



Vendor: Microsoft

Exam Code: SC-300

Exam Name: Microsoft Identity and Access Administrator

Version: 24.021

Important Notice

Product

Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within One year after your purchase.

You can login member center and download the latest product anytime. (Product downloaded from member center is always the latest.)

PS: Ensure you can pass the exam, please check the latest product in 2-3 days before the exam again.

Feedback

We devote to promote the product quality and the grade of service to ensure customers interest.

If you have any questions about our product, please provide Exam Number, Version, Page Number, Question Number, and your Login Account to us, please contact us at support@passleader.com and our technical experts will provide support in 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently.

If anyone who share the file we will disable the free update and account access.

Any unauthorized changes will be inflicted legal punishment. We will reserve the right of final explanation for this statement.

Order ID: ****

PayPal Name: ****

PayPal ID: ****

QUESTION 1**Case Study 1 - Contoso, Ltd****Overview**

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named ADatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question

You need to sync the ADatum users. The solution must meet the technical requirements.

What should you do?

- A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
- B. From PowerShell, run Set-ADSyncScheduler.
- C. From PowerShell, run Start-ADSyncSyncCycle.
- D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Answer: A

Explanation:

You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#filtering-options>

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis#azure-ad-connect-sync-topics>

QUESTION 2

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

You need to meet the planned changes and technical requirements for App1.

What should you implement?

- A. a policy set in Microsoft Intune
- B. an app configuration policy in Microsoft Intune
- C. an app registration in Azure AD
- D. Azure AD Application Proxy

Answer: C

Explanation:

You can assign a redirect URI as part of the registration process.

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

QUESTION 3**Case Study 1 - Contoso, Ltd****Overview**

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com.

The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

You create a Log Analytics workspace.

You need to implement the technical requirements for auditing.

What should you configure in Azure AD?

- A. Company branding
- B. Diagnostics settings
- C. External Identities
- D. App registrations

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/design-logs-deployment>

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-control-logging-monitoring>

QUESTION 4

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

Hotspot Question

You need to meet the technical requirements for the probability that user identities were compromised.

What 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 Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

Answer:

Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

Explanation:

User risk is a calculation of probability that an "identity" has been compromised.

Administrators can choose to block access, allow access, or allow access but require a password change using Azure AD self-service password reset.

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

QUESTION 5

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

Hotspot Question

You need to implement the planned changes and technical requirements for the marketing department.

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

NOTE: Each correct selection is worth one point.

Answer Area

To configure user access:

An access package
An access review
A conditional access policy

To enable collaboration with fabrikam.com:

An accepted domain
A connected organization
A custom domain name

Answer:

Answer Area

To configure user access:

An access package
An access review
A conditional access policy

To enable collaboration with fabrikam.com:

An accepted domain
A connected organization
A custom domain name

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization>

QUESTION 6

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

You need to meet the authentication requirements for leaked credentials.

What should you do?

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

Answer: A

Explanation:

Password hash synchronization

Risk detections like leaked credentials require the presence of password hashes for detection to occur. For more information about password hash synchronization, see the article, Implement password hash synchronization with Azure AD Connect sync.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#password-hash-synchronization>

QUESTION 7**Case Study 2 - Litware, Inc****Overview**

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

You need to configure the detection of multi-staged attacks to meet the monitoring requirements.

What should you do?

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

Answer: C

Explanation:

In order to enable these Fusion-powered attack detection scenarios, any data sources listed must be ingested using the associated Azure Sentinel data connectors.

<https://docs.microsoft.com/en-us/azure/sentinel/fusion#attack-detection-scenarios>

QUESTION 8

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

Hotspot Question

You need to 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.

Answer Area

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

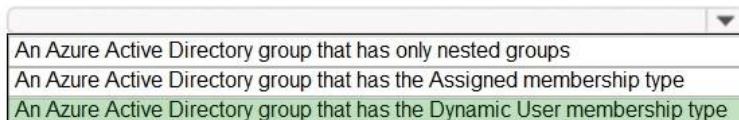
Answer:

Answer Area

Azure AD Connect settings to modify:



Assign Azure AD licenses to:



Explanation:

Box 1: Directory Extensions

You can use directory extensions to extend the schema in Azure Active Directory (Azure AD) with your own attributes from on-premises Active Directory.

Box 2: And AAD Group that has Dynamic User Membership Type

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 a Microsoft 365 group that has the appropriate licenses assigned.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-directory-extensions>

QUESTION 9

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector

and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

Hotspot Question

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

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

NOTE: Each correct selection is worth one point.

Answer Area

To manage Azure AD built-in role assignments, use:

Global administrator
Privileged role administrator
Security administrator
User access administrator

To manage Azure built-in role assignments, use:

Global administrator
Privileged role administrator
Security administrator
User access administrator

Answer:

Answer Area

To manage Azure AD built-in role assignments, use:

Global administrator
Privileged role administrator
Security administrator
User access administrator

To manage Azure built-in role assignments, use:

Global administrator
Privileged role administrator
Security administrator
User access administrator

Explanation:

For Azure AD roles in Privileged Identity Management, only a user who is in the Privileged Role Administrator or Global Administrator role can manage assignments for other administrators. Global Administrators, Security Administrators, Global Readers, and Security Readers can also view assignments to Azure AD roles in Privileged Identity Management.

For Azure resource roles in Privileged Identity Management, only a subscription administrator, a resource Owner, or a resource User Access administrator can manage assignments for other administrators. Users who are Privileged Role Administrators, Security Administrators, or Security Readers do not by default have access to view assignments to Azure resource roles in Privileged Identity Management.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

QUESTION 10

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

Hotspot Question

You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area

For on-premises applications:

Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish an application by using Azure AD Application Proxy.

Answer:

Answer Area

For on-premises applications:

- | |
|---|
| Configure Cloud App Security policies. |
| Modify the User consent settings for the enterprise applications. |
| Publish the applications by using Azure AD Application Proxy. |

For SharePoint Online:

- | |
|---|
| Configure Cloud App Security policies. |
| Modify the User consent settings for the enterprise applications. |
| Publish an application by using Azure AD Application Proxy. |

Explanation:

Configure Cloud App Security policies

Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Cloud App Security portal to further refine filters and set actions to be taken on a user.

Configure app-enforced settings

Conditional Access App Control uses a reverse proxy architecture and integrates with your IdP. When integrating with Azure AD Conditional Access, you can configure apps to work with Conditional Access App Control with just a few clicks, allowing you to easily and selectively enforce access and session controls on your organization's apps based on any condition in Conditional Access.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad#featured-apps>

<https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad#how-it-works>

QUESTION 11

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-On (Azure AD Seamless SSO).

You need to configure the Windows 10 computers to support Azure AD Seamless SSO.

What should you do?

- A. Configure Sign-in options from the Settings app.
- B. Enable Enterprise State Roaming.
- C. Modify the Intranet Zone settings.

D. Install the Azure AD Connect Authentication Agent.

Answer: C

Explanation:

You can gradually roll out Seamless SSO to your users using the instructions provided below. You start by adding the following Azure AD URL to all or selected users' Intranet zone settings by using Group Policy in Active Directory:

<https://autologon.microsoftazuread-sso.com>

In addition, you need to enable an Intranet zone policy setting called Allow updates to status bar via script through Group Policy.

more information in:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start>

QUESTION 12

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: C

Explanation:

You cannot assign licenses to group 3 because it is a device group. You cannot assign licenses to device groups.

You cannot assign licenses to group 4 and group 5. You cannot assign licenses to Microsoft 365 groups.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

QUESTION 13

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com.

Several users use their contoso.com email address for self-service sign-up to Azure Active Directory (Azure AD).

You gain global administrator privileges to the Azure AD tenant that contains the self-signed users.

You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

- A. Set-MsolCompanySettings
- B. Set-MsolDomainFederationSettings
- C. Update-MsolFederatedDomain
- D. Set-MsolDomain

Answer: A

Explanation:

Self-service sign-up: Method by which a user signs up for a cloud service and has an identity automatically created for them in Azure AD based on their email domain.

Azure AD cmdlet Set-MsolCompanySettings could help you to prevent creating user accounts with parameters:

AllowEmailVerifiedUsers (users can join the tenant by email validation)-->when is TRUE.

AllowAdHocSubscriptions (controls the ability for users to perform self-service sign-up)

e.g. Set-MsolCompanySettings -AllowEmailVerifiedUsers \$false -AllowAdHocSubscriptions \$false
Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup>

QUESTION 14

You have a Microsoft 365 tenant that uses the domain named fabrikam.com. The Guest invite settings for Azure Active Directory (Azure AD) are configured as shown in the exhibit. (Click the **Exhibit tab**.)

Guest user access

Guest user access restrictions (Preview) ⓘ

[Learn more](#)

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Admins and users in the guest inviter role can invite ⓘ

Yes

No

Members can invite ⓘ

Yes

No

Guests can invite ⓘ

Yes

No

Email One-Time Passcode for guests ⓘ

[Learn more](#)

Yes

No

Enable guest self-service sign up via user flows (Preview) ⓘ

[Learn more](#)

Yes

No

Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

A user named bsmith@fabrikam.com shares a Microsoft SharePoint Online document library to the users shown in the following table.

Name	Email	Description
User1	User1@contoso.com	A guest user in fabrikam.com
User2	User2@outlook.com	A user who has never accessed resources in fabrikam.com
User3	User3@fabrikam.com	A user in fabrikam.com

Which users will be emailed a passcode?

- A. User2 only
- B. User1 only
- C. User1 and User2 only
- D. User1, User2, and User3

Answer: A

Explanation:

When the email one-time passcode feature is enabled, newly invited users who meet certain conditions will use one-time passcode authentication. Guest users who redeemed an invitation before email one-time passcode was enabled will continue to use their same authentication method.

User 1 is already a registered guest user in fabrikan.com so will not receive additional OTP.

User 2 has never accessed fabrikam.com so WILL receive OTP each time they login.

User 3 (providing email addy is not a typo) will not receive a OTP as they are a domain user.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

QUESTION 15

You have 2,500 users who are assigned Microsoft Office 365 Enterprise 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: C

Explanation:

The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.

Note:

There are several versions of this QUESTION 1 in the exam. The QUESTION 1 has two possible correct answers:

- 1. the Licenses blade in the Azure Active Directory admin center
- 2. the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

- the Identity Governance blade in the Azure Active Directory admin center
- the Set-WindowsProductKey cmdlet
- the Set-AzureAdGroup cmdlet

Reference:

<https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0>

QUESTION 16

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

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

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

NOTE: Each correct selection is worth one point.

- A. email address
- B. redirection URL
- C. username
- D. shared key
- E. password

Answer: AB

Explanation:

Required values are:

Email address to invite - the user who will receive an invitation

Redirection url - the URL to which the invited user is forwarded after accepting the invitation. If you want to forward the user to the My Apps page, you must change this value to <https://myapps.microsoft.com> or <https://myapplications.microsoft.com>.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite#invite-guest-users-in-bulk>

QUESTION 17

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: E

Explanation:

In the M365 admin center, only users can be added to the mail-enabled security group.

You can only add licensed users to the group, unlicensed users won't even show up on the member select page.

Reference:

<https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/>

QUESTION 18

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 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

Explanation:

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications by using the same passwords. Pass-through Authentication signs users in by validating their passwords directly against on-premises Active Directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

QUESTION 19

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 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 conditional access policies.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign into both on-premises and cloud-based applications using the same passwords. It uses a lightweight on-premises agent that listens for and responds to password validation requests. If disabled user can not login.

Reference:

<https://docs.microsoft.com/en-us/answers/questions/3221/disable-account-sync.html>

QUESTION 20

You have an Azure Active Directory (Azure AD) tenant that contains a user named SecAdmin1. SecAdmin1 is assigned the Security administrator role.

SecAdmin1 reports that she cannot reset passwords from the Azure AD Identity Protection portal.

You need to ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of non-administrative users. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. Authentication administrator
- B. Helpdesk administrator
- C. Privileged authentication administrator
- D. Security operator

Answer: B

Explanation:

Authentication administrator: can reset passwords for non-admins but can't invalidate sessions.

Helpdesk administrator: Users with this role can change passwords, invalidate refresh tokens, manage service requests, and monitor service health. Invalidating a refresh token forces the user to sign in again.

Privileged Authentication Administrator: can reset all passwords (admins & non-admins) but can't invalidate any sessions.

Security Operator: can't reset any passwords.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#authentication-administrator>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-authentication-administrator>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator>

QUESTION 21

You configure Azure Active Directory (Azure AD) Password Protection as shown in the exhibit.
(Click the Exhibit tab.)

Custom smart lockout

Lockout threshold ⓘ ✓

Lockout duration in seconds ⓘ ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ Contoso Litware Tailwind project Zettabyte MainStreet

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

You are evaluating the following passwords:

- Pr0jectlitw@re
- T@ilw1nd
- C0nt0s0

Which passwords will be blocked?

- A. Pr0jectlitw@re and T@ilw1nd only
- B. C0nt0s0 only
- C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd
- D. C0nt0s0 and T@ilw1nd only
- E. C0nt0s0 and Pr0jectlitw@re only

Answer: C

Explanation:

After normalization we have :

- Pr0jectlitw@re -> projectlitware = 2 points
- T@ilw1nd -> tailwind =1 point
- C0nt0s0 -> contoso = 1 point

You need 5 points therefore everything is blocked.

QUESTION 22

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a verification code from the Microsoft Authenticator app
- B. security questions
- C. voice
- D. SMS

Answer: A

Explanation:

The Authenticator app can be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.

Incorrect Answers:

B: Security questions are not used as an authentication method but can be used during the self-service password reset (SSPR) process.

C, D: An automated voice call and an SMS requires mobile connectivity.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

QUESTION 23

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 resources 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

Explanation:

If your tenant was created on or after October 22, 2019, it is possible security defaults are already enabled in your tenant. To protect all of our users, security defaults are being rolled out to all new tenants created.

To enable CAP you have to disable Security defaults.

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

QUESTION 24

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

Explanation:

FIDO2 security device (biometrics, PIN, and NFC)

User can access device based on organization controls and authenticate based on PIN, biometrics using devices such as USB security keys and NFC-enabled smartcards, keys, or wearables.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

QUESTION 25

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

All users who run applications registered in Azure AD are subject to conditional access policies.

You need to prevent the users from using legacy authentication.

What should you include in the conditional access policies to filter out legacy authentication attempts?

- A. a cloud apps or actions condition
- B. a user risk condition
- C. a client apps condition
- D. a sign-in risk condition

Answer: C

Explanation:

Directly blocking legacy authentication

The easiest way to block legacy authentication across your entire organization is by configuring a Conditional Access policy that applies specifically to legacy authentication clients and blocks access.

Conditional Access policies apply to all client apps by default Client apps.

By default, all newly created Conditional Access policies will apply to all client app types even if the client apps condition is not configured.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

QUESTION 26

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: D

Explanation:

Leaked credentials indicates that the user's valid credentials have been leaked.

Note:

There are several versions of this question in the exam. The question can have other incorrect answer options, including the following:

- password spray
- malicious IP address
- unfamiliar sign-in properties

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

QUESTION 27

You have a Microsoft 365 tenant.

All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user-owned and are only registered in Azure AD.

You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.

Which policy type should you create?

- A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured
- B. an Azure AD conditional access policy that has session controls configured
- C. an Azure AD conditional access policy that has client apps conditions configured
- D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

Answer: B

Explanation:

You need to use "Use app enforced restrictions" from the "Session" control of the CA.

<https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

QUESTION 28

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory domain.

The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain. The VPN server does NOT support Azure Multi-Factor Authentication (MFA).

You need to recommend a solution to provide Azure MFA for VPN connections.

What should you include in the recommendation?

- A. Azure AD Application Proxy
- B. an Azure AD Password Protection proxy
- C. Network Policy Server (NPS)
- D. a pass-through authentication proxy

Answer: C

Explanation:

NPS (Network Policy and Access Service) is like a middle man between the VPN client and Azure MFA. The NPS role is installed on a domain-joined server or the domain controller and is configured to authenticate and authorize RADIUS requests from the VPN client.

The VPN should be configured to use RADIUS authentication and point to the NPS server.

The MFA NPS extension is installed anywhere but the VPN server. When a user/VPN client attempts to authenticate, it sends a RADIUS request to the NPS server through the VPN which performs the primary authentication and then triggers the NPS Extension for secondary authentication.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-vpn>

QUESTION 29

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

Explanation:

The AzureAD Password Protection proxy service initiates an outbound connection (Port 443) to Azure to pull the banned password list.

The downloaded banned password list is pulled by the agent installed on DCs.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

QUESTION 30

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

You create an enterprise application collection named HR Apps that has the following settings:

- Applications: App1, App2, App3
- Owners: Admin1
- Users and groups: HRUsers

All three apps have the following Properties settings:

- Enabled for users to sign in: Yes
- User assignment required: Yes
- Visible to users: Yes

Users report that when they go to the My Apps portal, they only see App1 and App2.

You need to ensure that the users can also see App3.

What should you do from App3?

- A. From Users and groups, add HRUsers.
- B. From Single sign-on, configure a sign-on method.
- C. From Properties, change User assignment required to No.
- D. From Permissions, review the User consent permissions.

Answer: A

Explanation:

User assignment and Visible to Users goes hand in hand for this.

If Visible to Users is set to Yes then this is the explanation from the 'i' next to it:

If this option is set to yes, then assigned users will see the application on My Apps and O365 app launcher. If this option is set to no, then no users will see this application on their My Apps and O365 launcher. Assigned User is the key here.

Unless the users are assigned to the app, then No one will see the application on their MyApps or O365 Launcher.

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

<https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portal-workspaces>

QUESTION 31

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 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. Application Insights in Azure Monitor
- B. access reviews in Azure AD
- C. Cloud App Discovery in Microsoft Cloud App Security
- D. enterprise applications in Azure AD

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports#using-traffic-logs-for-cloud-discovery>

QUESTION 32

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises 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 on-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 for Emergency1.
- C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporate network.
- D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.

Answer: A

Explanation:

Monitor sign-in and audit logs

Organizations should monitor sign-in and audit log activity from the emergency accounts and trigger notifications to other administrators.

When you monitor the activity on break glass accounts, you can verify these accounts are only used for testing or actual emergencies.

You can use Azure Log Analytics to monitor the sign-in logs and trigger email and SMS alerts to your admins whenever break glass accounts sign in.

QUESTION 33

You have a Microsoft 365 tenant.

In Azure Active Directory (Azure AD), you configure the terms of use.

You need to ensure that only users who accept the terms of use can access the resources in the tenant.

Other users must be denied access.

What should you configure?

- A. an access policy in Microsoft Cloud App Security.
- B. Terms and conditions in Microsoft Endpoint Manager.
- C. a conditional access policy in Azure AD
- D. a compliance policy in Microsoft Endpoint Manager

Answer: C

Explanation:

To configure Condition Access Terms of Use, at: Azure AD Conditional Access - Policies - Policy Name - Grant - myToUname - Terms Of Use Policy (Create the ToU settings first)

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

QUESTION 34

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: D

Explanation:

Technically you can create access review for Dynamic Device group (no errors/warnings during the creation), however it doesn't work and you will see a hitch "Warning - No access to review" for that access review in the list.

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

QUESTION 35

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

Name	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:

- Users to review: Members of a group
- Scope: Everyone
- Group: Group1
- Reviewers: Members (self)

Which users can perform access reviews for User3?

- A. User1, User2, and User3
- B. User3 only
- C. User1 only
- D. User1 and User2 only

Answer: B

Explanation:

Settings were self-reviewed so everyone will review themselves. So User3 is reviewed by User3.
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review>

QUESTION 36

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.

You need to ensure that the IT department users only have access to the Security administrator role when required.

What should you configure for the Security administrator role assignment?

- A. Expire eligible assignments after from the Role settings details
- B. Expire active assignments after from the Role settings details
- C. Assignment type to Active
- D. Assignment type to Eligible

Answer: D

Explanation:

"Assignment type to Eligible" so the admins can request the role in future, for a limited time based on the Role Setting of "Activation maximum duration (hours): 8 (by default)".
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

QUESTION 37

You have a Microsoft 365 tenant.

The Sign-ins activity report shows that an external contractor signed in to the Exchange admin center.

You need to review access to the Exchange admin center at the end of each month and block sign-ins if required.

What should you create?

- A. an access package that targets users outside your directory
- B. an access package that targets users in your directory
- C. a group-based access review that targets guest users
- D. an application-based access review that targets guest users

Answer: C

Explanation:

You can target a group with a conditional policy to detect and remediate the login at the end of each month.

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

QUESTION 38

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 administrators who are organized into 10 departments.

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

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Admin review ✓

Description (i)

Start date * 12/18/2020 (cal)

Frequency Monthly (▼)

Duration (in days) (i) 14

End (i) Never End by Occurrences

Number of times 0

End date 01/17/2021 (cal)

Users

Scope Everyone

Review role membership (permanent and eligible) *
Application Administrator and 72 others

Reviewers

Reviewers (Preview) Manager (▼)

(Preview) Fallback reviewers (i)
Megan Bowen

Upon completion settings (▼)

Start

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. No

Answer: B

Explanation:

Each access review would still send review approval to Megan as no manager has been set for the user accounts under review.

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

QUESTION 39

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 administrators who are organized into 10 departments.

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

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Admin review ✓

Description (i)

Start date * 12/18/2020 (cal)

Frequency Monthly (▼)

Duration (in days) (i) 14

End (i) Never End by Occurrences

Number of times 0

End date 01/17/2021 (cal)

Users

Scope Everyone

Review role membership (permanent and eligible) *
Application Administrator and 72 others

Reviewers

Reviewers (Preview) Manager (▼)

(Preview) Fallback reviewers (i)
Megan Bowen

Upon completion settings (▼)

Start

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 modify the properties of the IT administrator user accounts.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Modify the properties of the IT administrator user accounts is not like to modify admin review to assign a manager, so, Because admin review is not modified, Megan Brow as Fallback Reviewer will still receiving reviews, no manager has been assigned to admin review.

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

QUESTION 40

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 administrators who are organized into 10 departments.

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

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Admin review ✓

Description (i)

Start date * 12/18/2020 (cal)

Frequency (▼)

Duration (in days) (i) (▼)

End (i) Never End by Occurrences

Number of times

End date 01/17/2021 (cal)

Users

Scope Everyone

Review role membership (permanent and eligible) *
Application Administrator and 72 others

Reviewers

Reviewers (▼)

(Preview) Fallback reviewers (i)
Megan Bowen

Upon completion settings (▼)

Start

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 set Reviewers to Member (self).

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Members (self) - Use this option to have the users review their own role assignments. Groups assigned to the role will not be a part of the review when this option is selected. This option is only available if the review is scoped to Users and Groups.

Also Megan Brow still there as Fallback Reviewer so will still receiving reviews.

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

QUESTION 41

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 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 password writeback.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Password writeback is a feature of Azure AD Connect which ensures that when a password changes in Azure AD (password change, self-service password reset, or an administrative change to a user password) it is written back to the local AD – if they meet the on-premises AD password policy.

Technically, a password write-back operation is a password “reset” action. Password writeback removes the need to set up an on-premises solution for users to reset their password. It all happens in real time, and so users are notified immediately if their password could not be reset or changed for any reason.

Reference:

<https://docs.microsoft.com/en-us/answers/questions/3221/disable-account-sync.html>

QUESTION 42

Note: This question is part of 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 an Azure Active Directory (Azure AD) tenant that contains a group named Group1. You need to enable multi-factor authentication (MFA) for the users in Group1 only.

Solution: From Multi-Factor Authentication, you select Bulk update, and you provide a CSV file that contains the members of Group1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

QUESTION 43

Hotspot Question

You have a Microsoft 365 tenant named contoso.com.

Guest user access is enabled.

Users are invited to collaborate with contoso.com as shown in the following table.

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

From the External collaboration settings in the Azure Active Directory admin center, you configure the Collaboration restrictions settings as shown in the following exhibit.

Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

 Delete

TARGET DOMAINS

Outlook.com

From a Microsoft SharePoint Online site, a user invites user3@adatum.com to the site.

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 accept the invitation and gain access to the enterprise application.	<input type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

Invitations can only be sent to outlook.com. Therefore, User1 can accept the invitation and access the application.

Box 2. Yes

Invitations can only be sent to outlook.com. However, User2 has already received and accepted an invitation so User2 can access the application.

Box 3. No

Invitations can only be sent to outlook.com. Therefore, User3 will not receive an invitation.

QUESTION 44

Drag and Drop Question

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

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

You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed users.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Sign in to the Microsoft 365 admin center.	
Create a self-signed user account in the Azure AD tenant.	
From the Microsoft 365 admin center, add the domain name.	< > ^ v
Respond to the Become the admin message.	
From the Microsoft 365 admin center, remove the domain name.	
Create a TXT record in the contoso.com DNS zone.	

Answer:

Actions	Answer Area
From the Microsoft 365 admin center, add the domain name.	Create a self-signed user account in the Azure AD tenant.
From the Microsoft 365 admin center, remove the domain name.	< ^ > v
From the Microsoft 365 admin center, remove the domain name.	Sign in to the Microsoft 365 admin center.
From the Microsoft 365 admin center, remove the domain name.	Respond to the Become the admin message.
From the Microsoft 365 admin center, remove the domain name.	Create a TXT record in the contoso.com DNS zone.

