* Choose Require device to be marked as compliant and Require approved client app.
* Ensure that the option Require one of the selected controls is enabled.
* Enable the policy:
* Set Enable policy to On.
* Review and save the policy:
* Review all settings to ensure they meet the requirements.
* Click Create to save and implement the policy.

By following these steps, you will ensure that the Sg-Executive group members can only access company apps if they meet one of the specified conditions, either by using a compliant device or a protected client app.

This enhances the security posture of your organization by enforcing stricter access controls for executive- level users.

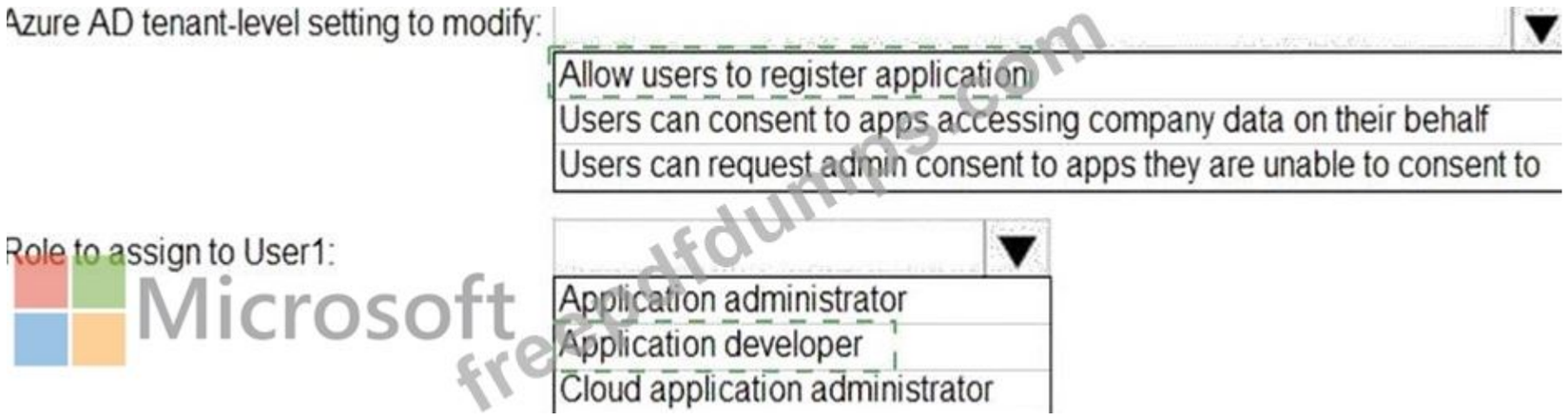
NEW QUESTION: 77
You have an Azure subscription that contains the users shown in the following table.



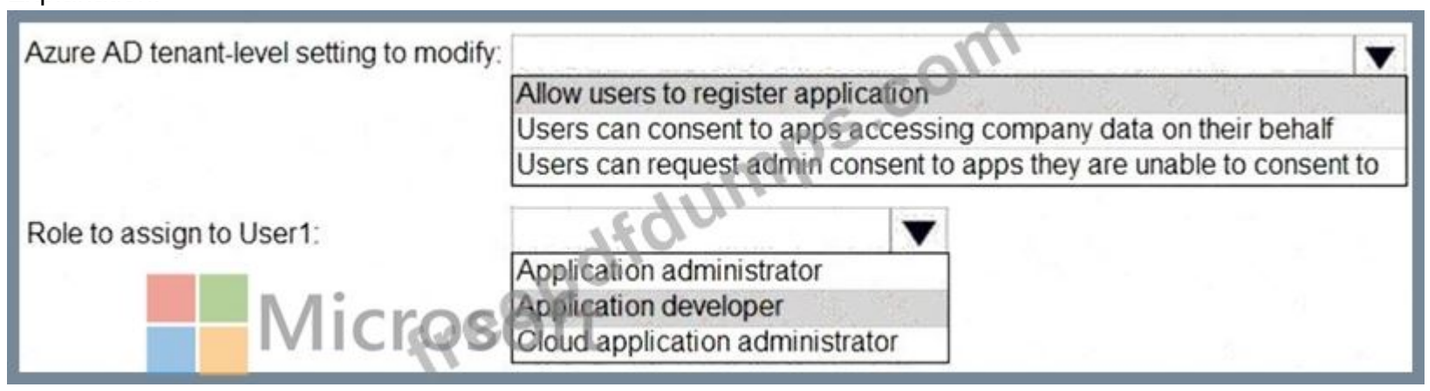
You need to implement Azure AD Privileged Identity Management (PIM).
Which users can use PIM to a ctivate their role permissions?
A. Admin! only
B. Admin2 only
C. Admin3 only
D. Admin1 and Admin2 only
E. Admin2 and Admin3 only
F. Admin1, Admin2, and Admin3
Answer: D (LEAVE A REPLY)
According to the Microsoft SC-300 official study guide and Microsoft documentation on Azure AD Privileged Identity Management (PIM), PIM is used to manage, control, and monitor access within Azure Active Directory (Azure AD), Azure resources, and Microsoft 365. However, not every administrative role within Azure or Microsoft 365 can be managed or activated through PIM.
To understand which administrators can use PIM, we need to review how Azure roles are structured:
* Account Administrator - This role is a classic subscription administrator role, not part of Azure AD role-based access control (RBAC). Therefore, it is not managed or activated through PIM.
* Service Administrator - Also a classic Azure subscription role, but it maps to the Owner role in Azure RBAC. PIM can manage and activate this role because it exists within the RBAC model, which PIM supports.
* SharePoint Administrator - This is an Azure AD directory role, not a classic subscription role, and is supported in Azure AD PIM. Azure AD PIM supports activation for directory roles such as Global Administrator, SharePoint Administrator, Exchange Administrator, etc.
From Microsoft's official documentation:
"Azure AD Privileged Identity Management can manage role assignments for both Azure AD directory roles and Azure resource roles (via Azure RBAC). Classic subscription administrator roles such as Account Administrator are not supported." Therefore, Admin1 (Account Administrator) cannot use PIM because their role is outside the scope of PIM.
Admin2 (Service Administrator) and Admin3 (SharePoint Administrator) can both use PIM since their roles are recognized by PIM as eligible for activation.

NEW QUESTION: 78
You need to configure app registration in Azure AD to meet the delegation requirements.
What should you do? To answer, select th e appropriate options in the answer area.
NOTE:Each correct selection is worth one point.

Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

NEW QUESTION: 79
You have a Microsoft Entra tenant that contains a group named Group1 and two users named User1 and User2. User1 is a member of Group1.
You register an enterprise application na med App1.
You enable self-service application access for App1 and configure the following settings:
Allow users to request access to this application: Yes
To which group should assigned users be added: Group1
Require approval before granting access to this application: Yes

Who is allowed to approve access to this application: User2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
User1 must request access to App1 before they can use the app.	○	○
If User2 requests access to App1, they will be added to Group1 automatically.	○	○
User2 can approve App1 requests by using the Microsoft Entra admin center.	○	○

Answer:

Statements	Yes	No
User1 must request access to App1 before they can use the app.	○	○
If User2 requests access to App1, they will be added to Group1 automatically.	○	○
User2 can approve App1 requests by using the Microsoft Entra admin center.	○	○

Explanation:

User1 must request access to App1 before they can use the app: No

If User2 requests access to App1, they will be added to Gro up1 automatically: Yes User2 can approve App1 requests by using the Microsoft Entra admin center: Yes Let's break this down step by step based on Microsoft Entra ID self-service application access and the configured settings, as outlined in Microsoft Iden tity and Access Administrator documentation.

Understanding Self-Service Application Access in Microsoft Entra ID:

Self-service application access in Microsoft Entra ID allows users to request access to applications without needing an administrator to manua lly assign them. This is configured on a per-application basis.

The settings for App1 are:

Allow users to request access to this application: Yes- Users can request access to App1.

To which group should assigned users be added: Group1- Users who are grante d access will be added to Group1, which provides the necessary permissions to use App1.

Require approval before granting access to this application: Yes- Access requests must be approved before the user is added to Group1.

Who is allowed to approve access to this application: User2- User2 is the designated approver for access requests to App1.

Statement 1: User1 must request access to App1 before they can use the app.

Analysis:

User1 is already a member of Group1, as stated in the question.
The self-service settings specify that users who are granted access to App1 will be added to Group1. This implies that membership in Group1 is what grants access to App1.
Since User1 is already a member of Group1, they already have access to App1. In Microsoft Entra ID, i f a user is already assigned to an application (either directly or via group membership), they do not need to request access through the self-service process-they can simply use the app.
The self-service access request process is for users who are not yet assigned to the app (i.e., not in Group1).
Since User1 is already in Group1, they do not need to request access.
Conclusion:This statement isNo. User1 does not need to request access because they are already a member of Group1 and can use App1 immediately.
Statement 2: If User2 requests access to App1, they will be added to Group1 automatically.
Analysis:
User2 is not a member of Group1 (the question does not state that User2 is in Group1).
The self-service settings allow users to request access to App1, an d the setting " To which group should assigned users be added: Group1 " means that users who are granted access will be added to Group1.
However, the setting " Require approval before granting access to this application: Yes " means that User2's request must be approved before they are added to Group1. The approver for App1 requests is User2 themselves, which introduces a potential conflict.
In Microsoft Entra ID, if a user is both the requester and the approver, the system typicallyallows them to approve thei r own request (unless additional policies prevent this, which is not specified in the question).
Therefore, User2 can request access and approve their own request.
Once the request is approved, User2 will be added to Group1 automatically as per the self-se rvice settings.
The term " automatically " in the statement refers to the process after approval-once approved, the addition to Group1 happens without further manual intervention.
Conclusion:This statement isYes. If User2 requests access to App1 and approves their own request, they will be added to Group1 automatically.
Statement 3: User2 can approve App1 requests by using the Microsoft Entra admin center.
Analysis:
The self-service settings specify that User2 is the designated approver for access requests to App1.
In Microsoft Entra ID, approvers can manage access requests through the Microsoft Entra admin center (via the " My Access " portal or the " Access Requests " section, depending on their role and permissions).
User2, as the designated approver, will rece ive a notification (via email or the My Access portal) when a request is made. They can then log into the Microsoft Entra admin center, navigate to the access requests section, and approve or deny the request.
Even though User2 is not explicitly an admin, the fact that they are designated as the approver for App1 requests grants them the ability to approve requests through the Microsoft Entra admin center.
Conclusion:This statement isYes. User2 can approve App1 requests using the Microsoft Entra admin cente r.
Additional Considerations:
If User2 were not allowed to approve their own request (e.g., due to a separation of duties policy), Statement
2 might be affected. However, Microsoft Entra ID does not enforce such a restriction by default, and the question d oes not specify any additional policies.
The Microsoft Entra admin center is the primary interface for managing access requests, but users can also approve requests via email links or the My Access portal. The statement specifically mentions the admin cent er, which is a valid method.
Conclusion:
Statement 1:No- User1 does not need to request access since they are already in Group1.
Statement 2:Yes- User2 will be added to Group1 automatically after their request is approved (by themselves).
Statement 3:Yes- User2 can approve requests using the Microsoft Entra admin center.
References:
Microsoft Entra ID documentation: " Configure self-service application access " (Microsoft Learn:

https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-self-se rvice) Microsoft Entra ID documentation: " Manage access requests " (Microsoft Learn:https://learn.microsoft.com
/en-us/entra/identity/governance/access-reviews-overview)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers self -service application access and approval workflows in Microsoft Entra ID.

NEW QUESTION: 80
You have a Microsoft Entra tenant that contains the devices shown in the following table.

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra registered
Device2	Windows 10	Microsoft Entra joined
Device3	Windows 10	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

You plan to configure Microsoft Entra Private Access. You deploy the Global Secure Access client to compatible devices. From which devices can you use Private Access?
A. Device1. Device2, Device3, and Device4
B. Device1 only
C. Device2 only
D. Device1. Device2. and Device3 only
E. Device2 and Device4 only
Answer: (SHOW ANSWER)

NEW QUESTION: 81
You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.
You have two Azure AD roles that have the Activation settings shown in the following table.

Name	Required justification on activation	Require approval to activate	Approvers
Role1	No	Yes	User1
Role2	Yes	No	None

The Azure AD roles have the Assignment settings shown in the following table.

Role	Allow permanent eligible assignment	Allow Permanent activate assignment	Require justification on active assignment
Role1	Yes	Yes	Yes
Role2	No	Yes	Yes

The Azure AD roles have the el igible users shown in the following table.

Role	Eligible assignment
Role1	User1, User2
Role2	User3

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

Answer:

Explanation:

Statement

Yes / No

If User1 requests Role1, the request will be approved automatically.

No

User1 can approve the request of User3 for Role2.

No

User1 must provide justification to approve the request of User2 for Role1.

Yes

According to the Microsoft SC-300 study guide, Exam Ref SC-300, and Microsoft Entra Privileged Identity Management (PIM) documentation, role activation and assignment settings in Azure AD PIM determine who can activate roles, who can approve activations, and whether justification is required. Let's analyze each configuration step-by-step.

Role1 Configuration Summary Setting

Value

Required justification on activation

No

Require approval to activate

Yes

Approvers

User1

Allow permanent eligible assignment

Yes

Allow permanent active assignment

Yes

Require justification on active assignment
Yes
Eligible Assignments: User1, User2
Role2 Configuration Summary Setting
Value
Required justification on activation
Yes
Require approval to activate
No
Approvers
None
Allow permanent eligible assignment
No
Allow permanent active assignment
Yes
Require justification on active assignment
Yes
Eligible Assignments: User3
Statement 1: "If User1 requests Role1, the request will be approved automatically."
* Role1 requires approval to activate.
* The approver is User1, but a user cannot self-approve their own request in Azure AD PIM.
* Therefore, even though User1 is listed as an approver, the system does not automatically approve self- requests.
# Answer: No
Statement 2: "User1 can approve the request of User3 for Role2."
* Role2 does not require approval to activate (approval = No).
* User3 is the only eligible member for Role2 and can activate it directly.
* Hence, no approval action exists for User1.
# Answer: No
Statement 3: "User1 must provide justification to approve the request of User2 for Role1."
* Role1 requires approval to activate, and User1 is the approver.
* The assignment settings for Role1 state: Require justification on active assignment = Yes.
* This means when approving or activating, the approver (User1) must enter a justification before approval.
# Answer: Yes

NEW QUESTION: 82
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs user accounts with a Microsoft 365 E5 subscription. You need to ensure that on-premises account lockout policies are applied to Microsoft Entra sign-ins. What should you configure?
A. Microsoft Entra Cloud Sync
B. Microsoft Entra Seamless Single Sign-on (Microsoft Entra Seamless SSO)
C. password hash synchronization
D. pass-through authentication

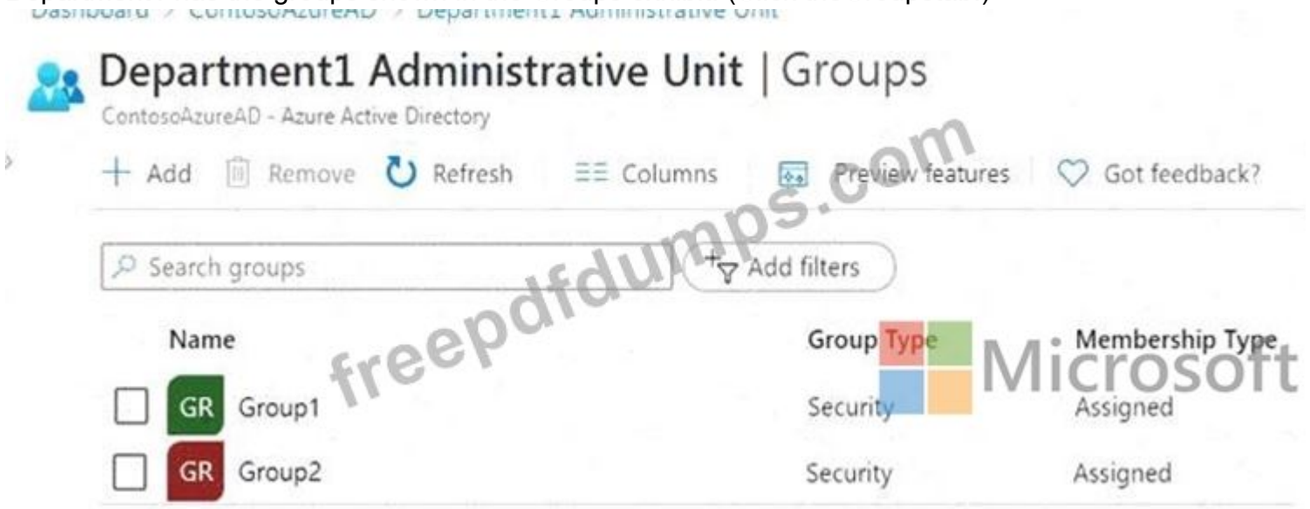
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83

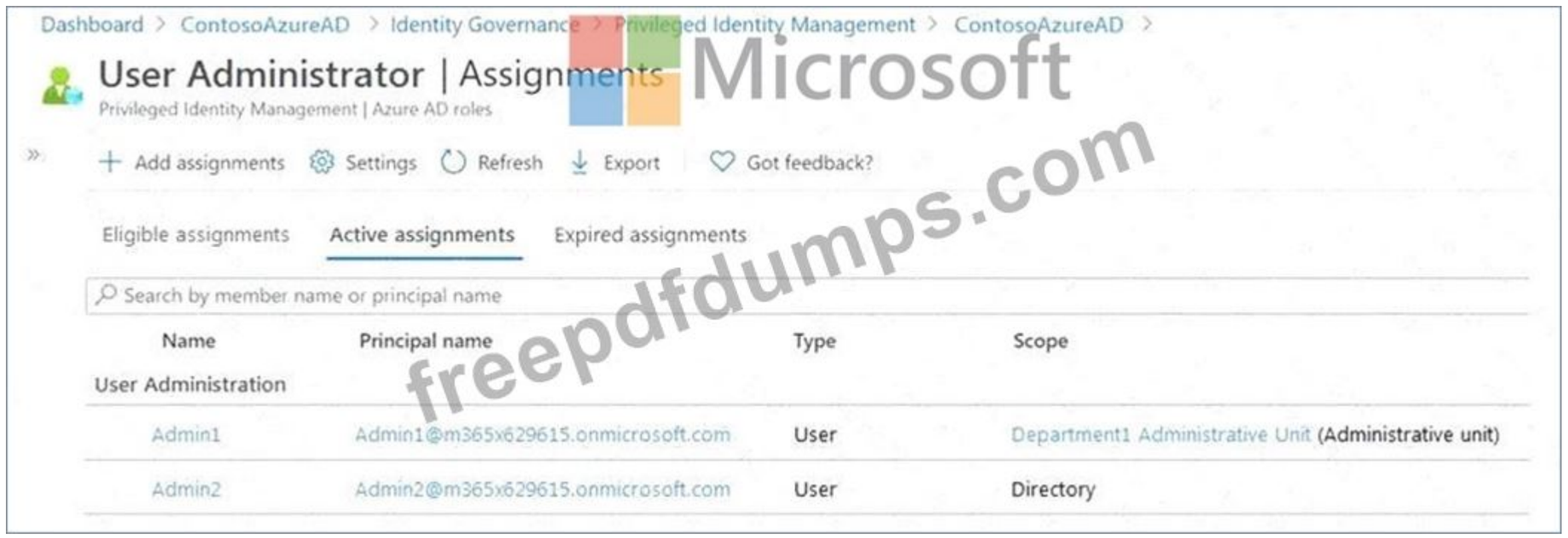
You have an Azure Active Directory (Azure AD) tenant that contains an administrative unit named Department1.

Department1 has the users shown in the Users exhibit. (Click theUserstab.)

Department1 has the groups shown in the Groups exhibit. (Click theGroupstab.)



Department1 has the user administrator assignments shown in the Assignments exhibit. (Click theAssignmentstab.)



The members of Group2 are shown in the Group2 exhibit. (Click theGroup2tab.)

For each of the f ollowing statements, select Yes if the statement is true. Otherwise, select No.

NOTE:Each correct selection is worth one point.

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

Answer:

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

Explanation:

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn documentation under "Manage Administrative Units in Azure Active Directory", Administrative Units (AUs) provide a way to delegate administrative permissions over subsets of Azure AD resources - such as specific users or groups - without granting directory-wide privileges.
* Department1 Administrative Unit contains User1, User2, Group1, and Group2.
* Admin1 is assigned the User Administrator role scoped to Department1 AU.
* Admin2 is assigned the User Administrator role scoped to the entire directory.
# Context Overview
* User3 and User4 are not members of Department1 AU - they belong only to Group2, but group membership does not automatically bring those users under AU scope.
* Admin1's permissions are limited strictly to users and groups within the Department1 AU. # Conclusion: Admin1 cannot reset the passwords of User3 and User4. Answer: No Statement 1: Admin1 can reset the passwords of User3 and User4.
* Both User1 and Group2 are in the Department1 AU, but in Azure AD, the User Administrator role scoped to an AU cannot manage group memberships unless explicitly delegated with Group Administrator privileges or unless the AU is configured to allow it.
* The User Administrator role allows password reset and user management, not group membership management. # Conclusion: Admin1 cannot add User1 to Group2. Answer: No Statement 2: Admin1 can add User1 to Group2.
* Admin2 has the User Administrator role assigned at the directory level, meaning global scope.
* Therefore, Admin2 can manage user credentials, including password resets, for all users in the tenant - including User1. # Conclusion: Admin2 can reset the password of User1. Answer: Yes Statement 3: Admin2 can reset the password of User1.
Supporting Reference (Microsoft Learn):
"Administrative units restrict scope for delegated administrators. A User Administrator scoped to an AU can reset passwords only for users in that AU. A User Administrator assigned at the directory level can reset passwords for any user."

NEW QUESTION: 84
You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Attribute Assignment Administrator
User1	User

The tenant contains the identities shown in the following table.

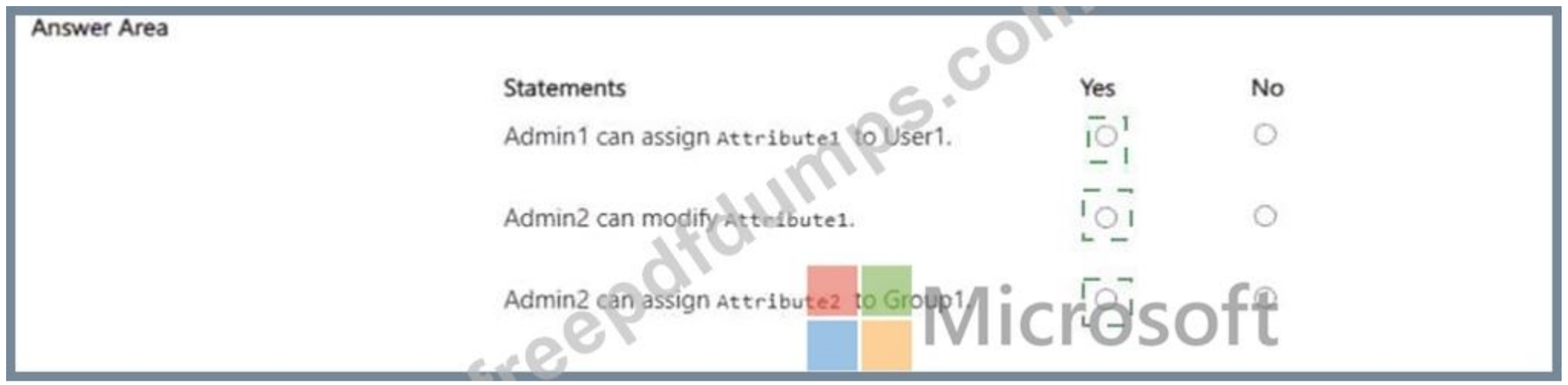
Name	Type
Group1	Security group
Service1	Service principal

You have an attribute set named Custom1 that contains the custom security attributes shown in the following table.

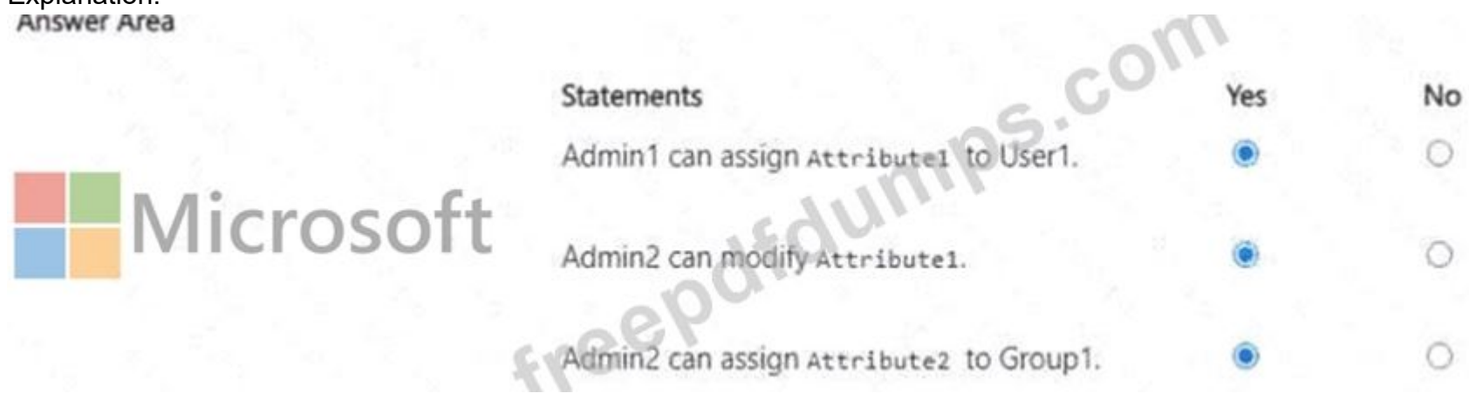
Name	Type
Attribute1	String
Attribute2	Integer

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

Answer:



Explanation:



NEW QUESTION: 85

You have a Mic rosoft Entra tenant.

You need to ensure that only users from specific external domains can be invited as guests to the tenant.

Which settings should you configure?

A. Cross-tenant access settings

B. External collaboration settings

C. Linked subscriptions

D. D . All identity providers

Answer: (SHOW ANSWER)
According to the Microsoft Entra External Identities module within the SC-300 curriculum, control over which external domains can be invited as guest users is managed under External collaboration settings i n the Entra admin center.
Administrators can specify "Allow invitations only to the specified domains" and list approved domains.
This ensures that guest invitations can only be sent to trusted business partners while blocking all others.
Cross-tenant access settings control authentication and access policies between trusted tenants, not invitation restrictions. Linked subscriptions and identity providers manage billing and authentication federation but do not control guest invitations.
Therefore, to re strict guest invitations to specific external domains, you must configure the External collaboration settings in Microsoft Entra ID.

NEW QUESTION: 86
You have a Microsoft 365 tenant.
All users must use the Mic rosoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.
You need to block the users automatically when they report an MFA request that they did not Initiate.
Solution: From the Azure portal, you configure the Account lockout settings for multi-factor authentication (MFA).
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
In SC-300, the mitigation for unsolicited MFA prompts (push fatigue) is Fraud alert on Azure AD MFA. The materials state that administrators can "allow users to report suspicious MFA prompts and automatically block the user when they select Report fraud in Mi crosoft Authenticator." By contrast, Account lockout settings are designed to "temporarily lock an account after a configurable number of consecutive MFA denials to thwart brute-force attempts," and they do not initiate an automatic block tied to a user's fraud report. The study guide further clarifies that fraud alerts "can automatically block the user for a specified period (default 90 days) when a fraudulent attempt is reported," which is precisely the behavior required in the scenario. Therefore, merely configuring Account lockout settings will not meet the goal of automatically blocking users when they report an unsolicited prompt.

NEW QUESTION: 87
You have a Microsoft Entra tenant.
You discover that a large number of new apps were added to the tenant.
You need to implement an approval process for new enterprise applications. What should you do?
A. From the Microsoft Defender portal, create a Cloud Discovery anomaly detection policy.
B. From the Microsoft Entra admin center, configure the Admin consent settings.
C. From the Microsoft Defender portal, configure an app connector.
D. From the Microsoft Entra admin center, configure an access review.
Answer: B (LEAVE A REPLY)
When many new enterprise applications appear in a Microsoft Entra tenant, it typically means that users are granting consent for apps to access organizational data. To control this behavior, administrators can use the Admin consent workflow, found in Microsoft Entra ID # Enterprise applications # Consent and permissions # Admin consent settings.
Microsoft documentation explains:
"The admin consent workflow allows users to request access to applications that require admin consent, providing administrators with visibility and control over which apps get access to organizational data." Enabling this workflow ensures that any new enterprise app requesting permissions beyond user-level consent must go through an approval process where an administrator can review and grant or deny access.

Options A and C refer to Defender for Cloud Apps, which detects and monitors discovered applications but does not enforce approval workflows. Option D (Access review) is used to periodically review user access, not app consent approval.

NEW QUESTION: 88
You have two Microsoft Entra tenants named contoso.com and fabhkam.com. Contoso.com contains the users shown in the following table.

Name	Type
User1	Member
User2	Member
User3	Guest

Contoso.com contains the groups shown in the following table.

Name	Membership type	Members
Group1	Assigned	User1
Group2	Assigned	Group1, User2

You chronization from contoso.com to fabrikam.com and enable cross-tenant synchronization for User3 and Group2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

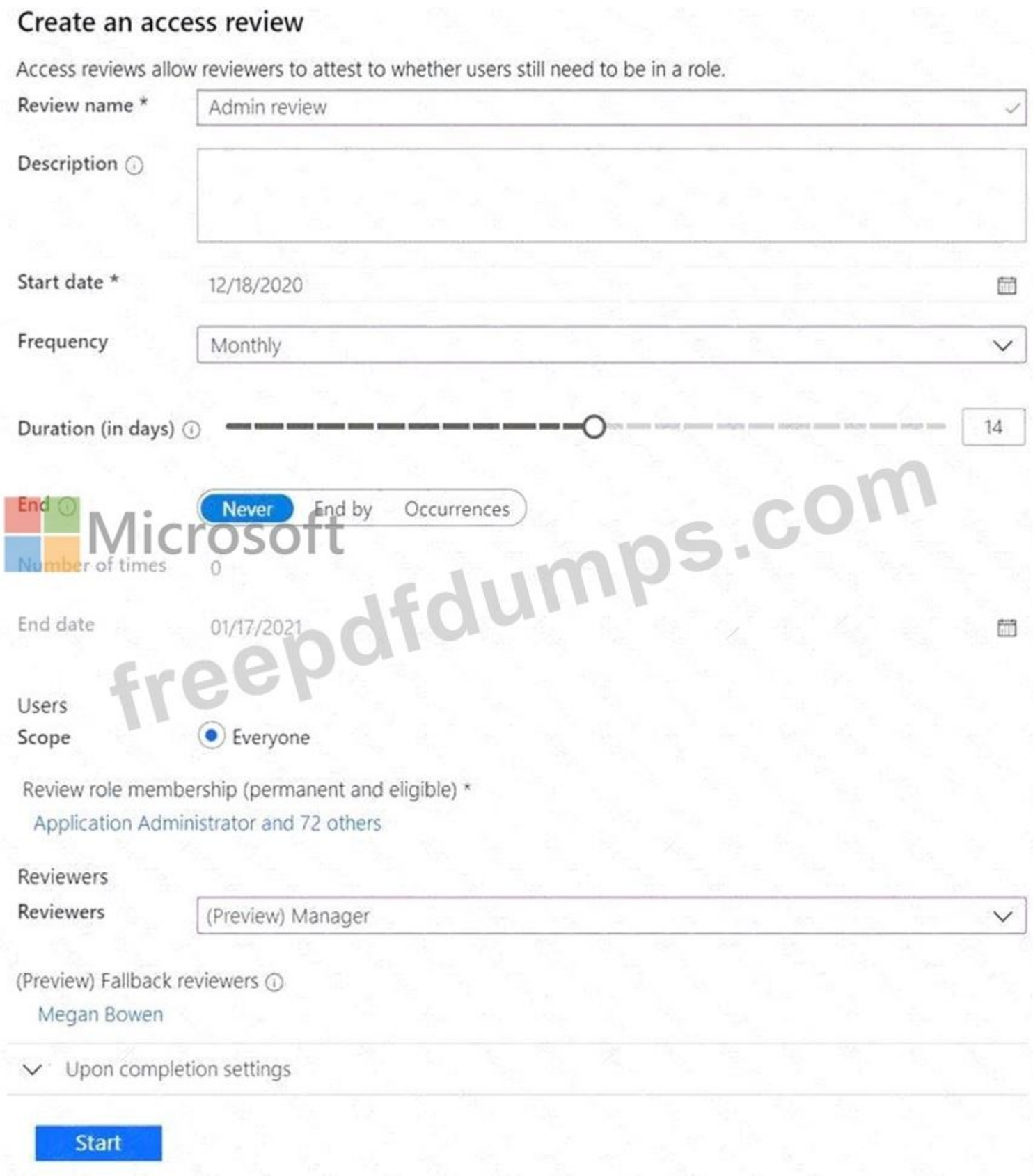
NEW QUESTION: 89
You have a Microsoft 365 E5 subscription.
You purchase the app governance add-on license.
You need to enable app governance integration.
Which portal should you use?
A. the Microsoft Defender for Cloud Apps portal
B. the Microsoft 365 admin center
C. Microsoft 365 Defender
D. the Azure Active Directory admin center
E. the Microsoft Purview compliance portal
Answer: (SHOW ANSWER)
As documented in Microsoft's App governance for Microsoft 365 guidance, App Governance is a security and compliance add-on that provides visibility and policy-based controls over OAuth-enabled applications integrated with Microsoft 365. Once you purchase and assign the app governance license, the integration and management of this feature are performed through the Microsoft 365 Defender portal.
In the Defender portal, administrators navigate to App governance under the Permissions & Apps section to enable integration, view insights, and configure policies. Microsoft documentation states:
"App governance capabilities are surfaced in the Microsoft 365 Defender portal (https://security.microsoft.
com) where you can monitor, alert, and remediate risky app behaviors connected to Microsoft 365 data." Therefore, the integration and monitoring are managed only in Microsoft 365 Defender, not in Azure AD, Purview, or Defender for Cloud Apps.

NEW QUESTION: 90
You have a Microsoft 365 tenant.
You need to ensure that you tan view Azure Active Directory (Azure AD) audit log information by using Azure Monitor.
What should you do first?
A. Run the Get-AzureADAuditDirectoryLogs cmdlet.
B. Create an Azure AD workbook.
C. Run the Set-AzureADTenantDetail cmdlet.
D. Modify the Diagnostics settings for Azure AD.
Answer: D (LEAVE A REPLY)
According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and Microsoft Learn module: "Monitor and troubleshoot Azure Active Directory", to integrate Azure Active Directory audit logs with Azure Monitor, Log Analytics, or Event Hubs, you must first configure Diagnostic settings in Azure AD.
Azure AD logs - including Audit Logs and Sign-in Logs - are stored natively within Azure AD for a limited retention period (14-30 days, depending on license). However, to analyze these logs over time, perform custom queries, or integrate them with monitoring or SIEM solutions, administrators must send them to Azure Monitor logs, Azure Storage, or Event Hubs.
The official documentation explicitly states:
"To send Azure AD logs to Azure Monitor, create a diagnostic setting in Azure Active Directory. From there, select which log categories (AuditLogs, SignInLogs, or NonInteractiveUserSignInLogs) you want to send to a Log Analytics workspace, Event Hub, or storage account." Steps outlined in the study guide and Microsoft Learn:
* Sign in to the Azure portal as a Global Administrator.
* Navigate to Azure Active Directory # Diagnostic settings.
* Select Add diagnostic setting.
* Choose the log categories (e.g., AuditLogs, SignInLogs).
* Select a destination - for instance, a Log Analytics workspace (for Azure Monitor integration).

This configuration is required before Azure Monitor can query or visualize Azure AD audit data.

NEW QUESTION: 91
Your on-premises network contains an Active Directory Domain Services (AD DS) domain and a certification authority (CA) named CAT.
You have a Microsoft Entra tenant.
You need to implement Microsoft Entra certificate-based authentication. The solution must ensure that users can sign in by using certificates issued by CAT What should you do first?
A. Enable auto-enrollment for CAT.
B. Deploy an Azure key vault.
C. Add CA1 as a Certificate Authority to the Microsoft Entra tenant.
D. Deploy Windows Hello for Business.
Answer: C (LEAVE A REPLY)
Microsoft Entra certificate-based authentication (CBA) allows users to sign in with X.509 certificates. The SC-300 guidance explains that before users can authenticate with on-premises certificates, the tenant must trust the issuing Certificate Authorities: you must "upload and configure the certificate authorities (root and any intermediates) that issue the user certificates," establishing the trust chain used to validate presented certificates. Only after the CA trust is configured can you map certificate fields and define authentication policies. Auto-enrollment (A) is optional operational convenience for issuing certs, not the first tenant configuration step. Azure Key Vault (B) is unrelated to validating client auth certificates. Windows Hello for Business (D) is a separate credential technology and not required for Entra CBA. Therefore, the first action is to add CA1 (and any intermediates) under Certificate Authorities in Microsoft Entra so that certificates issued by CA1 are recognized for sign-in.

NEW QUESTION: 92
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 secti on, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
You have 100 IT administrators who are organized into 10 departments.
You create the access review shown in the exhibit. (Click theExhibittab.)



You discover that all access review requests are received by Megan Bowen.

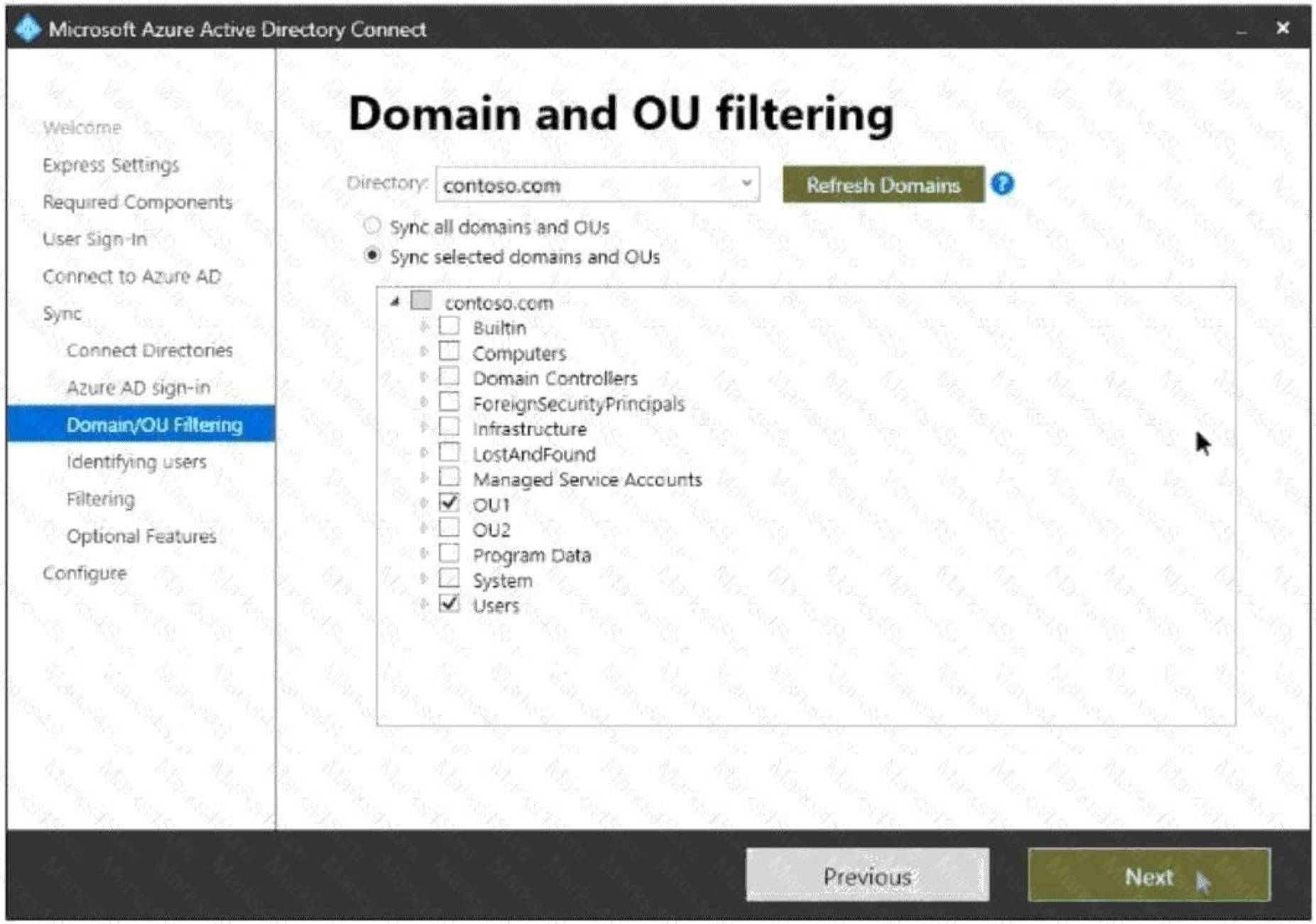
You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You add each manag er as a fallback reviewer.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
From the exhibit and the SC-300 Study Guide (Access Reviews section) , the access review is configured with the reviewer type set to (Preview) Manager, and Megan Bowen as the fallback reviewer.
In Azure AD Access Reviews, when "Manager" is selected as the reviewer type, the system automatically assigns each user's Azure AD-defined manager to review their access. However, if a user does not have a manager assigned in Azure AD, the review task defaults to the fallback reviewer (in this case, Megan Bowen).
Therefore, if all access review requests are going to Megan Bowen, that means users in the tenant do not have managers properly assigned in Azure AD user attributes.
Adding the department managers as fallback reviewers does not solve the issue because the fallback reviewer receives only the reviews for users without a manager, not based on department.
Microsoft documentation states:
"When 'Manager' is selected as the reviewer, the manager property from Azure AD is used. If a user does not have a manager, the fallback reviewer is used. Adding managers as fallback reviewers will not assign reviews based on departments."

NEW QUESTION: 93
You have a Microsoft 365 subscription that contains the following:
* An Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium P2 license
* A Microsoft SharePoint Online site named Site1
* A Microsoft Teams team named Team1
You need to create an entitlement management workflow to manage Site1 and Team1. What should you do first?
A. Create an access package.
B. Create a catalog.
C. Create an administrative unit.
D. Configure an app registration.
Answer: B (LEAVE A REPLY)
According to Microsoft Identity Governance documentation and the SC-300 study guide, entitlement management in Azure AD allows you to manage access to resources like SharePoint Online sites, Teams, groups, and applications through access packages. However, before an access package can be created, the administrator must first define a catalog.
A catalog is the logical container that holds all the resources (such as groups, Teams, and SharePoint sites) that can be made available in access packages. The process for entitlement management begins with catalog creation, followed by adding resources, then creating access packages that assign roles for those resources.
Therefore, the first step to managing Site1 (SharePoint site) and Team1 (Microsoft Teams team) within entitlement management is to create a catalog and add those resources to it.
This aligns with Microsoft documentation, which states:
"Before creating an access package, you must have a catalog that contains the resources to be made available for assignment."

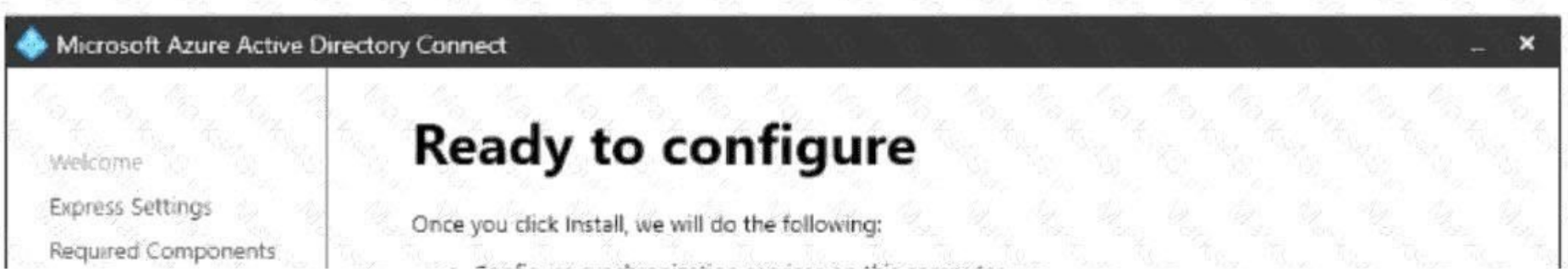
NEW QUESTION: 94
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.

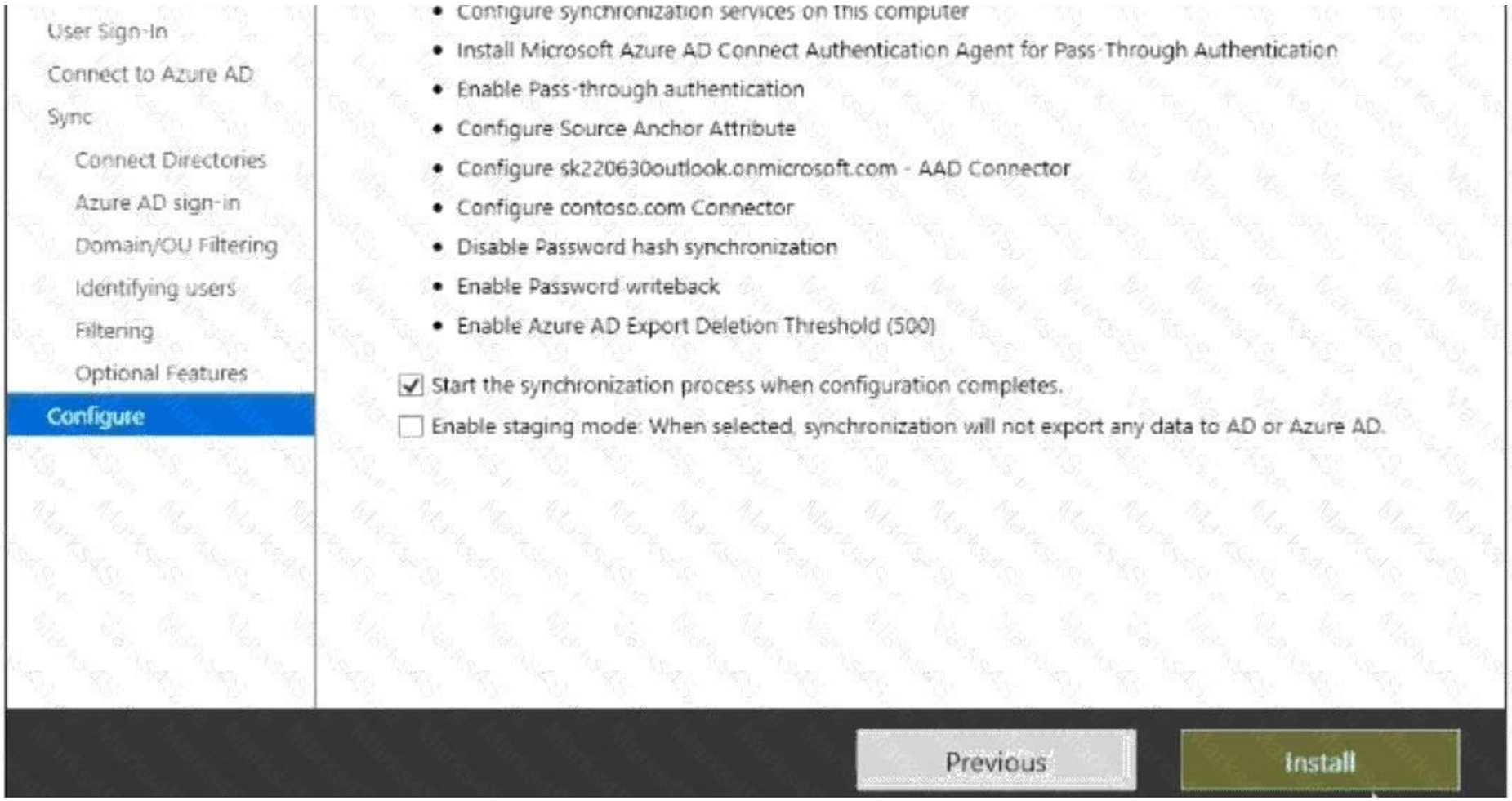
Name	Organizational unit (OU)
User1	OU1
User2	OU2

In Azure AD Connect. Domain/OU Filtering is configured as shown in the following exhibit.



Azure AD Connect is configured as shown in the following exhibit.





For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selec tion is worth one point.