Explanation:

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

QUESTION 45

Hotspot Question

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 point.

Answer Area

GroupA:

User1 only
User1 and Group1 only
User1, Group1, and Group2 only
User1, Group1, and Group4 only
User1, Group1, Group2, and Group3 only
User1, Group1, Group2, Group3, and Group4

GroupB:

User1 only
User1 and Group4 only
User1, Group1, and Group4 only
User1, Group1, Group2, and Group4 only
User1, Group1, Group2, Group3, and Group4

Answer:

Answer Area

GroupA:

User1 only
User1 and Group1 only
User1, Group1, and Group2 only
User1, Group1, and Group4 only
User1, Group1, Group2, and Group3 only
User1, Group1, Group2, Group3, and Group4

GroupB:

User1 only
User1 and Group4 only
User1, Group1, and Group4 only
User1, Group1, Group2, and Group4 only
User1, Group1, Group2, Group3, and Group4

Explanation:

Group A - User1, Group1, Group2 and Group3
Group A cannot contain M365 groups.

Group B - User1 only
M365 groups cannot contain other groups.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal>

QUESTION 46

Hotspot Question

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 the Users tab.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Users (Preview)

ContosoAzureAD - Azure Active Directory

[+ Add member](#) [Remove member](#) [Bulk operations](#) [Refresh](#) [Columns](#) [Preview features](#) [Got feedback?](#)

This page includes previews available for your evaluation. View previews →

Search users

[+ Add filters](#)

2 users found

Name	User principal name	User type	Directory synced
<input type="checkbox"/> US User1	User1@m365x629615.onmicrosoft.com	Member	No
<input type="checkbox"/> US User2	User2@m365x629615.onmicrosoft.com	Member	No

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

Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

[»](#) [+ Add](#) [Remove](#) [Refresh](#) [Columns](#) [Preview features](#) [Got feedback?](#)

Search groups

[+ Add filters](#)

Name	Group Type	Membership Type
<input type="checkbox"/> GR Group1	Security	Assigned
<input type="checkbox"/> GR Group2	Security	Assigned

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

Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

[»](#) [+ Add assignments](#) [Settings](#) [Refresh](#) [Export](#) [Got feedback?](#)

[Eligible assignments](#) [Active assignments](#) [Expired assignments](#)

Search by member name or principal name

Name	Principal name	Type	Scope
User Administration			
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory

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

Dashboard > ContosoAzureAD > Groups > Group2

 **Group2 | Members**
Group

Add members Remove Refresh Bulk operations Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

Direct members	
Name	User type
<input type="checkbox"/>  User3	Member
<input type="checkbox"/>  User4	Member

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
Admin1 can reset the passwords of User3 and User4.	<input type="radio"/>	<input type="radio"/>
Admin1 can add User1 to Group 2	<input type="radio"/>	<input type="radio"/>
Admin 2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1 can add User1 to Group 2	<input checked="" type="radio"/>	<input type="radio"/>
Admin 2 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Admin1 and Admin2 are not members of Administrative group(Department1). However Admin1 has User administrator role scope for Department1 and Admin2 has User administrator role scope for the whole directory

User 1 And User 2 are users of Department1

Group1(No members) and Group2(User 3 and User4 are members) are groups of Department1.

Box 1: No

Admin1 cannot reset the password for User 3 and User4 because they are part of group2.(User admin role assigned to admin unit cannot reset password of users present inside the group.

Admin1 can reset the password of User1 and User2 who are not part of any groups inside the admin unit)

Box 2: Yes

Admin1 can add/remove users to the GROUPS present inside the admin unit (Admin1 cannot add/remove users from USERS section)

Box 3: Yes

Admin2 is User admin at directory scope ,hence can reset password of any uses except the password of global admin/higher power roles

QUESTION 47

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that has Security defaults disabled.

You are creating a conditional access policy as shown in the following exhibit.

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users. [Learn more](#)

Name *

Policy1



Assignments

Users and groups ⓘ



Specific users included

Cloud apps or actions ⓘ



All cloud apps

Conditions ⓘ



0 conditions selected

Access controls

Grant ⓘ



0 controls selected

Session ⓘ



0 controls selected

Enable policy

Report-only

On

Off

Create

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

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the [answer choice].

Conditions settings
Enable policy setting
Grant settings
Sessions settings
Users and groups setting

To ensure that User1 is prompted for authentication every eight hours, you must configure the [answer choice].

Conditions settings
Enable policy setting
Grant settings
Sessions settings
Users and groups setting

Answer:

Answer Area

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the [answer choice].

Conditions settings
Enable policy setting
Grant settings
Sessions settings
Users and groups setting

To ensure that User1 is prompted for authentication every eight hours, you must configure the [answer choice].

Conditions settings
Enable policy setting
Grant settings
Sessions settings
Users and groups setting

Explanation:

Create a Conditional Access policy

- Under Access controls > Grant, select Grant access, Require multi-factor authentication, and select Select.
- Confirm your settings and set Enable policy to On.
- Select Create to create to enable your policy.

Sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#sign-in-frequency>

QUESTION 48

Hotspot Question

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 Area

Tool to use:

Azure AD Identity Protection
Identity Governance
Microsoft Defender for Cloud Apps
Microsoft Endpoint Manager

Policy type to create:

App discovery
App protection
Conditional access
OAuth app
Sign-in risk
User risk

Answer:

Answer Area

Tool to use:

Azure AD Identity Protection
Identity Governance
Microsoft Defender for Cloud Apps
Microsoft Endpoint Manager

Policy type to create:

App discovery
App protection
Conditional access
OAuth app
Sign-in risk
User risk

Explanation:

You can set permission policies so that you get automated notifications when an OAuth app meets certain criteria.

Malicious OAuth app consent Scans OAuth apps connected to your environment and triggers an alert when a potentially malicious app is authorized.

<https://docs.microsoft.com/en-us/cloud-app-security/app-permission-policy>

QUESTION 49

Hotspot Question

You have an on-premises datacenter 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 Area

Service to install on Server4:

Azure AD Application Proxy
The Azure AD Password Protection DC agent
The Azure AD Password Protection proxy service
Web Application Proxy in Windows Server

Rule to configure on Firewall1:

Allow incoming HTTPS connections from Azure AD to Server4.
Allow incoming IPsec connections from Azure AD to Server4.
Allow outbound HTTPS connections from Server4 to Azure AD.
Allow outbound IPsec connections from Server4 to Azure AD.

Answer:**Answer Area**

Service to install on Server4:

Azure AD Application Proxy
The Azure AD Password Protection DC agent
The Azure AD Password Protection proxy service
Web Application Proxy in Windows Server

Rule to configure on Firewall1:

Allow incoming HTTPS connections from Azure AD to Server4.
Allow incoming IPsec connections from Azure AD to Server4.
Allow outbound HTTPS connections from Server4 to Azure AD.
Allow outbound IPsec connections from Server4 to Azure AD.

Explanation:

Application Proxy is an Azure AD service you configure in the Azure portal. It enables you to publish an external public HTTP/HTTPS URL endpoint in the Azure Cloud, which connects to an internal application server URL in your organization.

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy>

QUESTION 50

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that has the default App registrations settings. The tenant contains the users shown in the following table.

Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

You purchase two cloud apps named App1 and App2. The global administrator registers App1 in Azure AD.

You need to identify who can assign users to App1, and who can register App2 in Azure AD.

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

NOTE: Each correct selection is worth one point.

Answer Area

Can assign users to App1:

Admin1 only
Admin3 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3 only
Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

Admin1 only
Admin3 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3 only
Admin1, Admin2, Admin3, and User1

Answer:

Answer Area

Can assign users to App1:

Admin1 only
Admin3 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3 only
Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

Admin1 only
Admin3 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3 only
Admin1, Admin2, Admin3, and User1

Explanation:

Only administrators (Admin1 - Application Administrator & Admin3 - Cloud application administrator) can manage/configure apps.

Name: Cloud application administrator

Description: Users in this role can add, manage, and configure enterprise applications, app registrations but will not be able to configure or manage on-premises like app proxy.

Azure AD - User settings - App registration: default is Yes (If this option is set to yes, then non-admin users may register custom-developed applications for use within this directory.)

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

QUESTION 51

Hotspot Question

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.

Save Discard Delete | Got feedback?

Enabled for users to sign-in? Yes No

Name

App1



Homepage URL

<https://app1.m365x629615.onmicrosoft.com/>



Logo



Select a file



User access URL

<https://myapps.microsoft.com/signin/App1/09df58d6-d29d-40de-b0d...>



Application ID

09df58d6-d29d-40de-b0d0-321fdc63c665



Object ID

03709d22-7e61-4007-a2a0-04dbdff269cd



Terms of Service Url

Publisher did not provide this information



Privacy Statement Url

Publisher did not provide this information



Reply Url

<https://contoso.com/App1/logon>



User assignment required?

Yes No

Visible to users?

Yes No

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

[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 Area**

[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:

Box 1: All users

"Enable for users to sign-in" is selected and "User assignment required" is set to No. Any user can login using the app url.

Box 2: Only users listed on the users and groups blade

User assignment required - This option does not affect whether or not an application appears on My Apps. To show the application there, assign an appropriate user or group to the application.

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-configure>

QUESTION 52

Hotspot Question

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.

... ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD > User Administrator >

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 completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every [answer choice].

8 hours
15 days
1 month

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a [answer choice].

global administrator only
global administrator or privileged role administrator
permanently assigned user administrator
privileged role administrator only

Answer:
Answer Area

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every [answer choice].

8 hours
15 days
1 month

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a [answer choice].

global administrator only
global administrator or privileged role administrator
permanently assigned user administrator
privileged role administrator only

Explanation:

Select at least one approver. If no specific approvers are selected, Privileged Role Administrators and Global Administrators become the default approvers.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan>

QUESTION 53

Hotspot Question

You have an Azure Active Directory (Azure AD) 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 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings:

- Name: Terms1
- 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, 2020
- Frequency: Monthly

On November 15, 2020, 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 Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	<input type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input checked="" type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

Because User1 has not yet accepted the terms on Device1.

Box 2: Yes

Because User1 has not yet accepted the terms on Device2. User1 will be prompted to register the device before the terms can be accepted.

Box 3: No

Because User1 has already accepted the terms on Device3. The terms do not expire until December 10th and then monthly after that.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

QUESTION 54

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

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

What should you do?

- A. Create an access review.
- B. Create an administrative unit.
- C. Modify Active assignments.
- D. Modify Role settings.

Answer: D

Explanation:

Role Setting details is where you need to be: Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Default Setting State

Require justification on activation Yes

Require ticket information on activation No

On activation, require Azure MFA Yes

Require approval to activate No

Approvers None

QUESTION 55

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com.

The domain contains an organizational unit (OU) named Contoso_Resources. The

Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question

Hotspot Question

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 Area

Object to create for each branch office:

An administrative unit
A custom role
A Dynamic User security group
An OU

Tool to use:

Azure Active Directory admin center
Active Directory Administrative Center
Active Directory module for Windows PowerShell
Microsoft 365 admin center

Answer:

Answer Area

Object to create for each branch office:

An administrative unit
A custom role
A Dynamic User security group
An OU

Tool to use:

Azure Active Directory admin center
Active Directory Administrative Center
Active Directory module for Windows PowerShell
Microsoft 365 admin center

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units>
Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support.

QUESTION 56

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named 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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

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

What should you include in the configuration?

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

Answer: B

Explanation:

Named Locations are part of Conditional Access Policies whereas "Trusted IPs" are in the legacy MFA settings, which would not be preferred.

The IP address will appear to be coming into Azure from the NAT'd public address not the internal network private address.

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

QUESTION 57

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

Hotspot Question

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

How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

(user.ObjectId -ne	▼)	and	(user.userType - eq	▼)			
<table border="1" style="width: 100%; border-collapse: collapse;"><tr><td style="padding: 2px;">"Guest"</td></tr><tr><td style="padding: 2px;">"Member"</td></tr><tr><td style="padding: 2px;">Null</td></tr></table>							"Guest"	"Member"	Null
"Guest"									
"Member"									
Null									

Answer:

Answer Area

(user.ObjectId -ne []) and (user.userType - eq [])

"Guest"
"Member"
Null

"Guest"
"Member"
Null

Explanation:

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

QUESTION 58**Case Study 2 - Litware, Inc****Overview**

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

Hotspot Question

You need to configure app registration in Azure AD to meet the delegation requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area

Azure AD tenant-level setting to modify:

Allow users to register application
Users can consent to apps accessing company data on their behalf
Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

Application administrator
Application developer
Cloud application administrator

Answer:

Answer Area

Azure AD tenant-level setting to modify:

Allow users to register application
Users can consent to apps accessing company data on their behalf
Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

Application administrator
Application developer
Cloud application administrator

Explanation:

- 1: Requirements for delegation clearly says " Prevent users to register applications"
- 2: User1 would need App Developer to register an app in tenant using "principle of least privilege"
<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles>

QUESTION 59

You have an Azure Active Directory (Azure AD) tenant that contains the following objects.

- A device named Devie1
- Users named User1, User2, User3, User4, and User5
- Five 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, Group4
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Assigned	User5

How many licenses are used if you assign the Microsoft 365 Enterprise E5 license to Group1?

- A. 0
- B. 2
- C. 3
- D. 4

Answer: B

Explanation:

Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#limitations-and-known-issues>

QUESTION 60

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 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

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>

QUESTION 61

Your network contains an Active Directory forest named contoso.com that is linked to an Azure

Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.

You need to prevent the synchronization of users who have the extensionAttribute15 attribute set to NoSync.

What should you do in Azure AD Connect?

- A. Create an inbound synchronization rule for the Windows Azure Active Directory connector.
- B. Configure a Full Import run profile.
- C. Create an inbound synchronization rule for the Active Directory Domain Services connector.
- D. Configure an Export run profile.

Answer: C

Explanation:

You create an inbound rule because information is taken from Active Directory to Metaverse object.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#negative-filtering-do-not-sync-these>

QUESTION 62

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.

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN IN



Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	2 agents

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: A

Explanation:

Pass-through authentication is configured, Sync user will try to authenticate on local AD and unable to authenticate due to internet outage only cloud users (User 1 and User 3) can be authenticated.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-current-limitations>

QUESTION 63

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 an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant.

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 Azure AD Password Protection.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Azure AD Password Protection

With this feature, you can use the same checks for passwords in AzureAD on your on-premises Active Directory implementation.

You can enforce both the Microsoft Global Banned Passwords and Custom banned-passwords list stored in Azure AD tenant.

The DC agent software must be installed on all DCs in a domain.

QUESTION 64

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. Managed Application Contributor for Subscription1.
- B. Application developer in Azure AD.
- C. Cloud application administrator in Azure AD.
- D. App Configuration Data Owner for Subscription1.

Answer: B

Explanation:

Application Developer can create application registrations independent of the 'Users can register applications' setting.

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

QUESTION 65

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection enabled.

You need to implement a sign-in risk remediation policy without blocking user access.

What should you do first?

- A. Configure access reviews in Azure AD.
- B. Enforce Azure AD Password Protection.
- C. Configure self-service password reset (SSPR) for all users.
- D. Implement multi-factor authentication (MFA) for all users.

Answer: D

Explanation:

To implement a sign-in risk remediation policy.

When a sign in risk policy triggers:

Azure AD MFA can be triggered, allowing a user to prove it's them by using one of their registered authentication methods, resetting the sign in risk.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

QUESTION 66

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You implement entitlement management to provide resource access to users at a company named Fabrikam, Inc. Fabrikam uses a domain named fabrikam.com.

Fabrikam users must be removed automatically from the tenant when access is no longer required.

You need to configure the following settings:

- Block external user from signing in to this directory: No
- Remove external user: Yes
- Number of days before removing external user from this directory: 90

What should you configure on the Identity Governance blade?

- A. Access packages
- B. Entitlement management settings
- C. Terms of use
- D. Access reviews

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users#manage-the-lifecycle-of-external-users>

QUESTION 67

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 past.

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: B

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention#how-long-does-azure-ad-store-the-data>

QUESTION 68

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, Role1, and Contributor only
- B. Group1 only
- C. Group1, App1, Contributor, and Role1
- D. Role1 and Contributor only

Answer: C

Explanation:

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>

QUESTION 69

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 by using the administrative portal. The log file must contain changes to conditional access policies.

What should you export from Azure AD?

- A. audit logs in CSV format

- B. sign-ins in CSV format
- C. audit logs in JSON format
- D. sign-ins in JSON format

Answer: C

Explanation:

You can also choose to download the filtered data, up to 250,000 records, by selecting the Download button. You can download the logs in either CSV or JSON format. You can use the JSON transform feature in the Power Query Editor in Excel to split each property in the JSON object in the AuditData column into multiple columns so that each property has its own column.

<https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records?view=o365-worldwide>

QUESTION 70

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 administrators who are organized into 10 departments.

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

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Admin review ✓

Description ⓘ

Start date * 12/18/2020

Frequency Monthly

Duration (in days) ⓘ 14

End ⓘ Never End by Occurrences

Number of times 0

End date 01/17/2021

Users

Scope Everyone

Review role membership (permanent and eligible) *
Application Administrator and 72 others

Reviewers

Reviewers (Preview) Manager

(Preview) Fallback reviewers ⓘ
Megan Bowen

Upon completion settings

Start

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 manager as a fallback reviewer.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The option of Fallback reviewer is when you set as reviewer to the manager or group owner and somehow that user is not having a manager in the directory. In those case, the fallback reviewer, which could be a department head would be the reviewer.

"Fallback reviewers are asked to do a review when the user has no manager specified in the directory or the group does not have an owner."

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

QUESTION 71

Drag and Drop Question

You have a Microsoft 365 E5 tenant.

You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Cloud App Security.

In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
From Microsoft Cloud App Security, create a session policy.	
Publish App1 in Azure Active Directory (Azure AD).	 
Create a conditional access policy that has session controls configured.	 
From Microsoft Cloud App Security, modify the Connected apps settings for App1.	

Answer:

Actions	Answer Area
	Publish App1 in Azure Active Directory (Azure AD).
	Create a conditional access policy that has session controls configured.
	From Microsoft Cloud App Security, modify the Connected apps settings for App1.
	From Microsoft Cloud App Security, create a session policy.

Explanation:

<https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-blocking-data-downloads-via-microsoft-cloud-app/ba-p/326357>