Answer Area

Statements	Yes	No
User1 can use self-service password reset (SSPR) to reset his password.	○	○
If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.	○	○
User2 can be added to a Microsoft SharePoint Online site as a member.	○	○

Answer:

Explanation:

User1 can use self-service password rese t (SSPR) to reset his password: Yes If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller: Yes User2 can be added to a Microsoft SharePoint Online site as a member: No Based on Microsoft's SC-300 Study Guide , Exam Ref SC-300: Microsoft Identity and Access Administrator

, and Azure AD documentation, Azure AD Connect synchronization is governed by OU filtering, authentication method, and synchronization scope.

In this configuration, Azure AD Connect is set to "Sync selected domains and OUs," and only OU1 is selected. Therefore, only objects (users, groups, etc.) located in OU1 are synchronized to Azure AD.

* User1 (in OU1) is synchronized to Azure AD. Since password writeback is enabled (as seen in the configuration "Enable password writeback"), User1 can perform Self-Service Password Reset (SSPR) from Azure AD, and the change will write back to on-premises AD. Hence, the first statement is Yes.

* Pass-through authentication is also enabled in the configuration ("Enable Pass-through authentication").

With PTA, when User1 accesses Microsoft 365 services (like Exchange Online), the authentication request is forwarded from Azure AD to an on-premises domain controller via the PTA agent. Therefore, authentication is handled by the local AD DS. Hence, the second statement is Yes.

* User2 (in OU2) is not synchronized, as OU2 was not selected in the Domain/OU filtering configuration.

This means User2 does not exist in Azure AD and cannot be granted access to Microsoft 365 resources, including SharePoint Online. Hence, the third statement is No.

This logic aligns with Microsoft documentation under "Configure filtering for Azure AD Connect," which states:
"Only objects from selected domains and organizational units are synchronized. Users outside selected OUs are excluded from Azure AD and cannot authenticate or access cloud resources."

NEW QUESTION: 95

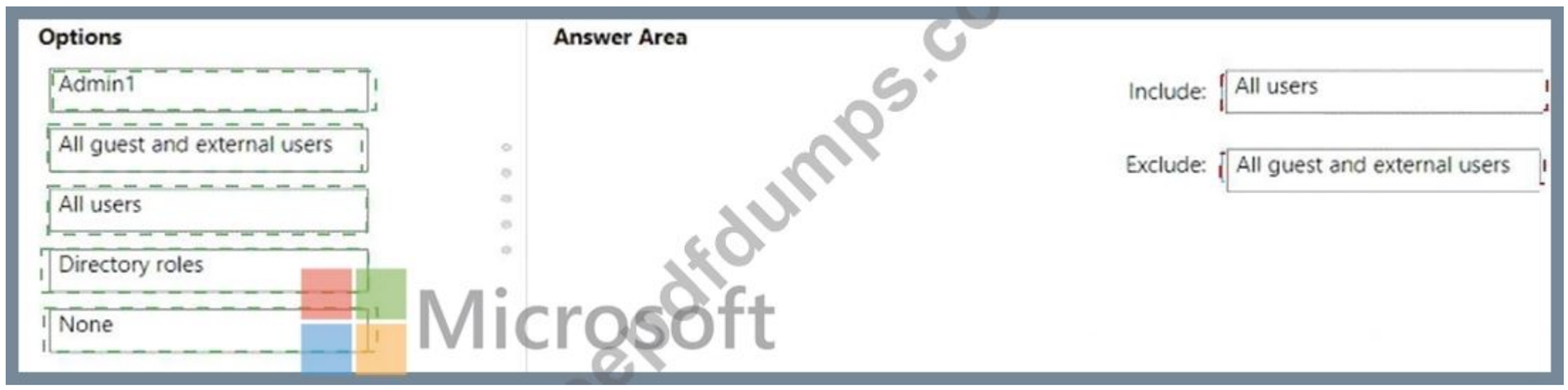
You have an Azure AD tenant that contains a user named Admin1.

Admin1 uses the Require password change for high-risk user's policy template to create a new Conditional Access policy.

Who is included and excluded by default in the policy assignment? To answer, drag the appropriate options to the correct target. Each option may be use d 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:



Explanation:

According to the Microsoft SC-300: Microsoft Identity and Access Administrator Official Study Guide and Microsoft Learn - Manage Conditional Access policies module, when an administrator creates a Conditional Access policy using the built-in Require password change for high-risk users template, the policy is automatically pre-configured with specific include and exclude assignments.

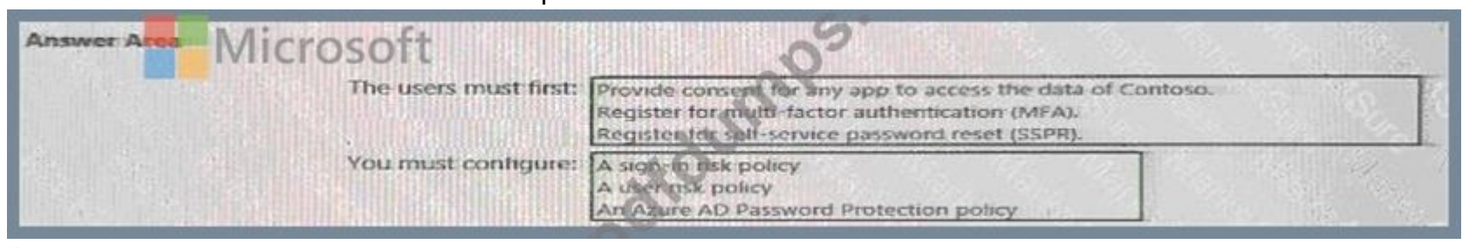
By default, this template targets "All users" in the tenant because the policy is designed to detect and remediate risky sign-ins or compromised accounts across the entire directory. However, since Azure AD B2B guest accounts and external users often have limited sig n-in scopes and cannot be subjected to organization- specific password policies, Microsoft's security baseline specifically excludes all guest and external users by default.

The intent behind this default configuration is to apply the password change requir ement to internal users while avoiding unnecessary enforcement on guest identities that do not manage

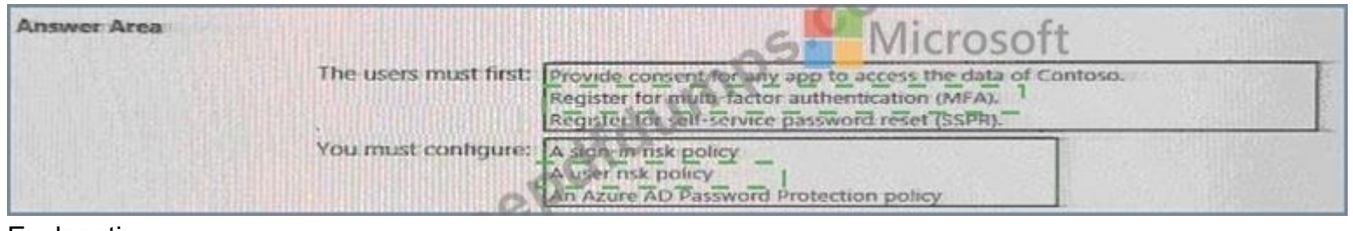
credentials within the host tenant.
From the Microsoft Learn - Conditional Access policy templates documentation:
"When you create a policy from the Requi re password change for high-risk users template, the policy is configured to include all users and exclude all guest and external users by default."

NEW QUESTION: 96
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.
A contractor uses the credentials of user1@outlook.com.
You need to ensure that you can provide the cont ractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.
What should you do?
A. Run theNew-AzureADMSInvitationcmdlet.
B. Configure the External collaboration settings.
C. Add a WS-Fed identity provider.
D. Implement Azure AD Connect.
Answer: (SHOW ANSWER)
According to the Microsoft Identity and Access Administrator (SC-300) official study guide and Microsoft Learn module "Manage External Identities" , when granting external users (such as contractors) access to Azure AD resources, the recommended method is to invite them as guest users (B2B collaboration users) into your Azure AD tenant.
The New-AzureADMSInvitation cmdlet is the PowerShell command used to create an Azure AD B2B guest invitation. It sends an invitation to an external user (such as user1@outlook.com) and, upon acceptance, creates a corresponding guest user account in the tenant (for example, user1_outlook.com#EXT#@contoso.
com). This account can then be assigned to enterprise applications like App1.
From Microsoft documentation:
"To provide external users access to resources in your organization, invite them as guests using Azure AD B2B collaboration. You can do this by running the New-AzureADMSInvitation cmdlet or via the Azure portal."
* B. Configure the External collaboration settings: These settings define collaboration policies (who can invite guests, restrictions, etc.) but do not invite users themselves.
* C. Add a WS-Fed identity provider: This is used to federate another identity provider (e.g., ADFS or another Azure AD tenant), not to onboard an individual external user.
* D. Implement Azure AD Connect: This tool synchronizes on-premises directories with Azure AD; it's not relevant for external users from Outlook.com.
Why not the other options: # Correct Answer: A. Run the New-AzureADMSInvitation cmdlet.

NEW QUESTION: 97
You need to meet the technical requirements for the probability that user identifies were compromised.
Wh at should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

The users must first: Register for multi-factor authentication (MFA)

You must configure: A user risk policy

According to Microsoft SC-300 official learning materials and Exam Ref SC-300: Mic rosoft Identity and Access Administrator , when the requirement is to address the probability that user identities were compromised, the appropriate feature is Azure AD Identity Protection. Identity Protection detects risky sign- ins and risky users through continuous analysis of login behavior, location, device, and credential exposure signals.

Two types of policies can be created:

* Sign-in risk policy - Triggers actions based on suspicious sign-in behavior (for example, unfamiliar location).
* User risk policy - Triggers actions when the user's overall identity is deemed at risk (for example, compromised credentials).

The documentation specifies:

"When user risk is detected, the policy can require the user to change their password to remediate the risk.

Users must first be registered for MFA to perform secure password change operations." Therefore, before the user risk policy can be enforced, users must be enrolled in multi-factor authentication (MFA). MFA is used during the remediation step (password change) to verify the user's identity securely.

Thus, to meet the requirement for "the probability that user identities were compromised," you configure a user risk policy in Azure AD Identity Protection, and ensure that users first register for MFA so that they can complete password change or verification flows when risks are detected.

NEW QUESTION: 98

You have a Microsoft Entra tenant that has a Microsoft Entra ID P1 license.

You need to review the Microsoft Entra ID sign-in logs to investigate sign-ins that occurred in the past.

For how long does Microsoft Entra ID store events in the sign-in logs?

A. 14 days

B. 30 days

C. 90days

D. 365 days

Answer: B (LEAVE A REPLY)

The retention period for Microsoft Entra (Azure AD) sign-in logs depends on the license (Free, P1, P2).

Microsoft's data retention documentation states that with a Microsoft Entra ID P1 license, sign-in data is retained for 30 days.

The relevant table in the "Microsoft Entra data retention" documentation shows:

* With Entra ID P1 or P2: sign-in activity is retained for 30 days
* (With Free tier, sign-in logs are retained for 7 days)

Therefore, under your scenario (tenant has ID P1 license), the logs are available for 30 days.

NEW QUESTION: 99

You have an Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

For which groups can you create an access review?

A. Group1 only

B. Group1 and Group4 only

C. Group1 and Group2 only

D. Group1, Group2, Group4, and Group5 only

E. Group1, Group2, Group3, Group4 and Group5

Answer: (SHOW ANSWER)

The SC-300 official study guide and Microsoft Learn: Manage Access Reviews confirm that Access Reviews in Azure AD can target user-based groups, Azure AD roles, and enterprise applications. However, dynamic device groups are not supported for access reviews.

NEW QUESTION: 100

You have an Azure subscription named Sub1.

You purchase a Microsoft Entra Permissions Management license.

You need to onboard Permissions Management.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE; Each correct selection is worth one point.

A. Implement a Microsoft Entra application proxy.

B. From Microsoft Entra Permissions Management, configure data collection.

C. Create a role assignment for Sub1.

D. From the Microsoft Entra admin center, configure the Diagnostic settings.

E. From the Microsoft Entra admin center, create an app registration.

F. From the Azure portal, create a data collection rule (DCR).

Answer: B,C (LEAVE A REPLY)

According to the official Microsoft SC-300 Study Guide and Microsoft Entra Permissions Management documentation, onboarding Microsoft Entra Permissions Management (formerly CloudKnox) involves two key setup tasks:

* Configuring Data Collection - After purchasing the license, you must connect your Azure subscription (s) to Permissions Management so it can inventory identities, roles, and permissions. This is done from the Microsoft Entra Permissions Management portal, where you enable data collection for each connected cloud environment (Azure, AWS, GCP). This process deploys the required collector identity (service principal) and defines the scope for data gathering.

* Creating Role Assignments - Permissions Management requires proper authorization to read role assignments, permissions, and activity data. You must create a role assignment at the subscription level (Sub1) using a least-privilege role (for example, Reader or CloudKnox Service Principal Role) for the Permissions Management application service principal. This ensures it can scan Azure resources for permission analysis.

Microsoft documentation confirms:

"To onboard Azure subscriptions, assign the CloudKnox service principal a Reader role on each subscription, and configure data collection from within Microsoft Entra Permissions Management."

NEW QUESTION: 101

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

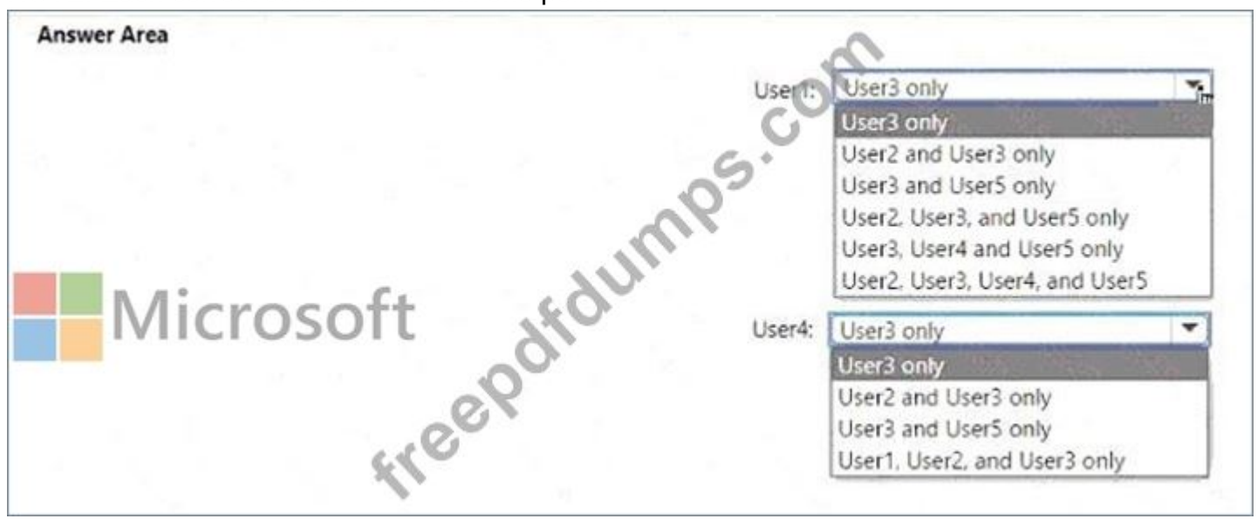
Name	Member of administrative unit
User1	AU1
User2	AU1
User3	AU1
User4	AU2
User5	Not a member of an administrative unit

The users are assigned the roles shown in the following table.

User	Role	Role scope
User1	Password Administrator	Organization
User2	Global Reader	Organization
User3	*None*	*Not applicable*
User4	Password Administrator	AU1
User5	*None*	*Not applicable*

For which users can User1 and User4 reset passwords? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

User

Can Reset Passwords For

User1

User3 and User5 only
User4
User3 only
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and official Microsoft Learn documentation on role-based access control (RBAC) and administrative units (AUs) , the scope of administrative privileges determines which users an administrator can manage.
Role Review:
* Password Administrator (Organization scope): Can reset passwords for non-administrators and users with lesser pri vileges across the entire organization. They cannot reset passwords for Global Administrators or users with equal/higher roles.
* Global Reader (Organization scope): Read-only access-cannot perform administrative actions (including password resets).
* Password Administrator (Scoped to AU1): Can reset passwords for users within AU1 who are non- administrators and whose roles are less privileged than their own.
User
Role
Scope
Members in Administrative Unit
User1
Password Administrator
Organization
AU1
User2
Global Reader
Organization
AU1
User3
None
N/A
AU1
User4
Password Administrator
AU1
AU2
User5
None
N/A
None
Step 1 - For User1 (Org-scoped Password Administrator): User1's permissions apply organization-wide, allowing resets for:
* Users without admin roles, including those in or outside any AU.
* Cannot reset passwords for users with equal or higher roles (e.g., Global Reader, Password Administrator).
# Therefore, User1 can reset passwords for:
* User3 (no role, AU1)
* User4 (Password Administrator in AU2) - # cannot reset equal role
* User5 (no role, no AU) #

Final for User1 # User3 and User5 only
Step 2 - For User4 (AU1-scoped Password Administrator): User4's permissions apply only within AU1 and to users with lesser privileges.
Within AU1:
* User1 (Org Password Admin) - # higher privilege
* User2 (Global Reader) - # higher privilege
* User3 (no role) - # can reset
Final for User4 # User3 only

NEW QUESTION: 102
You have an Azure subscription named Sub1 that contains two resource groups named RG1 and RG2. Sub1 contains the users shown in the following table.

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

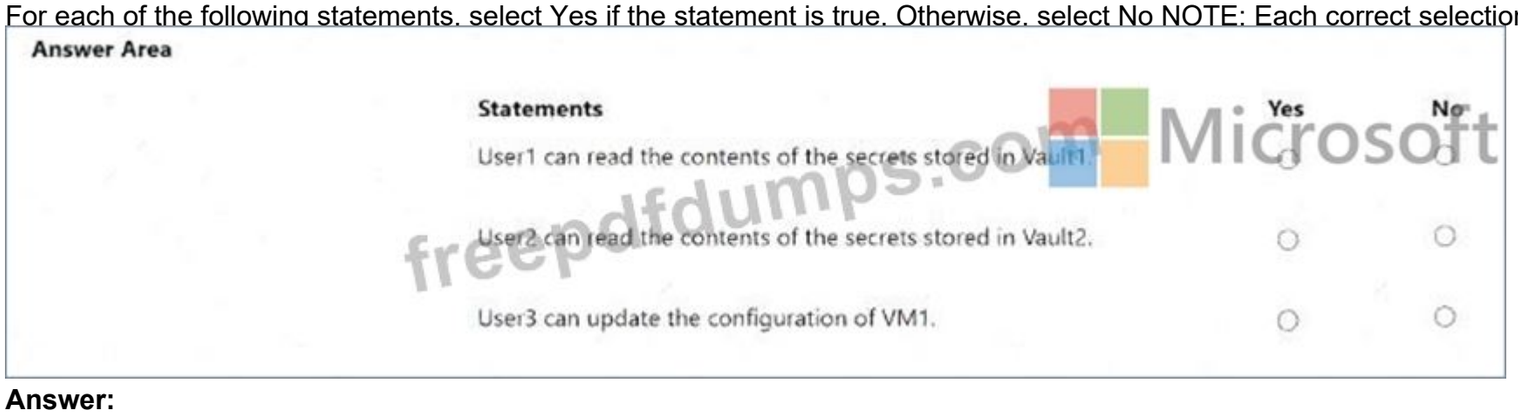
Sub1 contains the resources shown in the following table.

Name	Type	In resource group
VM1	Virtual machine	RG1
Vault1	Azure Key Vault	RG1
Vault2	Azure Key Vault	RG2

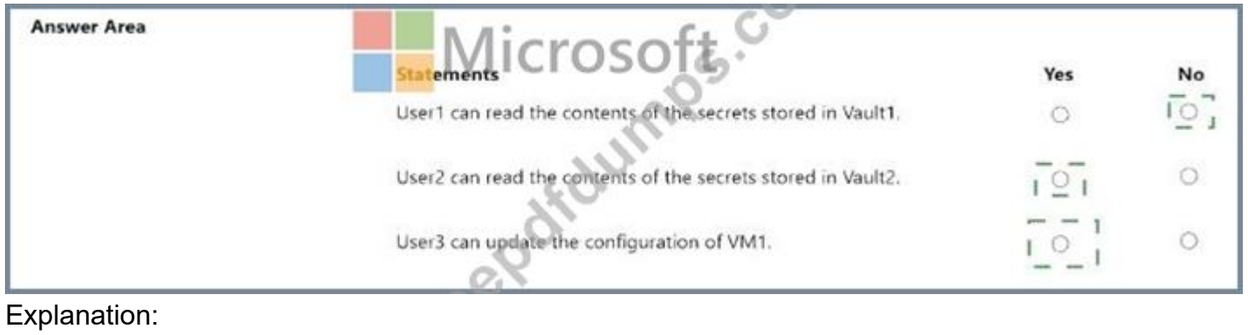
You create the role-based access control (RBAC) role assignments shown in the following table.

Role	Member of	Scope
Reader	Group1	Sub1
Key Vault Secrets User	Group2	RG2
Owner	Group3	RG1

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



Answer:



Explanation:

No
Yes
Yes
In Microsoft Entra/Azure RBAC, permissions are granted by role + scope and inherit down the hierarchy (subscription # resource group # resource). The SC-300 materials clarify that the Reader role is "a management-plane role that permits viewing resources but not modifying them or accessing data content s." Therefore, although Group1 has Reader at Sub1 , User1 (Group1, Group2) cannot read Key Vault secrets in Vault1 because Reader does not grant data-plane access. The study guide also notes for Azure Key Vault with RBAC: "Key Vault Secrets User can read se cret contents (get/list) for vaults in the assigned scope." Since Group2 holds Key Vault Secrets User at RG2 , any member of Group2 (including User2) can read secrets in Vault2 (which is in RG2). However, that assignment does not extend to RG1 , so it doesn' t help User1 with Vault1 . Finally, SC-300 coverage of built-in roles states: "Owner grants full access to all resources within the scope, including the ability to modify settings and delegate access." Because Group3 is Owner at RG1 , User3 can manage resour ces in RG1 , including updating the configuration of VM1 located there.
Result: User1 # No , User2 # Yes , User3 # Yes .

NEW QUESTION: 103
You ha ve a Microsoft Entra tenant.
You need to configure continuous access evaluation for app sign-ins and assign the configuration to users that are assigned the Application Administrator role.
What should you configure?
A. a Conditional Access policy
B. the Admin consent settings
C. a sign-in risk policy
D. an access review
Answer: A (LEAVE A REPLY)
Per Microsoft SC-300 Exam Ref and Microsoft Learn module: Implement Continuous Access Evaluation (CAE) , continuous access evaluation is configured and enforced thr ough Conditional Access policies .
CAE enables near real-time enforcement of access decisions based on user or session changes such as account disablement, password reset, or location change - without waiting for token expiration. To apply CAE for specific user groups or roles (e.g., Application Administrators), administrators must create or edit a Conditional Access policy and ensure Continuous Access Evaluation is enabled for relevant cloud apps.
Settings like Admin consent , Sign-in risk policy , and Access reviews serve different functions and do not enable continuous enforcement.
Thus, to configure CAE and assign it to Application Administrators, you must use a Conditional Access policy .

NEW QUESTION: 104
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
VM1	Virtual machine
App1	Azure App Service web app
Managed1	Managed identity
Managed2	Managed identity

You create a Microsoft Entra user named User1.
Which identities can you add to VM1 and App1? To answer, select the appropriate options in the answer area.
NOTE: Each correct answer is worth one point.

Answer:

Explanation:

VM1: Managed1 and Managed2 only
App1: A system-assigned managed identity and Managed2 only

Questions no: 269

Verified Answer :

* VM1: Managed1 and Managed2 only
* App1: A system-assigned managed identity and Managed2 only

Comprehensive and Detailed Explanation with all Microsoft SC-300: Identity and Access Administrator documents :

To answer this question, we must apply the principles of Managed Identities for Azure resource s .

Managed identities provide an automatically managed identity in Microsoft Entra ID for applications to use when connecting to resources that support Microsoft Entra authentication (like Azure Key Vault or SQL).

1. Understanding Identity Types:

* User Obje cts (User1): Standard user accounts are used for human sign-ins. You cannot assign a standard user object (like User1) as the identity of an Azure resource (like a VM or App Service). The resource must use a Service Principal or Managed Identity. Therefore , any option including User1 is incorrect.
* User-Assigned Managed Identities (Managed1, Managed2): These are standalone Azure resources that can be assigned to one or more Azure resources (like VMs or App Services).
* System-Assigned Managed Identities: These are enabled directly on the resource itself and share the resource ' s lifecycle.

2. Analysis for VM1:

* Azure Virtual Machines support User-assigned managed identities .
* You can assign multiple user-assigned identities to a single VM.

* Looking at the dropdown options for VM1:
* Options with User1 are invalid.
* This leaves Managed2 only or Managed1 and Managed2 only.
* Since both Managed1 and Managed2 are valid user-assigned identities available in the subscription, you can assign both.
* Conclusion: Select Managed1 and Managed2 only .
3. Analysis for App1:
* Azure App Services support both System-assigned and User-assigned managed identities concurrently.
* Looking at the dropdown options for App1:
* Options with User1 are invalid.
* Managed1 is not listed in the dropdown opt ions (Managed identities must be in the same region as the resource; often this question implies a region mismatch, or simply restricts the choice).
* Managed2 is listed as a valid user-assigned option.
* A system-assigned managed identity is listed as a valid option.
* Since you can configure an App Service to use both its system-assigned identity and a user- assigned identity simultaneously, the most complete correct answer identifies all capable identities.
* Conclusion: Select A system-assigned managed identity and Managed2 only .
Reference Extract:
" Managed identities for Azure resources provide Azure services with an automatically managed identity in Azure Active Directory... There are two types of managed identities: System-assigned ... and User-assigned
... You can assign a user-assigned managed identity to [Azure Virtual Machines and Azure App Service]. " (Source: Microsoft Learn - What are managed identities for Azure resources?)

NEW QUESTION: 105

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The tenant has the authentication methods shown in the following table.

Method	Target	Enabled
FIDO2	Group2	Yes
Microsoft Authenticator app	Group1	Yes
SMS	Group3	Yes

Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?

A. User1 only

B. User2 only

C. User3 only

D. User1 and User2 only

E. User2 and User3 only

Answer: A (LEAVE A REPLY)

According to Microsoft's SC-300: Microsoft Identity and Access Administrator Study Guide and Exam Ref SC-300, the behavior of the sign-in process depends on which authentication

methods are enabled for the user or their group. Azure AD supports multiple strong authentication methods, such as Microsoft Authenticator app, FIDO2, and SMS, which can be targeted to specific user groups.
The question specifies that the tenant's configuration enables the following methods:
* FIDO2 # Group2 (Yes)
* Microsoft Authenticator app # Group1 (Yes)
* SMS # Group3 (Yes)
And user membership is:
* User1 # Group1
* User2 # Group2
* User3 # Group3
The key phrase in the question is:
"Sign in to cloud apps by matching a number shown in the app with a number shown on their phone." This specific sign-in experience refers to the number matching feature in the Microsoft Authenticator app.
* Number matching is a security enhancement in Azure AD MFA that requires the user to confirm a sign- in by matching a number displayed on the sign-in screen with the number shown in their Microsoft Authenticator app notification.
* According to Microsoft Learn:
"When using the Microsoft Authenticator app for MFA, users will be prompted to enter or match a number displayed on the screen. This feature strengthens authentication by preventing accidental approvals." Therefore:
* Only User1, who is a member of Group1 (the group enabled for Microsoft Authenticator app), will experience number matching when signing in.
* User2 uses FIDO2, which employs a hardware key or biometric verification - not number matching.
* User3 uses SMS, which involves a one-time passcode (OTP) - again, not number matching.
Hence, only User1 will sign in to cloud apps using number matching.

NEW QUESTION: 106

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.
A contractor uses the credentials of user1@outlook.com.
You need to ensu re that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.
What should you do?

A. Run the New-AzADUser cmdlet.

B. Configure the External collaboration settings.

C. Add a WS-Fed identity provider.

D. Create a guest user account in contoso.com.

Answer: D (LEAVE A REPLY)

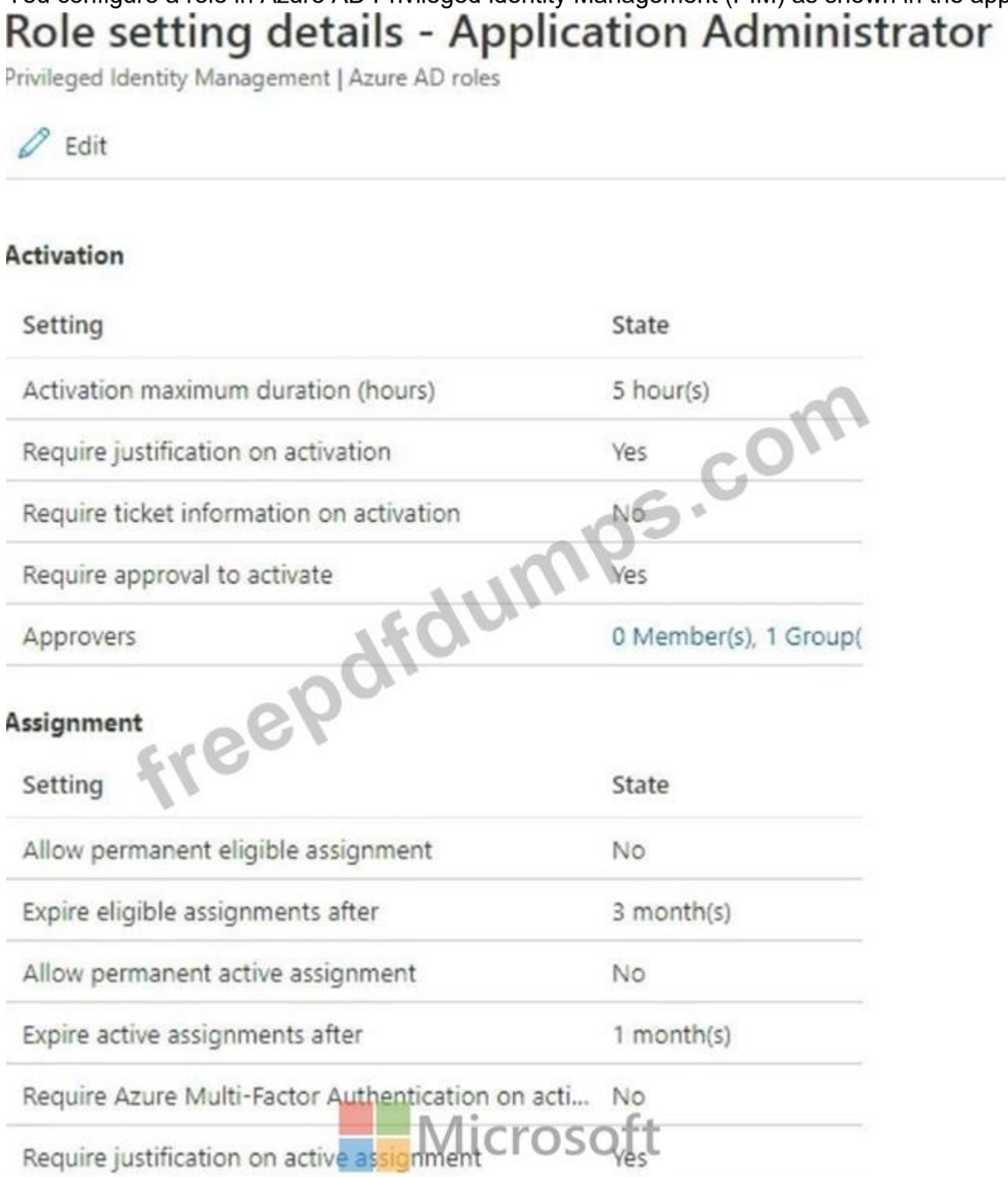
SC-300 coverage of Azure AD B2B collaboration states that to grant an external person access to your enterprise application, you invite them as a guest using their existing identity (such as a Microsoft account like user1@outlook.com). The documentation emphasizes that B2B "lets you collaborate with external users by adding them to your directory as guest users using their existing credentials." Once invited, the guest can authenticate in their home identity provider and be assigned to the target enterprise application (App1) through app role assignment or group membership. You do not need to create a new managed user or add a WS-Federation identity provider for Outlook.com; Azure AD natively supports Microsoft Accounts for B2B invitations, controlled by External collaboration settings (which generally allow invitations to any domain by default). Consequently, to ensure the contractor can authenticate as user1@outlook.com and access App1, you should create a guest user (invite) in the contoso.com tenant and assign that guest to App1.

NEW QUESTION: 107
You have an Azure AD tenant that contains an access package named Package1 and a user named User1.
Package1 is configured as shown in the following exhibit.

You need to ensure that User1 can modify the review frequency of Package1. The solution must use the principle of least privilege.
Which role should you assign to User1?
A. Privileged rol e administrator
B. User administrator
C. External Identity Provider administrator
D. Security administrator
Answer: B (LEAVE A REPLY)
This question refers to Azure AD Entitlement Management under Identity Governance . The goal is to let User1 modify the review frequency (i.e., Access Reviews) for an existing access package named Package1
, following the principle of least privilege .
In Azure AD, the ability to create and manage access packages, catalogs, and access reviews is granted through certain admini strative roles:
* Global Administrator and Identity Governance Administrator - Full control over all Identity Governance settings.
* Catalog Owner or Access Package Manager - Manage access packages and settings within a catalog.
* User Administrator - Can config ure access reviews and manage users, groups, and limited governance settings.
* Privileged Role Administrator , Security Administrator , and External Identity Provider Administrator - Have no direct control over access review settings in Entitlement Management.
From Microsoft documentation ("Azure AD Entitlement Management Delegation and Roles"):

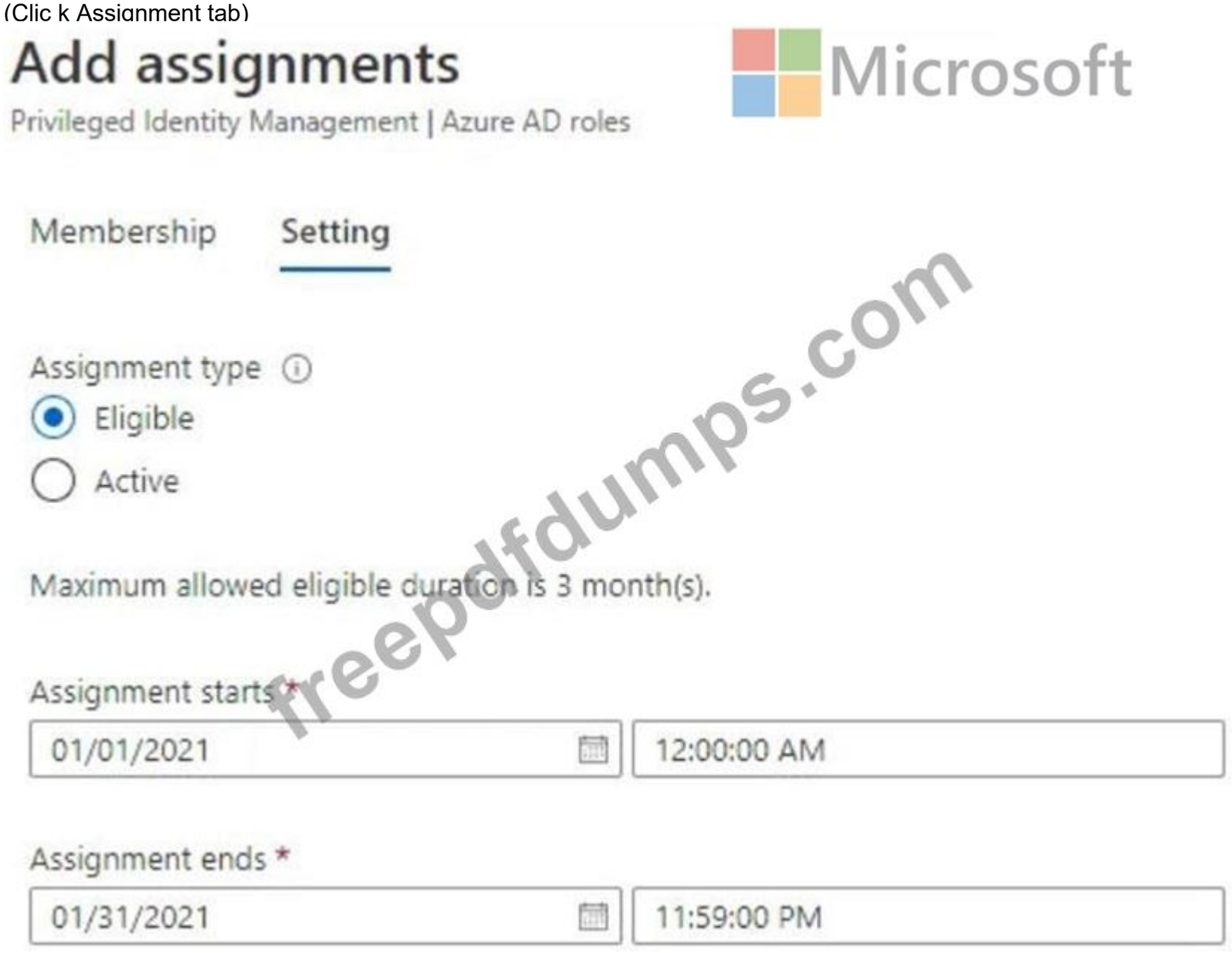
"A user administrator can manage access reviews and entitlement management settings for the directory and assigned catalogs, including adjusting the review f requency or review settings." Thus, to modify the Access Review configuration (frequency, reviewers, etc.) in Package1 , the User Administrator role provides the minimum necessary privilege without granting excessive permissions like Identity Governance Adm inistrator or Global Administrator.

NEW QUESTION: 108
You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, Use r1, and User3, You create a group named Group1. You add User2 and User3 to Group1.
You configure a role in Azure AD Privileged identity Management (PIM) as shown in the application administrator exhibit. (Click the application Administrator tab.)



Group1 is configured as the approver for the application administrator role.
You configure User2to be eligible for the application administrator role.

For User1, you add an assignment to the Application administrator role as shown in the Assignment exhibit.
(Clic k Assignment tab)



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

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	○	○
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	○	○
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	○	○

Answer:

Answer Area

Explanation:

< Statement 1 # No

Statement 2 # No

Statement 3 # Yes

According to the Microsoft SC-300: Microsoft Identity and Access Administrator study guide and Azure AD Privileged Identity Management (PIM) documentation, roles in PIM can be configured for eligible or active assignments.

* User1 is assigned automatically - No The "Add assignments" screen shows User1's assignment type as Eligible, not Active. Eligible assignments mean the user is not automatically granted the role; they must activate it manually when needed. Therefore, User1 is not assigned automatically to the Application Administrator role.

* When User2 requests role assignment, only User3 can approve - No The Role setting details show that approval is required to activate and that the approver is listed as Group1. Because both User2 and User3 are members of Group1, any member of the group can approve the request, not only User3. Hence, the statement that only User3 can approve is incorrect.

* User1's approval on January 31, 2021, at 23:00 - Yes The configuration shows an activation maximum duration of 5 hours. Therefore, if User1's request is approved at 23:00 on January 31, the role remains active for 5 hours - until 04:00 on February 1, 2021. This aligns precisely with the parameters displayed in the exhibit.

As confirmed in Microsoft documentation ("Configure role settings in Azure AD PIM"), activation settings define how long a user can remain active after approval, and group approvers allow any member of that group to approve activations.

NEW QUESTION: 109

You have a Microsoft 365 E5 subscription.

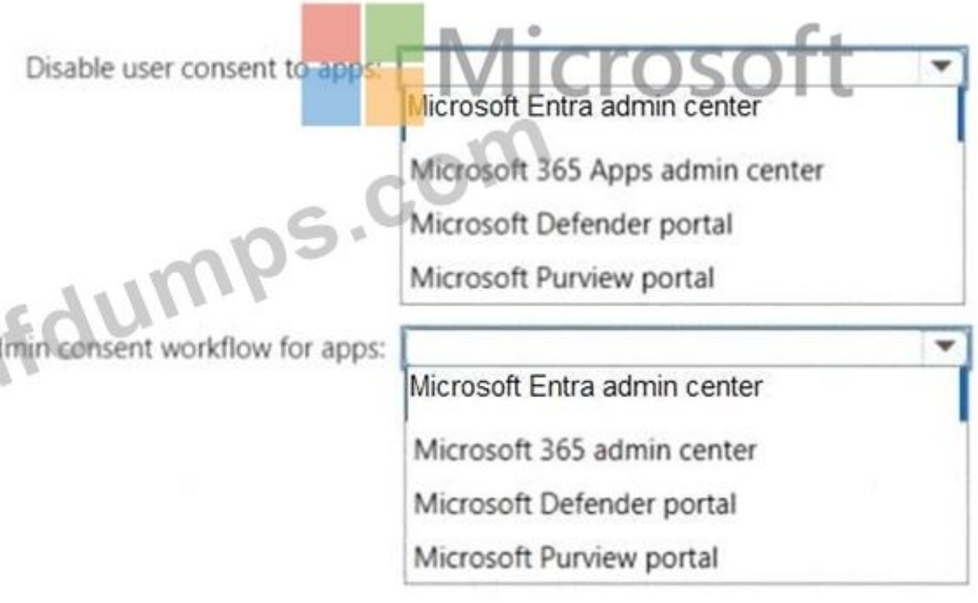
You need to configure app consent for the subscription. The solution must meet the following requirements:

* Disable user consent to apps.
* Configure admin consent workflow for apps.

Which portal should you use for each requirement? To answer, select the appropriate options in the answer area.

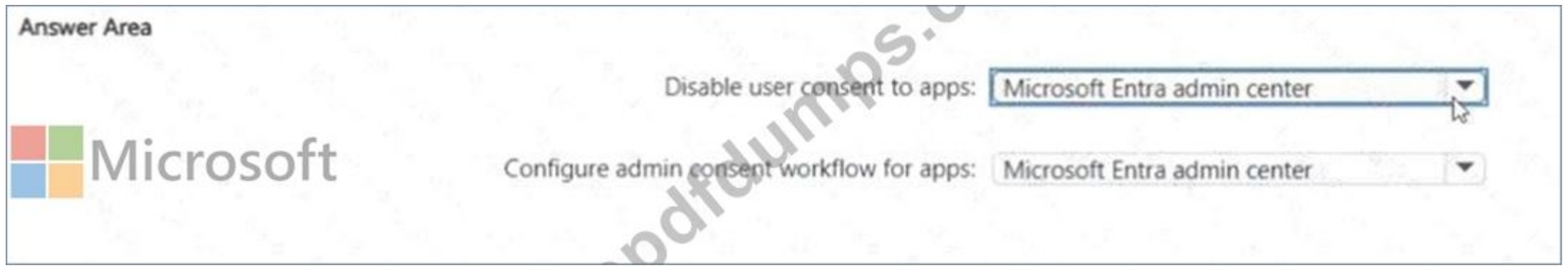
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:



NEW QUESTION: 110

You have an Azure AD tenant that contains the groups shown in the following table.

Name	Owner	Number of internal users	Number of guest users
Group1	User1	500	25
Group2	User2	295	100

You create an access review for Group1 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	All users
Reviewers	Users review own access

You create an access review for Group2 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	Guest users only
Reviewers	Group owner

What is the minimum number of Azure AD Premium P2 licenses requi red for each group? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Based on the official Microsoft SC-300 study guide and Microsoft Entra ID (Azure AD) licensing documentation, the licensing requirement for Access Reviews depends on who is being reviewed and how the review is configured .

Access reviews are an Azure AD Premium P2 feature (included in Microsoft 365 E5), and the licensing model specifies that:

"Each user who is part of an access review (either being reviewed or reviewing) must have an Azure AD Premium P2 license, except in cases where guest users are reviewed by internal reviewers - in that case, only the reviewers require a license." Let's analyze each configuration:

* Members: 500 internal + 25 guest users = 525 total members.
* Review Type: Teams + Groups
* Review Scope: All users
* Reviewers: Users review own access

Group1 Since all users (internal and guest) review their own access, every member is considered an active participant in the review. Therefore, each of the 525 members (500 internal + 25 guests) must have an Azure AD Premium P2 license.

Group1 = 525 licenses required

* Members: 295 internal + 100 guest users = 395 total members.
* Review Type: Teams + Groups
* Review Scope: Guest users only
* Reviewers: Group owner

Group2 Here, only guest users are being reviewed, and the reviewer is the group owner (User2). Since the guest users don't require licenses when being reviewed by an internal reviewer, only the group owner (User2) needs a P2 license.

Group2 = 1 license required

According to Microsoft Licensing Guidance (SC-300 Official Content):

"If guest users review their own access, each guest requires a P2 license. If the review is conducted by an internal user (owner or admin), only that reviewer requires the license."

NEW QUESTION: 111

Task 1
You need to deploy multi factor authentication (MFA). The solution must meet the following requirements:
* Require MFA registration only for members of the Sg-Finance group.
* Exclude Debra Berger from having to register for MFA.
* Implement the solution without using a Conditional Access policy.

Answer:

See the Explanation for the complete step by step solution.

Explanation:

To deploy Multi-Factor Authentication (MFA) for only the members of the Sg-Finance group, excluding Debra Berger, and without using a Conditional Access policy, you can follow these steps:

* Open the Microsoft Entra admin center:
* Sign in as a Security Administrator or Global Administrator.
* Navigate to MFA settings:
* Go to Users > Active users.
* On the Active users page, select Multi-factor authentication.
* Manage user settings:
* Find and select the Sg-Finance group.
* Enable MFA for this group by setting the requirement status to Enabled.
* Exclude a user from MFA:
* In the Multi-factor authentication page, search for Debra Berger.
* Set her MFA status to Disabled to exclude her from MFA registration.
* Verify the configuration:
* Ensure that all members of the Sg-Finance group have MFA enabled except for Debra Berger.
* Communicate the change:
* Inform the Sg-Finance group members about the MFA requirement and provide instructions on how to register for MFA.
* Monitor the setup:
* Check the sign-in logs to confirm that MFA is being prompted for the Sg-Finance group members and not for Debra Berger.

NEW QUESTION: 112

You have a Microsoft Entra tenant that contains a user named User1.

You have an Azure subscription named Sub1. User1 is assigned the Owner role for Sub1.

You need to ensure that User1 can onboard Sub1 to Microsoft Entra Permissions Management The solution must follow the principle of least pri vilege.

Which role should you assign for Sub1, and which role should you assign to User1 for the tenant? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

Explanation:

According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and official Microsoft Learn documentation ("Onboard Azure subscriptions to Microsoft Entra Permissions Management"), onboarding an Azure subscription to Microsoft Entra Permissions Management (EPM) requires a combination of Azure RBAC and Entra role permissions.
Step 1 - Azure (Sub1) Scope At the subscription level, the person onboarding must be able to grant the Permissions Management service principal access to the subscription. This requires "Microsoft.Authorization
/*/Write" permissions, which are included in the User Access Administrator and Owner roles.
However, applying the principle of least privilege, Microsoft recommends User Access Administrator rather than Owner because the Owner role includes full management rights to all resources, which exceeds what's needed for onboarding. The User Access Administrator role allows assigning roles and permissions but not managing resource content.
"Assign the User Access Administrator role at the subscription level to grant permissions needed to onboard into Permissions Management while following least-privilege principles." (Reference: SC-300 Exam Guide, Module "Implement and manage Microsoft Entra Permissions Management.") Step 2 - Microsoft Entra (Tenant) Scope At the tenant level, onboarding actions (such as connecting the subscription, managing connectors, and configuring data ingestion) require a directory role that grants access to EPM features. Microsoft documentation specifies that the Permissions Management Administrator role provides this exact access.
"The Permissions Management Administrator role is required in the Entra tena nt to configure connectors and manage onboarded cloud environments." The Global Administrator or Security Administrator could perform this task but would violate the least- privilege requirement since their permissions are far broader.
Final Selection: Sco pe
Role
Explanation:
Sub1
User Access Administrator
Allows assigning required permissions to onboard subscription
Tenant
Permissions Management Administrator
Provides the necessary rights to onboard and manage Permissions Management

NEW QUESTION: 113
You have an Azure AD tenant that contains a user named User1 and the conditional access policies shown in the following table.

Name	Status	Conditional access requirement
CAPolicy1	On	Users connect from a trusted IP address.
CAPolicy2	On	Users' devices are marked as compliant.
CAPolicy3	Report-only	The sign-in risk of users is low.