QUESTION 72

Hotspot Question

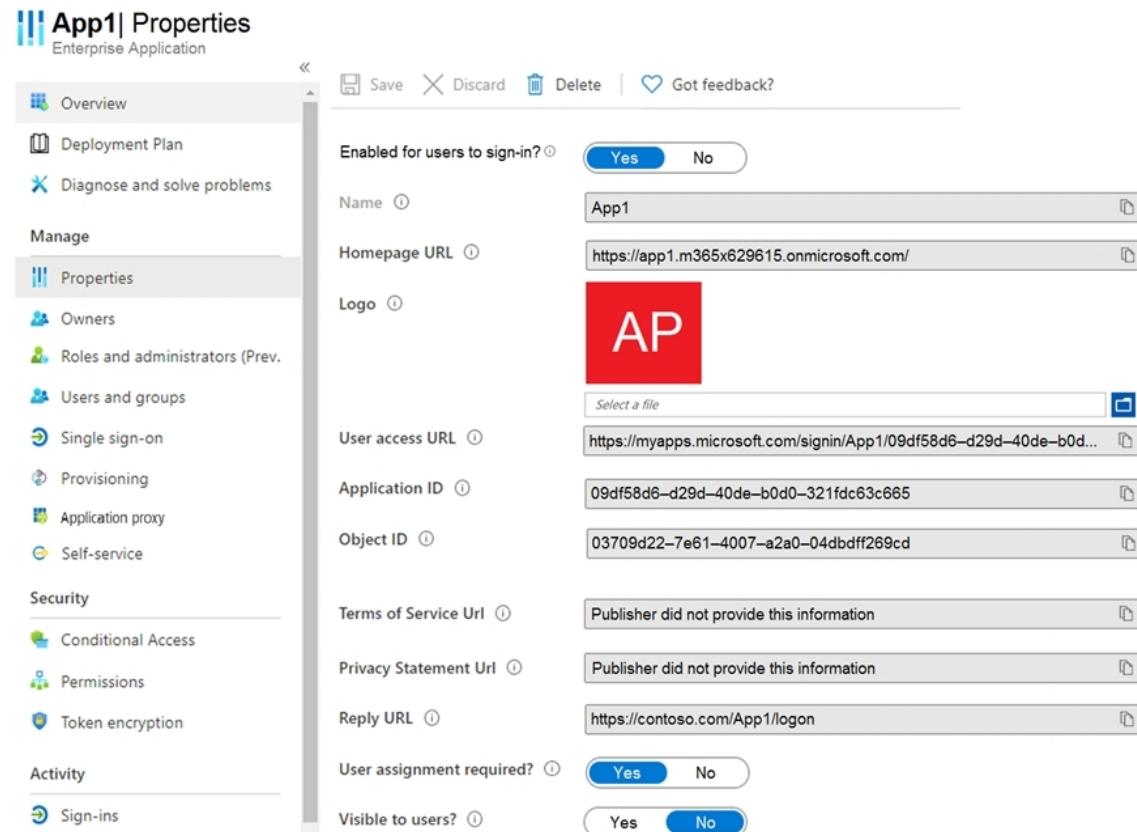
You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit. (Click the Group1 tab.)

```
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 the App1 Properties tab.)

Dashboard > ContosoAzureAD > Enterprise applications > App1



The screenshot shows the 'App1 Properties' page in the Azure portal. The left sidebar lists tabs: Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties is selected), Owners, Roles and administrators (Prev.), Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, Security, Conditional Access, Permissions, Token encryption, Activity, and Sign-ins. The main content area shows the following details for App1:

- Enabled for users to sign-in? Yes
- Name: App1
- Homepage URL: https://app1.m365x629615.onmicrosoft.com/
- Logo: A red square with the letters 'AP' in white.
- User access URL: https://myapps.microsoft.com/signin/App1/09df58d6-d29d-40de-b0d...
- Application ID: 09df58d6-d29d-40de-b0d0-321fdc63c665
- Object ID: 03709d22-7e61-4007-a2a0-04dbdff289cd
- Terms of Service Url: Publisher did not provide this information
- Privacy Statement Url: Publisher did not provide this information
- Reply URL: https://contoso.com/App1/logon
- User assignment required? Yes
- Visible to users? No

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

Dashboard > ContosoAzureAD > Enterprise applications > App1

App1 | Self-service

Enterprise application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Pre...)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

< Save Discard

Allow users to request access to this application? Yes No

To which group should assigned users be added? Select Group Group1

Require approval before granting access to this application? Yes No

Who is allowed to approve access to this application? Select approvers 1 users selected

To which role should users be assigned in this application? * Default Access

Select approvers

User1
User1@m365x629615.onmicrosoft.com
Selected

User2
User2@m365x629615.onmicrosoft.com

User3
User3@m365x629615.onmicrosoft.com

User4
User4@m365x629615.onmicrosoft.com

Selected approvers

User1
User1@m365x629615.onmicrosoft.com

Remove

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:

Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	<input type="radio"/>	<input checked="" type="radio"/>
After you configure self-service for App1, the owner of Group1 is User1.	<input checked="" type="radio"/>	<input type="radio"/>
App1 appears in the Microsoft Office 365 app launcher of User4.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No

Only direct members will have access. Approved users will be added to Group 1.

Box 2: Yes

The approver will automatically become owner of the Group 1 after self service is configured.

Box 3: No

Visible to users is NO. So no one will be able to see the app.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users>

QUESTION 73

Hotspot Question

You have a Microsoft 365 tenant and an Active Directory domain named adatum.com.

You deploy Azure AD Connect by using the Express Settings.

You need to configure self-service password reset (SSPR) to meet the following requirements:

- When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.
- Passwords must be synced between the tenant and the domain regardless of where the password was reset.

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

NOTE: Each correct selection is worth one point.

Answer Area

From the Password reset blade in the Azure Active Directory admin center, configure:

▼
Authentication methods
Notifications
Properties
Registration

From Azure AD Connect, enable:

▼
Federation with Active Directory Federation Services (AD FS)
Pass-through authentication
Password hash synchronization
Password writeback

Answer:

Answer Area

From the Password reset blade in the Azure Active Directory admin center, configure:

▼
Authentication methods
Notifications
Properties
Registration

From Azure AD Connect, enable:

▼
Federation with Active Directory Federation Services (AD FS)
Pass-through authentication
Password hash synchronization
Password writeback

Explanation:

You have Go to Azure active directory > under Manage section Password reset blade > Authentication methods & check the Security Questions

In order to sync password between Domain & tenant either you have to do password hash sync & Pass through authentication with password writeback enable in Azure Ad Connect.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions>

QUESTION 74

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.

What should you do first?

- 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: C

Explanation:

Requirement is for program which is a part of Access Reviews. Catalog is for Access Packages.
<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview>

QUESTION 75

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to ensure that Azure AD External Identities pricing is based on monthly active users (MAU).

What should you configure?

- A. a user flow

- B. the terms of use
- C. a linked subscription
- D. an access review

Answer: C

Explanation:

To take advantage of MAU billing, your Azure AD tenant must be linked to an Azure subscription.
<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing#what-do-i-need-to-do>

QUESTION 76

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. an app password
- C. Windows Hello for Business
- D. SMS

Answer: C

Explanation:

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.

Incorrect Answers:

A: The Microsoft Authenticator app requires a mobile phone that runs Android or iOS

B: An app password can be used to open an application but it cannot be used to sign in to a computer.

D: SMS requires a mobile phone

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview>

QUESTION 77

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 must use the Microsoft 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 Notifications settings for multi-factor authentication (MFA).

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to configure the fraud alert settings.

Fraud alert setting literally has an option to configure it to automatically block.

To enable and configure fraud alerts, complete the following steps:

1. Go to Azure Active Directory > Security > MFA > Fraud alert.
2. Set Allow users to submit fraud alerts to On.
3. Configure the Automatically block users who report fraud or Code to report fraud during initial greeting setting as needed.
4. Select Save.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert>

QUESTION 78

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 must use the Microsoft 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

Explanation:

You need to configure the fraud alert settings.

Fraud alert setting literally has an option to configure it to automatically block.

To enable and configure fraud alerts, complete the following steps:

1. Go to Azure Active Directory > Security > MFA > Fraud alert.
2. Set Allow users to submit fraud alerts to On.
3. Configure the Automatically block users who report fraud or Code to report fraud during initial greeting setting as needed.
4. Select Save.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert>

QUESTION 79

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 must use the Microsoft 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 Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to configure the fraud alert settings.

Fraud alert setting literally has an option to configure it to automatically block.

To enable and configure fraud alerts, complete the following steps:

1. Go to Azure Active Directory > Security > MFA > Fraud alert.
2. Set Allow users to submit fraud alerts to On.
3. Configure the Automatically block users who report fraud or Code to report fraud during initial greeting setting as needed.
4. Select Save.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert>

QUESTION 80

Your company requires that users request access before they can access corporate applications.

You register a new enterprise application named MyApp1 in Azure Active Directory (Azure AD) and configure single sign-on (SSO) for MyApp1.

Which settings should you configure next for MyApp1?

- A. Self-service
- B. Provisioning
- C. Application proxy
- D. Roles and administrators

Answer: A

Explanation:

Users can self discover apps, users can request access for app, can configure list of individuals to approve or require business approval before granting access to application.

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

QUESTION 81

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

Name	Type
User1	User
Guest1	Guest
Identity1	Managed identity

Which objects can you add as eligible in Azure AD Privileged Identity Management (PIM) for an Azure AD role?

- A. User1, Guest1, and Identity1
- B. User1 and Guest1 only
- C. User1 only
- D. User1 and Identity1 only

Answer: B

Explanation:

You cannot assign service principals as eligible to Azure AD roles, Azure roles, and Privileged Access groups but you can grant a time limited active assignment to all three.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan>

QUESTION 82

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection 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: C

Explanation:

Creating a Sentinel instance and configuring the Azure AD Connector = configuring the Azure AD connector within Sentinel settings, as detailed here: <https://learn.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>

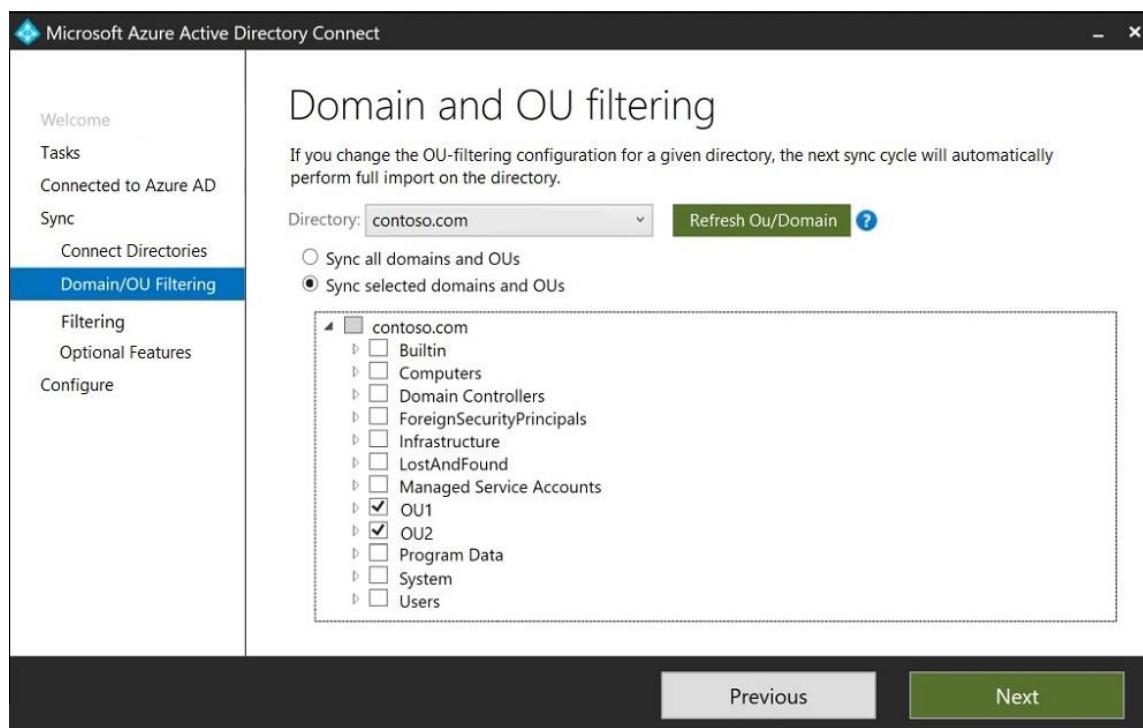
QUESTION 83

Hotspot Question

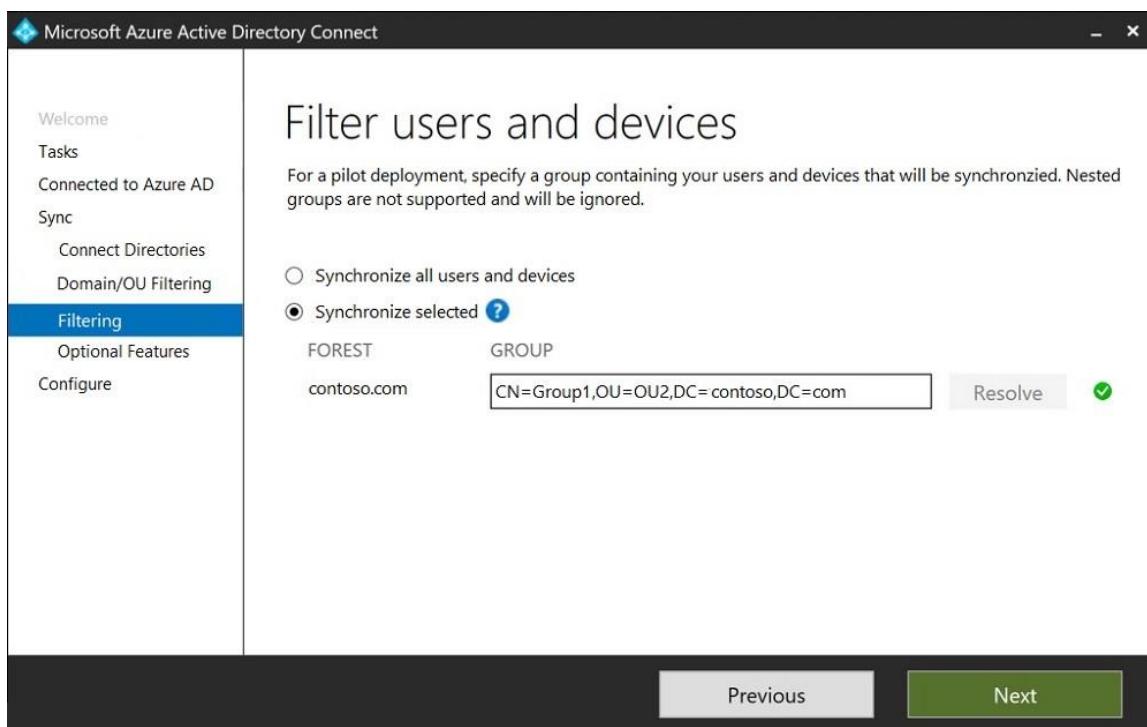
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

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 exhibit. (Click the Domain and OU Filtering tab.)



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



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

Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
Group2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>
Group2 syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Only direct members of Group1 are synced. Group2 will sync as it is a direct member of Group1 but the members of Group2 will not sync.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>

QUESTION 84

Drag and Drop Question

You have a new Microsoft 365 tenant that uses a domain name of contoso.onmicrosoft.com.

You register the name contoso.com with a domain registrar.

You need to use contoso.com as the default domain name for new Microsoft 365 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.

Actions	Answer Area
Delete the contoso.onmicrosoft.com domain.	
Add a custom domain name of contoso.com.	
Set the domain to primary.	
Create a new TXT record in DNS.	
Successfully verify the domain name.	

Answer:

Actions	Answer Area
Delete the contoso.ommicrosoft.com domain.	Add a custom domain name of contoso.com.
	Create a new TXT record in DNS.
	Successfully verify the domain name.
	Set the domain to primary.

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide>

QUESTION 85

Hotspot Question

You have a Microsoft 365 tenant.

You need to identify users who have leaked credentials. The solution must meet the following requirements:

- Identify sign-ins by users who are suspected of having leaked credentials.
- Flag the sign-ins as a high-risk event.
- Immediately enforce a control to mitigate the risk, while still allowing the user to access applications.

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

NOTE: Each correct selection is worth one point.

Answer Area

To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require password change

Answer:

Answer Area

To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require password change

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

QUESTION 86

Hotspot Question

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 Area

Configure the user risk policy:

User3 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

View the risky users report:

User3 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

Answer:

Answer Area

Configure the user risk policy:

User3 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

View the risky users report:

User3 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

Explanation:

Box 1: User 3 only

Box 2: User 3 and User 4 only

Conditional Access Administrator

- Does not have access to Identity Protection | User risk policy
- Does not have "Grants access to Risky Users Report"

Authentication Administrator

- Does not have access to Identity Protection | User risk policy
- Does not have "Grants access to Risky Users Report"

Security Administrator

- Has update access to Identity Protection | User risk policy
- microsoft.directory/identityProtection/allProperties/update = Update all resources in Azure AD Identity Protection
- Grants access to Risky Users Report

Security Operator

- Has only read access to Identity Protection | User risk policy
- microsoft.directory/identityProtection/allProperties/allTasks = Create and delete all resources, and read and update standard properties in Azure AD Identity Protection
- Grants access to Risky Users Report

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

QUESTION 87

Hotspot Question

Your company has a Microsoft 365 tenant.

All users have computers that run Windows 10 and are joined to the Azure Active Directory (Azure AD) tenant.

The company subscribes to a third-party cloud service named Service1. Service1 supports Azure AD authentication and authorization based on OAuth. Service1 is published to the Azure AD gallery.

You need to recommend a solution to ensure that the users can connect to Service1 without being prompted for authentication. The solution must ensure that the users can access Service1 only from Azure AD-joined computers. The solution must minimize administrative effort.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Ensure that the users can connect to Service1 without being prompted for authentication:

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy
- An OAuth policy

Answer:

Answer Area

Ensure that the users can connect to Service1 without being prompted for authentication:

An app registration in Azure AD
Azure AD Application Proxy
An enterprise application in Azure AD
A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

Azure AD Application Proxy
A compliance policy
A conditional access policy
An OAuth policy

Explanation:

Service1 support OAuth for Authentication & authorization, however Service1 is published in Azure AD gallery, hence we will use An enterprise application in Azure AD blade to register for SSO.

Conditional access policy - to ensure users access from Azure AD joined computers.

QUESTION 88

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that contains the following group:

Name: Group1

Members: User1, User2

Owner: User3

On January 15, 2021, you create an access review as shown in the exhibit. (Click the Exhibit tab.)

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name *	Review1	✓
Description ⓘ		
Start date *	01/15/2021	
Frequency	Monthly	
Duration (in days) ⓘ	14	
End ⓘ	<input type="radio"/> Never <input checked="" type="radio"/> End by Occurrences	
Number of times	0	
End date *	02/15/2021	
Users		
Users to review	Members of a group	
Scope	<input type="radio"/> Guest users only <input checked="" type="radio"/> Everyone	
Group *	Group1	
Reviewers		
Reviewers	Members (self)	
Programs		
Link to program > Default Business Flow		
✓ Upon completion settings ✓ Advanced settings		
<input type="button" value="Start"/>		

Users answer the Review1 question as shown in the following table.

User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

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
On February 5, 2021, User1 can answer the Review1 question again.	<input type="radio"/>	<input type="radio"/>
On January 25, 2021, User2 can answer the Review1 question again.	<input type="radio"/>	<input type="radio"/>
On January 22, 2021, User3 can answer the Review1 question.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	<input type="radio"/>	<input checked="" type="radio"/>
On January 25, 2021, User2 can answer the Review1 question again.	<input checked="" type="radio"/>	<input type="radio"/>
On January 22, 2021, User3 can answer the Review1 question.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No

The review end date is 14 days after the start (January 15), the end of the review cycle for the month is January 29. After that date, the review cycle will not start again until February 15.

Box 2: Yes

The user will not be removed from the group until the end of the access review period.

Box 3: No

Reviews are for Group1, which User3 is not a member of.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/review-your-access>

QUESTION 89

Hotspot Question

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc.

Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com. Both domain names are used for Fabrikam email addresses.

You plan to create an access package named package1 that will be accessible only to the users at Fabrikam.

You create a connected organization for Fabrikam.

You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses.

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

NOTE: Each correct selection is worth one point.

Answer Area

To allow access for users who have fabrikam.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

Answer:

Answer Area

To allow access for users who have fabrikam.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance**
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD**
- The External collaboration settings in Azure AD**

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-request-policy>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>

QUESTION 90**Case Study 1 - Contoso, Ltd****Overview**

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named ADatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question

You need to allocate licenses to the new users from ADatum. The solution must meet the technical requirements.

Which type of object should you create?

- A. a Dynamic User security group
- B. An OU
- C. A distribution group
- D. An administrative unit

Answer: A

Explanation:

Prompt states "License allocation for new users must be assigned automatically based on the location of the user." This would indicate a Dynamic Group with the Attribute of location to determine a License.

QUESTION 91

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

Hotspot Question

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

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

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

NOTE: Each correct selection is worth one point.

Configure the Azure AD Password Protection proxy service on:

DC1
SERVER1
SERVER2

Configure the password list:

In Azure AD
On DC1
On SERVER1
On SERVER2

Answer:

Configure the Azure AD Password Protection proxy service on:

DC1
SERVER1
SERVER2

Configure the password list:

In Azure AD
On DC1
On SERVER1
On SERVER2

Explanation:

Box 1: Server 2

Box 2: In Azure AD

The password protection proxy is installed on a member server. You enable the banned p/w list in Azure AD, the proxy downloads it and passes it to the DCs in the domain.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

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 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 must use the Microsoft 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 Fraud alert settings for multi-factor authentication (MFA).

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt using the Microsoft Authenticator app or through their phone.

The following fraud alert configuration options are available:

- Automatically block users who report fraud.
- Code to report fraud during initial greeting.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

QUESTION 93

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User2, 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.)

Role setting details - Application Administrator

Privileged Identity Management | Azure AD roles

 Edit

Activation

Setting	State
Activation maximum duration (hours)	5 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	Yes
Approvers	0 Member(s), 1 Group(

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on acti...	No
Require justification on active assignment	Yes

Group1 is configured as the approver for the application administrator role.

You configure User2 to be eligible for the application administrator role.

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

Add assignments

Privileged Identity Management | Azure AD roles

Membership **Setting**

Assignment type ⓘ

- Eligible
 Active

Maximum allowed eligible duration is 3 month(s).

Assignment starts *

01/01/2021		12:00:00 AM
------------	--	-------------

Assignment ends *

01/31/2021		11:59:00 PM
------------	--	-------------

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.	<input type="radio"/>	<input checked="" type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input checked="" type="radio"/>	<input type="radio"/>
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.	<input type="radio"/>	<input checked="" type="radio"/>

Answer:

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input type="radio"/>	<input checked="" type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input checked="" type="radio"/>	<input type="radio"/>
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.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

User1 is eligible from 1/1/2021 to 1/31/2021.

However, here the Application Administrator role requires approval.

Box 2: Yes

Approvers are not able to approve their own role activation requests.

Box 3: Yes

User1 is eligible from 1/1/2021 to 1/31/2021.

Activation maximum duration (hours) is set to 5 hours.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow>

QUESTION 94

Hotspot Question

You have a Microsoft 365 tenant.

You configure a conditional access policy as shown in the Conditional Access policy exhibit.

(Click the Conditional Access policy tab.)

Home > ContosoAzureAD > Security > Conditional access policies

Policy1 ...

Conditional access policy

 Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Policy1

Assignments

Users and groups ⓘ

All users

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Enable policy

Report-only  On 

Save

Grant

X

Control user access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ
[See list of approved client apps](#)

Require app protection policy ⓘ
[See list of policy protected client apps](#)

Require password change ⓘ

For multiple controls

Require all the selected controls

Require one of the selected controls

You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)

... > Privileged Identity Management > ContosoAzureAD > User Administrator >

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	1 Member(s), 0 Group

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

You view the User administrator role assignments as shown in the Role assignments exhibit.
(Click the Role assignments tab.)

... > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

» [+ Add assignments](#) [⚙️ Settings](#) [⟳ Refresh](#) [⬇️ Export](#) | [❤️ Got feedback?](#)

[Eligible assignments](#) [Active assignments](#) [Expired assignments](#)

Search by member name or principal name

Name	Principal name	Type	Scope	Membership
User Administrator				
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin3	Admin3@m365x629615.onmicrosoft.com	User	Directory	Direct

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	<input type="radio"/>	<input type="radio"/>
Admin2 can request activation of the User administrator role for a period of two hours.	<input type="radio"/>	<input type="radio"/>
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can request activation of the User administrator role for a period of two hours.	<input checked="" type="radio"/>	<input type="radio"/>
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 95

As the Azure Administrator for your organization, you need to create several security groups and populate those groups based on specific profile attributes of your users. As users join your organization, they should be automatically added to the correct group. What should you configure

for this?

- A. Power Groups
- B. Smart Groups
- C. Microsoft 365 Groups
- D. Dynamic Groups

Answer: D

QUESTION 96

Your organization has implemented Azure AD Connect to help support its Hybrid cloud initiatives and has synced all on-prem AD users to Azure AD. To meet organization compliance requirements, you need to ensure you can enforce password policies and limit sign-in hours for your users. Your solution should require the least administrative overhead. Which cloud authentication method should you use?

- A. Hybrid Authentication
- B. Federated Authentication
- C. Azure AD Password Hash synchronization
- D. Azure AD Pass-through authentication

Answer: D

QUESTION 97

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 names of litwareinc.com and contoso.com

Users can request access by using package 1.

Users at Fabrikam and Litware use all their respective domain names for email addresses.

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

You need to configure connected organizations for Fabrikam and Litware so that any of 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: C

QUESTION 98

Hotspot Question

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- Users that are assigned Role1 can create or delete instances of Azure Container Apps.
- Users that are assigned Role2 can enforce adaptive network hardening rules.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role1:

- Microsoft.App
- Microsoft.Compute
- Microsoft.Management
- Microsoft.Security

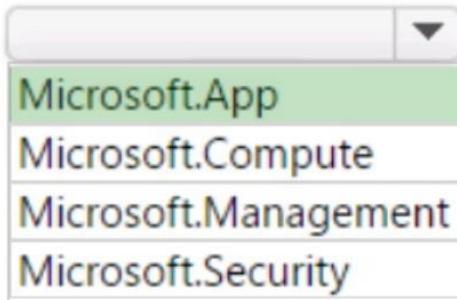
Role2:

- Microsoft.App
- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security

Answer:

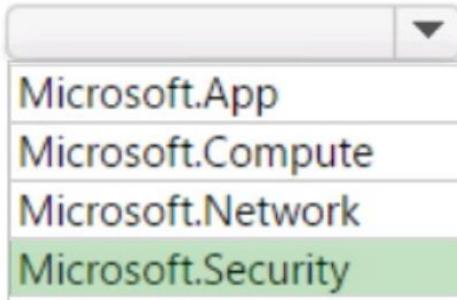
Answer Area

Role1:



Microsoft.App
Microsoft.Compute
Microsoft.Management
Microsoft.Security

Role2:



Microsoft.App
Microsoft.Compute
Microsoft.Network
Microsoft.Security

Explanation:

Role1: Microsoft.App

<https://learn.microsoft.com/en-us/azure/container-apps/quickstart-portal#prerequisites>

Role2: Microsoft.Security

<https://learn.microsoft.com/en-ie/rest/api/defenderforcloud/adaptive-network-hardenings/enforce?tabs=HTTP>

QUESTION 99

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 App1.
Which groups can you assign to App1?

- A. Group1 and Group3
- B. Group2 only
- C. Group3 only
- D. Group1 only
- E. Group1 and Group4

Answer: E

Explanation:

Group-based assignment requires Azure Active Directory Premium P1 or P2 edition. Group-based assignment is supported for Security groups only.

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

QUESTION 100

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 portal, create a continuous report.

Answer: C

Explanation:

One of the prerequisites to using a session policy is "The relevant apps should be deployed with Conditional Access App Control", which is done via the Azure AD Admin Center.

<https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad#prerequisites-to-using-session-policies>

<https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-aad>

QUESTION 101

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: C

Explanation:

The following authentication methods are available for SSPR (self-service password reset)

- app notification
 - Mobile app code
 - Email
 - Mobile phone
 - Office phone (available only for tenants with paid subscriptions)
 - Security questions
- <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

QUESTION 102

Your organization wants to take advantage of group based licensing, allowing various licenses to be automatically assigned to users based on security groups that they are a part of. As the cloud administrator, which license must your users have in order to take advantage of group based licensing?

- A. Azure AD P1
- B. Azure AD P2
- C. Office 365 E3
- D. Any of the above

Answer: D

QUESTION 103

You are the cloud administrator for Whizlabs Inc. and you have been tasked to implement multi-factor authentication for all of your users. In preparation for this, you need to ensure that all users are properly registered for multi-factor Authentication. Of the choices below, which one can NOT be used as an authentication method?

- A. Microsoft Authenticator App
- B. Security Questionright
- C. FIDO2 Security Key
- D. SMS
- E. Voice Call

Answer: B

QUESTION 104

Your company is currently reviewing all of its operating procedures and looking for ways to optimize efficiencies. One area of concern is the amount of time that Help Desk Administrators are spending on user issues. What is a service that you can implement to help reduce the calls and tickets opened for the Help Desk Administrators?

- A. Application Proxy
- B. Multi Factor Authentication
- C. Active Directory Connect
- D. Self Service Password Reset

Answer: D

QUESTION 105

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.

remember multi-factor authentication on trusted device (learn more)

Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)
Number of days users can trust devices for
NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. Learn more about reauthentication prompts.

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.

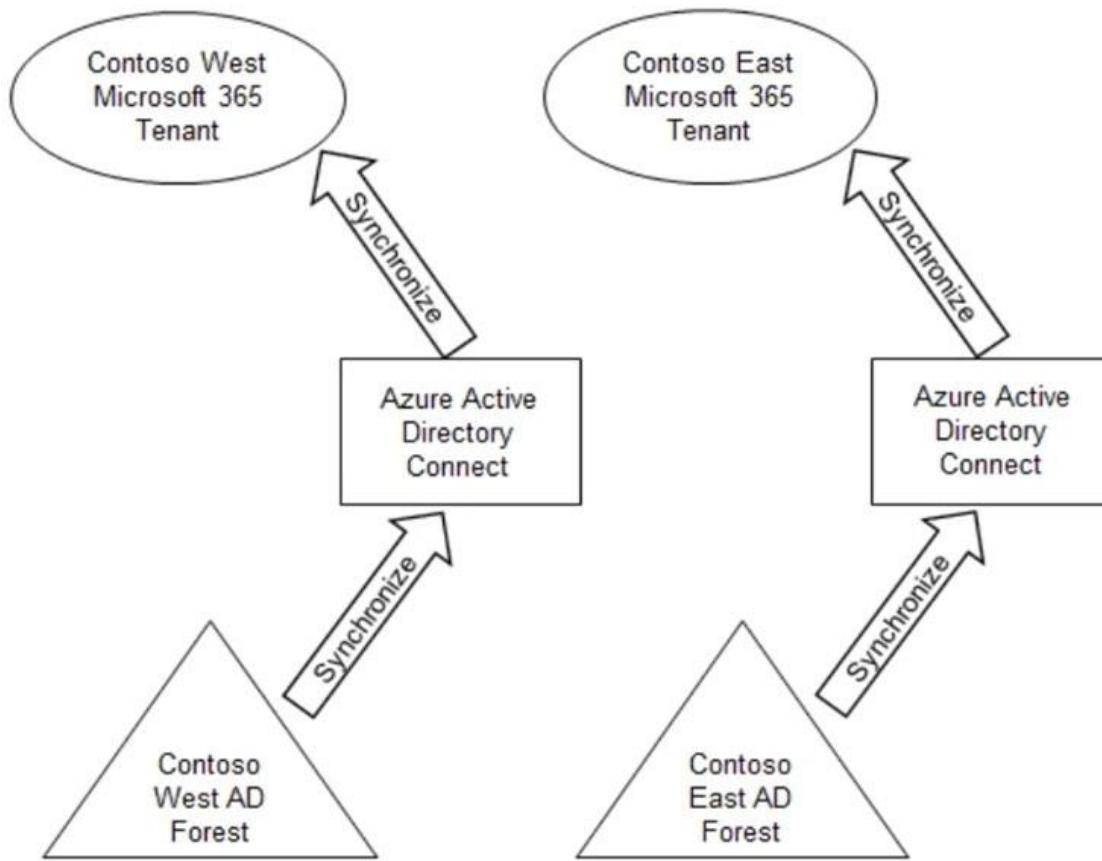
Name	Multi-factor auth status
User1	Enforced
User2	Enforced
User3	Enforced
- D.

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

Answer: B

QUESTION 106

Your company has two divisions named Contoso East and Contoso West. The Microsoft 365 identity architecture for 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?

- Configure The exiting Azure AD Connect server in Contoso Cast to sync the Contoso East Active Directory forest to the Contoso West tenant.
- Configure Azure AD Application Proxy in the Contoso West tenant.
- 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.
- Invite the Contoso East users as guests in the Contoso West tenant.

Answer: D

Explanation:

Before any of your users can grant SharePoint Online team site access to external guests, you will have to enable guest sharing from within Azure Active Directory.

Reference:

<https://redmondmag.com/articles/2020/03/11/guest-access-sharepoint-online-team-sites.aspx>

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/multi-tenant-common-considerations>

QUESTION 107

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

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AI user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure AD, you create an assignment for the Insights administrator role.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

QUESTION 108

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AI user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure monitor, you modify the action group.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Yes, you modify the action group from Azure Monitor.

<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups#configure-notifications>

QUESTION 109

Due to a recent company acquisition, you have inherited a new Azure tenant with 1 subscription associated that you have the manage. The security has been neglected and you are looking for a quick and easy way to enable various security settings like requiring users to Register for Multi-factor authentication, blocking legacy authentication protocols, and protecting privileged activities

like access to the Azure portal. What is the best way to enforce these settings with the least amount of administrative effort.

- A. Enable Security Defaultsright
- B. Configure Conditional Access Policies
- C. Configuring an Azure Policy
- D. Utilize Active Directory Sign-In Logs

Answer: A

QUESTION 110

You recently created a new Azure AD Tenant for your organization, Lead2pass Inc and you were assigned a default domain of whizlabs.onmicorosft.com. You want to use your own custom domain of whizlabs.com. You added the custom domain via the Azure portal and now you have to validate that you are the owner of the custom domain through your registrar. What type of record will you need to add to your domain registrar?

- A. TXT record
- B. A record
- C. CNAME record
- D. CAA record

Answer: A

QUESTION 111

You are looking to improve your organizations security posture after hearing about breaches and hacks of other organizations on the news. You have been looking into Azure Identity Protection and you are commissioning a team to begin implementing this service. This team will need full access to Identity Protection but would not need to reset passwords. You should follow the principle of least privilege. What role should you grant this new team?

- A. Security Operator
- B. Global Administrator
- C. Security Administratorright
- D. HelpDesk Administrator

Answer: C

QUESTION 112

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

An administrator deletes User1.

You need to identify the following:

- How many days after the account of User1 is deleted can you restore the account?
- Which is the least privileged role that can be used to restore User1?

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

NOTE: Each correct selection is worth one point.

Answer Area

Number of days:

15
30
90
180

Role:

User administrator
Network administrator
Helpdesk administrator
Domain name administrator

Answer:

Answer Area

Number of days:

15
30
90
180

Role:

User administrator
Network administrator
Helpdesk administrator
Domain name administrator

QUESTION 113

Drag and Drop Question

Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.

Attire AD Connect is installed on a server named Server1.

You deploy a new server named Server1 that runs Windows Server 2019.

You need to implement a failover server for Azure AD Connect. The solution must minimize how long it takes to fail over if Server1 fails.

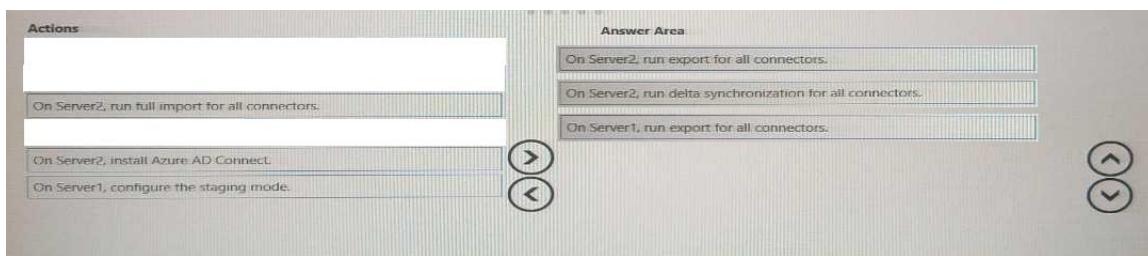
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
On Server1, run export for all connectors.	
On Server2, run export for all connectors.	
On Server2, run full import for all connectors.	
On Server2, run delta synchronization for all connectors.	