You need to evaluate which policies will be applied User1 when User1 attempts to sign-in from various IP addresses.
Which feature should you use?
A. Access reviews

B. Identity Secure Score
C. The What If tool
D. the Microsoft 365 network connectivity test tool
Answer: C (LEAVE A REPLY)
According to Microsoft Entra Conditional Access documentation and the SC-300 study guide, the What If tool in Azure AD is specifically designed to simulate Conditional Access policy results for a given user scenario. It allows administrators to input details such as user identity, location (IP address), device state, and application to determine which Conditional Access policies would apply before actual enforcement.
From Microsoft documentation:
"The What If tool allows admins to simulate a sign-in event for a specific user and evaluate which Conditional Access policies will be applied or excluded." Other options do not serve this function:
* Access Reviews: Used for periodic access validation, not policy simulation.
* Identity Secure Score: Provides improvement recommendations, not policy evaluation.
* Microsoft 365 network connectivity test tool: Tests network connectivity, not policy application.

NEW QUESTION: 114
You have an Azure subscription that contains an Azure SQL database named db1.
You deploy an Azure App Service web app named App1 that provide product information to us ers that connect to App1 anonymously.
You need to provide App1 with Access to db1. The solution must meet the following requirements:
* Credentials must only be available to App1.
* Administrative effort must be minimized.
Which type of credentials should you use?
A. a user-assigned managed identity
B. an Azure AD user account
C. A SQL Server account
D. a system-assigned managed identity
Answer: (SHOW ANSWER)
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn documentation on Managed Identities for Azure Resources , the recommended and most secure method for an Azure resource (like an App Service) to access another Azure resource (such as an Azure SQL Database) is through Managed Identities.
Managed identities allow Azure services to authenticate securely to other Azure services that support Azure AD authentication, without requiring the use of credentials stored in code, configuration files, or key vaults.
There are two types of managed identities:
* System-assigned managed identity
* Created and tied directly to the lifecycle of a specific Azure resource (e.g., App Service).
* When the resource (App1) is deleted, the identity is automatically deleted as well.
* Best suited when a single resource requires authentication to access another Azure service.
* User-assigned managed identity
* Created as an independent Azure resource.
* Can be assigned to multiple services and managed separately.
* Useful for scenarios requiring shared identity or cross-service authentication management.
* App1 (Azure App Service) must access db1 (Azure SQL Database).
* Credentials should be available only to App1, meaning other resources should not share or reuse the identity.

* Administrative effort should be minimized, implying automatic management of credentials and lifecycle.
Scenario Analysis: Hence, a system-assigned managed identity is the best solution because it meets all three conditions:
* No manual credential management (Azure handles authentication token issuance automatically).
* The identity exists only for App1 (it's unique to that resource).
* Simplified lifecycle - identity is created and deleted automatically with App1.
# Official Microsoft Documentation (aligned with SC-300 exam objectives):
"System-assigned managed identities are ideal for scenarios where a single Azure resource requires access to another Azure service and you want Azure to automatically manage the identity's lifecycle."
"Managed identities eliminate the need for developers to manage credentials in code or configuration files."

NEW QUESTION: 115
You have an Azure AD tenant that uses Azure AD Identity Pr otection and contains the resources shown in the following table.

Name	Type	Configuration
Risk1	User risk policy	Users that have a high severity risk must reset their password upon next sign-in.
User1	User	Not applicable

Azure Multi-Factor Authentication (MFA) is enabled for all users.
User1 triggers a medium severity alert that requires additional investigation.
You need to force User1 to reset his passwo rd the next time he signs in. the solution must minimize administrative effort.
What should you do?
A. Configure a sign-in risk policy.
B. Mark User1 as compromised.
C. Reconfigure the user risk policy to trigger on medium or low severity.
D. Reset the Azure MFA registration for User1.
Answer: B (LEAVE A REPLY)
According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and Microsoft Learn: "Azure AD Identity Protection - User Risk Policies and Remediation", Azure AD Identity Protection provides mechanisms to automatically or manually remediate risky user accounts based on detected user risk levels (low, medium, high).
The scenario states:
* A User risk policy (Risk1) exists that requires users with a high severity risk to reset their password upon next sign-in.
* User1 has triggered a medium severity alert, not high.
* The goal is to force User1 to reset his password on the next sign-in, with minimal administrative effort.
* A. Configure a sign-in risk policy: This policy targets sign-in risks (suspicious sign-ins), not user risks, and would not directly force a password reset - it only enforces MFA or blocks access.
* B. Mark User1 as compromised: # When an administrator marks a user as compromised in Azure AD Identity Protection, it immediately elevates the user's risk level to "high." Since the existing User risk policy (Risk1) automatically forces password reset for high-risk users, User1 will be required to change his password the next time he signs in - satisfying the requirement automatically. This approach uses the existing configuration, meeting the "minimize administrative effort" criterion.
* C. Reconfigure the user risk policy to trigger on medium or low severity: This would affect all users globally, not just User1, which is not minimal effort and could increase false positives.
* D. Reset the Azure MFA registration for User1: This affects MFA credentials, not password resets, and doesn't remediate risk.
Analysis of Options: From Microsoft's documentation:
"Marking a user as compromised increases their risk level to High, triggering any configured user risk policy to require password reset upon next sign-in." Therefore, the most efficient and compliant action according to Microsoft's SC-300 study materials is to mark User1 as compromised.

NEW QUESTION: 116
You have an Azure Active Directory (Azure AD) tenant that contains the following objects:
A device named Device1
Users named User1, User2, User3, User4, and User5
Groups named Group1, Group2, Group3, Group4, and Group5
The groups are configured as shown in the following table.

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group3
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?
A. Group1 and Group4 only
B. Group1, Group2, Group3, Group4, and Group5
C. Group1 and Group2 only
D. Group1 only
E. Group1, Group2, Group4, and Group5 only
Answer: E (LEAVE A REPLY)
SC-300 teaches that group-based licensing supports security groups and Microsoft 365 groups, with assigned or dynamic user membership. The guide states: "Licenses can be assigned to groups whose members are users ; nested groups aren't processed and devices cannot be licensed ." Applying this to the table: Group1 (Security-Assigned) and Group2 (Security-Dynamic User) are valid; Group4 (Microsoft 365-Assigned) and Group5 (Microsoft 365-Dynamic User) are also valid. Group3 is a Security-Dynamic Device group and therefore ineligible because "device objects do not receive user licenses." Consequently, the Office 365 E5 license can be assigned directly to Group1, Group2, Group4, and Group5 only.

NEW QUESTION: 117
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 Microsoft 365 E5 subscription.
You create a user named User1.
You need to ensure that User1 can update the status of identity Secure Score improvement actions.
Solution: You assign the User Administrator role to User1.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Expla nation:
The User Administrator role allows management of user accounts, licenses, and group memberships within Azure AD but does not grant access to security configurations, Secure Score dashboards, or improvement actions.
According to Microsoft's Secure Score documentation:
"Only users with Global Administrator, Security Administrator, or Security Reader roles can access Microsoft Secure Score. To modify improvement action statuses, the user must be a

Security Administrator or Global Administrator." Therefore, a User Administrator cannot update Secure Score improvement actions.

NEW QUESTION: 118
Task 3
You need to add the LinkedIn application as a resource to the Sales and Marketing access package. The solution must NOT remove any other resources from the access package.
Answer:
See the Explanation for the complete step by step solution.
Explanation:
To add the LinkedIn application as a resource to the Sales and Marketing access package without removing any other resources, you can follow these steps:
Sign in to the Microsoft Entra admin center:
Ensure you have the role of Global Administrator or Identity Governance Administrator.
Navigate to Entitlement Management:
Go to Identity governance > Entitlement management > Access packages1.
Select the Sales and Marketing access package:
Find and select the Sales and Marketing access package to modify it.
Add a new resource:
Within the access package details, select Resources.
Click on + Add resource.
Search for and select the LinkedIn application from the list of available resources.
Configure the resource role:
Assign the appropriate role for the LinkedIn application that users in the Sales and Marketing access package will have.
Review and update the access package:
Ensure that the LinkedIn application has been added as a resource.
Confirm that no other resources have been removed from the access package.
Save the changes:
After reviewing, save the changes to the access package.
Communicate the update:
Notify the relevant users about the addition of the LinkedIn application to their access package.
By following these steps, you will successfully add the LinkedIn application to the Sales and Marketing access package without affecting the other resources.

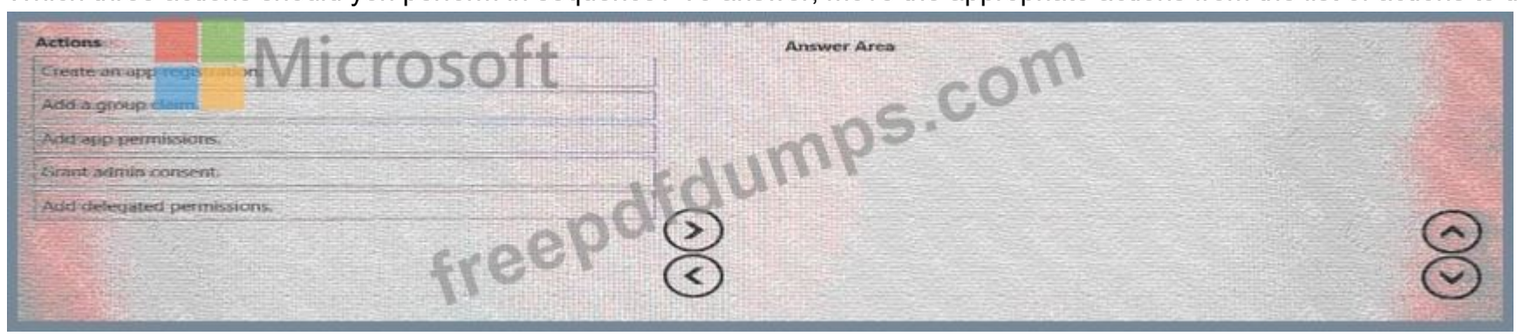
NEW QUESTION: 119
You need to configure the detection of multi-staged attacks to meet the monitoring requirements.
What should you do?
A. Customize the Azure S entinel rule logic.
B. Create a workbook.
C. Add Azure Sentinel data connectors.
D. Add an Azure Sentinel playbook.
Answer: A (LEAVE A REPLY)
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "M onitor and respond to Azure AD events with Azure Sentinel" , multi-staged attacks are advanced threat scenarios that require correlation of multiple events - for example, a suspicious sign-in followed by abnormal Office 365 activity.
The scenario in the question states:

"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." Azure Sentinel's Fusion rule is a built-in, machine-learning-driven correlation rule that automatically detects multi-stage attacks by analyzing anomalies across multiple data sources such as Azure AD sign-in logs, Office 365 activity, and security alerts.
However, to fine-tune detection or meet specific organizational monitoring requirements, administrators can customize the rule logic in Sentinel analytics. This allows you to define how different signals and events are correlated, what thresholds trigger an alert, and how Sentinel interprets combined anomalies.
Microsoft documentation states:
"Fusion uses correlation logic in analytics rules to detect complex multi-stage attacks. Administrators can customize rule logic to meet specific detection requirements and fine-tune alert sensitivity ." The other options do not meet the requirement:
* B. Create a workbook # Used for visualization and reporting, not detection.
* C. Add data connectors # Used to ingest data sources; this is already configured.
* D. Add a playbook # Used for automated response, not for detection logic configuration.
# Correct Answer: A. Customize the Azure Sentinel rule logic

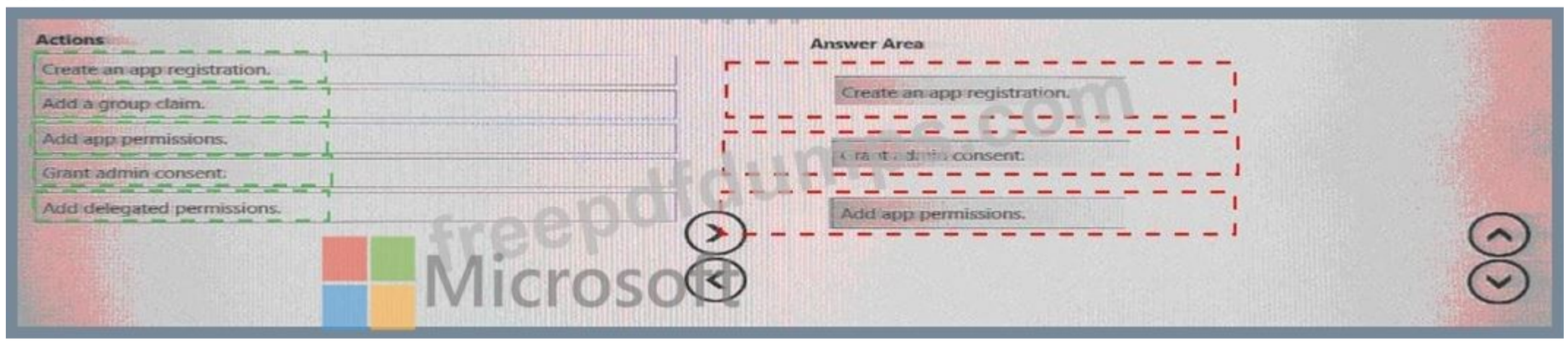
NEW QUESTION: 120
You have multiple on-premises devices that run either Windows or Linux.
You have a Microsoft 365 E5 subscription.
You configure Microsoft Entra Internet Access.
You need to ensure that all the on-premises devices route internet traffic through Global Secure Access for security policy evaluation.
What should you do in the Microsoft Entra admin center?
A. Deploy the Global Secure Access client.
B. Create a remote network.
C. Create a named location.
D. Create an access package.
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Microsoft Entra Internet Access, Global Secure Access, and the requirements for routing internet traffic from on-premises devices, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding the Scenario and Requirements:
On-premises devices running Windows or Linux:The devices are located in an on-premises environment (e.g., a corporate office or branch) and run either Windows or Linux operating systems.
Microsoft 365 E5 subscription:This subscription includes Microsoft Entra ID P2 and Microsoft Entra Internet Access, which are part of the Global Secure Access suite. This provides the necessary licensing for the solution.
Microsoft Entra Internet Access:This is a Secure Web Gateway (SWG) solution that securesinternet and SaaS app access by routing traffic through Microsoft's Security Service Edge (SSE) for policy evaluation (e.g., web content filtering, Conditional Access).
Requirement:All on-premises devices must route their internet traffic through Global Secure Access for security policy evaluation. Global Secure Access is the unified framework for Microsoft Entra Internet Access and Microsoft Entra Private Access, providing a centralized way to manage network traffic security.
How Global Secure Access Routes Internet Traffic:
Global Secure Access can route internet traffic in two primary ways:
Global Secure Access Client:This client is installed on individual devices (e.g., Windows, macOS, Android, iOS) and routes traffic from the device to Microsoft's SSE for policy evaluation. The client is user-aware and integrates with Microsoft Entra ID for identity-based policies.
Remote Network:This method creates an IPsec tunnel between an on-premises network (e.g., a branch office) and Microsoft's SSE. All internet-bound traffic from devices in the network is

routed through the tunnel for security policy evaluation, without requiring a client on each device.
The question involvesmultiple on-premises devicesrunning Windows or Linux, which suggests a network- level solution may be more practical than installing a client on each device, especially since Linux support for the Global Secure Access client is limited.

NEW QUESTION: 121
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.
The comp any is developing a web service named App1.
You need to ensure that App1 can use Microsoft Graph to read directory data in contoso.com.
Which three actions should yon 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:

According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn module "Implement and manage enterprise applications," when developing an application that needs to access Microsoft Graph or other protected APIs on behalf of an organization, you must perform several configuration steps within Azure Active Directory (Azure AD).

Step 1 - Create an app registration:
Every application that requires access to Microsoft Graph must be registered in Azure AD. The registration process establishes an identity for the app and generates an Application (client) ID and a directory (tenant) ID.
This is done in Azure portal # Azure Active Directory # App registrations # New registration . This enables Azure AD to issue tokens to the app.
Step 2 - Add app permissions:
After registration, you must configure permissions under API permissions in the app's registration settings.
For server-to-server access (no user sign-in), Application permissions are used; for delegated access (on behalf of a user), Delegated permissions are added. In this case, since App1 will read directory data from Microsoft Graph, you assign the Microsoft Graph # Directory.Read.All permission.
Step 3 - Grant admin consent:
Application permissions require admin consent before the app can access directory data. An Azure AD administrator must grant these permissions by selecting "Grant admin consent for contoso.com." This allows the app to use the permissions organization-wide.
From Microsoft's documentation:
"To enable an application to call Microsoft Graph, register the app, configure required API permissions, and grant admin consent for those permissions."
Correct Answer Order:
* Create an app registration
* Add app permissions
* Grant admin consent

NEW QUESTION: 122
You need to resolve the issue of I-.Group1. What should you do first?
A. Recreate the IT-Group 1 group.
B. Change Members hip type of IT-Group1 to Dynamic Device
C. Add an owner to IT_Group1.
D. Change Membership type of IT-Group1 to Dynamic User
Answer: A (LEAVE A REPLY)
Assigning built-in directory roles (like Device Administrators) to a group requires a role-assignable group.
The SC-300 documentation explains: "You can assign Azure AD roles to a cloud security group by creating the group with the setting 'Azure AD roles can be assigned to the group.'" It further emphasizes: "This attribute is immutable; you must decide at cr eation time. You cannot convert an existing group to be role- assignable later." When a standard security group is not created as role-assignable, it will not appear in the picker when attempting to assign a directory role-exactly the behavior observed: "gr oups that aren't role- assignable cannot be selected for Azure AD role assignments." Therefore, the first step is to recreate IT_Group1 as a role-assignable security group (often called an "eligible for role assignment" group) and then assign the Device Administrators role to that group. Changing membership types (Dynamic User or Dynamic Device) or adding owners does not convert an existing group into a role-assignable one and thus would not resolve the issue.

NEW QUESTION: 123
You have a Microsoft 36S subscription. The subscription contains users that use Microsoft Outlook 2016 and Outlook 2013 clients. You need to implement tenant restrictions. The solution

must minimize administrative effort. What should you do first?

A. Upgrade the Outlook 2013 clients to Outlook 2016.

B. Configure the Outlook 2013 clients to use modem authentication.

C. Upgrade all the Outlook clients to Outlook 2019.

D. From the Exchange admin center, configure Organization Sharing.

Answer: A (LEAVE A REPLY)

Tenant Restrictions in Microsoft 365 are designed to prevent users from accessing external tenants while allowing access to approved tenants. According to the SC-300 exam material and Microsoft's Tenant Restrictions documentation, only modern authentication-capable clients (OAuth 2.0) can enforce tenant restrictions.

Outlook 2013 by default uses basic authentication, which does not support tenant restrictions. Outlook

2016 (and later versions) use modern authentication, making them compatible.

Microsoft Documentation: "Tenant restrictions require modern authentication to enforce access control.

Legacy clients like Outlook 2013 must be upgraded to Outlook 2016 or newer."

NEW QUESTION: 124

You have an Azure Active Directory (Azure AD) tenant.

You need to review the Azure AD sign-in logs to investigate sign-ins that occurred in the pa st.

For how long does Azure AD store events in the sign-in logs?

A. 14 days

B. 30 days

C. 90 days

D. 365 days

Answer: A (LEAVE A REPLY)

In Azure AD Monitoring and Reporting documentation and the SC-300 Study Guide (Module: Monitor and report on identity and access) , sign-in logs in Azure Active Directory are retained for a default duration of 14 days.

The sign-in logs contain information about user sign-in activity, including application usage, conditional access policies, and multi-factor authentication details. These logs are accessible through the Azure portal # Azure Active Directory # Sign-ins, or programmatically via Microsoft Graph.

Microsoft specifies:
"Azure AD stores sign-in activity for 14 days by default. For longer retention, you must integrate w ith Azure Monitor (Log Analytics), Azure Storage, or Event Hub." This 14-day retention limit applies to tenants without additional premium log retention solutions.

NEW QUESTION: 125

You have a Microsoft Entra tenant that contains two remote networks named RemoteNetworkl and RemoteNetwork2 and the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1
User3	Group2

You have the devices shown in the following table.

Answer:

Explanation:

NEW QUESTION: 126

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
Group1	Group that has the Assigned membership type
App1	Enterprise application in Azure Active Directory (Azure AD)
Contributor	Azure subscription role
Role1	Azure Active Directory (Azure AD) role

For which resources can you create an access review?

A. Group1, App1, Contributor, and Role1
B. Hotel and Contributor only
C. Group1, Role1, and Contributor only
D. Group1 only

Answer: A (LEAVE A REPLY)

Access reviews require an Azure AD Premium P2 license.

Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.

Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start- security-review?toc=/azure/active-directory/governance/toc.json

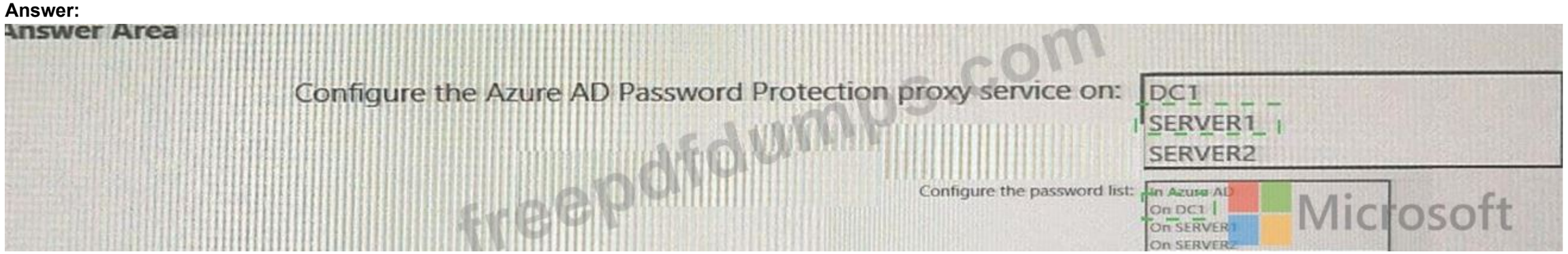
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview According to the Microsoft Identity and Access Administrator (SC-300) official study guide and

Microsoft Learn training module "Manage Access Reviews", Azure AD Access Reviews allow administrators to periodically evaluate user access to critical resources across Azure AD and Azure.
The exam objectives explicitly list access review capabilities that apply to the following resource types:
Groups (Microsoft 365 or security groups) - Access reviews can be used to ensure that group memberships are up to date. In this case, Group1 is eligible since it has an Assigned membership type, which means access reviews can target its members.
Enterprise applications (App1) - Access reviews can assess users who have access to enterprise applications registered in Azure AD, ensuring that only the right users retain application access.
Azure AD roles (Role1) - Access reviews can be created for privileged directory roles (like Global Administrator or custom roles such as Role1) to validate continued need for elevated permissions.
Azure subscription roles (Contributor) - Access reviews can also be applied to Azure resources and management groups when integrated with Azure AD Privileged Identity Management (PIM). This ensures least-privilege access by reviewing roles like "Contributor." Therefore, based on Microsoft documentation:
"Access reviews can be configured for Azure AD groups, enterprise applications, Azure AD roles, and Azure resource roles to ensure that access rights remain appropriate." This means all four - Group1, App1, Contributor, and Role1 - are supported targets for access reviews.

NEW QUESTION: 127
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Conditional Access policies. You need to block access to cloud apps when a user is assessed as high risk.
Which type of policy should you create in the Microsoft Defender for Cloud Apps?
A. OAuth app policy
B. anomaly detection polio
C. access policy
D. activity policy
Answer: (SHOW ANSWER)
According to the Microsoft SC-300 Study Guide and Microsoft Defender for Cloud Apps documentation, an access policy in Microsoft Defender for Cloud Apps (MCAS) enables administrators to enforce real-time session control and conditional access based on user risk or session context. These policies integrate directly with Azure AD Conditional Access and Microsoft Defender for Identity signals to determine when a user's session should be allowed, monitored, or blocked.
The documentation specifies:
"Access policies are used to control user access and session activities in real-time. You can use these policies to block access, require session control, or limit downloads when risk conditions such as 'user risk = high' are detected." In this case, since the requirement is to block access to cloud apps when a user is assessed as high risk, an access policy in Defender for Cloud Apps must be used. Other options are not applicable because:
* OAuth app policy controls permissions granted to third-party apps.
* Anomaly detection policy detects unusual activities but does not block access.
* Activity policy monitors specific user actions within apps.

NEW QUESTION: 128
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 cor rect 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.