On Server2, install Azure AD Connect.	
On Server1, configure the staging mode.	

Move items between the Actions and Answer Area using the following buttons:

- Move selected item to the right (→)
- Move selected item to the left (←)
- Move all items to the right (⤒)
- Move all items to the left (⤑)

Answer:



The screenshot shows a software interface with two main sections: 'Actions' on the left and 'Answer Area' on the right.

Actions:

- On Server2, run full import for all connectors.
- On Server2, install Azure AD Connect.
- On Server1, configure the staging mode.

Answer Area:

- On Server2, run export for all connectors.
- On Server2, run delta synchronization for all connectors.
- On Server1, run export for all connectors.

Between the 'Actions' and 'Answer Area' sections are two circular arrows: a right-pointing arrow between the lists and a double-headed vertical arrow on the far right.

QUESTION 114

Hotspot Question

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

Name	User type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

For which users can you configure the Job title property and the Usage location property in Azure AD? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Job title property:

User2 only
 User1 and User2 only
 User2 and User3 only
 User1, User2, and User3

Usage location property:

User2 only
 User1 and User2 only
 User2 and User3 only
 User1, User2, and User3

Answer:

Job title property:

User2 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Usage location property:

User2 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Explanation:

Box 1: User2 and User3 only

Job title property for directory synched users cannot be updated from Azure AD.

Box 2: User1, User2, and User3

Invite users with Azure Active Directory B2B collaboration, Update user's name and usage location.

To assign a license, the invited user's Usage location must be specified. Admins can update the invited user's profile on the Azure portal.

1. Go to Azure Active Directory > Users and groups > All users. If you don't see the newly created user, refresh the page.
2. Click on the invited user, and then click Profile.
3. Update First name, Last name, and Usage location.
4. Click Save, and then close the Profile blade.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal>

<https://docs.microsoft.com/en-us/power-platform/admin/invite-users-azure-active-directory-b2b-collaboration#update-users-name-and-usage-location>

QUESTION 115

You are the lead cloud administrator for Lead2pass Inc. and you just hired a new employee that will be in charge of Azure AD Support issues. This new employee needs the ability to reset the passwords for all types of users when requested, including users with the user admin, global admin, or password admin roles. You need to ensure that you follow the principle of least privilege when granting access. What role should you grant the new employee?

- A. Password Admin
- B. Global Admin
- C. Security Admin
- D. User Admin

Answer: B

QUESTION 116

Your organization is considering allowing employees to work remotely and to use their own

devices to access many of the organization's resources. However, to help protect against potential data loss, your organization needs to ensure that only approved applications can be used to access the company data. What can you configure to meet this requirement?

- A. Privileged Identity Management
- B. Conditional Access Policies
- C. RBAC roles
- D. Azure Security Center

Answer: B

QUESTION 117

Your organization is looking to tighten its security posture when it comes to Azure AD users' passwords. There have been reports on local news recently of various organizations having user identities compromised due to using weak passwords or passwords that resemble the organization name or local sports team names. You want to provide protection for your organization as well as supplying a list of common words that are not acceptable passwords. What should you configure.

- A. Azure AD Password Protection
- B. Azure AD Privileged Identity Management
- C. Azure Defender for Passwords
- D. Azure AD Multi-factor Authentication

Answer: A

QUESTION 118

You have hired a new Azure Engineer that will be responsible for managing all aspects of enterprise applications and app registrations. This engineer will not need to manage anything application proxy related. You need to grant the proper role to the engineer to perform his job duties while maintaining the principle of least privilege. What role should you grant?

- A. Global Administrator
- B. Application Administrator
- C. Cloud Application Administrator
- D. Enterprise Administrator

Answer: C

QUESTION 119

You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

You need to ensure that users can connect to Exchange only run email clients that use Modern authentication protocols.

You need to ensure that use Modern authentication.

What should you implement?

- 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: C

QUESTION 120

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure monitor, you create a data collection rule.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Data Collection Rules (DCRs) define the data collection process in Azure Monitor. DCRs specify what data should be collected, how to transform that data, and where to send that data. Some DCRs will be created and managed by Azure Monitor to collect a specific set of data to enable insights and visualizations.

Reference:

[>](https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-rule-overview)

QUESTION 121

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. Configure an app registration.

- B. Create an Administrative unit.
- C. Create an access package.
- D. Create a catalog.

Answer: C

Explanation:

All access packages must be put in a container called a catalog. A catalog defines what resources you can add to your access package. If you don't specify a catalog, your access package will be put into the general catalog.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>

QUESTION 122

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

Name	Type
Role1	Azure Active Directory (Azure AD) role
Role2	Azure subscription role

You need to create a custom Azure subscription role named Role3 by using the Azure portal. Role3 will use the baseline permissions of an existing role.

Which roles can you clone to create Role3?

- A. Role2 only
- B. built-in Azure subscription roles only
- C. built-in Azure subscription roles and Role2 only
- D. built-in Azure subscription roles and built-in Azure AD roles only
- E. Role1, Role2 built-in Azure subscription roles, and built-in Azure AD roles

Answer: C

Explanation:

<https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#clone-a-role>

QUESTION 123

Your organization is a 100% Azure cloud based organization with no on-premise resources. You recently completed an acquisition of another company that is 100% on-premise with no cloud premise. You need to immediately provide your cloud users with access to a few of the acquired companies on-premise web applications. What service can you implement to ensure Azure Active Directory can still be used to authenticate to the on-premise applications?

- A. Azure Active Directory Connect
- B. Azure Security Center
- C. Azure Active Directory Application Proxyright
- D. Azure Active Directory Domain Services

Answer: C

QUESTION 124

Your organization is working with a new consulting firm to help with the design, development, and deployment of a new IT service. The consultants will be joining your organization at various points throughout the project and will not know what permissions they need or who to request the access from. As the Cloud Administrator, what can you implement to ensure consultants can easily request and get all of the access they need to do their job?

- A. Azure Arm Templates
- B. Azure Blueprints
- C. Azure Policies
- D. Azure AD Entitlement Management

Answer: D

QUESTION 125

Drag and Drop Question

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company 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 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.

Actions	Answer Area
Add a group claim.	
Create an app registration.	
Grant admin consent.	
Add delegated permissions.	
Add app permissions.	

Answer:

Actions

Add a group claim.

Add delegated permissions.

Answer Area

Create an app registration.

Add app permissions.

Grant admin consent.

Explanation:

1. Create an app registration:

Your app must be registered with the Microsoft identity platform and be authorized by either a user or an administrator for access to the Microsoft Graph resources it needs.

2. Add app permissions:

After the consents to permissions for your app, your app can acquire access tokens that represent the app's permission to access a resource in some capacity. Encoded inside the access token is every permission that your app has been granted for that resource.

3. Grant admin consent:

Higher-privileged permissions require administrator consent.

Reference:

<https://docs.microsoft.com/en-us/graph/permissions-reference>

QUESTION 126

Hotspot Question

You have a Microsoft 36S tenant.

You create a named location named HighRiskCountries that contains a list of high-risk countries.

You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country.

What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Configure HighRiskCountries by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Configure Sign-in frequency by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Answer:

Answer Area

Configure HighRiskCountries by using:

- A cloud app or action
- A condition**
- A grant control
- A session control

Configure Sign-in frequency by using:

- A cloud app or action
- A condition**
- A grant control**
- A session control**

Explanation:

Reference:

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

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

QUESTION 127

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that has multi-factor authentication (MFA) enabled.

The account lockout settings are configured as shown in the following exhibit.

Account lockout

Temporarily lock accounts in the multi-factor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate.

Number of MFA denials to trigger account lockout *

✓

Minutes until account lockout counter is reset *

✓

Minutes until account is automatically unblocked *

✓

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

A user account will be locked out if the user enters the wrong [answer choice] three times.

If a user account is locked, the user can sign in again successfully after [answer choice] minutes.

Answer:

Answer Area

A user account will be locked out if the user enters the wrong [answer choice] three times.

If a user account is locked, the user can sign in again successfully after [answer choice] minutes.

QUESTION 128

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity.

While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. email
- C. security questions
- D. a verification code from the Microsoft Authenticator app

Answer: D

Explanation:

The Authenticator app can be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.

Incorrect Answers:

A: A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the logon.

B: An email requires network connectivity.

C: Security questions are not used as an authentication method but can be used during the self-service password reset (SSPR) process.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app>

QUESTION 129

Hotspot Question

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.

Devices | Device settings ...

Default Directory - Azure Active Directory

Save Discard Got feedback?

All devices

Device settings

Enterprise State Roaming

BitLocker keys (Preview)

Diagnose and solve problems

Activity

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

Users may join devices to Azure AD ⓘ

All Selected None

Selected
No member selected

Users may register their devices with Azure AD ⓘ

All None

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication ⓘ

Yes No

⚠ We recommend that you require Multi-Factor Authentication to register or join devices using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

Maximum number of devices per user ⓘ

5

Additional local administrators on all Azure AD joined devices

[Manage Additional local administrators on All Azure AD joined devices](#)

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 Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	<input type="radio"/>	<input type="radio"/>
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to Yes.	<input type="radio"/>	<input type="radio"/>
Admin2 is a local administrator on Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to Yes .	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 is a local administrator on Device3.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No

Maximum number of devices: This setting enables you to select the maximum number of Azure AD joined or Azure AD registered devices that a user can have in Azure AD.

Box 2: Yes

You must be assigned one of the following roles to view or manage device settings in the Azure portal:

- Global Administrator
- Cloud Device Administrator
- Global Reader
- Directory Reader

Box 3: No

Additional local administrators on Azure AD joined devices (Device is Registered not Joined)

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

QUESTION 130

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure AD, you create an assignment for the Insights administrator role.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Permissions should be given to a Security Administrator.

Insights Administrator is an administrator Ofc365 Viva app. (Employee Experience Platform).

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator>

QUESTION 131

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure AD, you modify the Diagnostics settings.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Need to go to Azure monitor to modify action group not diagnostic settings.

QUESTION 132

Drag and Drop Question

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	<ul style="list-style-type: none">• User administrator role• Device Administrators role• Identity Governance Administrator role
User2	<ul style="list-style-type: none">• Records Management role• Quarantine Administrator role group
User3	<ul style="list-style-type: none">• Endpoint Security Manager role• Intune Role Administrator role

Which portal should you use to configure each user? To answer, drag the appropriate portals to the 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	Answer Area
Azure Active Directory admin center	
Exchange admin center	User1: _____
Microsoft 365 compliance center	User2: _____
Microsoft Endpoint Manager admin center	User3: _____
SharePoint admin center	

Answer:

Portals	Answer Area
Exchange admin center	User1: Azure Active Directory admin center
	User2: Microsoft 365 compliance center
	User3: Microsoft Endpoint Manager admin center
SharePoint admin center	

Explanation:

User 1: Azure Active Directory Admin Center

User 2: Microsoft Purview admin center (legacy Microsoft Compliance Admin center)

These roles came from Exchange, Microsoft is not enforcing the roles permission from Exchange, Microsoft is recommending using Microsoft Purview Admin center. I believe this answer is too old. It could be true years ago, however, Microsoft today is with MS Purview to assign these roles. Record management and Quarantine role are known as SCC (security and compliance center) SCC roles have evolved from Exchange role groups design to MS Purview.

User 3: Microsoft Endpoint Manager Admin Center

You will see these two roles in the endpoint admin center.

QUESTION 133

You have an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant. The tenant uses pass-through authentication.

A corporate security policy states the following:

- Domain controllers must never communicate directly to the internet.
- Only required software must be installed on servers.

The Active Directory domain contains the on-premises servers shown in the following table.

Name	Description
Server1	Domain controller (PDC emulator)
Server2	Domain controller (infrastructure master)
Server3	Azure AD Connect server
Server4	Unassigned member server

You need to ensure that users can authenticate to Azure AD if a server fails.

On which server should you install an additional pass-through authentication agent?

- A. Server4
- B. Server2
- C. Server1
- D. Server3

Answer: A

Explanation:

The standalone Authentication Agents can be installed on any Windows Server 2016 or later, with TLS 1.2 enabled. The server needs to be on the same Active Directory forest as the users whose passwords you need to validate.

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start>

QUESTION 134

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 contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.

What should you do?

- A. Run the New-AzureADMSInvitation cmdlet.
- B. Configure the External collaboration settings.
- C. Add a WS-Fed identity provider.
- D. Implement Azure AD Connect.

Answer: A

Explanation:

By default, all users in your organization, including B2B collaboration guest users, can invite external users to B2B collaboration. If you want to limit the ability to send invitations, you can turn invitations on or off for everyone, or limit invitations to certain roles.
<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure>

QUESTION 135

You have 2,500 users who are assigned Microsoft Office 365 Enterprise 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 Administrative units blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Groups blade in the Azure Active Directory admin center
- D. the Set-MsolUserLicense cmdlet

Answer: D

Explanation:

The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.

Note:

There are several versions of this QUESTION 1 in the exam. The QUESTION 1 has two possible correct answers:

- 3. the Licenses blade in the Azure Active Directory admin center
- 4. the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

- the Identity Governance blade in the Azure Active Directory admin center
- the Set-WindowsProductKey cmdlet
- the Set-AzureAdGroup cmdlet

Reference:

<https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0>

QUESTION 136

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant and an Azure web app named App1.

You need to provide guest users 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 process.

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 Area

One-time password:

A linked subscription
An identity provider
Azure AD Privileged Identity Management (PIM)
The External collaboration settings

User details:

A user flow
Access reviews
An access package
The tenant properties

Answer:

Answer Area

One-time password:

A linked subscription
An identity provider
Azure AD Privileged Identity Management (PIM)
The External collaboration settings

User details:

A user flow
Access reviews
An access package
The tenant properties

Explanation:

Box 1: Identity Provider

First you'll enable self-service sign-up for your tenant and federate with the identity providers you want to allow external users to use for sign-in.

Box 2: User Flow

Then you'll create and customize the sign-up user flow and assign your applications to it.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity-providers>

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/self-service-sign-up-overview>

QUESTION 137

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

You need to bulk create 25 new user accounts by uploading a template file.

Which properties are required in the template file?

- A. displayName, identityIssuer, usageLocation, **and** userType
- B. accountEnabled, givenName, surname, **and** userPrincipalName
- C. accountEnabled, displayName, userPrincipalName, **and** passwordProfile
- D. accountEnabled, passwordProfile, usageLocation, **and** userPrincipalName

Answer: C

Explanation:

Name [displayName] -> Required

User name [userPrincipalName] -> Required

Initial password [passwordProfile] -> Required,

Block sign in (Yes/No) [accountEnabled] -> Required

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-add>

QUESTION 138

Hotspot Question

A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:

- Pa55w0rd12
- Pa55w0rd12
- Pa55w0rd12
- Pa55w.rd12
- Pa55w.rd123
- Pa55w.rd123
- Pa55w.rd123
- Pa55word12
- Pa55word12
- Pa55word12
- Pa55w.rd12

You need to identify how many sign-in attempts were tracked for User1, and how User1 can

unlock her account before the 300-second lockout duration expires.

What should identify? To answer, select the appropriate

NOTE: Each correct selection is worth one point.

Answer Area

Tracked sign-in attempts:

4
5
10
11

Unlock by:

Clearing the browser cache
Signing in by using inPrivate browsing mode
Performing a self-service password reset (SSPR)

Answer:

Answer Area

Tracked sign-in attempts:

4
5
10
11

Unlock by:

Clearing the browser cache
Signing in by using inPrivate browsing mode
Performing a self-service password reset (SSPR)

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

QUESTION 139

You have an Azure Active Directory (Azure AD) tenant that contains cloud-based enterprise apps.

You need to group related apps into categories in the My Apps portal.

What should you create?

- A. tags
- B. collections
- C. naming policies
- D. dynamic groups

Answer: B

Explanation:

On the My Apps portal, applications appear in default collections and your custom app collections. The Apps collection in My Apps is a default collection that contains all the applications that have been assigned to you, sorted alphabetically.

<https://support.microsoft.com/en-us/account-billing/customize-app-collections-in-the-my-apps-portal-2dae6b8a-d8b0-4a16-9a5d-71ed4d6a6c1d>

QUESTION 140

You have an Azure Active Directory Premium P2 tenant.

You create a Log Analytics workspace.

You need to ensure that you can view Azure Active Directory (Azure AD) audit log information by using Azure Monitor.

What should you do first?

- A. Run the `Set-AzureADTenantDetail` cmdlet.
- B. Create an Azure AD workbook.
- C. Modify the Diagnostics settings for Azure AD.
- D. Run the `Get-AzureADAuditDirectoryLogs` cmdlet.

Answer: C

Explanation:

AAD/Diagnostic Settings/Add Diagnostic Settings/Export Settings/Send to Log Analytic Workspace.

<https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics#send-logs-to-azure-monitor>

QUESTION 141

Hotspot Question

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

Name	Role
User1	None
User2	Privileged authentication administrator
User3	Global administrator

In Azure AD Privileged Identity Management (PIM), you configure the Global administrator role as shown in the following exhibit.

[!\[\]\(8a8fbd26e26f307b8da73370386bcdc6_img.jpg\) Edit](#)

Setting	State
Activation maximum duration (hours)	1 hour(s)
vRequire justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

User1 is eligible for the Global administrator role.

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 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role.	<input type="radio"/>	<input type="radio"/>
User2 must approve all activation requests for the Global administrator role.	<input type="radio"/>	<input type="radio"/>
User2 and User3 can edit the Global administrator role assignment.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must approve all activation requests for the Global administrator role.	<input type="radio"/>	<input checked="" type="radio"/>
User2 and User3 can edit the Global administrator role assignment.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

MFA is required on activation

Box 2: No

The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.

The Privileged Role Administrator can manage role assignments, including the Global Administrator role, in Azure Active Directory, as well as within Azure AD Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

Box 3: No

The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.

The Privileged Role Administrator can manage role assignments, including the Global

Administrator role, in Azure Active Directory, as well as within Azure AD Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

QUESTION 142

Case Study 3 - A. Datum Corp

Overview

A. Datum Corporation is a consulting company in Montreal. A. Datum recently acquired a Vancouver-based company named Litware, Inc.

Existing Environment

A Datum Environment

The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

A. Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect. A. Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Name	Role
User1	None
User2	None
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

The tenant contains the groups shown in the following table.

Name	Type	Membership type	Owner	Members
IT_Group1	Security	Assigned	None	All users in the IT department
AdatumUsers	Security	Assigned	None	User1, User2

Existing Environment

Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment

Problem Statements

A. Datum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role To IT_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

Requirements

Planned Changes

- A. Datum plans to implement the following changes;
- Configure self-service password reset {SSPR}.
 - Configure multi-factor authentication (MFA) for all users.
 - Configure an access review for an access package named Package1.
 - Require admin approval for application access to organizational data.
 - Sync the AD DS users and groupsoftlitware.com with the Azure AD tenant.
 - Ensure that only users that are assigned specific admin roles can invite guest users.
 - Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Requirements

Technical Requirements

- A. Datum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR.

Available methods must include:

- Email
- Phone
- Security questions
- The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

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 the litware.com domain

Answer: B

QUESTION 143

Case Study 3 - A. Datum Corp

Overview

A. Datum Corporation is a consulting company in Montreal. A. Datum recently acquired a Vancouver-based company named Litware, Inc.

Existing Environment

A Datum Environment

The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

A. Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect. A. Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Name	Role
User1	None
User2	None
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

The tenant contains the groups shown in the following table.

Name	Type	Membership type	Owner	Members
IT_Group1	Security	Assigned	None	All users in the IT department
AdatumUsers	Security	Assigned	None	User1, User2

Existing Environment

Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment

Problem Statements

A. Datum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role To IT_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

Requirements

Planned Changes

- A. Datum plans to implement the following changes;
- Configure self-service password reset {SSPR}.
 - Configure multi-factor authentication (MFA) for all users.
 - Configure an access review for an access package named Package1.
 - Require admin approval for application access to organizational data.
 - Sync the AD DS users and groupsoftlitware.com with the Azure AD tenant.
 - Ensure that only users that are assigned specific admin roles can invite guest users.
 - Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Requirements

Technical Requirements

- A. Datum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR.

Available methods must include:

- Email
- Phone
- Security questions
- The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

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: C

Explanation:

Azure Portal> Azure AD > Identity Governance > (Entitlement Management Heading) Access Packages > + New Access Package (from the top bar) > (Resources tab) + Applications > (Requests tab) in the section "users who can requests" we check box " for users in your directory), and then "all members(incl. guests), and then in the section " approval, we select "Yes" ..etc

QUESTION 144

Case Study 3 - A. Datum Corp

Overview

A. Datum Corporation is a consulting company in Montreal. A. Datum recently acquired a Vancouver-based company named Litware, Inc.

Existing Environment

A Datum Environment

The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

A. Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect. A. Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Name	Role
User1	None
User2	None
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

The tenant contains the groups shown in the following table.

Name	Type	Membership type	Owner	Members
IT_Group1	Security	Assigned	None	All users in the IT department
AdatumUsers	Security	Assigned	None	User1, User2

Existing Environment

Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment

Problem Statements

A. Datum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role To IT_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

Requirements

Planned Changes

- A. Datum plans to implement the following changes;
- Configure self-service password reset {SSPR}.
 - Configure multi-factor authentication (MFA) for all users.
 - Configure an access review for an access package named Package1.
 - Require admin approval for application access to organizational data.
 - Sync the AD DS users and groupsoftitware.com with the Azure AD tenant.
 - Ensure that only users that are assigned specific admin roles can invite guest users.
 - Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Requirements

Technical Requirements

- A. Datum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR.

Available methods must include:

- Email
- Phone
- Security questions
- The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

Hotspot Question

You implement the planned changes for SSPR.

What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Number of authentication methods required:

Authentication methods that can be used:

 Microsoft Authenticator only
 Security questions only
 Email and phone only
 Phone and Microsoft Authenticator only
 Email, phone, and Microsoft Authenticator only
 Email, phone, Microsoft Authenticator, and security questions

Answer:

Answer Area

Number of authentication methods required:

1
2
3
4

Authentication methods that can be used:

Microsoft Authenticator only
Security questions only
Email and phone only
Phone and Microsoft Authenticator only
Email, phone, and Microsoft Authenticator only
Email, phone, Microsoft Authenticator, and security questions

Explanation:

Box 1: 2

Why: By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced.

Box 2: Email, phone and Microsoft Authenticator only

Why: The two-gate policy requires two pieces of authentication data, such as an email address, authenticator app, or a phone number, and it prohibits security questions.

A two-gate policy applies in the following circumstances:

.....

Security administrator
Service support administrator
SharePoint administrator
Skype for Business administrator
User administrator

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>

QUESTION 145**Case Study 3 - A. Datum Corp****Overview**

A. Datum Corporation is a consulting company in Montreal. A. Datum recently acquired a Vancouver-based company named Litware, Inc.

Existing Environment**A Datum Environment**

The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

A. Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect. A. Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Name	Role
User1	None
User2	None
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

The tenant contains the groups shown in the following table.

Name	Type	Membership type	Owner	Members
IT_Group1	Security	Assigned	None	All users in the IT department
AdatumUsers	Security	Assigned	None	User1, User2

Existing Environment

Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment

Problem Statements

A. Datum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role To IT_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

Requirements

Planned Changes

A. Datum plans to implement the following changes;

- Configure self-service password reset {SSPR}.
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groupsoflitware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Requirements

Technical Requirements

A. Datum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.

- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.

- Users must provide one authentication method to reset their password by using SSPR.

Available methods must include:

- Email

- Phone

- Security questions

- The Microsoft Authenticator app

- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.

- The principle of least privilege must be used.

Drag and Drop Question

You need to resolve the recent security incident issues.

What should you configure for each incident? To answer, drag the appropriate policy types to the correct issues. Each policy type 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.

Policy Types	Answer Area
An authentication method policy	Leaked credentials: <input type="text"/>
A Conditional Access policy	A sign-in from a suspicious browser: <input type="text"/>
A sign-in risk policy	Resources accessed from an anonymous IP address: <input type="text"/>
A user risk policy	

Answer:

Policy Types	Answer Area
An authentication method policy	Leaked credentials: A user risk policy
A Conditional Access policy	A sign-in from a suspicious browser: A sign-in risk policy
A sign-in risk policy	Resources accessed from an anonymous IP address: A sign-in risk policy
A user risk policy	

Explanation:

Box 1: A user risk policy

User-linked detections include:

Leaked credentials: This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials.

User risk policy

Identity Protection can calculate what it believes is normal for a user's behavior and use that to base decisions for their risk. User risk is a calculation of probability that an identity has been compromised. Administrators can make a decision based on this risk score signal to enforce organizational requirements. Administrators can choose to block access, allow access, or allow access but require a password change using Azure AD self-service password reset.

Box 2: A sign-in risk policy

Suspicious browser: Suspicious browser detection indicates anomalous behavior based on suspicious sign-in activity across multiple tenants from different countries in the same browser.

Box 3: A sign-in risk policy

A sign-in risks include activity from anonymous IP address: This detection is discovered by Microsoft Defender for Cloud Apps. This detection identifies that users were active from an IP address that has been identified as an anonymous proxy IP address.

Note: The following three policies are available in Azure AD Identity Protection to protect users and respond to suspicious activity. You can choose to turn the policy enforcement on or off, select users or groups for the policy to apply to, and decide if you want to block access at sign-in or prompt for additional action.

* User risk policy

Identifies and responds to user accounts that may have compromised credentials. Can prompt the user to create a new password.

* Sign in risk policy

Identifies and responds to suspicious sign-in attempts. Can prompt the user to provide additional forms of verification using Azure AD Multi-Factor Authentication.

* MFA registration policy

Makes sure users are registered for Azure AD Multi-Factor Authentication. If a sign-in risk policy prompts for MFA, the user must already be registered for Azure AD Multi-Factor Authentication.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

QUESTION 146
Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question

You need to resolve the issue of the sales department users.

What should you configure for the Azure AD tenant?

- A. the Device settings
- B. the Access reviews settings
- C. the User settings
- D. Security defaults

Answer: B

Explanation:

Access Review: Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

QUESTION 147

Drag and Drop Question

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 of least 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 the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles	Answer Area
Global administrator	
Global reader	User1: <input type="text"/>
Reports reader	User2: <input type="text"/>
Security operator	
Security reader	
User administrator	

Answer:

Roles	Answer Area
Global administrator	
Global reader	User1: User administrator
Reports reader	
Security operator	User2: Security reader

Explanation:

User 1: User Administrator

Create, update, or delete access review of a group or of an app User Administrator.

User 2: Security Reader

Read access review of an Azure AD role Security Reader.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/deploy-access-reviews#what-resource-types-can-be-reviewed>

QUESTION 148

Hotspot Question

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-factor authentication (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 Area

Object type:

- An administrative unit
- A custom administrator role
- A dynamic group
- A Microsoft 365 group

Role:

- Authentication administrator
- Groups administrator
- Helpdesk administrator
- Password administrator

Answer:

Answer Area

Object type:

- An administrative unit
- A custom administrator role
- A dynamic group
- A Microsoft 365 group

Role:

- Authentication administrator
- Groups administrator
- Helpdesk administrator
- Password administrator

QUESTION 149

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- Use custom catalogs and custom programs for Identity Governance.

- Ensure that User1 can create enterprise applications in Azure AD.
- Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

Hotspot Question

You need to 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

Feature:

An authentication method policy
A Conditional Access policy
An MFA registration policy
The Multi-Factor Authentication Server settings

Grace period:

7 days
14 days
28 days

Answer:

Answer Area

Feature:

An authentication method policy
A Conditional Access policy
An MFA registration policy
The Multi-Factor Authentication Server settings

Grace period:

7 days
14 days
28 days

Explanation:

Box 1: An MFA registration policy

Box 2: 14 days

Multi-factor authentication (MFA): multi-factor authentication is a type of authentication that requires the use of two or more verification factors to gain access to a system. Azure MFA offers a 14 day grace period after being initiated.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy#policy-configuration>

QUESTION 150

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question

You need to modify the settings of the User administrator role to meet the technical requirements.

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

NOTE: Each correct selection is worth one point.

- A. Select Require justification on activation.
- B. Select Require ticket information on activation.
- C. Modify the Expire eligible assignments after setting.
- D. Set all assignments to Eligible.
- E. Set all assignments to Active.

Answer: AD

Explanation:

Scenario: Configure the User administrator role to require justification and approval to activate. Require justification.

You can require that users enter a business justification when they activate. To require justification, check the Require justification on active assignment box or the Require justification on activation box.

To require justification need assignment to be Eligible instead of Active.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

QUESTION 151

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question

You need to resolve the issue of the guest user invitations.

What should you do for the Azure AD tenant?

- A. Configure the Continuous access evaluation settings.
- B. Configure a Conditional Access policy.
- C. Configure the Access reviews settings.
- D. Modify the External collaboration settings.

Answer: D

Explanation:

You can add enable 'Guest Inviter' role. But you cannot enable self-service role for 'Office 365' apps. So far, that is only available for apps you build.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure#configure-settings-in-the-portal>

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/self-service-sign-up-user-flow#enable-self-service-sign-up-for-your-tenant>

QUESTION 152

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. You need to ensure that User1 can create new catalogs and add resources to the catalogs they own.

What should you do?

- A. From the Roles and administrators blade, modify the Groups administrator role.
- B. From the Roles and administrators blade, modify the Service support administrator role.
- C. From the Identity Governance blade, modify the Entitlement management settings.
- D. From the Identity Governance blade, modify the roles and administrators for the General catalog.

Answer: C

Explanation:

Delegate entitlement management

By default, only Global Administrators and User Administrators can create and manage catalogs, and can manage all catalogs. Users added to entitlement management as Catalog creators can also create catalogs and will become the owner of any catalogs they create.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-delegate-catalog#as-an-it-administrator-delegate-to-a-catalog-creator>

QUESTION 153

Hotspot Question

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

Name	Role
User1	Security administrator
User2	Privileged authentication administrator
User3	Service support administrator

User2 reports that he can only configure multi-factor authentication (MFA) to use the Microsoft Authenticator app.

You need to ensure that User2 can configure alternate MFA methods.

Which configuration is required, and which user should perform the configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Configuration:

Enable access reviews.
Enable Azure AD Privileged Identity Management (PIM).
Modify security defaults.

User:

User1 only
User2 only
User3 only
User1 and User2 only
User1 and User3 only
User2 and User3 only

Answer:**Answer Area**

Configuration:

Enable access reviews.
Enable Azure AD Privileged Identity Management (PIM).
Modify security defaults.

User:

User1 only
User2 only
User3 only
User1 and User2 only
User1 and User3 only
User2 and User3 only

Explanation:

Box 1: Modify security defaults

Privileged Authentication Administrator

Users with this role can set or reset any authentication method (including passwords) for any user, including Global Administrators. Privileged Authentication Administrators can force users to re-register against existing non-password credential (such as MFA or FIDO) and revoke 'remember MFA on the device', prompting for MFA on the next sign-in of all users.

The Authentication Administrator role has permission to force re-registration and multifactor

authentication for standard users and users with some admin roles.

Role	Manage user's auth methods	Manage per-user MFA	Manage MFA settings	Manage auth method	Manage password protection policy
Authentication Administrator	Yes for some users (see above)	Yes for some users (see above)	No	No	No
Privileged Authentication Administrator	Yes for all users	Yes for all users	No	No	No
Authentication Policy Administrator	No	No	Yes	Yes	Yes

Box 2: User1 only

Security Administrator.

Users with this role have permissions to manage security-related features in the Microsoft 365 Defender portal, Azure Active Directory Identity Protection, Azure Active Directory Authentication, Azure Information Protection, and Office 365 Security & Compliance Center.

Incorrect:

Not User3. Service Support Administrator.

Users with this role can create and manage support requests with Microsoft for Azure and Microsoft 365 services, and view the service dashboard and message center in the Azure portal and Microsoft 365 admin center.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

QUESTION 154

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 Microsoft Teams chat
- a mobile app notification

- C. a mobile app code
- D. an FID02 security token

Answer: C

Explanation:

The following authentication methods are available for SSPR (self-service password reset)

- app notification
- Mobile app code
- Email
- Mobile phone
- Office phone (available only for tenants with paid subscriptions)
- Security questions

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

QUESTION 155

You have an Azure Active Directory (Azure AD) tenant that uses Azure AD Identity Protection 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 password the next time he signs in. The solution must minimize administrative effort.

What should you do?

- A. Reconfigure the user risk policy to trigger on medium or low severity.
- B. Mark User1 as compromised.
- C. Reset the Azure MIFA registration for User1.
- D. Configure a sign-in risk policy.

Answer: B

Explanation:

Scenario: User compromised (True positive)

'Risky users' report shows an at-risk user [Risk state = At risk] with low risk [Risk level = Low] and that user was indeed compromised.

Feedback: Select the user and click on 'Confirm user compromised'.

What happens under the hood? Azure AD will move the user risk to High [Risk state = Confirmed compromised; Risk level = High] and will add a new detection

'Admin confirmed user compromised'.

Notes: Currently, the 'Confirm user compromised' option is only available in 'Risky users' report. The detection 'Admin confirmed user compromised' is shown in the tab 'Risk detections not linked to a sign-in' in the 'Risky users' report.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback>

QUESTION 156

Hotspot Question

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

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Enabled but never used
User2	Group2	Disabled
User3	Group1, Group2	Enforced and used

In Azure AD Identity Protection, you configure a user risk policy that has the following settings:

- Assignments:
 - Users: Group1
 - User risk: Low and above

Controls:

- Access: Block access

- Enforce policy: On

In Azure AD Identify Protection, you configure a sign-in risk policy that has the following settings:

- Assignments:

- Users: Group2
- Sign-in risk: Low and above

▪ Controls:

- Access: Require multi-factor authentication

- Enforce policy: On

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can sign in from an anonymous IP address.	<input type="radio"/>	<input type="radio"/>
User2 can sign in from an anonymous IP address.	<input type="radio"/>	<input type="radio"/>
User3 can sign in from an anonymous IP address.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can sign in from an anonymous IP address.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in from an anonymous IP address.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can sign in from an anonymous IP address.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Sign-in from an anonymous IP address falls into Sign-in risk. This means only members of Group 2 will be affected by Identity Protection.

Box 1: Yes

User1 can log in from any IP as user's IP is not scrutinized. The user is not in scope of Sign-In policy.

Box 2: No

User2 cannot login. This user is in scope of the Sign-In policy and will be challenged to perform MFA. Since MFA is disabled, MFA challenge will be unsuccessful - login fails.

Box 3: Yes

User3 can log in. This user is also in scope of the Sign-In policy, but since user's MFA is working (hence assuming a successful MFA challenge) the user will be granted access.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

QUESTION 157

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. an email to an address outside your organization
- B. a smartcard
- C. an FID02 security token
- D. a Microsoft Teams chat

Answer: A

Explanation:

The following authentication methods are available for SSPR (self-service password reset)

- app notification
- Mobile app code
- Email

- Mobile phone
 - Office phone (available only for tenants with paid subscriptions)
 - Security questions
- <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

QUESTION 158

You have an Azure Active Directory (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?

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only

Answer: A

Explanation:

Microsoft Authenticator

You can also allow your employee's phone to become a passwordless authentication method.

You may already be using the Authenticator app as a convenient multi-factor authentication option in addition to a password. You can also use the Authenticator App as a passwordless option.

The Authenticator App turns any iOS or Android phone into a strong, passwordless credential. Users can sign in to any platform or browser by getting a notification to their phone, matching a number displayed on the screen to the one on their phone, and then using their biometric (touch or face) or PIN to confirm.

FIDO2 security keys

The FIDO (Fast IDentity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication. FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard.

FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign in to their resources without a username or password using an external security key or a platform key built into a device.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

QUESTION 159

You have an Azure Active Directory (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 to 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

Explanation:

The Azure AD conditional access What if tool allows you to understand the impact of your conditional access policies on your environment. Instead of test driving your policies by performing multiple sign-ins manually, this tool enables you to evaluate a simulated sign-in of a user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report. The report does not only list the applied conditional access policies but also classic policies if they exist.

Reference:

<https://azure.microsoft.com/en-us/updates/azure-ad-conditional-access-what-if-tool-is-now-available>

QUESTION 160

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. an app password

- B. voice
- C. Windows Hello for Business
- D. security questions

Answer: C

Explanation:

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview>

QUESTION 161

You create a conditional access policy that blocks access when a user triggers a high-severity 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 Active Directory (Azure AD)
- C. the activity logs in Microsoft Defender for Cloud Apps
- D. access reviews in Azure Active Directory (Azure AD)

Answer: A

Explanation:

The Azure AD conditional access What if tool allows you to understand the impact of your conditional access policies on your environment. Instead of test driving your policies by performing multiple sign-ins manually, this tool enables you to evaluate a simulated sign-in of a user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report. The report does not only list the applied conditional access policies but also classic policies if they exist.

Reference:

<https://azure.microsoft.com/en-us/updates/azure-ad-conditional-access-what-if-tool-is-now-available>

QUESTION 162

Hotspot Question

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

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Disabled
User2	Group2	Enforced

You have the locations shown in the following table.

Name	Private address space	Public NAT address space
Location1	10.10.0.0/16	20.93.15.0/24
Location2	192.168.0.0/16	193.17.17.0/24

The tenant contains a named location that has the following configurations:

- Name: Location1
- Mark as trusted location: Enabled

IPv4 range: 10.10.0.0/16 -

MFA has a trusted IP address range of 193.17.17.0/24.

- Name: CAPolicy1
- Assignments
 - Users or workload identities: Group1
 - Cloud apps or actions: All cloud apps
- Conditions
- Locations: All trusted locations
- Access controls
- Grant
 - Grant access: Require multi-factor authentication
 - Session: 0 controls selected
- Enable policy: On

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements

If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.

If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.

If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.

Explanation:

Box 1: No

User1 will not be prompted for MFA because user not in CA scope and MFA is disabled.

Box 2: Yes

User2's source IP is 10.10.1.160, the public IP of which is in the range of 20.93.15.0/24, which isn't a trusted MFA range. Besides, User2 is a per-user MFA-enforced user. Therefore, User2 will be prompted for MFA.

Box 3: No

The public IP address of 192.168.1.20 is in the space of 193.17.17.0/24, which is an MFA-trusted IP range. Although user2 is a per-user MFA-enforced user, it won't be prompted for MFA.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

QUESTION 163

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Email one-time passcode for guests set to Yes.

You invite the guest users shown in the following table.

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

Which users will receive a one-time passcode, and how long will the passcode be valid? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users:

Guest1 only
Guest2 only
Guest3 only
Guest1 and Guest2 only
Guest2 and Guest3 only
Guest1, Guest2, and Guest3

Valid for:

30 minutes
60 minutes
24 hours
48 hours

Answer:

Users:

Valid for:

Explanation:

Box 1: Guest3 only

When does a guest user get a one-time passcode?

When a guest user redeems an invitation or uses a link to a resource that has been shared with them, they'll receive a one-time passcode if:

They don't have an Azure AD account

They don't have a Microsoft account

The inviting tenant didn't set up federation with social (like Google) or other identity providers.

Box 2: 30 minutes

One-time passcodes are valid for 30 minutes. After 30 minutes, that specific one-time passcode is no longer valid, and the user must request a new one. User sessions expire after 24 hours.

After that time, the guest user receives a new passcode when they access the resource. Session expiration provides added security, especially when a guest user leaves their company or no longer needs access.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode>

QUESTION 164

You have an Azure Active Directory (Azure AD) tenant that contains 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 configurations:

- Users can consent to apps accessing company data on their behalf: No
- Users can consent to apps accessing company data for the groups they own: No
- 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. User1
- B. User2
- C. Admin1
- D. Admin2

Answer: C

Explanation:

To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow>

QUESTION 165

You have a Microsoft 365 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. Configure the Outlook 2013 clients to use modern authentication.
- B. Upgrade the Outlook 2013 clients to Outlook 2016.
- C. From the Exchange admin center, configure Organization Sharing.
- D. Upgrade all the Outlook clients to Outlook 2019.

Answer: B

Explanation:

From October 13, 2020 onward, only these versions of Office are supported for connecting to Microsoft 365 (and Office 365) services:

Microsoft 365 Apps for enterprise (previously named Office 365 ProPlus)

Microsoft 365 Apps for business (previously named Office 365 Business)

Office LTSC 2021, such as Office LTSC Professional Plus 2021

Office 2019, such as Office Professional Plus 2019
Office 2016, such as Office Standard 2016

Note:

Office 2019 and Office 2016 will be supported for connecting to Microsoft 365 (and Office 365) services until October 2023.

Note: Client software: To support tenant restrictions, client software must request tokens directly from Azure AD, so that the proxy infrastructure can intercept traffic. Browser-based Microsoft 365 applications currently support tenant restrictions, as do Office clients that use modern authentication (like OAuth 2.0).

Reference:

<https://docs.microsoft.com/en-us/deployoffice/endofsupport/microsoft-365-services-connectivity>

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/tenant-restrictions>

QUESTION 166

Hotspot Question

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant.

The tenant contains the groups shown in the following table.

Name	Source	Member of
Group1	Cloud	Group3
Group2	Active Directory domain	None
Group3	Cloud	None

The tenant contains the users shown in the following table.

Name	Directory-synced	Member of
User1	No	Group1
User2	No	Group2
User3	Yes	Group3

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

Setting	Value
Review type	Teams + Groups
Review scope	All users
Group	Group2, Group3
Reviewers	Users review own access
If reviewers don't respond	Remove access

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 will be removed automatically from Group 1 if the user does not respond to the review request.	<input type="radio"/>	<input type="radio"/>
User 2 will be removed automatically from Group 3 if the user does not respond to the review request.	<input type="radio"/>	<input type="radio"/>
User 3 will be removed automatically from Group 2 if the user does not respond to the review	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 will be removed automatically from Group 1 if the user does not respond to the review request.	<input type="radio"/>	<input checked="" type="radio"/>
User 2 will be removed automatically from Group 3 if the user does not respond to the review request.	<input type="radio"/>	<input checked="" type="radio"/>
User 3 will be removed automatically from Group 2 if the user does not respond to the review	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No

User1 is member of Group1. Group1 is in the cloud. Group1 is member of Group3. Group3 is in the cloud.

The access review applies to Group3, but not to Group1. The access review is setup to remove access if reviewers don't respond.

Box 2: No

User2's membership cannot be managed since he is a part of Group2 which is an AD group (not AAD).

Box 3: No

User3 is member of Group3, not of Group2.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

QUESTION 167

You have a Microsoft 365 E5 subscription that contains a web app named App1.

Guest users are regularly granted access to App1.

You need to ensure that the guest users that have NOT accessed App1 during the past 30 days have their access removed. The solution must minimize administrative effort.

What should you configure?

- A. a Conditional Access policy
- B. a compliance policy
- C. a guest access review
- D. an access review for application access

Answer: D

Explanation:

Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group members or application access.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

QUESTION 168

Hotspot Question

You have an Azure Active Directory (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 member of Azure Active Directory Premium P2 licenses required for each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Group1:

 1
 500
 525

Group2:

 1
 100
 295
 395

Answer:

Group1:

1
500
525

Group2:

1
100
295
395

Explanation:

Box 1: 500

Scenario = An administrator creates an access review of Group C with 50 member users and 25 guest users. Makes it a self-review.

Calculation = 50 licenses for each user as self-reviewers.*

Number of licenses = 50

* Azure AD External Identities (guest user) pricing is based on monthly active users (MAU), which is the count of unique users with authentication activity within a calendar month. This model replaces the 1:5 ratio billing model, which allowed up to five guest users for each Azure AD Premium license in your tenant.

Box 2: 1

For Group2:

Review scope: Guest users only. Reviewers: Group Owner.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#license-requirements>

QUESTION 169

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a group named All Company and has the following Identity Governance settings:

- Block external users from signing in to this directory: Yes
- Remove external user: Yes
- Number of days before removing external user from this directory: 30

On March 11, 2022, you create an access package named Package1 that has the following settings:

- Resource roles
- 1. Name: All Company

2. Type: Group and Team
3. Role: Member
- Lifecycle
1. Access package assignment expire: On date
2. Assignment expiration date: April 1, 2022

On March 1, 2022, you assign Package1 to the guest users shown in the following table.

Name	Email address
Guest1	guest1@outlook.com
Guest2	guest2@outlook.com

On March 2, 2022, you assign the Reports reader role to Guest1.

On April 1, 2022, you invite a guest user named Guest3 to contoso.com.

On April 4, 2022, you add Guest3 to the All Company group.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
On May 5, 2022, the Guest1 account is in contoso.com.	<input type="radio"/>	<input type="radio"/>
On May 5, 2022, the Guest2 account is in contoso.com.	<input type="radio"/>	<input type="radio"/>
On May 5, 2022, the Guest3 account is in contoso.com.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
On May 5, 2022, the Guest1 account is in contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
On May 5, 2022, the Guest2 account is in contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
On May 5, 2022, the Guest3 account is in contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

On March 2, 2022, you assign the Reports reader role to Guest1.

On April 1 the access package assignment expires. After another 30 days, well before May 5, the guest user account is removed.

Box 2: No

On April 1 the access package assignment expires. After another 30 days, well before May 5, the

guest user account is removed.

Box 3: Yes

Note: Lifecycle

On the Lifecycle tab, you specify when a user's assignment to the access package expires. You can also specify whether users can extend their assignments.

In the Expiration section, set Access package assignments expires to On date, Number of days, Number of hours, or Never.

For On date, select an expiration date in the future.

For Number of days, specify a number between 0 and 3660 days.

For Number of hours, specify a number of hours.

Based on your selection, a user's assignment to the access package expires on a certain date, a certain number of days after they are approved, or never.

Note 2: By default, when an external user no longer has any access package assignments, they are blocked from signing in to your directory. After 30 days, their guest user account is removed from your directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-lifecycle-policy>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users>

QUESTION 170

You have an Azure Active Directory (Azure AD) tenant named Contoso that contains a terms of use (Toll) named Terms1 and an access package. Contoso users collaborate with an external organization named Fabrikam. Fabrikam users must accept Terms1 before being allowed to use the access package.

You need to identify which users accepted or declined Terms1.

What should you use?

- A. sign-in logs
- B. the Usage and Insights report
- C. provisioning logs
- D. audit logs

Answer: D

Explanation:

View Azure AD audit logs

If you want to view more activity, Azure AD terms of use policies include audit logs. Each user consent triggers an event in the audit logs that is stored for 30 days.

You can view these logs in the portal or download as a .csv file.

To get started with Azure AD audit logs, use the following procedure:

1. Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.
2. Browse to Azure Active Directory > Security > Conditional Access > Terms of use.
3. Select a terms of use policy.
4. Select View audit logs.
5. On the Azure AD audit logs screen, you can filter the information using the provided lists to target specific audit log information.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

QUESTION 171

You have an Azure Active Directory (Azure AD) 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

Explanation:

You can ask the guests themselves or a decision maker to participate in an access review and recertify (or attest) to the guests' access.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews>

QUESTION 172

Hotspot Question

You have a Microsoft 365 E5 subscription.

You create an access review for Azure Active Directory (Azure AD) roles.

You need to ensure that users who do not respond to review requests are removed automatically from the roles. The solution must minimize administrative effort.

Which two settings should you modify? To answer, select the settings in the answer area.

NOTE: Each correct selection is worth one point.

Reviewers

Reviewers

Members (self)



^ Upon completion settings

Auto apply results to resource ⓘ Enable Disable

If reviewers don't respond ⓘ No change



Action to apply on denied guest users ⓘ Remove user's membership from the resource

(Preview) At end of review, send + Select User(s) or Group(s)
notification to

^ Advanced settings

Show recommendations ⓘ Enable DisableRequire reason on approval ⓘ Enable DisableMail notifications ⓘ Enable DisableReminders ⓘ Enable Disable

Additional content for reviewer email ⓘ

Answer:

Reviewers

Reviewers

Members (self)



^ Upon completion settings

Auto apply results to resource <small>i</small>	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
If reviewers don't respond <small>i</small>	No change
Action to apply on denied guest users <small>i</small>	Remove user's membership from the resource
(Preview) At end of review, send notification to	+ Select User(s) or Group(s)

^ Advanced settings

Show recommendations <small>i</small>	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
Require reason on approval <small>i</small>	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
Mail notifications <small>i</small>	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
Reminders <small>i</small>	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
Additional content for reviewer email <small>i</small>	

Explanation:

Box 1: If Reviewers don't respond, remove access.

Box 2: Additional Content for Reviewer email.

QUESTION 173**Case Study 2 - Litware, Inc****Overview**

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

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

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

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

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

Hotspot Question

How should the access be setup to the on-premises applications?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Configure the Azure AD Password Protection proxy service on:

DC1
SERVER1
SERVER2

Configure the password list:

In Azure AD
On DC1
On SERVER1
On SERVER2

Answer:

Configure the Azure AD Password Protection proxy service on:

DC1
SERVER1
SERVER2

Configure the password list:

In Azure AD
On DC1
On SERVER1
On SERVER2

Explanation:

The password protection proxy is installed on a member server. You enable the banned password list in Azure AD, the proxy downloads it and passes it to the DCs in the domain.
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

QUESTION 174

You have an Azure Active Directory (Azure AD) 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 User3 are members of Au1.

User5 is assigned the User administrator role for Au1.

For which users can User5 reset passwords?

- A. User1, User2, and User3
- B. User1 and User2 only
- C. User3 and User4 only
- D. User2 and User3 only

Answer: D

Explanation:

Adding a group to an administrative unit brings the group itself into the management scope of the administrative unit, but not the members of the group. In other words, an administrator scoped to

the administrative unit can manage properties of the group, such as group name or membership, but they cannot manage properties of the users or devices within that group (unless those users and devices are separately added as members of the administrative unit).

<https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

QUESTION 175

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

Name	Usage location	Department	Job title
User1	United States	Sales	Associate
User2	Finland	Sales	SalesRep
User3	Australia	Sales	Manager

You create a dynamic user group and configure the following rule syntax.