NEW QUESTION: 129

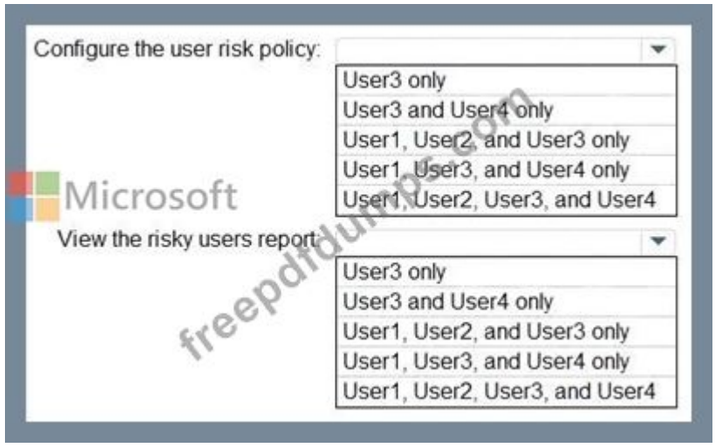
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Role
User1	Conditional Access administrator
User2	Authentication administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure AD Identity Protection.

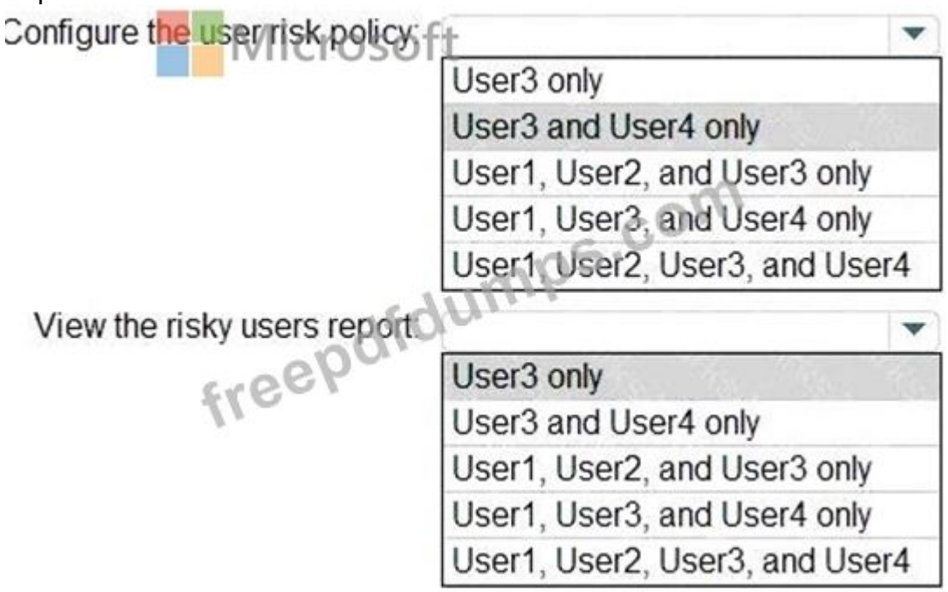
Which users can configure the user risk policy, and which users can view the risky users report? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



According to the Microsoft SC-300: Identity and Access Administrator Study Guide and official documentation for Azure AD Identity Protection , the ability to configure and view risk-based policies depends on the administrative roles assigned in Azure AD.

* User Risk Policy Configuration: The user risk policy determines how Azure AD responds when a user's sign-in is determined to be risky. According to the Microso ft Learn documentation:

"Only users assigned the Global Administrator, Security Administrator, or Conditional Access Administrator roles can create and manage risk policies in Azure AD Identity Protection." In the scenario, User3 is the Security Administra tor , which gives full rights to configure both sign-in risk and user risk policies. Although User1 (Conditional Access Administrator) can manage Conditional Access policies, only Security Administrator or Global Administrator can configure the user risk po licy in Identity Protection. Therefore, User3 only can perform this configuration.
* Viewing Risky Users Report: Viewing Identity Protection reports, including risky users , risky sign- ins , and risk detections , can be done by users with the following roles:
"Security Reader, Security Operator, Security Administrator, and Global Administrator can view Identity Protection reports." This means both User3 (Security Administrator) and User4 (Security Operator) can access and view these reports.

NEW QUESTION: 130
You have an Azure subscription that contains a storage account named storage1.
You plan to deploy an app named App1 that will be hosted on multiple virtual machines. The virtual machines will authenticate to a Third-party API by using secrets You need to recommend an authentication solution for the virtual machines The solution must meet the following requirements
* Securely store secrets.
* Ensure that credentials do NOT need to be stored in the App1 code.
* Ensure that the virtual machines can access Azure resources by using Microsoft Entra authentication.
* Minimize administrative effort.
What should you include in the recommendation?
A. user accounts and Storage Service Encryption
B. user accounts and Azure Key Vault
C. user-assigned managed identities and Azure Key Vault
D. system-assigned managed identities and Storage Service Encryption
Answer: C (LEAVE A REPLY)
SC-300 materials explain that managed identities for Azure resources provide an automatically managed identity in Microsoft Entra ID that apps can use to request tokens, thereby "eliminat[ing] the need to manage credentials" and avoiding secrets in code. They also state that Azure Key Vault is the recommended store for secrets and that apps should access Key Vault by presenting an Entra token from a managed identity rather than an embedded key. For scenarios with multiple virtual machines running the same workload, the guidance highlights user-assigned managed identities: they are created as standalone identities and "can be assigned to one or more instances," which means you grant Key Vault access once to the shared identity and attach it to all VMs. This minimizes administration compared to system-assigned identities (which are tied 1:1 to each VM lifecycle). With this approach, the VMs obtain Entra tokens via the user-assigned managed identity to call Azure resources and to authenticate to Key Vault; the application then retrieves the third-party API secret from Key Vault at runtime. This meets all requirements: secrets are securely stored, no credentials in code, VMs use Entra authentication, and operational effort is reduced by reusing a single identity across the VM fleet.

NEW QUESTION: 131
You have an Azure subscription named Sub1.
You plan to deploy Microsoft Entra Permissions Management.
You need to ensure that Permission Management can onboard Sub1. The solution must follow the principle of least privilege.
How should you complete the PowerShell command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

In Microsoft Entra Permissions Management (formerly CloudKnox), onboarding an Azure subscription requires granting the Permissions Management service principal the minimum rights needed to discover identities, roles, and permissions across that subscription. The SC-300 materials emphasize the principle of least privilege for onboarding: assign Reader at the subscription scope so the service can inventory resources and permissions without the ability to change them. After onboarding, if you want automated remediation/right-sizing, you can additionally grant User Access Administrator (or perform changes manually), but that elevation is not required merely to onboard and collect data.
Accordingly, you complete the PowerShell by creating an RBAC assignment for the application (service principal) at the subscription scope using New-AzRoleAssignment and specifying -RoleDefinitionName Reader. Creating a new custom role (New-AzRoleDefinition) is unnecessary, and New-AzTag is unrelated to RBAC. Choosing Owner or Contributor would exceed the access required for onboarding and violate least-privilege guidance. The correct, minimal configuration is therefore: assign Reader to the Permissions Management application at the /subscriptions/<SubscriptionId> scope using New-AzRoleAssignment.

NEW QUESTION: 132

You have a Microsoft Entra tenant named contoso.com.

You plan to bulk invite business-to-business (B2B) collaboration users.

Which two parameters must you include when you create the bulk invite file? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. username

B. email address

C. password

D. shared key

E. redirection URL
Answer: B,E (LEAVE A REPLY)

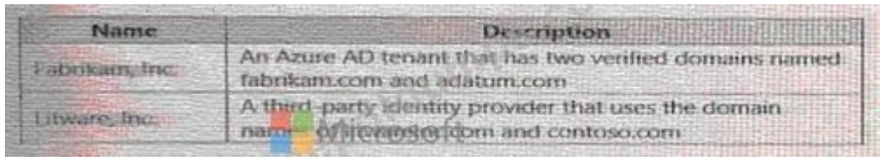
NEW QUESTION: 133
You cr eate a conditional access policy that blocks access when a user triggers a high-seventy sign-in alert.
You need to test the policy under the following conditions;
* A user signs in from another country.
* A user triggers a sign-in risk.
What should you use to complete the test?
A. the Conditional Access What If tool
B. sign-ins logs in Azure AD
C. access reviews in Azure AD
D. the activity logs in Microsoft Defender for Cloud Apps
Answer: A (LEAVE A REPLY)
The Conditional Access What If tool is designed to simulate sign-ins under various conditions to test Conditional Access policies without performing real sign-ins . Microsoft's SC-300 guide specifies that this tool is essential for validating the effect of a policy based on user, location, device, or risk l evel.
In this case, the administrator wants to test a policy that blocks access when a high-severity sign-in alert (sign-in risk) occurs and when a user signs in from another country . These scenarios are based on risk and location conditions-both supported in the What If tool simulation.
Microsoft Learn: "Use the What If tool to simulate sign-ins and verify whether a specific Conditional Access policy will be applied."

NEW QUESTION: 134
You have a Microso ft 365 tenant.
You currently allow email clients that use Basic authentication to conned to Microsoft Exchange Online.
You need to ensure that users can connect t to Exchange only run email clients that use Modern authentication protocols.
What should you implement?
You need to ensure that use Modern authentication
A. a compliance policy in Microsoft Endpoint Manager
B. a conditional access policy in Azure Active Directory (Azure AD)
C. an application control profile in Microsoft Endpoint Manager
D. an OAuth policy in Microsoft Cloud App Security
Answer: B (LEAVE A REPLY)
In Microsoft 365, Basic authentication is an outdated protocol that sends credentials in plain text and does not support MFA. To enforce Modern authentication (OAuth 2.0), which is required for stronger identity protection and token-based access, administrators must block legacy authentication using Conditional Access policies in Azure AD.
According to the SC-300 study guide and Microsoft Learn module "Implement Conditional Access policies" , this can be achieved by:
* Creating a Conditional Access policy in Azure AD.
* Targeting the Exchange Online cloud app.
* Setting the condition Client apps # Other clients (legacy authentication) to block access.
Modern authentication clients (like Outlook 2016+, Outlook on the web, and Outlook mobile) use secure OAuth tokens that comply with Conditional Access requirements (such as MFA, device compliance, or trusted location).
Compliance policies or application control profiles in Microsoft Endpoint Manager do not manage authentication protocols, and Microsoft Cloud App Security OAuth policies govern third-party app permissions, not Exchange connectivity.

Therefore, the correct approach to ensure only Modern authentication clients can connect is to enforce this through a Conditional Access policy in Azure AD.

NEW QUESTION: 135

Your company has an Azure Active Directory (Azure AD) tenant named contosri.com. The company has the business partners shown in the following table.



Name	Description
Fabrikam, Inc.	An Azure AD tenant that has two verified domains named fabrikam.com and adatum.com
Litware, Inc.	A third-party identity provider that uses the domain name of litwareinc.com and contoso.com

users can request access by using package 1.

Users at Fabrikam and Litware us e ail then respective domain names for email addresses.

You plan to create an access package named packaqe1 that will be accessible only to the Fabrikam and Litware users.

You need to configure connected organizations for Fabrikam and litware so that any o f their users can request access by using package1.

What is the minimum of connected organization that you should create.

A. 1

B. 2

C. 3

D. 4

Answer: B (LEAVE A REPLY)

According to the official Microsoft SC-300: Microsoft Identity and Access Administrator St udy Guide and Exam Ref SC-300 textbook, when configuring Entitlement Management in Azure AD Identity Governance

, connected organizations are used to define which external directories or domains are allowed to request access to specific access packages. A c onnected organization represents a single external organization whose users can be invited as guests (B2B collaboration users) or allowed to request access packages.

Each connected organization is identified by its verified domain names. For example, if yo u have two separate companies, Fabrikam, Inc. and Litware, Inc. , and they each have distinct verified domains - fabrikam.com, adatum.com (for Fabrikam), and litwareinc.com, contoso.com (for Litware) - they must each be configured as separate connected orga nizations because connected organizations are defined at the organization level, not per domain.

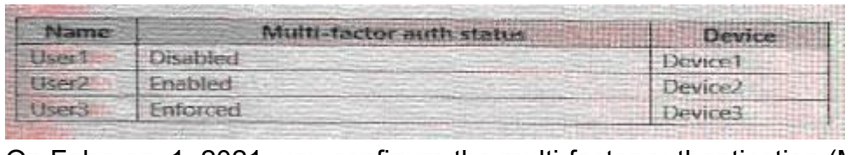
Even though each organization may have multiple verified domains, the configuration treats all of an organization's verified domains as part of the same connec ted organization.

Therefore, to allow users from both Fabrikam and Litware to request access to Package1 , you must create two connected organizations - one for Fabrikam and one for Litware.

This behavior is confirmed in Microsoft documentation and training modules under "Manage connected organizations" in Azure AD Entitlement Management, which states that "each external organization that requires access must have its own connected organization entry, regardless of how many domains it owns."

NEW QUESTION: 136

You create the Azure Active Directory (Azure AD) users shown in the following table.



Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

On February 1, 2021, you configure the multi-factor authentication (MFA) settings as shown in the following exhibit.

The users authentication to Azure AD on their devices as shown in the following table.

Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

On February 26, 2021, what will the multi-factor auth status be for each user?

A.

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

B.

Name	Multi-factor auth status
User1	Enabled
User2	Enabled
User3	Enabled

C.

Name	Multi-factor auth status
User1	Enforced
User2	Enforced
User3	Enforced

D.

Name	Multi-factor auth status
User1	Disabled
User2	Enforced
User3	Enforced

Answer: B (LEAVE A REPLY)

This scenario is based on how Azure AD Multi-Factor Authentication (MFA) statuses transition between Disabled, Enabled, and Enforced states, as documented in the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Microsoft Learn - Configure and deploy MFA in Azure Active Directory.

Let's analyze the details step-by-step using the exhibits:

* Initial MFA Configuration (February 1, 2021)
* User1: Disabled
* User2: Enabled
* User3: Enforced
* MFA Policy Setting
* "Allow users to remember multi-factor authentication on devices they trust" is enabled.
* "Number of days users can trust devices for" is 20 days.This means that once a user completes MFA on a trusted device, they won't be prompted again for 20 days on that same device.
* User Sign-in Activity:
* User1: Signs in on Feb 2 and again on Feb 21
* User2: Signs in on Feb 5
* User3: Already in Enforced state (so continuous MFA enforcement applies) State Transitions per Microsoft Documentation:
* Disabled: User cannot register or use MFA.
* Enabled: User is registered for MFA but not yet required at every sign-in. Once they complete registration, they remain Enabled until admin enforces it.
* Enforced: User must use MFA at every sign-in.

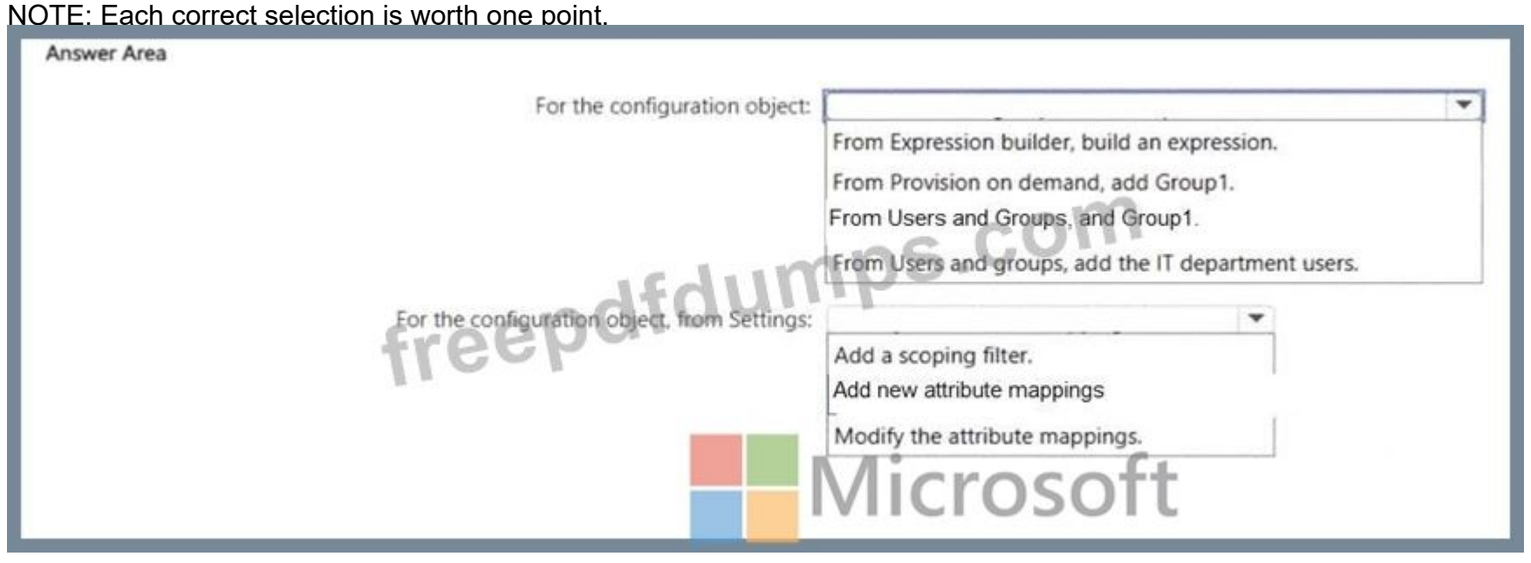
Timeline Evaluation:

* User1 was initially Disabled, so even though they sign in multiple times (Feb 2 and Feb 21), MFA remains disabled unless the admin manually changes the setting - therefore, User1 = Disabled.
* User2 was Enabled on Feb 1, and signed in on Feb 5 - this allows them to register for MFA (move from Enabled # Enforced) once registration completes. By Feb 26, they would be in Enforced state.
* User3 was already Enforced from the start, and their state remains unchanged.

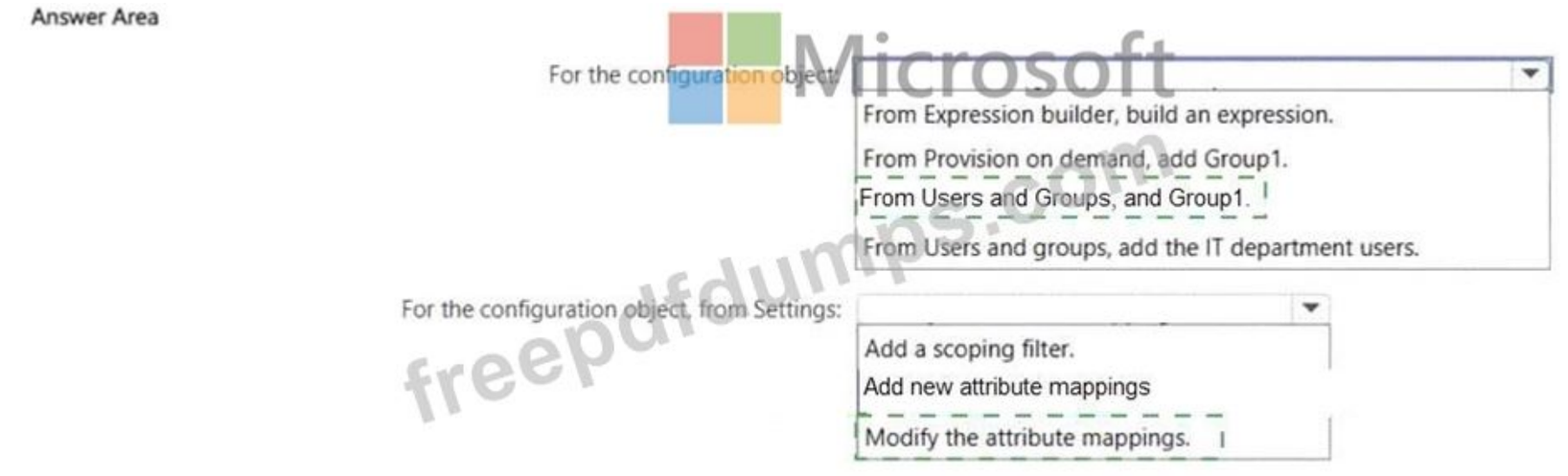
Thus, by February 26, 2021, the MFA status should be:

* User1: Disabled
* User2: Enforced
* User3: Enforced
This matches Option B exactly.
Microsoft references (Azure AD MFA Overview):
"Enabled users move to Enforced when they complete MFA registration. Enforced users must use MFA every time they sign in."

NEW QUESTION: 137
You have a Microsoft Entra tenant named contoso.com that contains a group named Groupl. Groupl contains
50 users in your company ' s IT department and 50 users in your company ' s accounts department You have a partner company that has a Microsoft Entra tenant named fabrikam.com.
You configure cross-tenant synchronization between contoso.com and fabrikam.com.
You need to sync the members of Group1 to fabrikam.com. The solution must meet the following requirements:
* Ensure that only the IT department users sync with fabrikam.com
* Minimize administrative effort.
What should you do in the Cross-tenant synchronization settings? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

NEW QUESTION: 138

You have an Azure subscription named Sub1 that uses Microsoft Entra Permissions Management. Sub1 contains a user named User1. User1 is granted multiple permissions across Sub1.

You need to replace all the permissions granted to User1 with read-only permissions. The solution must minimize administrative effort.

What should you do on the Remediation tab in Permissions Management?

A. From the Roles/Policies subtab. create a role.

B. From the My Requests subtab, create a new request.

C. From the Permissions subtab, use a quick a ction.

D. From the Role/Policy Template subtab. create a template.

Answer: C (LEAVE A REPLY)

Within the Remediation tab of Microsoft Entra Permissions Management, the Permissions subtab allows you to view, filter, and manage the permissions directly assign ed to identities. It supports operations such as Read

, Update , and Delete on granted permissions.

If you need to change a user's permissions (for example, reduce all of User1's permissions to read-only), the quick action capability in the Permissions subta b is the most efficient method. Using the quick action, you can right-size, remove, or adjust permissions for a user in bulk across their assigned permissions. This is less administrative effort than creating new roles or templates The Roles/Policies subta b (option A) deals with role definitions (CRUD operations), not directly editing a given user's permissions.

The My Requests subtab (option B) is for requesting elevated permissions, not for bulk modifying existing assignments.

The Role/Policy Template tab (option D) is for defining templates; using them is less direct and more overhead when you already have assignments to adjust.

Hence, the correct and minimal-effort choice is to use the quick action in the Permissions subtab of the Remediation tab to chan ge User1's permissions to read-only.

NEW QUESTION: 139

You need to meet the planned changes and technical requirements for App1.
What should you implement?
A. a policy set in Microsoft Endpoint Manager
B. an app configuratifon policy in Micros oft Endpoint Manager
C. an app registration in Azure AD
D. Azure AD Application Proxy
Answer: (SHOW ANSWER)
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "Publish on-premises apps for remote access using Azure AD Application Proxy", Azure AD Application Proxy enables secure remote access to internal, on-premises web applications without requiring VPN access.
In the scenario, App1 is an on-premises application hosted within the Litware network, and the technical requirements specify that it must be securely accessible to both internal and external users - including Fabrikam guest accounts - through Azure AD authentication.
Microsoft's official documentation states:
"Azure AD Application Proxy provides se cure remote access to on-premises web applications, integrating with Azure AD for single sign-on (SSO) and conditional access policies." Given that the environment already includes a server (SERVER1) running the Azure AD Application Proxy connector, and that Litware wants to enforce Azure AD Conditional Access and MFA for App1, Azure AD Application Proxy is the correct implementation.
The other options are not suitable:
* A. Policy set in Microsoft Endpoint Manager: Used for device compliance and app management, not for publishing on-premises apps.
* B. App configuration policy in Endpoint Manager: Used for mobile app configuration (e.g., MAM policies), not for access publishing.
* C. App registration in Azure AD: Used for modern cloud or SaaS apps integration, but App1 is on- premises and needs proxy access.
answer: D. Azure AD Application Proxy
Topic 2, Litware, IncOverview
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 V PN 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 s ynchronization 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 litw are.com by using gu est 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 s ubscription 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 au dit 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 Pri vileged 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 conta in all the Azure AD user accountsfor 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.

NEW QUESTION: 140

You need implement the planned changes for application access to organizational data. What should you configure?

A. authentication methods

B. the User consent settings

C. access packages

D. an application proxy

Answer: B (LEAVE A REPLY)

The requirement is:

"Require admin approval for application access to organizational data." According to the Microsoft SC-300 exam guide and Microsoft documentation on "Configure consent settings for applications", Azure AD provides User consent settings under Enterprise applications # Consent and permissions to control how applications can request permissions to access organizational data.

By default, users can consent to allow apps to access organizational data on their behalf, which can create security risks. To ensure tighter control, administrators can:

* Disable user consent entirely, or
* Require admin consent workflow so that when users try to grant an app access, it must first be approved by an administrator.