```
user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "SalesRep")
```

Which users will be added to the group?

- A. User1 only
- B. User2 only
- C. User3 only
- D. User1 and User2 only
- E. User1 and User3 only
- F. User1, User2, and User3

Answer: A

Explanation:

```
user.usageLocation -in ["US","AU"] == User 1 & User 3
-and (user.department -eq "Sales") == User 1 & User 3
-and -not (user.jobTitle -eq "Manager") == User 1
-or (user.jobTitle -eq "SalesRep")
```

QUESTION 176

You have an Azure AD tenant that contains a user named User1.

User1 needs to manage license assignments and reset user passwords.

Which role should you assign to User1?

- A. Helpdesk administrator
- B. Billing administrator
- C. License administrator
- D. User administrator

Answer: D

Explanation:

Only User Access Admin fits in both the requirement : manage license assignments and reset user passwords.

QUESTION 177

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all 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 Set-MsolUserLicense cmdlet
- B. the Set-AzureADGroup cmdlet
- C. the Set-WindowsProductKey cmdlet
- D. the Administrative units blade in the Azure Active Directory admin center

Answer: A

Explanation:

The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.

Note:

There are several versions of this QUESTION 11in the exam. The QUESTION 11has two possible correct answers:

the Licenses blade in the Azure Active Directory admin center
the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

- the Identity Governance blade in the Azure Active Directory admin center
- the Set-WindowsProductKey cmdlet
- the Set-AzureAdGroup cmdlet

Reference:

<https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0>

QUESTION 178

Hotspot Question

Your on-premises network contains an Active Directory domain that uses Azure AD Connect to sync with an Azure AD tenant.

You need to configure Azure AD Connect to meet the following requirements:

- User sign-ins to Azure AD must be authenticated by an Active Directory domain controller.
- Active Directory domain users must be able to use Azure AD self-service password reset (SSPR) .

What 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

Authentication by the domain controller:

Federation with Active Directory Federation Services (AD FS)
Pass-through authentication
Password hash synchronization

SSPR:

Device writeback
Group writeback
Password hash synchronization
Password writeback

Answer:**Answer Area**

Authentication by the domain controller:

Federation with Active Directory Federation Services (AD FS)
Pass-through authentication
Password hash synchronization

SSPR:

Device writeback
Group writeback
Password hash synchronization
Password writeback

QUESTION 179

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 Exchange Administrator role to User1.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read-and-write-roles>

QUESTION 180

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

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read-and-write-roles>

QUESTION 181

You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

You need to ensure that users can connect to Exchange only from email clients that use Modern authentication protocols.

What should you implement?

- A. an OAuth policy in Microsoft Defender for Cloud Apps
- B. a conditional access policy in Azure Active Directory (Azure AD)
- C. a compliance policy in Microsoft Endpoint Manager
- D. an application control profile in Microsoft Endpoint Manager

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

QUESTION 182

You have an Azure subscription that contains an Azure SQL database named db1.

You deploy an Azure App Service web app named App1 that provides product information to users 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 system-assigned managed identity
- B. an Azure Active Directory (Azure AD) user account
- C. a SQL Server account
- D. a user-assigned managed identity

Answer: A

QUESTION 183

Hotspot Question

You have an Azure subscription that contains the following virtual machine:

- Name: V1
- 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 V1.
- 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 V1.	<input type="radio"/>	<input type="radio"/>
You can assign Managed3 to V1.	<input type="radio"/>	<input type="radio"/>
You can assign VM1 the Owner role for RG1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can assign Managed2 to V1.	<input checked="" type="radio"/>	<input type="radio"/>
You can assign Managed3 to V1.	<input checked="" type="radio"/>	<input type="radio"/>
You can assign VM1 the Owner role for RG1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

You can use user assigned managed identities in more than one Azure region.

<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-faq#can-the-same-managed-identity-be-used-across-multiple-regions>

QUESTION 184

Hotspot Question

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 June 1, Admin4 performs the following actions:

- Deletes a certificate named Certificate1 from KeyVault1
- Deletes a secret named Secret1 from KeyVault2

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
Admin1 can recover Secret1 on June 7.	<input type="radio"/>	<input type="radio"/>
Admin2 can purge Certificate1 on June 12.	<input type="radio"/>	<input type="radio"/>
Admin3 can purge Certificate1 on June 14.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Admin1 can recover Secret1 on June 7.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can purge Certificate1 on June 12.	<input type="radio"/>	<input checked="" type="radio"/>
Admin3 can purge Certificate1 on June 14.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

Key Vault Administrator can perform all data plane operations on a key vault.

And purge protection is disabled for KeyVault2.

NB: Purge protection is an optional Key Vault behavior and is not enabled by default.
Do not mismatch with soft-delete

Box 2: No

We are still in the Purge protection remaining period.

NB: Also the Key Vault contributor role doesn't allow to get access to certificate

Box 3: No

We are still in the Purge protection remaining period.

Even if the Certificate Officer role allow to get access to certificate

QUESTION 185

You have an Azure AD tenant.

You open the risk detections report.

Which risk detection type is classified as a user risk?

- A. password spray
- B. anonymous IP address
- C. unfamiliar sign-in properties
- D. Azure AD threat intelligence

Answer: D

Explanation:

Sign-in Risk policies cover:

- Anonymous IP address
- Additional Risk detected
- Admin confirmed user compromised
- Anomalous token
- Atypical travel
- Azure AD threat intelligence
- Impossible travel
- Malicious IP
- Malware linked IP
- Mass Access to sensitive files
- New country
- Password spray
- Suspicious browser
- Suspicious inbox forwarding
- Suspicious inbox manipulation rules
- token issuer anomaly
- Unfamiliar sign-in properties

User risk policies cover:

- Additional risk detected
- Anomalous user activity
- Azure AD threat intelligence
- Leaked credentials
- Possible attempt to access Primary Refresh Token (PRT)

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

QUESTION 186

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. a smartcard
- B. a mobile app code
- C. a mobile app notification
- D. an email to an address outside your organization

Answer: B

Explanation:

When using a mobile app as a method for password reset, like the Microsoft Authenticator app, the following considerations apply:

- When administrators require one method be used to reset a password, verification code is the only option available.
 - When administrators require two methods be used to reset a password, users are able to use notification OR verification code in addition to any other enabled methods.
- <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#mobile-app-and-sspr>

QUESTION 187

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

Explanation:

Examples for Sign-In Risk:

- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked credentials
- Password spray

QUESTION 188

Hotspot Question

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

Name	User risk level
User1	Low
User2	Medium
User3	High

You have the Azure AD Identity Protection policies shown in the following table.

Type	Users	User risk	Sign-in risk	Controls
User risk policy	All users	Low and above	Unconfigured	Block access
Sign-in risk policy	All users	Unconfigured	High	Block access

You review the Risky users report and the Risky sign-ins report and perform actions for each user as shown in the following table.

User	Action
User1	Confirm user compromised
User2	Confirm sign-in safe
User3	Dismiss user risk
User2	Confirm user compromised

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	<input type="radio"/>	<input type="radio"/>
User2 can sign in by using multi-factor authentication (MFA).	<input type="radio"/>	<input type="radio"/>
User3 can sign in from an anonymous IP address.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	<input type="radio"/>	<input checked="" type="radio"/>
User2 can sign in by using multi-factor authentication (MFA).	<input type="radio"/>	<input checked="" type="radio"/>
User3 can sign in from an anonymous IP address.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

Blocked access prevents self-remediation through password resets & Azure AD MFA.

Box 3: No

Blocked access prevents self-remediation through password resets & Azure AD MFA

Box 3: Yes

Anonymous IP address sign-in risk is Medium.

QUESTION 189

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 User1 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: D

Explanation:

Application Administrator = Can create and manage all aspects of app registrations and enterprise apps.

Cloud Application Administrator = Can create and manage all aspects of app registrations and enterprise apps ***except App Proxy***.

Service Support Administrator = Can read service health information and manage support tickets.

Application Developer = Can create application registrations independent of the 'Users can register applications' setting.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

QUESTION 190

Drag and Drop Question

You have a Microsoft 365 E5 subscription and an Azure subscription.

You need to meet the following requirements:

- Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials.
- Delegate the ability to create new virtual machines.

What should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature 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.

Features	Answer Area
Azure AD built-in roles	Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials:
Azure AD managed identities	Delegate the ability to create new virtual machines:
Azure role-based access control (Azure RBAC)	

Answer:

Features	Answer Area
Azure AD built-in roles	Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials:
Azure AD managed identities	Delegate the ability to create new virtual machines:
Azure role-based access control (Azure RBAC)	Azure role-based access control (Azure RBAC)

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#configure-role-assignments-for-the-vm>

QUESTION 191

Hotspot Question

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The AD DS domain contains the organizational units (OUs) shown in the following table.

Name	Description
OU1	Syncs with Azure AD
OU2	Does NOT sync with Azure AD

You need to create a break-glass account named BreakGlass.

Where should you create BreakGlass, and which role should you assign to BreakGlass? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Location:

Azure AD
OU1
OU2

Role:

Billing Administrator
Global Administrator
Owner
Privileged Role Administrator

Answer:

Answer Area

Location:

Azure AD
OU1
OU2

Role:

Billing Administrator
Global Administrator
Owner
Privileged Role Administrator

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access#how-to-create-an-emergency-access-account>

QUESTION 192

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 Site1. The solution must meet the following requirements:

- Automatically approve requests from users based on their group membership.
- Automatically 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 policy.

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>

QUESTION 193

Hotspot Question

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- Users that are assigned Role1 can manage application security groups.
- Users that are assigned Role2 can manage Azure Firewall.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role1:

Microsoft.App
Microsoft.Computer
Microsoft.Network
Microsoft.Security

Role2:

Microsoft.App
Microsoft.Management
Microsoft.Network
Microsoft.Security

Answer:

Answer Area

Role1:

Microsoft.App
Microsoft.Computer
Microsoft.Network
Microsoft.Security

Role2:

Microsoft.App
Microsoft.Management
Microsoft.Network
Microsoft.Security

Explanation:

<https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork>

QUESTION 194

Drag and Drop Question

You have a Microsoft 365 E5 tenant.

You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Defender for Cloud Apps.

In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Publish App1 in Azure AD.	
Create a conditional access policy that has session controls configured.	➤
From Microsoft Defender for Cloud Apps, create a session policy.	◀
From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.	▲ ▼

Answer:

Actions	Answer Area
Publish App1 in Azure AD.	
Create a conditional access policy that has session controls configured.	➤ ◀
From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.	▲ ▼
From Microsoft Defender for Cloud Apps, create a session policy.	

Explanation:

<https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-blocking-data-downloads-via-microsoft-cloud-app/ba-p/326357>

QUESTION 195

You have an Azure Active Directory (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. App1 requires admin consent to access Azure AD before the app can be used.

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

Admin consent requests

Users can request admin consent to apps they are unable to consent to Yes No

Who can review admin consent requests

Reviewer type	Reviewers
Users	4 users selected.
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests Yes No

Selected users will receive request expiration reminders Yes No

Consent request expires after (days) 30

Admin1, Admin2, Admin3, and User1 are added as reviewers.

Which users can review and approve the admin consent requests?

- A. Admin1 only
- B. Admin1, Admin2 and Admin3 only
- C. Admin1, Admin2, and User1 only

- D. Admin1 and Admin2 only
- E. Admin1, Admin2, Admin3, and User1

Answer: D

Explanation:

To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator. The reviewer must already have one of these admin roles assigned; simply designating them as a reviewer doesn't elevate their privileges.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow>

QUESTION 196

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. activity policy
- C. file policy
- D. anomaly detection policy

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/defender-cloud-apps/user-activity-policies>

QUESTION 197

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 hosts PDF files.

You need to prevent users from printing the files directly from Site1.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

- A. activity policy
- B. access policy
- C. file policy
- D. session policy

Answer: D

Explanation:

<https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad>

QUESTION 198

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 portal?

- A. access policy
- B. OAuth app policy
- C. anomaly detection policy
- D. activity policy

Answer: A

Explanation:

Microsoft Defender for Cloud Apps access policies enable real-time monitoring and control over access to cloud apps based on user, location, device, and app.

<https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>

QUESTION 199

You have a Microsoft 365 E5 subscription.

Users authorize third-party cloud apps to access their data.

You need to configure an alert that will be triggered when an app requires high permissions and is authorized by more than 20 users.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

- A. anomaly detection policy
- B. OAuth app policy
- C. access policy
- D. activity policy

Answer: B

Explanation:

In addition to the existing investigation of OAuth apps connected to your environment, you can set permission policies so that you get automated notifications when an OAuth app meets certain criteria. For example, you can automatically be alerted when there are apps that require a high permission level and were authorized by more than 50 users.

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy>

QUESTION 200

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: B

Explanation:

User2 is the only one who has access to Application.write for the calendar.

QUESTION 201

You have an Azure AD tenant that contains a user named User1 and a registered app named App1.

User1 deletes the app registration of App1.

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

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-restore-app>

QUESTION 202

Hotspot Question

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

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

	Name ↑	Group Type	Membership Type	Source	Security enabled
<input type="checkbox"/>	All Company	Microsoft 365	Assigned	Cloud	No
<input type="checkbox"/>	Group1	Microsoft 365	Assigned	Cloud	Yes
<input type="checkbox"/>	Group2	Security	Assigned	Cloud	Yes
<input type="checkbox"/>	Group3	Security	Dynamic	Cloud	Yes
<input type="checkbox"/>	Group4	Security	Assigned	Windows Server AD	Yes

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.



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 add an Azure AD 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:

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 add an Azure AD 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

QUESTION 203

You have an Azure AD tenant that contains two users named User1 and User2.

You plan to perform the following actions:

- Create a group named Group1.
- Add User1 and User2 to Group1.
- Assign Azure AD roles to Group1.

You need to create Group1.

Which two settings can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Group type: Microsoft 365
Membership type: Assigned
- B. Group type: Security
Membership type: Assigned
- C. Group type: Security
Membership type: Dynamic User
- D. Group type: Microsoft 365
Membership type: Dynamic User
- E. Group type: Security
Membership type: Dynamic Device

Answer: AB

QUESTION 204

Drag and Drop Question

You have a Microsoft 365 E5 subscription.

You need to perform the following tasks:

- Identify the locations and IP addresses used by Azure AD users to

sign in.

- Review the Azure AD security settings and identify improvement recommendations.
- Identify changes to Azure AD users or service principals.

What should you use for each task? To answer, drag the appropriate resources to the correct requirements. Each resource 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.

Resources	Answer Area
Audit logs	Identify the locations and IP addresses used by Azure AD users to sign in:
Identity secure score	Identify changes to Azure AD users or service principals:
Provisioning logs	Review the Azure AD security settings and identify improvement recommendations:
Sign-in logs	

Answer:

Resources	Answer Area
	Identify the locations and IP addresses used by Azure AD users to sign in: Sign-in logs
Provisioning logs	Identify changes to Azure AD users or service principals: Audit logs
	Review the Azure AD security settings and identify improvement recommendations: Identity secure score

QUESTION 205

Case Study 3 - A. Datum Corp

Overview

A. Datum Corporation is a consulting company in Montreal. A. Datum recently acquired a Vancouver-based company named Litware, Inc.

Existing Environment

A Datum Environment

The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

A. Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect. A. Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Name	Role
User1	None
User2	None
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

The tenant contains the groups shown in the following table.

Name	Type	Membership type	Owner	Members
IT_Group1	Security	Assigned	None	All users in the IT department
AdatumUsers	Security	Assigned	None	User1, User2

Existing Environment

Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment

Problem Statements

A. Datum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role To IT_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

Requirements

Planned Changes

A. Datum plans to implement the following changes;

- Configure self-service password reset {SSPR}.
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groupsoflitware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Requirements

Technical Requirements

A. Datum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.

- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.

- Users must provide one authentication method to reset their password by using SSPR.

Available methods must include:

- Email

- Phone

- Security questions

- The Microsoft Authenticator app

- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.

- The principle of least privilege must be used.

You need to resolve the issue of IT_Group1.

What should you do first?

A. Change Membership type of IT_Group1 to Dynamic User.

B. Recreate the IT_Group1 group.

C. Change Membership type of IT Group1 to Dynamic Device.

D. Add an owner to IT_Group1.

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept>

QUESTION 206

Case Study 3 - A. Datum Corp

Overview

A. Datum Corporation is a consulting company in Montreal. A. Datum recently acquired a Vancouver-based company named Litware, Inc.

Existing Environment

A Datum Environment

The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

A. Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect. A. Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Name	Role
User1	None
User2	None
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

The tenant contains the groups shown in the following table.

Name	Type	Membership type	Owner	Members
IT_Group1	Security	Assigned	None	All users in the IT department
AdatumUsers	Security	Assigned	None	User1, User2

Existing Environment

Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment

Problem Statements

A. Datum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role To IT_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

Requirements

Planned Changes

A. Datum plans to implement the following changes;

- Configure self-service password reset {SSPR}.
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groupsoflitware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Requirements

Technical Requirements

A. Datum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.

- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.

- Users must provide one authentication method to reset their password by using SSPR.

Available methods must include:

- Email

- Phone

- Security questions

- The Microsoft Authenticator app

- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.

- The principle of least privilege must be used.

You need to implement the planned changes for Package1.

Which users can create and manage the access review?

A. User3 only

B. User4 only

C. User5 only

D. User3 and User4

E. User3 and User5

F. User4 and User5

Answer: E

Explanation:

To create and perform an access review for users, you need to have one of the following roles:

- Global administrator

- User administrator

- Identity Governance Administrator

- Privileged Role Administrator (for reviews of role-assignable groups only)

- (Preview) Microsoft 365 or AAD Security Group owner of the group to be reviewed

<https://learn.microsoft.com/en-us/azure/active-directory/governance/manage-access-review#create-and-perform-an-access-review-for-users>

QUESTION 207

You have the Azure resources shown 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 VM1 only
- D. User1, VM1, and App1 only
- E. User1, Group1, VM1, and App1

Answer: E

QUESTION 208

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You needed 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 Groups blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Identity Governance blade in the Azure Active Directory admin center
- D. the Licenses blade in the Azure Active Directory admin center

Answer: D

QUESTION 209

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 Security Operator role to User1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

With read and write access, you can make changes and directly interact with identity secure score.

Global administrator

Security administrator

Exchange administrator

SharePoint administrator

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#who-can-use-the-identity-secure-score>

QUESTION 210

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 SharePoint Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

With read and write access, you can make changes and directly interact with identity secure score.

Global administrator

Security administrator

Exchange administrator

SharePoint administrator

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#who-can-use-the-identity-secure-score>

QUESTION 211

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

You need to ensure that Admin1 can perform only the following tasks:

- From the Microsoft 365 admin center, create and manage service requests.
- From the Microsoft 365 admin center, read and configure service health.

- From the Azure portal, create and manage support tickets.

The solution must minimize administrative effort.

What should you do?

- A. Create an administrative unit and add Admin1.
- B. Enable Azure AD Privileged Identity Management (PIM) for Admin1.
- C. Assign Admin1 the Helpdesk Administrator role.
- D. Create a custom role and assign the role to Admin1.

Answer: C

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator>

QUESTION 212

Hotspot Question

You have an Azure AD tenant that contains a user named User1. User1 is assigned the User Administrator role.

You need to configure External collaboration settings for the tenant to meet the following requirements:

- Guest users must be prevented from querying staff email addresses.