The SC-300 study materials explicitly describe:

"To require administrator approval before an app can access organizational data, configure the User consent settings to use the admin consent workflow." This aligns perfectly with the stated requirement - to ensure admin approval is required before apps gain access to organizational data.

Other options are incorrect:

* Authentication methods manage MFA and SSPR, not app consent.
* Access packages are part of Identity Governance for resource access, not app consent.
* Application Proxy publishes on-premises apps, not related to app consent permissions.

NEW QUESTION: 141

You havean Azure AD tenant that contains the users shown in the following table.

Name	Role
Admin1	Cloud application administrator
Admin2	Application administrator
Admin3	Security administrator
User1	None

You add an enterprise application named App1 to Azure AD and set User1 as the owner of App1 requires admin c onsent to access Azure AD before the app can be used.

You configure the Admin consent requests strong as shown in the following exhibit.

Admin consent requests.

A. Admm1 only

B. Admm1 and Admin2 only
C. Admm1 Admm2 and Admin3 only
D. Admln1, Admin2. and User1 only
E. Admm1 Admm2. Admm3, and User1
Answer: (SHOW ANSWER)
This scenario involves Admin Consent Requests in Azure AD. When users try to use apps that require admin consent , requests are sent to designated reviewers who can approve or deny them.
* Admin1 : Cloud Application Administrator - can review and approve admin consent requests.
* Admin2 : Application Administrator - can review and approve admin consent requests.
* Admin3 : Security Administrator - cannot approve app consent requests because this ro le does not have application management privileges.
* User1 : No role assigned - can be listed as a reviewer but cannot approve , only receive notifications.
From Microsoft Documentation:
"Only users with sufficient permissions, such as the Application Adminis trator or Cloud Application Administrator roles, can grant admin consent in response to consent requests."
Therefore, only Admin1 and Admin2 meet the requirement to review and approve.

NEW QUESTION: 142
You have an Azure subscription named Sub1 ilia1 contains a storage account named storage1. You need to deploy two apps named App1 and App2 that will have the following configurations:
* App1 will be deployed as a registered app in Sub1.
* App1 will access storage1 by using Microsoft Entra authentication.
* App2 will access storage1 by using a single Microsoft Entra identity.
* App2 be hosted on two new virtual machines named VM1 and VM2.
The solution must minimize administrative effort.
Which type of identity will each app use to access storage1? To answer, select the appropriate options in the answer area.

Answer:

Answer Area

Explanation:

In SC-300 materials covering Microsoft Entra application identities and managed identities for Azure resources, an app you register in the tenant is represented for access control by a service principal: "An application registration creates an application object in its home tenant and a corresponding service principal in any tenant where the app is used. The service principal is the identity used for sign-in, consent, and authorization to resources." This aligns with App1 being a registered app that must authenticate to Storage by Microsoft Entra; the principal you grant roles to on the storage account is the service principal of that app.

For App2, the requirement is to access Storage "by using a single Microsoft Entra identity" while the workload runs on two VMs (VM1 and VM2). SC-300 explains: "A user-assigned managed identity is an independent Azure resource. You can assign the same user-assigned identity to one or more Azure resources." In contrast, "A system-assigned managed identity is enabled on a single Azure resource and is deleted with that resource." Because App2 must share one identity across multiple hosts, the correct choice is a user- assigned managed identity, which provides a single, reusable identity whose lifecycle is separate from VM1 and VM2 and can be granted Storage roles once and used by both machines.

NEW QUESTION: 143

Your company has a Microsoft 365 tenant.

The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.

The users are prohibited from having a mobile phone in the call center.

You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft
365
services.

What should you include in the solution?

A. a named network location

B. the Microsoft Authenticator app

C. Windows Hello for Business authentication

D. FIDO2 tokens

Answer: D (LEAVE A REPLY)

SC-300 materials describe FIDO2 security keys as a passwordless method that works well for shared workstations and environments where phones are not permitted. The documentation explains that "FIDO2 security keys are phishing-resistant, standards-based credentials that allow users to sign in with a portable hardware device" and that "the user performs a gesture on the key (PIN or biometrics) to complete authentication." It further clarifies that "Azure AD passwordless methods (FIDO2 security keys, Windows Hello for Business, Authenticator) satisfy

strong authentication requirements and can meet MFA prompts." Because the call-center computers don't have biometrics and phones are prohibited, Authenticator and Windows Hello for Business are unsuitable. A named network location does not provide MFA by itself. By issuing FIDO2 keys (tokens) to agents, you meet the MFA requirement with a factor the user has (the key) plus a secure local gesture (PIN), which SC-300 documents as accepted for Azure AD strong/MFA.

NEW QUESTION: 144

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2019	Domain controller
Server2	Windows Server 2019	Domain controller
Server3	Windows Server 2019	Azure AD Connect

The domain controllers are prevented from communicating to the internet.

You implement Azure AD Password Protection on Server1 and Server2.

You deploy a new server named Server4 that runs Windows Server 2019.

You need to ensure that Azure AD Password Protection will continue to work if a single server fails.

What should you implement on Server4?

A. Azure AD Connect

B. Azure AD Application Proxy

C. Password Change Notification Service (PCNS)

D. the Azure AD Password Protection proxy service

Answer: D (LEAVE A REPLY)

According to the Microsoft SC-300 official exam reference and Microsoft's official documentation, Azure AD Password Protection provides password policy enforcement and banned password protection for both cloud and on-premises environments.

The solution requires two primary components:

* Domain Controllers (DC Agents) - enforce password policies within the domain.

* Proxy Service (Azure AD Password Protection Proxy) - communicates with Azure AD to download the latest password policies and banned password lists and then shares them with the DC agents.

In the scenario, Server1 and Server2 are domain controllers that already have Azure AD Password Protection installed but cannot communicate with the internet directly. That means they rely on the proxy service running on a separate server to connect securely to Azure AD.

To ensure high availability, Microsoft recommends deploying at least two proxy servers. This ensures continuous synchronization of the password policy even if one proxy fails.

From the Microsoft documentation:

"For redundancy, deploy at least two proxy servers. The proxy service retrieves the global and custom banned password lists from Azure AD and replicates them to all domain controllers running the DC agent." Thus, installing the Azure AD Password Protection proxy service on Server4 ensures service continuity if one of the proxy servers fails.

NEW QUESTION: 145

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 s tated 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 th e review screen.

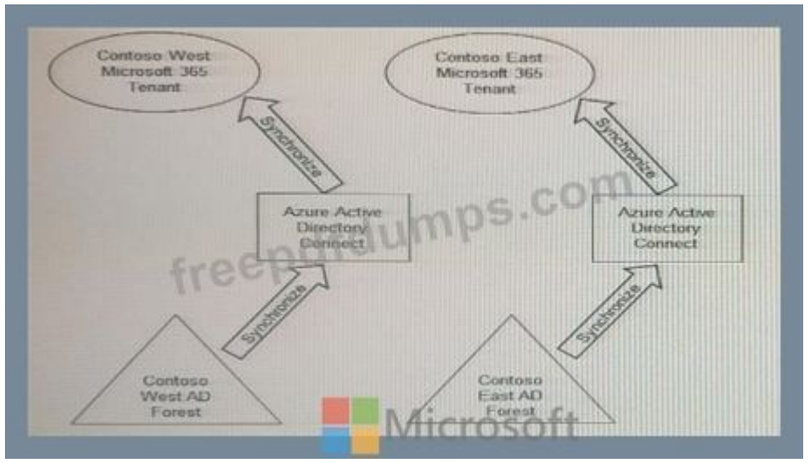
You have an Active Directory forest that syncs to a Microsoft Entra tenant.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Microsoft Entra for up to 30 minutes.

You need t o ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Microsoft Entra.

Solution: You configure Microsoft Entra Password Protection.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
The SC-300 curriculum emphasizes synchronization behavior between on-premises Active Directory (AD) and Microsoft Entra ID using Microsoft Entra Connect. By default, directory synchronization occurs every 30 minutes, which means a user dis abled in AD can still authenticate to Microsoft Entra for up to 30 minutes until the next synchronization cycle.
The proposed solution- Microsoft Entra Password Protection -is not related to authentication delay or sign-in blocking. Password Protection enforces strong password policies and prevents the use of weak or compromised passwords during account creation or reset. It does not control sign-in states or enforce real- time disablement.
To meet the goal of immediately blocking authentication when an a ccount is disabled in AD, you must implement Microsoft Entra Connect with Pass-through Authentication (PTA) or federation (AD FS) .
These options validate sign-ins against the on-premises AD in real time, ensuring instant blocking of disabled accounts.
Micr osoft documentation confirms:
"Password Protection does not affect authentication latency or synchronization frequency. To ensure disabled accounts cannot sign in, use Pass-through Authentication or federation for real-time validation."

NEW QUESTION: 146
Your company has two divisions named Contoso East and Contoso West. The Microsoft 365 identity architecture tor both divisions is shown in the following exhibit.



You need to assign users from the Contoso East division access to Microsoft SharePoint Online sites in the Contoso West tenant. The solution must not require additional Microsoft 3G5 licenses.
What should you do?
A. Configure the exiting Azure AD Connect server in Contoso Cast to sync the Contoso East Active Directory forest to th e Contoso West tenant.
B. Configure Azure AD Application Proxy in the Contoso West tenant.
C. Deploy a second Azure AD Connect server to Contoso East and configure the server to sync the Contoso East Active Directory forest to the Contoso West tenant.
D. I nvite the Contoso East users as guests in the Contoso West tenant.
Answer: D (LEAVE A REPLY)
In SC-300, Microsoft emphasizes Azure AD B2B collaboration for cross-tenant access without extra Microsoft 365 licensing. The guidance explains that organizations can invite external users as guests to their tenant to access Microsoft 365 resources such as SharePoint Online and Teams , and guest access does not require an additional Microsoft 365 license for the guest . The host tenant remains licensed for the workloa ds being accessed, and Azure AD billing for B2B collaboration is handled through External Identities (MAU) if configured. The study con tent also notes that synchronizing a single on-premises AD forest to multiple Azure AD tenants is not a supported topolog y with a single Azure AD Connect server, and

deploying another AAD Connect to sync the same identities to a second tenant introduces complexity and is unnecessary when the requirement is simply to let users in one tenant access resources in another. Applic ation Proxy (publishing on-prem apps) is unrelated to granting SharePoint Online cross-tenant access. Therefore, the minimum-effort, license-compliant approach is to invite Contoso East users as B2B guests in the Contoso West tenant and assign them the req uired SharePoint permissions.

NEW QUESTION: 147
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: (SHOW ANSWER)
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.

NEW QUESTION: 148
You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant syncs to an on-premis es Active Directory domain.
You plan to create an emergency-access administrative account named Emergency1. Emergency1 will be assigned the Global administrator role in Azure AD. Emergency1 will be used in the event of Azure AD functionality failures and o n-premises infrastructure failures.
You need to reduce the likelihood that Emergency1 will be prevented from signing in during an emergency.
What should you do?
A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.
B. Require Azure AD Privileged Identity Management (PIM) activation of the Global administrator role forEmergency1.
C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporatenetwork.
D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.
Answer: D (LEAVE A REPLY)
According to Microsoft's official SC-300 Identity and Access Administrator study guide and Microsoft Learn module: Manage emergency access accounts in Azur e AD , an emergency access (break-glass) account must always be configured to maintain administrative control during service outages or authentication failures. The study material explicitly emphasizes that these accounts must not rely on on-premises infrastructure or Conditional Access policies that could block sign-ins in an emergency. The recommended configuration is to exclude the emergency account from Conditional Access rules, enable cloud-only authentication, and require strong authentication (MFA) to prevent compromise.
The exam guide states:
"Emergency access accounts should be cloud-only, assigned the Global Administrator role, and configured with multi-factor authentication that does not depend on the organization's normal identity provider or on- premises systems." Options like restricting sign-in to corporate networks (Option C) or requiring Privileged Identity Management activation (Option B) could

lock out access if the Azure AD or network is unavailable. Azure Monitor alerts (Option A) help with monitoring but do not prevent sign-in issues. Therefore, the correct answer per Microsoft's best practice is to enforce MFA for the account to ensure security without relying on on-premises dependencies.

NEW QUESTION: 149
You have an Azure subscription that contains a user named User1 and an Azure Key Vault named Vault1.
You need to ensure that User1 can read the metadata of certificates, keys, and secrets stored in Vault1. The solution must follow the principle of least privilege.
Which role should you assign to User1?
A. Key Vault Crypto User
B. Key Vault Crypto Officer
C. Key Vault Reader
D. Key Vault Secrets User
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Azure Key Vault roles, permissions, and the principle of least privilege, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Azure Key Vault and the Requirement:
Azure Key Vault is a service that securely stores and manages cryptographic keys, secrets, and certificates. It uses role-based access control (RBAC) to manage permissions for users, groups, and applications.
The question requires that User1 canread the metadataof certificates, keys, and secrets in Vault1. In Azure Key Vault, "metadata" refers to the properties of these objects (e.g., name, creation date, expiration date), not the actual content (e.g., the secret value, key value, or certificate private key).
The solution must follow theprinciple of least privilege, meaning User1 should be granted the minimum permissions necessary to perform the task, without access to unnecessary actions (e.g., modifying or deleting objects).
Azure Key Vault RBAC Roles and Permissions:
Azure Key Vault supports built-in RBAC roles that define specific permissions for managing keys, secrets, and certificates. Let's examine each role in the options:
Key Vault Crypto User:
This role allows a user to perform cryptographic operations using keys (e.g., encrypt, decrypt, sign, verify) and to read key metadata.
Permissions include: Microsoft.KeyVault/vaults/keys/read (read key metadata) and cryptographic operations like encrypt, decrypt, etc.
However, this role does not grant permissions to read metadata for secrets or certificates, and it includes cryptographic operation permissions, which are not needed for the task.
Key Vault Crypto Officer:
This role is designed for managing keys and performing cryptographic operations. It includes permissions to create, delete, update, and read keys, as well as perform cryptographic operations.
Permissions include: Microsoft.KeyVault/vaults/keys/* (full control over keys).
This role does not grant access to secrets or certificates and provides more permissions than needed (e.g., create, delete), violating the principle of least privilege.
Key Vault Reader:
This role provides read-only access to the metadata of all objects in the Key Vault (keys, secrets, and certificates).
Permissions include: Microsoft.KeyVault/vaults/read (read vault properties) and Microsoft.KeyVault/vaults/*
/read (read metadata for keys, secrets, and certificates).
Importantly, this role does not allow access to the actual content of the objects (e.g., the secret value, key value, or certificate private key), only the metadata. It also does not allow write operations (e.g., create, update, delete).
This aligns perfectly with the requirement to "read the metadata" and follows the principle of least privilege.
Key Vault Secrets User:

This role allows a user to read the content of secrets (not just metadata) and perform operations like getting the secret value.
Permissions include: Microsoft.KeyVault/vaults/secrets/get (read secret values) and Microsoft.KeyVault
/vaults/secrets/read (read secret metadata).
This role does not grant access to keys or certificates, and it provides more access than needed (reading the secret value, not just metadata), violating the principle of least privilege.
Applying the Principle of Least Privilege:
The task requires User1 to read the metadata of certificates, keys, and secrets, but not to access their content or perform any write operations.
Key Vault Readeris the most appropriate role because:
It grants read-only access to the metadata of all objects (keys, secrets, certificates).
It does not allow access to the content of the objects (e.g., secret values), which is not required.
It does not allow write operations (e.g., create, delete), adhering to the principle of least privilege.
The other roles either provide too much access (e.g., Key Vault Crypto Officer, Key Vault Secrets User) or do not cover all required objects (e.g., Key Vault Crypto User, Key Vault Secrets User).
Analysis of the Options:
A: Key Vault Crypto User:
Incorrect. This role only allows reading key metadata and performing cryptographic operations, but it does not provide access to secrets or certificates metadata. It also grants unnecessary cryptographic permissions.
B: Key Vault Crypto Officer:
Incorrect. This role provides full control over keys, which is far more than needed, and does not grant access to secrets or certificates metadata.
C: Key Vault Reader:
Correct. This role provides read-only access to the metadata of keys, secrets, and certificates, exactly matching the requirement while following the principle of least privilege.
D: Key Vault Secrets User:
Incorrect. This role allows reading secret values (not just metadata) and does not provide access to keys or certificates metadata. It grants more access than needed.
Additional Considerations:
If the question had asked for User1 to read the content of secrets (not just metadata), the Key Vault Secrets User role might be considered, but it still wouldn't cover keys and certificates.
Custom RBAC roles could be created to fine-tune permissions, but the question asks for a built-in role, and Key Vault Reader is the best fit.
The question does not specify whether User1 needs to perform other actions (e.g., cryptographic operations, managing the vault). If additional permissions were needed, a combination of roles or a custom role might be required, but the principle of least privilege guides us to the minimal role.
Conclusion:To ensure User1 can read the metadata of certificates, keys, and secrets in Vault1 while following the principle of least privilege, theKey Vault Readerrole should be assigned.
This role provides the exact permissions needed without granting unnecessary access. Therefore, the correct answer isC.
References:
Azure Key Vault documentation: "Azure Key Vault RBAC roles" (Microsoft Learn:https://learn.microsoft.
com/en-us/azure/key-vault/general/rbac-guide)
Azure Key Vault documentation: "Secure access to a key vault" (Microsoft Learn:https://learn.microsoft.com
/en-us/azure/key-vault/general/secure-your-key-vault)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers Azure Key Vault access control and the principle of least privilege.

NEW QUESTION: 150
You have 2,500 users who are assigned Microsoft Office 365 Enterpris e E3 licenses. The licenses are assigned to individual users.
From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.
You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.
What should you use?

A. the Identity Governance blade in the Azure Active Directory admin center
B. the Set-AzureAdUser cmdlet
C. the Licenses blade in the Azure Active Directory admin center
D. the Set-WindowsProductKey cmdlet
Answer: (SHOW ANSWER)
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Microsoft Learn module "Manage licenses in Azure Active Directory", the most efficient way to manage or remove product licenses from a large group of users is by using group-based licensing through the Licenses blade in the Azure Active Directory admin center.
In this scenario:
* 2,500 users were individually assigned Office 365 E3 licenses.
* The same users are now assigned Microsoft 365 E5 licenses via group assignment (using group-based licensing).
When a user is assigned a license directly and later receives another license through a group, Azure AD continues to track both - the direct and inherited assignments. To remove the E3 licenses efficiently, you can use the Licenses blade to remove all direct assignments in bulk rather than editing each user individually.
* In the Azure AD admin center, navigate to: Azure Active Directory # Licenses # All products # Office 365 E3.
* Select Licensed users.
* Select all users (or filter based on the direct assignment type).
* Click Remove license assignment to remove the E3 licenses.
Step-by-Step (as per Microsoft documentation): This method removes the E3 licenses for all directly assigned users in a single operation-achieving the goal with the least administrative effort.
* A. Identity Governance blade: Used for access reviews, entitlement management, and lifecycle workflows-not license management.
* B. Set-AzureADUser cmdlet: Manages user properties but does not directly manage license assignments (you would need Set-AzureADUserLicense or Set-MgUserLicense , which is more manual).
* D. Set-WindowsProductKey cmdlet: Used for activating Windows OS, not Microsoft 365 licensing.
Why the other options are incorrect:

NEW QUESTION: 151
You have an Azure Active Directory (Azure AD) tenant that contains Azure AD Privileged Identity Management (PIM) role settings for the User administrator role as shown in the following exhibit.

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

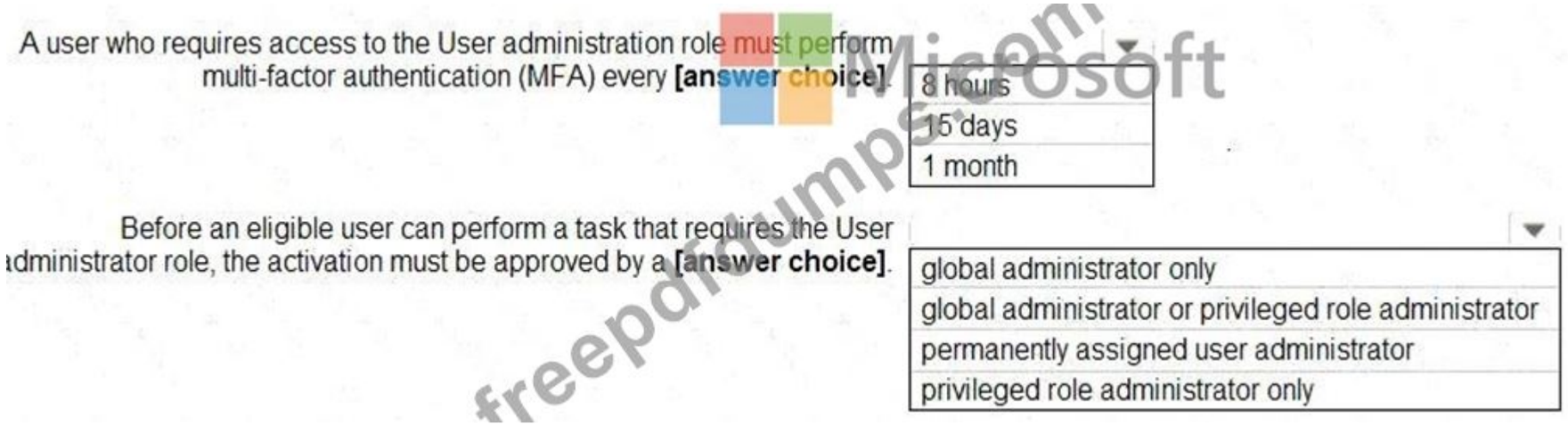
Activation

SETTING	STATE
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	None

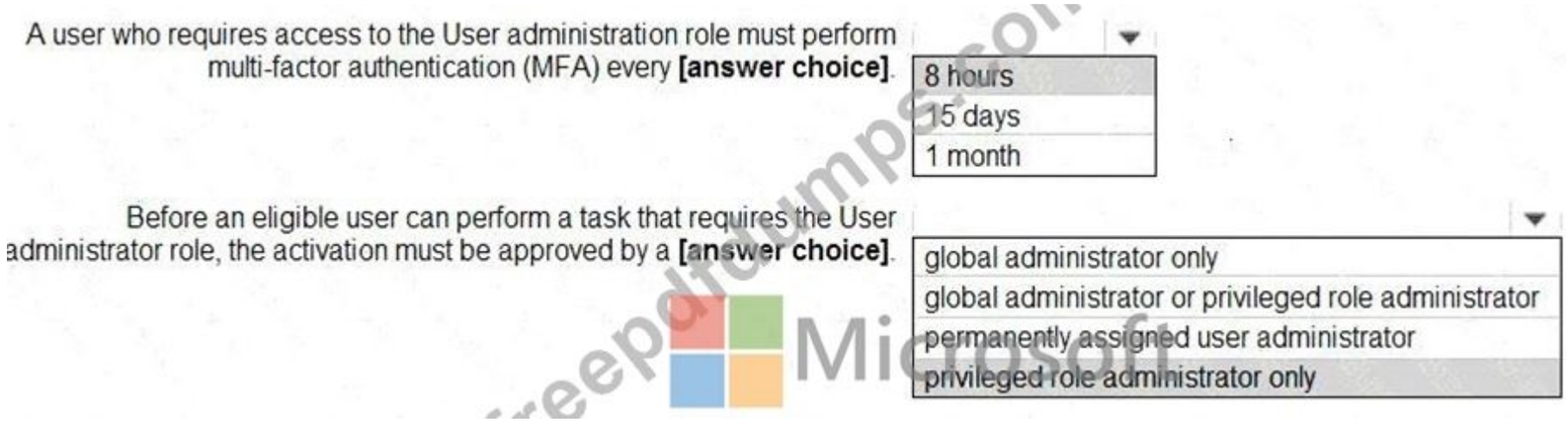
Assignment

SETTING	STATE
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

Use the drop-down menus to select the answer choice that compl etes each statement based on the information presented in the graphic.
NOTE:Each correct selection is worth one point.



Answer:



In Azure AD Privileged Identity Management (PIM), MFA can be enforced at role activation. The setting "On activation, require Azure MFA: Yes" means a user must complete MFA each time they activate the role.
Because the "Activation maximum duration (hours)" is 8 hours, any user who needs the User Administrator role beyond that window must re-activate the role and therefore perform MFA again. The study guide explains: "Requiring MFA on activation ensures strong verification at the moment privileges are eleva ted." It also states: "Activation maximum duration controls how long the user holds the role before needing to re- activate." For approvals, the role settings show "Require approval to activate: Yes" and "Approvers: None." PIM behavior for Azure AD roles is that "if no approver list is configured for a role, activation requests are routed to Privileged Role Administrators and Global Administrators." The exam materials emphasize: "Privileged Role Administrator manages role settings, including approval workflows, and can approve eligible activations; Global Administrator also has approval capability when no explicit approvers are defined." Therefore, the correct selections are 8 hours for MFA (per activation window) and global administrator or privileged role administrator as the approver when none are explicitly assigned.

NEW QUESTION: 152
Task 10
You need to create a group named Audit. The solution must ensure that the members of Audit can activate the Security Reader role.

Answer:
See the Explanation for the complete step by step solution.
Explanation:
To create a group named "Audit" and ensure that its members can activate the Security Reader role, follow these steps:
* Open the Microsoft Entra admin center:
* Sign in with an account that has the Security Administrator or Global Administrator role.
* Navigate to Groups:
* Go to Teams & groups > Active teams and groups1.
* Create the security group:
* Select Add a security group.
* On the Set up the basics page, enter "Audit" as the group name.
* Add a description if necessary and choose Next1.
* Edit settings:
* On the Edit settings page, select whether you want Microsoft Entra roles to be assignable to this group and select Next1.
* Assign roles:
* After creating the group, go to Roles > All roles.
* Find and select the Security Reader role.
* Under Assignments, choose Assign.
* Select the "Audit" group to assign the role to its members2.
* Review and finish:
* Review the settings to ensure the "Audit" group is created with the ability for its members to activate the Security Reader role.
* Finish the setup and save the changes.
By following these steps, you will have created the "Audit" group and enabled its members to activate the Security Reader role, which allows them to view security-related information without having permissions to change it. Remember to communicate the new group and role assignment to the relevant stakeholders in your organization.

NEW QUESTION: 153
You have a Microsoft Entra tenant that contains a terms of use (ToU) named Terms1. You create a Conditional Access policy named Policy1 to deploy Terms1. You need to configure Policy1 to require users to accept Terms1. Which settings should you configure for Policy1?
A. Conditions
B. Session
C. Grant
D. Target resources
Answer: (SHOW ANSWER)
Conditional Access policies evaluate Assignments (users, cloud apps), optional Conditions , and then enforce Access controls . In SC-300, Terms of use (ToU) is enforced via Grant controls : the policy must " require terms of use " so that users must accept a specified ToU before access is granted. The documentation states that the ToU experience is applied when a policy includes the control to " require terms of use ," and this control lives under the Grant section (alongside controls like require MFA, require compliant device, etc.
). Therefore, to deploy Terms1 with Policy1 , configure the Grant controls and select Require terms of use and choose Terms1 . Conditions or Session settings do not trigger ToU acceptance; they refine when or how access is permitted. Target resources select apps, but the enforcement of acceptance is strictly a Grant control.

NEW QUESTION: 154
You have a Microsoft 365 subscription.

You plan to deploy an app named App1 that will have the following configurations:
* Will be registered in Microsoft Entra
* Will run as a service wit hout user interaction
* Will collect audit logs associated with user sign-ins
* Will access resources by using the Microsoft Graph API
You need to ensure that App1 can access Microsoft Graph.
What should you use?
A. application permissions
B. delegated per missions
C. a custom role-based access control (RBAC) role
D. a built-in role-based access control (RBAC) role
Answer: (SHOW ANSWER)
In Microsoft Entra (Azure AD) app registrations, permissions are categorized as either delegated or application.
* Delegated permissions are used when an app acts on behalf of a user who is signed in.
* Application permissions are used when an app acts as itself, without user interaction - typically for background services, daemons, or APIs.
Because App1 is a service application that will:
* Run without user interaction,
* Access the Microsoft Graph API, and
* Collect audit logs (sign-in logs) -
It requires application permissions such as AuditLog.Read.All or Directory.Read.All granted to the app identity itself.
Microsoft documentation states:
"Applications that run as background services or daemons use application permissions when calling Microsoft Graph APIs that access organization data without a signed-in user."

NEW QUESTION: 155
You have a Microsoft 365 E5 subscription.
You need to ensure that users are prompted to accept a custom terms of use (Toll) agreement when they sign in to the subscription.
What should you configure?
A. an access package
B. a Conditional Access policy
C. a lifecycle workflow
D. an authentication method
Answer: B (LEAVE A REPLY)
To enforce a Terms of Use (ToU) prompt when users sign in, the SC-300 exam and Microsoft Learn materials specify configuring it under a Conditional Access policy. The ToU object must first be created in Microsoft Entra ID # Identity Governance # Terms of Use, then linked to a Conditional Access policy via Grant Controls # Require Terms of Use.
Access packages and lifecycle workflows (A, C) handle identity lifecycle and provisioning, not authentication- time prompts. Authentication methods (D) manage how users sign in but not policy-based ToU enforcement.

NEW QUESTION: 156
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 Microsoft 365 tenant.
All users m ust use the Microsoft Authenticator app for multi-factor authentication (MFA) whenaccessing Microsoft 365 services.
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.
You need to block the users automatically when they report an MFA request that they did not initiate.
Solution: From the Azure portal, you configure the Notifications settings for multi-factor authentication (MFA).
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
E xplanation:
In the SC-300 materials covering Azure AD MFA configuration, Microsoft distinguishes between Notifications (which control whether the Microsoft Authenticator sends push prompts) and Fraud alert settings (which determine what happens when a user reports an unexpected prompt). The study guide notes that notifications "enable push approvals to the app," but this does not take action when a user reports a suspicious prompt. To satisfy the requirement "block the users automatically when they report an MFA request they didn't initiate," you must use Fraud alert options. The documentation states that administrators can "allow users to submit fraud alerts" and "block users who report fraud" so that "reported accounts are immediately blocked until an administrator unblocks them." These options are part of the tenant's MFA service settings, not the Notifications section. In other words, simply configuring Notifications won't automatically block users who tap Report in Microsoft Authenticator; you must explicitly enable the setting to block users upon fraud reports. Therefore, the proposed solution-changing Notifications settings-does not meet the goal. The correct approach is to enable Fraud alert and select Block users who report fraud, ensuring automatic protection when users report unexpected MFA prompts.

NEW QUESTION: 157
Your company has a Microsoft Entra tenant that contains a user named User 1.
The company has two departments named marketing and finance.
You need to grant permissions to User1 to manage only the users in the marketing department.
What should you create first?
A. an administrative unit
B. a Microsoft 365 group
C. a management group
D. a resource group
Answer: (SHOW ANSWER)
The Microsoft SC-300 Exam Ref and Microsoft Learn module: "Manage administrative units" specify that administrative units (AUs) are used to delegate administrative permissions over subsets of users or groups within an Entra tenant.
In this scenario, the goal is to allow User1 to manage only the users in the marketing department. The correct approach is to create an administrative unit (AU) for the marketing department and then assign User1 an appropriate role (for example, User Administrator) scoped to that AU.
Microsoft 365 groups, management groups, and resource groups serve different purposes:
* Microsoft 365 groups are for collaboration.
* Management groups organize Azure subscriptions.
* Resource groups group Azure resources.
Only administrative units in Entra ID provide delegated role-based administration for user subsets.

NEW QUESTION: 158
You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server.

You enable Microsoft Entra login for the virtual machines.
Users report that they cannot sign in to the virtual machines by using their Microso ft Entra credentials.
You need to ensure that the users can sign in to the virtual machines.
What should you do first?
A. Ensure that the virtual machines can accesshttps://enterpriseregistration.windows.net.
B. Revoke the primary refresh token.
C. From the Microsoft Entra admin center, delete the device registrations of the virtual machines.
D. Enable SSH client support for OpenSSH.
Answer: (SHOW ANSWER)
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and Microsoft Learn documentation on "Enable Microsoft Entra login for Windows Server and Windows virtual machines in Azure", successful sign-in to Azure VMs using Microsoft Entra (formerly Azure AD) credentials requires network connectivity to specific Microsoft identity endpoints. One of the most critical endpoints is
https://enterpriseregistration.windows.net , which is used during the device registration and Microsoft Entra Join process.
When you enable Microsoft Entra login for Azure VMs, each VM must register itself as a device in the directory to allow authentication using Entra credentials. If the VM cannot reach the enterprise registration service, the registration fails, meaning the VM will not appear as a valid device in Entra ID. Consequently, users attempting to log in with their Entra credentials will encounter sign-in errors because the system cannot validate their device trust and user token against the identity service.
Microsoft documentation explicitly states:
"To enable Microsoft Entra sign-in to Windows VMs in Azure, the VM must be able to communicate with Microsoft Entra endpoints, including https://enterpriseregistration.windows.net , to complete device registration." Options B, C, and D are unrelated to initial configuration issues. Revoking refresh tokens or deleting device registrations would not resolve connectivity or registration failures. SSH support (option D) is applicable to Linux VMs, not Windows.

NEW QUESTION: 159
You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Department
User1	Marketing
User2	Marketing
User3	Engineering
User4	Engineering
User5	Finance
User6	Finance

The tenant contains the administrative units shown in the following table.

Name	Description
AU1	Contains all the users in the marketing department Contains all the resources for the marketing department Contains User1 and User2
AU2	Contains all the users in the engineering department Contains all the resources for the engineering department Contains User3 and User4
AU3	Contains Group4, User5, and User6,

You perform the following actions:
* Assign User1 the User Administrator role for AU2.
* Assign User3 the Groups Administrator role for AU1.
* Assign User5 the Authentication Administrator role for AU3.

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

Answer:

Explanation:

NEW QUESTION: 160
You have a Microsoft Entra tenant.
You need to ensure that users are prevented from consenting to high-privilege permission requests for enterprise applications. The solution must ensure that the users can consent to low-risk permission requests.
What should you modify first?
A. Permission classifications
B. Admin consent settings

C. App registrations
D. User consent settings
Answer: (SHOW ANSWER)

NEW QUESTION: 161
You have an Azure subscription that contains two virtual machines named VM1 and VM2 and an Azure SQL managed instance named SQL1.
You need to ensure that VM1 and VM2 can retrieve data from SQL1. The solution must minimize administrative effort.
What should you create first?
A. a managed identity
B. a certificate
C. a Microsoft Entra user account
D. a shared access signature (SAS) token
Answer: A (LEAVE A REPLY)

NEW QUESTION: 162
You have an Azure subscription that contains the following virtual machine Name: VM1 Azure region: East US System-assigned managed identity: Disabled You create the managed identities shown in the following table.

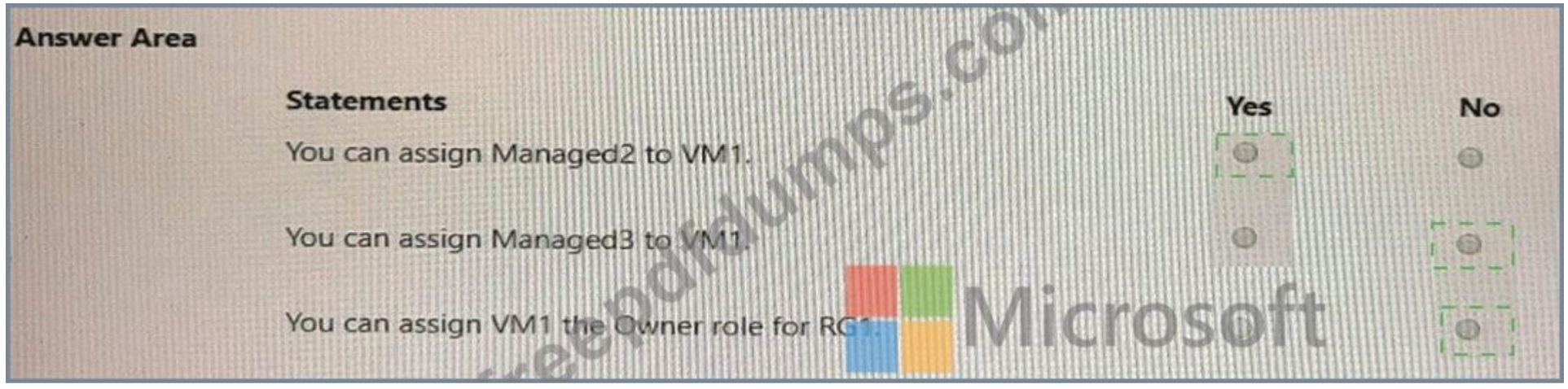
Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

You perform the following actions:
* Assign Managed1 to VM1.
* Create a resource group named RG1 in the West US region.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can assign Managed2 to VM1.	○	○
You can assign Managed3 to VM1.	○	○
You can assign VM1 the Owner role for RG1.	○	○

Answer:



Explanation:

Yes

NO

No

This question tests understanding of Azure Managed Identities - both system-assigned and user-assigned - and their regional restrictions and role assignment capabilities.

Let's break it down carefully based on official Microsoft documentation and SC-300 study material:

* VM1 Region: East US
* System-assigned Managed Identity: Disabled (so we can only use user-assigned identities)
* Managed Identities available:
* Managed1 - East US
* Managed2 - East US
* Managed3 - West US

Step 1: Understanding the setup

Step 2: Regional assignment rule According to Microsoft documentation:

"A user-assigned managed identity can be used only by resources in the same Azure region as the managed identity." That means:

* A VM in East US can use user-assigned managed identities that are also located in East US only.
* A VM in East US cannot use a user-assigned managed identity created in West US.

Therefore:

* # Managed2 (East US) # can be assigned to VM1 (East US).
* # Managed3 (West US) # cannot be assigned to VM1 (East US).

Step 3: Role assignment capability The question also includes:

"You can assign VM1 the Owner role for RG1."

Per Azure RBAC design and SC-300 guidelines:

* Azure roles (such as Owner, Contributor, Reader) can only be assigned to Azure AD security principals, which include users, groups, service principals, and managed identities - but not to Azure resources themselves (like a VM directly).
* Therefore, you cannot assign a role to VM1 as an object; you can only assign roles to VM1's managed identity (if it had one enabled).

Since VM1's system-assigned identity is disabled and the user-assigned identity (Managed1) already attached cannot represent the VM itself for new role assignments, VM1 cannot directly hold the Owner role for RG1.

NEW QUESTION: 163

You have an Azure Active Directory (Azure AD) tenant.
You configure self-service password reset (SSPR) by using the following settings:
* Require users to register when signing in: Yes
* Number of methods required to reset: 1
What is a valid authentication method available to users?
A. home prions
B. mobile app notification
C. a mobile app code
D. an email to an address in your organization
Answer: B (LEAVE A REPLY)
Based on the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and the official Microsoft Learn documentation for Azure AD Self-Service Password Reset (SSPR), when configuring password reset policies, administrators define how users verify their identity before resetting their password.
When Require users to register when signing in = Yes, users are prompted to register their authentication methods.
The setting Number of methods required to reset = 1 means a single verification method is sufficient for password reset.
Valid authentication methods for SSPR as per Microsoft documentation include:
* Mobile app notification (Microsoft Authenticator push notification)
* Mobile app code (verification code from the Microsoft Authenticator app)
* Email (to an alternate, non-organizational email address)
* Mobile phone (SMS or voice call)
* Office phone (if registered)
Option D, "an email to an address in your organization," is not allowed because SSPR does not use corporate email accounts for verification to avoid dependency on the same credentials being reset.
Therefore, the correct valid authentication method under the given configuration is B. Mobile app notification.

NEW QUESTION: 164
You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365
Group4	Mail-enabled security

In Azure AD. you add a new enterprise application named Appl. Which groups can you assign to App1?
A. Group1 and Group2 only
B. Group2 only
C. Group3 only
D. Group1 only
E. Group1 and Group4
Answer: (SHOW ANSWER)
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Microsoft Learn documentation on Azure AD group assignments for enterprise applications, only specific group types in Azure AD can be assigned to enterprise applications (service principals).
Azure AD allows group-based assignment for enterprise applications only when the group is a Security group or a Mail-enabled security group. This is because Azure AD uses security groups for authorization purposes.

Let's analyze the groups from the table:
Group
Type
Assignable to App1?
Reason
Group1
Security
Yes
Security groups are used for managing access permissions and can be assigned to apps.
Group2
Distribution
No
Distribution groups are used for email distribution lists and cannot be used for access management.
Group3
Microsoft 365
No
Microsoft 365 (formerly Office 365) groups manage collaboration resources like Teams and SharePoint but are not supported for enterprise app assignments.
Group4
Mail-enabled security
Yes
Mail-enabled security groups combine mailing capabilities with security functionality and can be used to assign permissions to applications.
The Microsoft documentation states:
"You can assign access to enterprise applications in Azure AD to users, security groups, and mail-enabled security groups. Distribution lists and Microsoft 365 groups are not supported for app assignments." Thus, for App1, which is an enterprise application, you can assign only Group1 (Security) and Group4 (Mail-enabled Security).

NEW QUESTION: 165
You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site na med Site1 and a Microsoft 365 group named Group1. You need to ensure that the members of Group1 can access Site1 for 90 days. The solution must minimize administrative effort. What should you use?
A. an access review
B. a lifecycle workflow
C. an access package
D. a Conditional Access policy
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation with all Microsoft SC-300: Identity and Access Administrator documents: = According to the SC-300 exam guide and the official Microsoft Entra ID (Azure A D) Entitlement Management documentation, access packages provide a streamlined way to manage resource access lifecycle for users - including SharePoint Online sites, Microsoft 365 Groups, Teams, and applications - with the ability to define time-limited access.
When you configure an access package, you can:
* Include resources like SharePoint Online sites and Microsoft 365 groups.
* Assign users or groups (like Group1) as eligible requesters.
* Set an access duration (for example, 90 days) after which access automatically expires.
The feature requires minimal administrative effort because the process is automated: the access duration ensures that permissions are revoked without manual intervention.

Microsoft documentation confirms:
"Entitlement management access packages enable you to define access policies for users and automatically remove access after a specified time period, minimizing administrative overhead." Therefore, to grant Group1 members access to Site1 for 90 days, the correct and most efficient solution is to use an access package rather than an access review, workflow, or Conditional Access policy.

NEW QUESTION: 166
You create a new Microsoft 365 E5 tenant.
You need to ensure that when users connect to the Microsoft 365 portal from an anonymous IP address, they are prompted to use multi-factor authentication (MFA).
What should you configure?
A. a sign-in risk policy
B. a user risk policy
C. an MFA registration policy
Answer: A (LEAVE A REPLY)
Explanat ion:
In Azure AD Identity Protection, a sign-in risk policy can trigger Conditional Access controls (like MFA) when risky sign-ins are detected.
According to the SC-300 training module "Implement and manage user risk policies" , a sign-in risk is associate d with a specific authentication attempt , for instance, when a user connects from an anonymous IP address , TOR network, or unfamiliar location. To enforce MFA only when such sign-in conditions are detected, administrators must use a sign-in risk policy .
Microsoft states: "Sign-in risk policies can enforce MFA or block access when sign-in risk meets the configured threshold, such as sign-ins from anonymous IPs."

NEW QUESTION: 167
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 questi on 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 Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.
You deploy an Azure subscription and enable Microsoft 365 Defender.
You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.
Solution: From the Microsoft 365 Defender portal, you add the Amazon Web Services app connector.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
The AWS connector in Microsoft Defender for Cloud Apps is designed t o integrate activity logs, user authentication data, and app permissions granted through OAuth. This connector enables monitoring of OAuth token use, identity federation events, and cross-service authentication.
From the official Microsoft Learn content:
" When the AWS app connector is added, Defender for Cloud Apps collects OAuth activity and permissions information to detect anomalous behavior or excessive app permissions." This

fulfills the requirement to monitor OAuth authentication requests from AWS and its associated accounts. Therefore, adding the AWS app connector meets the goal .

NEW QUESTION: 168

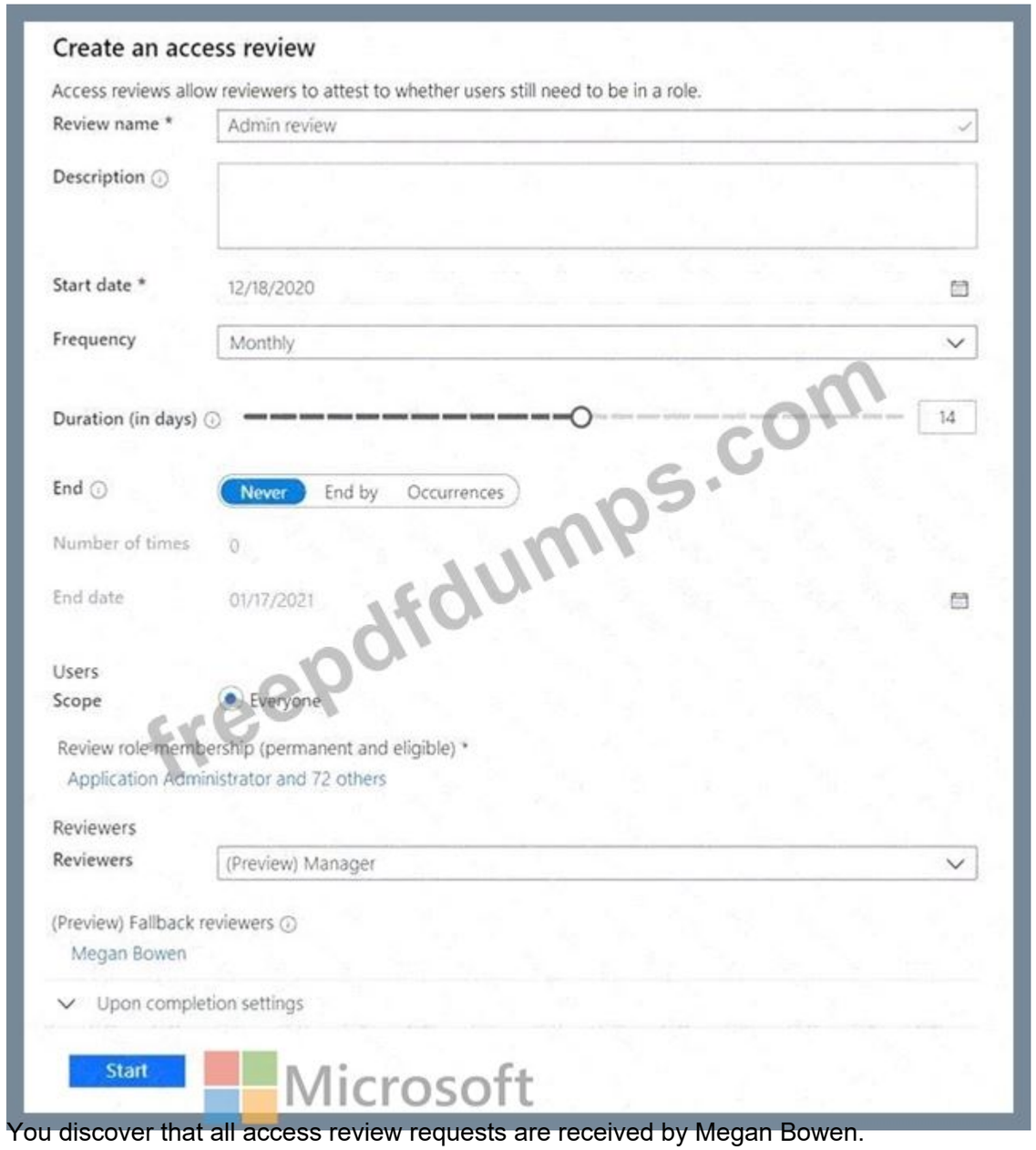
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Microsof t 365 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click theExhibittab.)



You discover that all access review requests are received by Megan Bowen.

You need to ensur e that the manager of each department receives the access reviews of their respective department.

Solution: You set Reviewers toMember (self).

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

In Azure AD access reviews, the Reviewer type determines who gets the review tasks. The SC-300 materials explain that selecting "Members (self)" triggers self-attestation, meaning each user only reviews their own access . The guidance states that when you use Members (self), "each user reviews only their own access," and owners or other people do not receive tasks for others. Your goal is for each department's manager to review their staff's access. For that, the documented reviewer choice is Manager (leveraging the user's manager attribute) and, optionally, fallback reviewers to catch users without a manager value. The exhibits show all requests going to Megan Bowen, which typically occurs when Manager is selected but many users lack a populated manager attribute-thus the tasks fall back to the specified fallback reviewer. Changing the reviewer to Members (self) would not route tasks to managers; it would simply ask every user to attest to their own access, failing the goal of manager-based attestation by department. Therefore, the proposed solution does not meet the requirement.