- Guest users must be able to access the tenant only if they are invited by User1.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Guest user access restrictions:

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite restrictions:

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite quest users including admins (most restrictive)

Enable guest self-service

sign up via user flows:

No
Yes

Answer:

Answer Area

Guest user access restrictions:

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)**

Guest invite restrictions:

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member
- Only users assigned to specific admin roles can invite guest users**
- No one in the organization can invite quest users including admins (most restrictive)

Enable guest self-service

sign up via user flows:

No
Yes

QUESTION 213

Hotspot Question

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You need to ensure that user authentication always occurs by validating passwords against the AD DS domain.

What should you configure, and what should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Configure:

Azure AD Password protection
Cross-tenant synchronization
Pass-through authentication
Password hash synchronization

Use:

Azure AD Connect
Microsoft Identity Manager (MIM)
The Microsoft Entra admin center
The Microsoft Purview compliance portal

Answer:

Answer Area

Configure:

Azure AD Password protection
Cross-tenant synchronization
Pass-through authentication
Password hash synchronization

Use:

Azure AD Connect
Microsoft Identity Manager (MIM)
The Microsoft Entra admin center
The Microsoft Purview compliance portal

QUESTION 214

A user named User1 receives an error message when attempting to access the Microsoft Defender for Cloud Apps portal.

You need to identify the cause of the error. The solution must minimize administrative effort.

What should you use?

- A. Log Analytics
- B. sign-in logs
- C. audit logs
- D. provisioning logs

Answer: B

QUESTION 215

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Yammer.

You need prevent users from signing in to Yammer from high-risk locations.

What should you do in the Microsoft Defender for Cloud Apps portal?

- A. Create an access policy.
- B. Create an activity policy.
- C. Unsanction Yammer.
- D. Create an anomaly detection policy.

Answer: A

Explanation:

<https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>

QUESTION 216

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. an email to an address outside your organization
- B. a mobile app notification
- C. an FIDO2 security token
- D. an email to an address in your organization

Answer: A

Explanation:

When using a mobile app as a method for password reset, like the Microsoft Authenticator app, the following considerations apply:

- When administrators require one method be used to reset a password, verification code is the only option available.
 - When administrators require two methods be used to reset a password, users are able to use notification OR verification code in addition to any other enabled methods.
- <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#mobile-app-and-sspr>

QUESTION 217

You have an Azure AD tenant.

You configure User consent settings to allow users to provide consent to apps from verified publishers.

You need to ensure that the users can only provide consent to apps that require low impact permissions.

What should you do?

- A. Create an enterprise application collection.
- B. Create an access review.
- C. Create an access package.
- D. Configure permission classifications.

Answer: D

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-permission-classifications?pivots=portal>

QUESTION 218

Hotspot Question

You have a Microsoft 365 E5 subscription that contains a user named User1.

You configure app governance integration.

User1 needs to view the App governance dashboard. The solution must use the principle of the least privilege.

Which role should you assign to User1, and which portal should User1 use to view the dashboard? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role:

- Application Administrator
- Application Developer
- Cloud Application Administrator

Portal:

- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Defender for Cloud Apps portal
- The Microsoft Purview compliance portal

Answer:

Answer Area

Role:

- Application Administrator
- Application Developer
- Cloud Application Administrator

Portal:

- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Defender for Cloud Apps portal
- The Microsoft Purview compliance portal

Explanation:

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#roles>

QUESTION 219

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 Azure AD users.

Which specification should the apps support?

- A. OAuth 2.0
- B. WS-Fed
- C. SCIM 2.0
- D. LDAP 3

Answer: C

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/user-provisioning>

QUESTION 220

You have a Microsoft 365 E5 subscription that contains a user named User1.

You need to ensure that User1 can create access reviews for Azure AD roles. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Privileged role administrator
- B. Identity Governance Administrator
- C. User administrator
- D. User Access Administrator

Answer: C

Explanation:

To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources. To create access reviews for Azure AD roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-roles-and-resource-roles-review#prerequisites>

QUESTION 221

Hotspot Question

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 eligible 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 Area

Statements	Yes	No
If User1 requests Role1, the request will be approved automatically.	<input type="radio"/>	<input type="radio"/>
User1 can approve the request of User3 for Role2.	<input type="radio"/>	<input type="radio"/>
User1 must provide justification to approve the request of User2 for Role1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If User1 requests Role1, the request will be approved automatically.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can approve the request of User3 for Role2.	<input type="radio"/>	<input checked="" type="radio"/>
User1 must provide justification to approve the request of User2 for Role1.	<input checked="" type="radio"/>	<input type="radio"/>

QUESTION 222

Hotspot Question

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

Name	Role
Admin1	Global Administrator
Admin2	Application Administrator
Admin3	Cloud Application Administrator
Admin4	Application Developer
User1	None

You plan to deploy an on-premises app named App1. App1 will be registered in Azure AD and will use Azure AD Application Proxy.

You need to delegate the installation of the Application Proxy connector and ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which user should perform the installation, and which role should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User that should perform the installation:

Admin1
Admin2
Admin3
Admin4

Assign User1 the role of:

Application Administrator
Application Developer
Cloud Application Administrator
Global Administrator

Answer:

Answer Area

User that should perform the installation:

Admin1
Admin2
Admin3
Admin4

Assign User1 the role of:

Application Administrator
Application Developer
Cloud Application Administrator
Global Administrator

QUESTION 223

Hotspot Question

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	<i>None</i>	<i>Not applicable</i>
User4	Password Administrator	AU1
User5	<i>None</i>	<i>Not applicable</i>

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 Area

User 1:

- User3 only
- User2 and User5 only
- User3 and User5 only
- User2, User3, and User5 only
- User3, User4 and User5 only
- User2, User3, User4, and User5

User 4:

- User3 only
- User2 and User3 only
- User3 and User5 only
- User1, User2, and User3 only

Answer:

Answer Area

User 1:

- User3 only
- User2 and User5 only
- User3 and User5 only
- User2, User3, and User5 only
- User3, User4 and User5 only
- User2, User3, User4, and User5**

User 4:

- User3 only
- User2 and User3 only
- User3 and User5 only
- User1, User2, and User3 only**

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords>

QUESTION 224

You have a Microsoft 365 E5 subscription that contains a user named User1. User is eligible for the Application administrator role.

User1 needs to configure a new connector group for an application proxy.

What should you use 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

QUESTION 225

You have an Azure subscription that contains a registered app named App1.

You need to review the sign-in activity for App1. The solution must meet the following requirements:

- Identify the number of failed sign-ins.
- Identify the success rate of sign-ins.
- Minimize administrative effort.

What should you use?

- A. Sign-in logs
- B. Access reviews
- C. Audit logs
- D. Usage & insights

Answer: D

QUESTION 226

Your company has an Azure AD tenant that contains a user named User1.

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. The solution must ensure that User1 does NOT have permissions to manage the users in the finance department.

What should you create first?

- A. a management group
- B. an administrative unit
- C. a resource group
- D. a Microsoft 365 group

Answer: B

QUESTION 227

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.

Expiration

Access package assignments expire ⓘ

On date Number of days Number of hours (Preview) Never

Assignments expire after (number of days)

365

Show advanced expiration settings

Access Reviews

Require access reviews *

Yes No

Starting on ⓘ

03/01/2022

Review frequency ⓘ

Annually Bi-annually Quarterly Monthly Weekly

Duration (in days) ⓘ

90 ✓

Maximum 175

Reviewers ⓘ

- Self-review
- Specific reviewer(s)
- Manager

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. Security administrator
- B. Privileged role administrator
- C. External Identity Provider administrator
- D. User administrator

Answer: D

Explanation:

To enable reviews of access packages, you must meet the prerequisites for creating an access package:

- Microsoft Azure AD Premium P2 or Microsoft Entra ID Governance
- Global administrator, Identity Governance administrator, User administrator, Catalog owner, or Access package manager

QUESTION 228

Hotspot Question

You have an Azure subscription.

Azure AD logs are sent to a Log Analytics workspace.

You need to query the logs and graphically display the number of sign-ins per user.

How should you complete the query? To answer, select the appropriate options in the answer area,

NOTE: Each correct selection is worth one point.

Answer Area

SigninLogs

| where ResultType == 0

| login_count = count() by Identity

| extend

| print

| project

| render

| summarize

columnchart

| extend

| print

| project

| render

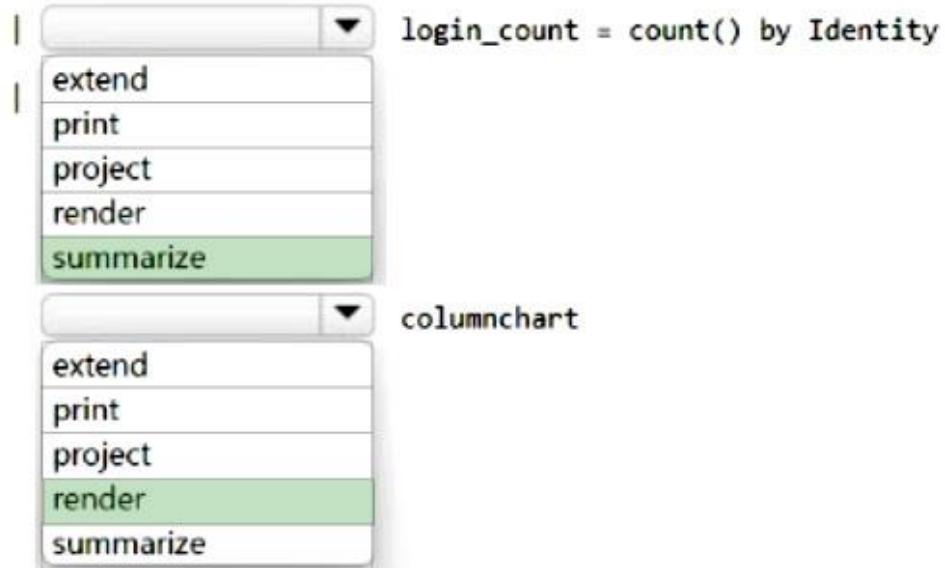
| summarize

Answer:

Answer Area

SigninLogs

| where ResultType == 0



QUESTION 229

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 administrative effort.

What should you do first?

- A. Create a Conditional Access policy.
- B. Create a Defender for Cloud Apps access policy.
- C. Create an app configuration policy in Microsoft Endpoint Manager.
- D. From the Microsoft Defender for Cloud Apps portal, unsanction Facebook.

Answer: D

Explanation:

Unsanctioning an app doesn't block use, but enables you to more easily monitor its use with the Cloud Discovery filters. You can then notify users of the unsanctioned app and suggest an alternative safe app for their use, or generate a block script using the Defender for Cloud Apps APIs to block all unsanctioned apps.

<https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery#sanctioningunsanctioning-an-app>

QUESTION 230

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).

You need to identify users that are eligible for the Cloud Application Administrator role.

Which blade in the Privileged Identity Management settings should you use?

- A. Azure resources
- B. Privileged access groups
- C. Review access
- D. Azure AD roles

Answer: B

QUESTION 231

Hotspot Question

You have a Microsoft 365 E5 subscription.

You need to create a dynamic user group that will include all the users that do NOT have a department defined in their user profile.

How should you complete the membership rule? To answer, select the appropriate options in the answer area.

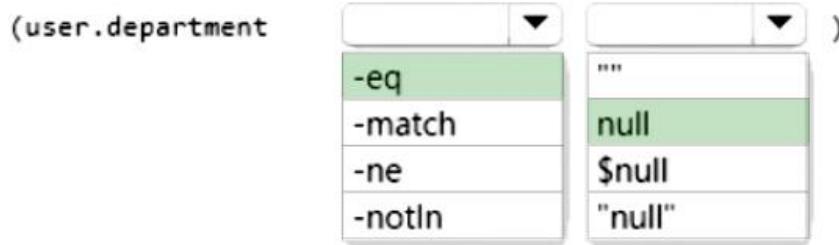
NOTE: Each correct selection is worth one point.

Answer Area

(user.department	<input type="button" value="▼"/>)	<input type="button" value="▼"/>
-eq		""	
-match		null	
-ne		\$null	
-notIn		"null"	

Answer:

Answer Area



Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#use-of-null-values>

QUESTION 232

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all 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 Update-MgGroup cmdlet
- B. the Licenses blade in the Azure Active Directory admin center
- C. the Set-WindowsProductKey cmdlet
- D. the Administrative units blade in the Azure Active Directory admin center

Answer: B

QUESTION 233

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

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Application Administrator

You need to compare the role permissions of each user. The solution must minimize administrative effort.

What should you use?

- A. the Microsoft 365 Defender portal
- B. the Microsoft 365 admin center
- C. the Microsoft Entra admin center
- D. the Microsoft Purview compliance portal

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/admin-roles-page#compare-roles>

QUESTION 234

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com.

Several users use their contoso.com email address for self-service sign-up to Azure AD.

You gain global administrator privileges to the Azure AD tenant that contains the self-signed users.

You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

- A. Update-MgOrganization
- B. Update-MgPolicyPermissionGrantPolicyExclude
- C. Update-MgDomain
- D. Update-MgDomainFederationConfiguration

Answer: B

Explanation:

The Update-MgPolicyPermissionGrantPolicyExclude cmdlet is used to exclude a policy from being applied to a specific set of users. In this case, you can use the cmdlet to exclude the self-service sign-up policy from being applied to users with the contoso.com SMTP address space.

QUESTION 235

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 can 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 FIDO2 security key
- B. a hardware token
- C. a one-time passcode email

- D. Windows Hello for Business
- E. the Microsoft Authenticator app

Answer: AE

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-combined>

- Hardware token is not an option to register.
- a one-time passcode email is not even listed.
- Windows Hello for Business is not even listed.

QUESTION 236

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. SMS
- B. Windows Hello for Business
- C. voice
- D. a notification through the Microsoft Authenticator app

Answer: B

QUESTION 237

You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

You need to ensure that users can connect to Exchange Online only from email clients that use Modern authentication protocols.

What should you implement?

- A. a conditional access policy in Azure AD
- B. a compliance policy in Microsoft Intune
- C. an OAuth policy in Microsoft Defender for Cloud Apps
- D. an application control profile in Microsoft Intune

Answer: A

Explanation:

<https://learn.microsoft.com/en-gb/entra/identity/conditional-access/howto-conditional-access-policy-block-legacy>

QUESTION 238

You plan to deploy a new Azure AD tenant.

Which multifactor authentication (MFA) method will be enabled by default for the tenant?

- A. Microsoft Authenticator
- B. SMS
- C. voice call
- D. email OTP

Answer: A

Explanation:

Security defaults users are required to register for and use multifactor authentication using the Microsoft Authenticator app using notifications. Users might use verification codes from the Microsoft Authenticator app but can only register using the notification option. Users can also use any third party application using OATH TOTP to generate codes.

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#authentication-methods>

QUESTION 239

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3 and a Microsoft SharePoint Online site named Site1.

The subscription contains the devices shown in the following table.

Name	Azure AD	Compliance
Device1	Joined	Noncompliant
Device2	Registered	Compliant
Device3	None	<i>Not applicable</i>

The users sign in to the devices as shown in the following table.

User	Device
User1	Device1
User2	Device2
User3	Device3

You have a Conditional Access policy that has the following settings:

- Name: CA1
- Assignments
 - o Users and groups: User1, User2, User3
 - o Cloud apps or actions: SharePoint - Site1
- Access controls
- o Session: Use app enforced restrictions

From the SharePoint admin center, you configure Access control for unmanaged devices to allow limited, web-only access.

Which users will have full access to Site1?

- A. User1 only
- B. User2 only
- C. User3only
- D. User1 and User2 only
- E. User1, User2, and User3

Answer: A

Explanation:

<https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-managed-unmanaged-devices?view=o365-worldwide&tabs=Managed>

QUESTION 240

You have an Azure AD tenant named contoso.com that contains the resources shown in the following table.

Name	Description
Au1	Administrative unit
CAPolicy1	Conditional Access policy
Package1	Access package

You create a user named Admin1.

You need to ensure that Admin1 can enable Security defaults for contoso.com.

What should you do first?

- A. Delete Package1.
- B. Delete CAPolicy1.
- C. Assign Admin1 the Authentication Administrator role for Au1.
- D. Configure Identity Governance.

Answer: B

Explanation:

To configure security defaults in your directory, you must be assigned at least the Security Administrator role. By default the first account in any directory is assigned a higher privileged role known as Global Administrator.

Organizations that choose to implement Conditional Access policies that replace security defaults must disable security defaults. (Imply that Conditional Access policies has conflict with security defaults)

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>

QUESTION 241

You have an Azure AD tenant and a .NET web app named App1.

You need to register App1 for Azure AD authentication.

What should you configure for App1?

- A. the executable name

- B. the bundle ID
- C. the package name
- D. the redirect URI

Answer: D

QUESTION 242

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. security questions
- C. voice
- D. Windows Hello for Business

Answer: D

QUESTION 243

You have an Azure AD 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 for Cloud Apps 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 for Cloud Apps portal, configure an app connector.
- D. From the Microsoft Entra admin center, configure an access review.

Answer: B

QUESTION 244

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: C

QUESTION 245

Your company purchases a new Microsoft 365 E5 subscription and an app named App1.

You need to create a Microsoft Defender for Cloud Apps access policy for App1.

What should you do first?

- A. Configure a Conditional Access policy to use app-enforced restrictions.
- B. Configure a Token configuration for App1.
- C. Add an API permission for App1.
- D. Configure a Conditional Access policy to use Conditional Access App Control.

Answer: D

QUESTION 246

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 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 Google Workspace app connector.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Microsoft Defender for Cloud Apps is now part of Microsoft 365 Defender, which correlates signals from across the Microsoft Defender suite and provides incident-level detection,

investigation, and powerful response capabilities. For more information, see Microsoft Defender for Cloud Apps in Microsoft 365 Defender.

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions>

QUESTION 247

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 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 Microsoft Azure app connector.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions>

QUESTION 248

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 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: B

Explanation:

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions>

QUESTION 249

Your company purchases a Microsoft 365 E5 subscription.

A user named User1 is assigned the Security Administrator role.

You need to ensure that User1 can create Microsoft Defender for Cloud Apps session policies.

What should you do first?

- A. Create a Conditional Access policy and select Require app protection policy.
- B. Create a Conditional Access policy and select Use Conditional Access App Control.
- C. Assign the Cloud Application Administrator role to User1.
- D. Assign the Cloud App Security Administrator role to User1.

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad>

QUESTION 250

You have an Azure AD Premium P2 tenant.

You create a Log Analytics workspace.

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

What should you do first?

- A. Modify the Diagnostics settings for Azure AD.
- B. Run the Update-MgOrganization cmdlet.
- C. Run the Update-MgDomain cmdlet.
- D. Create an Azure AD workbook.

Answer: A

QUESTION 251

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 administrative effort.

What should you do first?

- A. From the Microsoft 365 Defender portal, unsanction Facebook.
- B. Create a Defender for Cloud Apps access policy.
- C. Create an app configuration policy in Microsoft Intune.
- D. Create a Conditional Access policy.

Answer: A

QUESTION 252

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

Name	Role
User1	Global Administrator
User2	User Administrator
User3	Groups Administrator
User4	None

From the tenant, you configure a naming policy for groups.

Which users are affected by the naming policy?

- A. User2 only
- B. User3only
- C. User2 and User3 only
- D. User3 and User4 only
- E. User1, User2, and User3 only
- F. User1, User2, User3, and User4

Answer: D

Explanation:

Naming policy doesn't apply to certain directory roles, such as Global Administrator or User Administrator.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy#roles-and-permissions>.

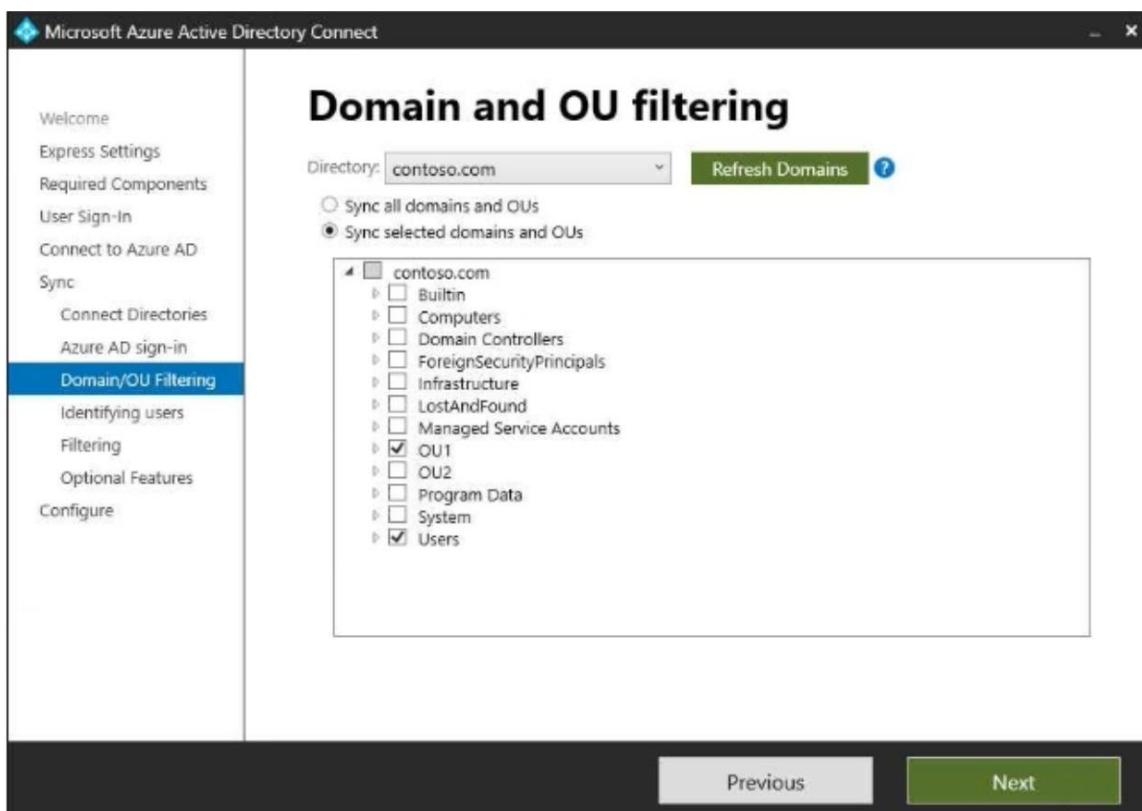
QUESTION 253

Hotspot Question

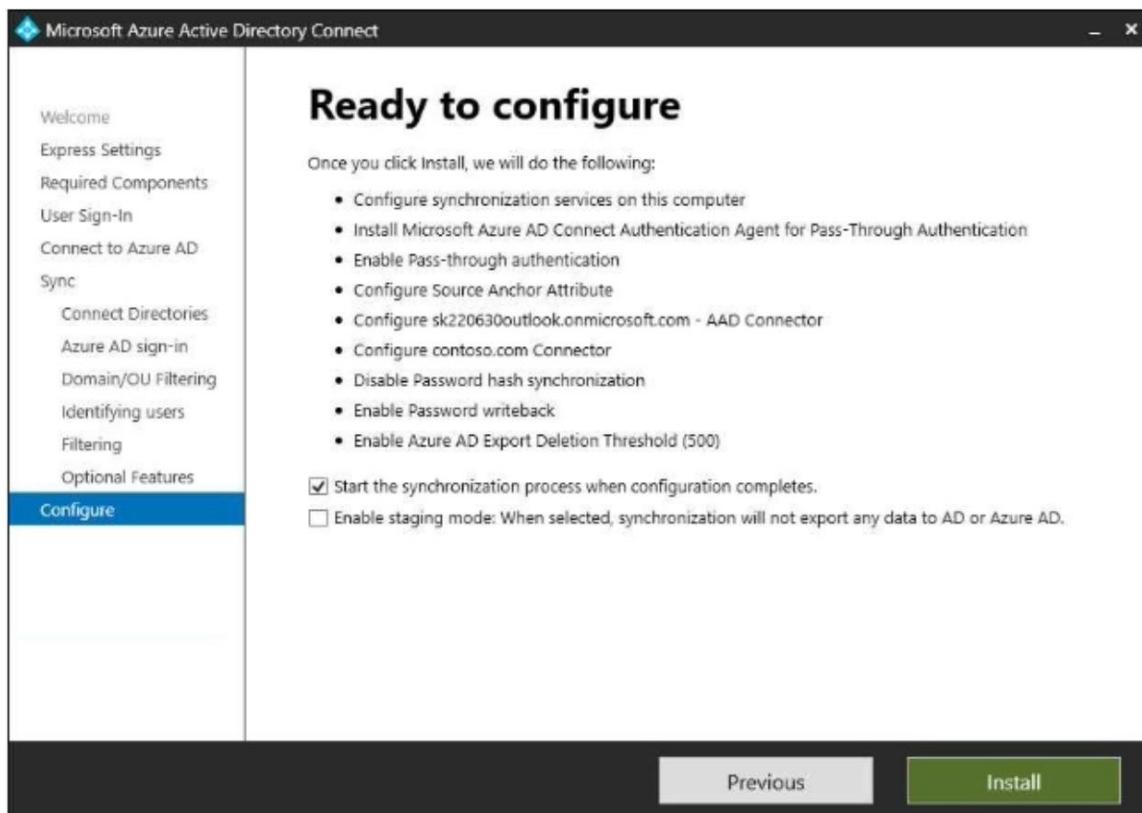
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.

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 selection is worth one point.

Answer Area

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

Answer:**Answer Area**

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

QUESTION 254

Hotspot Question

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

Name	Type
User1	User
User2	User
Vault1	Azure Key Vault

You need to configure access to Vault1. The solution must meet the following requirements:

- Ensure that User1 can manage and create keys in Vault1.
- Ensure that User2 can access a certificate stored in Vault1.
- Use the principle of least privilege.

Which role should you assign to each user? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:

Key Vault Certificates Officer
Key Vault Crypto Officer
Key Vault Secrets Officer

User2:

Key Vault Certificates Officer
Key Vault Crypto Officer
Key Vault Secrets Officer

Answer:

Answer Area

User1:

Key Vault Certificates Officer
Key Vault Crypto Officer
Key Vault Secrets Officer

User2:

Key Vault Certificates Officer
Key Vault Crypto Officer
Key Vault Secrets Officer

Explanation:

<https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide#azure-built-in-roles-for-key-vault-data-plane-operations>

QUESTION 255

Drag and Drop Question

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

Admin1 uses the Require password change for high-risk users 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 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

Options
 Admin1

 All guest and external users

 All users

 Directory roles

 None

Answer Area

 Include:

 Exclude:
Answer:
Options
 All guest and external users

 Directory roles

 None

Answer Area

 Include: All users

 Exclude: Admin1

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk-user>

QUESTION 256

Hotspot Question

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

The users have the devices shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Azure AD joined
Device3	Android	Azure AD registered

You create the following two Conditional Access policies:

- Name: CAPolicy1
- Assignments
 - o Users or workload identities: Group1
 - o Cloud apps or actions: Office 365 SharePoint Online
 - o Conditions
 - Filter for devices: Exclude filtered devices from the policy
 - Rule syntax: device.displayName -startsWith 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 that 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.

Statements	Yes	No
User1 can access Site1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can access Site1 from Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can access Site1 from Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Site1 from Device2.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can access Site1 from Device3.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 257

Drag and Drop Question

You have an Azure subscription that is linked to an Azure AD tenant named contoso.com. The subscription contains a group named Group1 and a virtual machine named VM1.

You need to meet the following requirements:

- Enable a system-assigned managed identity for VM1.
- Add VM1 to Group1.

How should you complete the PowerShell script? To answer, drag the appropriate cmdlets to the correct targets. Each cmdlet 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.

Cmdlets	Answer Area
Get-AzADGroup	\$vm = [REDACTED] Cmdlet -ResourceGroupName myResourceGroup -Name vm1
Get-AzADServicePrincipal	Update-AzVM -ResourceGroupName myResourceGroup -VM \$vm -IdentityType SystemAssigned
Get-AzVM	\$displayname = [REDACTED] Cmdlet -displayname "vm1"
Update-AzADServicePrincipal	\$group = Get-AzADGroup -searchstring "group1"
Update-AzVM	Add-AzureADGroupMember -ObjectId \$group.id -RefObjectId \$displayname.id

Answer:

Cmdlets Get-AzADGroup Update-AzADServicePrincipal Update-AzVM**Answer Area**

```
$vm =  Get-AzVM -ResourceGroupName myResourceGroup -Name vm1  
Update-AzVM -ResourceGroupName myResourceGroup -VM $vm -IdentityType SystemAssigned  
$displayname =  Get-AzADServicePrincipal -displayname "vm1"  
$group = Get-AzADGroup -searchstring "group1"  
Add-AzureADGroupMember -ObjectId $group.id -RefObjectId $displayname.id
```

QUESTION 258

Hotspot Question

You have an Azure AD tenant.

You need to configure the following External Identities features:

- B2B collaboration
- Monthly active users (MAU)-based pricing

Which two settings should you configure? To answer, select the settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



External Identities

Contoso Ltd - Azure Active Directory



Search

<<



Overview



Cross-tenant access settings



All identity providers



External collaboration settings



Diagnose and solve problems

Self-service sign up



Custom user attributes



All API connectors



User flows

Subscriptions



Linked subscriptions

Lifecycle management



Terms of use



Access reviews

Answer:

Answer Area



External Identities

Contoso Ltd - Azure Active Directory



Search

<<



Overview



Cross-tenant access settings



All identity providers



External collaboration settings



Diagnose and solve problems

Self-service sign up



Custom user attributes



All API connectors



User flows

Subscriptions



Linked subscriptions

Lifecycle management



Terms of use



Access reviews

QUESTION 259

You have an Azure AD tenant that contains the external user shown in the following exhibit.

Overview Monitoring Properties

Basic info



External User

external195_gmail.com#EXT#@sk230415outlook.onmicrosoft.com
Guest

User principal name	external195_gmail.com#EXT#@sk230415outlook.onmicrosoft.com		Group members	0
Object ID	2b353249-fa3d-4c8e-b69d-fa6c6c60fa1c		Applications	0
Created date time	Apr 30, 2023, 11:58 AM		Assigned roles	0
User type	Guest		Assigned licenses	0
Identities	mail			

My Feed



Account status

Enabled

[Edit](#)



Sign-ins

Last sign-in: -- --

[See all sign-ins](#)



B2B collaboration

Invitation state: Accepted

[Reset redemption status](#)

You update the email address of the user.

You need to ensure that the user can authenticate by using the updated email address.

What should you do for the user?

- A. Modify the Authentication methods settings.
- B. Reset the password.
- C. Revoke the active sessions.
- D. Reset the redemption status.

Answer: D

Explanation:

<https://learn.microsoft.com/en-us/entra/external/external-id/reset-redemption-status>

Update the guest user's sign-in information after they've redeemed your invitation for B2B collaboration. There might be times when you'll need to update their sign-in information, for example when:

- The user wants to sign in using a different email and identity provider
- etc

To manage these scenarios previously, you had to manually delete the guest user's account from your directory and reinvite the user. Now you can use the Microsoft Entra admin center, PowerShell or the Microsoft Graph invitation API to reset the user's redemption status and reinvite the user while keeping the user's object ID, group memberships, and app assignments.

QUESTION 260

You have an Azure AD 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. External collaboration settings
- B. All identity providers
- C. Cross-tenant access settings
- D. Linked subscriptions

Answer: A

QUESTION 261

You have an Azure AD tenant that contains a user named User1 and a Microsoft 365 group named Group1. User1 is the owner of Group1.

You need to ensure that User1 is notified every three months to validate the guest membership of Group1.

What should you do?

- A. Configure the External collaboration settings.
- B. Create an access review.
- C. Configure an access package.
- D. Create a group expiration policy.

Answer: B

Explanation:

An access review is a process that allows you to review and manage the access of users and groups to resources. You can use access reviews to validate the guest membership of Group1 every three months.

QUESTION 262

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 App1.

Answer: A

Explanation:

To ensure that users can request admin consent for App1 in your Azure AD tenant, you should first enable admin consent requests for the tenant.

Enabling admin consent requests allows users to initiate the process of requesting admin consent for applications that require it. By default, users do not have the ability to grant admin consent for applications. Enabling this feature ensures that users can request admin consent for App1 without having to rely on an administrator to initiate the process.

QUESTION 263

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 must use the Microsoft 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 Active Directory admin center, you configure the Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Report suspicious activity and the legacy Fraud Alert implementation can operate in parallel. You can keep your tenant-wide Fraud Alert functionality in place while you start to use Report suspicious activity with a targeted test group.

If Fraud Alert is enabled with Automatic Blocking, and Report suspicious activity is enabled, the user will be added to the blocklist and set as high-risk and in-scope for any other policies configured. These users will need to be removed from the blocklist and have their risk remediated to enable them to sign in with MFA.

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings#report-suspicious-activity-and-fraud-alert>

QUESTION 264

You have an Azure subscription that contains a user named User1.

The App registration settings for the Azure AD tenant are configured as shown in the following exhibit.

Enterprise applications

Manage how end users launch and view their applications

App registrations

Users can register applications 

Yes

No

User1 builds an ASP.NET web app named App1.

You need to ensure that User1 can register App1. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Application Developer
- B. Cloud App Security Administrator
- C. Cloud Application Administrator
- D. Application Administrator

Answer: A

Explanation:

Assign the Application Developer role to grant the ability to create application registrations when the Users can register applications setting is set to No. This role also grants permission to consent on one's own behalf when the Users can consent to apps accessing company data on their behalf setting is set to No.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#grant-individual-permissions-to-create-and-consent-to-applications-when-the-default-ability-is-disabled>

QUESTION 265

Hotspot Question

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

Name	Type	Location
RG1	Resource group	East US
Managed1	Managed identity	East US
Managed2	Managed identity	West US

The subscription contains the virtual machines shown in the following table.

Name	Location	Identity
VM1	East US	System-assigned
VM2	West US	System-assigned
VM3	East US	Managed1
VM4	West US	<i>None</i>

Which identities can be assigned the Owner role for RG1, and to which virtual machines can you assign Managed2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Identities with Owner role:

- Managed1 only
- Managed1, VM1, and VM3 only
- Managed1, Managed2, and VM1 only
- Managed1, Managed2, VM1, and VM2 only
- Managed1, Managed2, VM1, VM2, and VM3 only

Virtual machines assigned to Managed2:

- VM4 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM1, VM2, VM3, and VM4

Answer:

Answer Area

Identities with Owner role:

- Managed1 only
- Managed1, VM1, and VM3 only
- Managed1, Managed2, and VM1 only
- Managed1, Managed2, VM1, and VM2 only
- Managed1, Managed2, VM1, VM2, and VM3 only

Virtual machines assigned to Managed2:

- VM4 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM1, VM2, VM3, and VM4

QUESTION 266

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You plan to increase app security for the subscription.

You need to identify which apps do NOT require user authentication.

What should you do in the Microsoft 365 Defender portal?

- A. Review the cloud app catalog.
- B. Create an OAuth policy and review alerts.
- C. Create a snapshot Cloud Discovery report.
- D. Create a discovered app query.

Answer: A

Explanation:

To identify which apps do NOT require user authentication in the Microsoft 365 Defender portal, you should review the cloud app catalog.

Reviewing the cloud app catalog in the Microsoft 365 Defender portal provides you with a comprehensive list of all the apps connected to your Microsoft 365 environment. It allows you to see which apps require user authentication and which ones do not.

QUESTION 267

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

Name	Role
Admin1	Account Administrator
Admin2	Service Administrator
Admin3	SharePoint Administrator

You need to implement Azure AD Privileged Identity Management (PIM).

Which users can use PIM to activate their role permissions?

- A. Admin1 only
- B. Admin2 only
- C. Admin3 only
- D. Admin1 and Admin2 only
- E. Admin2 and Admin3 only
- F. Admin1, Admin2, and Admin3

Answer: C

Explanation:

You cannot manage the following classic subscription administrator roles in Privileged Identity Management:

- Account Administrator

- Service Administrator

- Co-Administrator

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-roles>

QUESTION 268

Hotspot Question

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

Apps:

No apps
App4 only
App3 and App4 only
App2, App3, and App4 only
App1, App2, App3, and App4

App4 settings:

No settings
Self-service only
App roles and Client secret only
Users and groups and Self-service only
App roles, Users and groups, Client secret, and Self-service

Answer:**Answer Area**

Apps:

No apps
App4 only
App3 and App4 only
App2, App3, and App4 only
App1, App2, App3, and App4

App4 settings:

No settings
Self-service only
App roles and Client secret only
Users and groups and Self-service only
App roles, Users and groups, Client secret, and Self-service

Explanation:

After you delete an app registration, the app remains in a suspended state for 30 days. During that 30-day window, the app registration can be restored, along with all its properties.

Box 1: App1, App2, App3, and App4

Box 2: App roles, Users and groups, client secrets, and Self-service

<https://learn.microsoft.com/en-us/entra/identity-platform/howto-restore-app>

QUESTION 269

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 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 GitHub app connector.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Adding the GitHub app connector to Microsoft Defender for Cloud Apps will allow you to monitor OAuth authentication requests from GitHub to Microsoft 365. However, it will not allow you to monitor OAuth authentication requests to your AWS account, Google Workspace subscription, or Azure subscription.

QUESTION 270

You have an Azure AD tenant.

You plan to implement Azure AD Privileged Identity Management (PIM).

Which roles can you manage by using PIM?

- A. Global Administrator only
- B. Global Administrator and Security Administrator only
- C. Global Administrator, Security Administrator, and Security Contributor only
- D. Account Administrator, Global Administrator, Security Administrator, and Security Contributor only

Answer: B

Explanation:

You can manage just-in-time assignments to all Microsoft Entra roles and all Azure roles using Privileged Identity Management (PIM) in Microsoft Entra ID.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

QUESTION 271

Hotspot Question

Your company uses Microsoft Entra ID to manage user and guest access to its Microsoft 365 services.

You have recently enabled Guest access to enable your users to collaborate with another company on projects. The current user setting configuration is shown in the three exhibits.

Default user role permissions

[Learn more](#)

Users can register applications No Yes

Restrict non-admin users from creating tenants Yes No

Users can create security groups No Yes

Guest user access

[Learn more](#)

Guest user access restrictions Guest users have the same access as members (most inclusive)

Guest users have limited access to properties and memberships of directory objects

Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Administration center

[Learn more](#)

Restrict access to Microsoft Entra admin center No Yes

LinkedIn account connections

[Learn more](#)

Allow users to connect their work or school account with LinkedIn * Yes

Selected group

No

Allow users to connect their work or school account with LinkedIn * AWS-WS  Edit

Home > IamITGeek | User settings >

User features ...

 Save  Discard

i Starting Sept. 30th, 2022 [Combined registration experiences for multifactor authentication and SSPR](#) will be enabled for all tenants.

Users can use preview features for My Apps 

None Selected All

Users can use the combined security information registration experience 

None Selected All

Select a group

[AWS-WS](#)

Administrators can access My Staff 

None Selected All

Select a group

[AVD-Users](#)

One of the new project teams you need to collaborate have the following requirements:

Username	Group Association	Requirements
User-GU-A	None	<ul style="list-style-type: none"> Requires same access as UserC
UserA	AVD-Users, AWS-WS	<ul style="list-style-type: none"> Should not be able to access preview features for My Apps Needs to access LinkedIn with Microsoft Entra ID account
UserB	AVD Users	<ul style="list-style-type: none"> Requires access to My Staff Needs to be able to use the combined security information registration experience
UserC	AWS-WS	<ul style="list-style-type: none"> Needs to access LinkedIn with the Microsoft Entra ID account
UserD	AVD-Users	<ul style="list-style-type: none"> Should not be able to access preview features for My Apps Needs to access LinkedIn with the Microsoft Entra ID account

Some of the users report:

- User-GU-A (guest user) reports that they do not currently have the same access as UserC.

- UserB reports that they cannot use the combined security information registration experience.
- UserD reports that they cannot access LinkedIn with their Microsoft Entra ID account.

You need to update the user settings within Microsoft Entra to meet the users' requirements. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statement	Yes	No
You should change Guest User access to be more inclusive to allow User-GU-A to have the same access as UserC.	<input type="radio"/>	<input type="radio"/>
You need to add UserB to the AWS-WS group to allow them access to My Staff.	<input type="radio"/>	<input type="radio"/>
Only UserA and UserD can access the Combined Security Information Registration Experience.	<input type="radio"/>	<input type="radio"/>

Answer:

Statement	Yes	No
You should change Guest User access to be more inclusive to allow User-GU-A to have the same access as UserC.	<input checked="" type="radio"/>	<input type="radio"/>
You need to add UserB to the AWS-WS group to allow them access to My Staff.	<input type="radio"/>	<input checked="" type="radio"/>
Only UserA and UserD can access the Combined Security Information Registration Experience.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

You should change Guest user access to be more inclusive to allow User-GU-A to have the same access as UserC. With the current configuration of the User Settings and User Features, as shown in the three exhibits, Guest user access is set to limit access to properties and memberships of directory objects. To allow User-GU-A to have the same access as UserC, this setting would need to change to the most inclusive setting, which is Guest users have the same access as members.

You do not need to add UserB to the AWS-WS group to allow them access to My Staff. With the current configuration of the User Settings and User Features, as shown in the three exhibits, we can see that only the AVD-Users group have been added to the setting Administrator can access My Staff option. As UserB is already a member of this group, they already have the access they need to access My Staff, and you do not need to add them to the AWS-WS group.

Not only UserA and UserD can access the Combined Security Information Registration Experience. With the current configuration of the User Settings and User Features, as shown in the three exhibit images, we can see that the AVD-Users group is selected under the Users can use the combined security information registration experience setting. In this scenario, UserA, UserB, and UserD are all in the AVD-User group.

QUESTION 272

A company has a hybrid environment with both on-premises Active Directory and Microsoft Entra ID. An IT administrator notices that users are not syncing anymore from the on-premises directory to the cloud.

You need to make sure that Active Directory and Microsoft Entra ID are in sync.

What is the first step you should take to troubleshoot the issue?

- A. Check the network connectivity between the on-premises and Microsoft Entra ID
- B. Check the Microsoft Entra Connect sync configuration
- C. Check the Microsoft Entra Connect Health sync status
- D. Check the Event Viewer for error messages

Answer: C

Explanation:

You should check the Microsoft Entra Connect Health sync status as the very first step to troubleshoot the issue. Microsoft Entra Connect Health is a feature of Microsoft Entra ID that allows you to monitor and troubleshoot the directory synchronization between your on-premises Active Directory and Microsoft Entra ID. To do this, you would check the Microsoft Entra Connect Health dashboard seeing as it provides real-time monitoring and alerting for the synchronization service, including the status of the sync engine, the number of objects synced, and any errors that may have occurred. By checking the Microsoft Entra Connect Health dashboard and identifying the root cause of the issue, the IT administrator can then take the appropriate steps to resolve the issue and re-establish the sync between on-premises Active Directory and Microsoft Entra ID.

Your first step should not be to check the Event Viewer for error messages. The very first step to troubleshoot the issue with Microsoft Entra Connect should be to check Microsoft Entra Connect Health sync status in a centralized dashboard to identify the root cause of the issue. Only after this first step should you check the event log on the server running the Microsoft Entra Connect to see if there are any relevant events or errors that may be related to the syncing issue.

You should not check the Microsoft Entra Connect sync configuration as the very first step to troubleshoot the issue. Verifying the Microsoft Entra Connect sync configuration is one of the next steps during the troubleshooting. In this step you should check the Microsoft Entra Connect sync service and ensure that it is running and configured correctly. If the service is stopped, the administrator should start it again and check the configuration to ensure that it is correct.

You should not check the network connectivity between the on-premises and Microsoft Entra ID as the very first step to troubleshoot the issue. The first step is to identify the root cause of the issue. If the issue is related to network connectivity, the administrator should check the network connection between the on-premises and Microsoft Entra ID environments to ensure that there is no problem with it, such as a firewall restriction.

QUESTION 273

Your organization has an existing Microsoft 365 tenant. The following end-user devices have been onboarded into your tenant:

Device Name	Operating System	Join Type	Device Location
DeviceA	Windows 10 20H2	Microsoft Entra Registered	User's Home
DeviceD	Windows 10 20H2	Hybrid Microsoft Entra	UK Office
DeviceF	Windows 11	Microsoft Entra Registered	Italy Office
DeviceC	Windows 10 22H2	Microsoft Entra Registered	Italy Office
DeviceB	Windows 11	Hybrid Microsoft Entra	UK Office
DeviceE	Windows 11	Hybrid Microsoft Entra	UK Office

You set up a conditional access policy as shown in the exhibits. The support desk receives complaints that users are unable to access cloud resources due to MFA registration failing.

Device platforms ×

Apply policy to selected device platforms.

[Learn more ↗](#)

Configure ⓘ

Yes No

Include Exclude

- Any device
- Select device platforms
 - Android
 - iOS
 - Windows Phone
 - Windows
 - macOS
 - Linux

Grant access

- Require multifactor authentication ⓘ
- Require authentication strength ⓘ
- Require device to be marked as compliant ⓘ
- Require Microsoft Entra hybrid joined device ⓘ

Control user access based on their physical location. [Learn more ↗](#)

Configure ⓘ

Include **Exclude**

- Any location
- All trusted locations
- All Compliant Network locations (Preview)
- Selected locations

Select

[Uk Office](#)

Uk Office

You need to report which of the new devices have been blocked from accessing cloud resources.

Which three devices does the Conditional Access policy block from accessing cloud resources?
Each correct answer presents part of the solution.

- A. DeviceE
- B. DeviceF
- C. DeviceD
- D. DeviceB
- E. DeviceA
- F. DeviceC

Answer: BEF**Explanation:**

The Conditional Access policy will block DeviceA, DeviceC, and DeviceF from accessing cloud resources in the tenant.

The policy Access Control settings is configured to only grant access if to devices that are Hybrid Microsoft Entra joined and located in the UK Office. In this scenario, these three devices are all Microsoft Entra Registered only so they will be blocked and they are all located outside of the UK office.

DeviceB, DeviceD, and DeviceE will all be granted access as they meet the requirement set in the policy of being Hybrid Microsoft Entra joined devices and located in the UK Office.

QUESTION 274

Drag and Drop Question

Your company is planning on using Privileged Identity Management (PIM) to grant administrative access to Azure resources.

You are setting up PIM for the first time and establish the workflow that will be used to ensure that PIM can be used by the first user.

What roles should you use for the following actions, while following the principle of least privilege? To answer, drag the appropriate role to each action. A role may be used once, more than once, or not at all.

To determine the users and roles to be managed using PIM

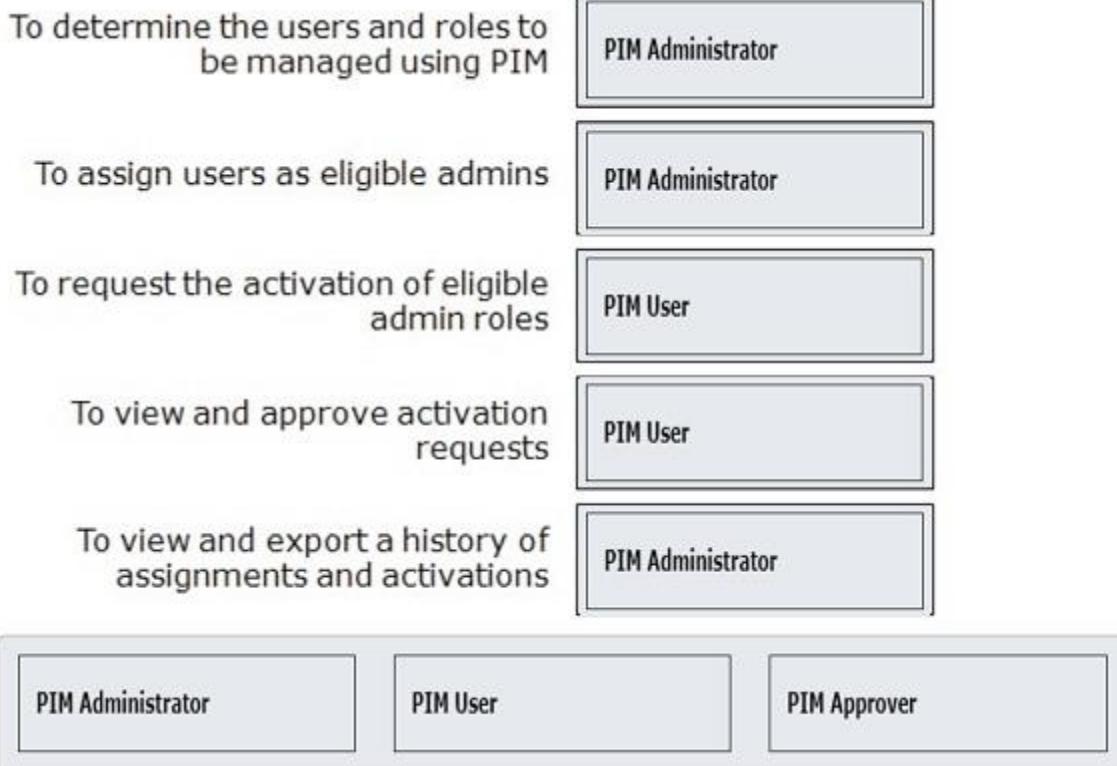
To assign users as eligible admins

To request the activation of eligible admin roles

To view and approve activation requests

To view and export a history of assignments and activations

PIM Administrator**PIM User****PIM Approver****Answer:**



Explanation:

You should use the Privileged Identity Management (PIM) Administrator role to determine the users and roles to be managed using PIM. The PIM Administrator will be the person performing the initial setup of PIM and will therefore need to collect the requirements for the implementation.

You should use the PIM Administrator role to assign users as eligible admins. The PIM Administrator will determine and configure which users will have which rights within the environment. As this is an administrative task, the PIM Administrator role will be required for this.

You should use the PIM User role to request the activation of eligible admin roles. When users require elevated rights for their account, they can create a PIM activation request to be granted the requested permissions.

You should use the PIM Approver role to view and approve activation requests. When PIM requests are created, the PIM Approver will approve or deny the request for the elevated permissions.

You should use the PIM Administrator role to view and export a history of assignments and activations. The PIM Administrator can access the history to make sure compliance requirements are met.

QUESTION 275

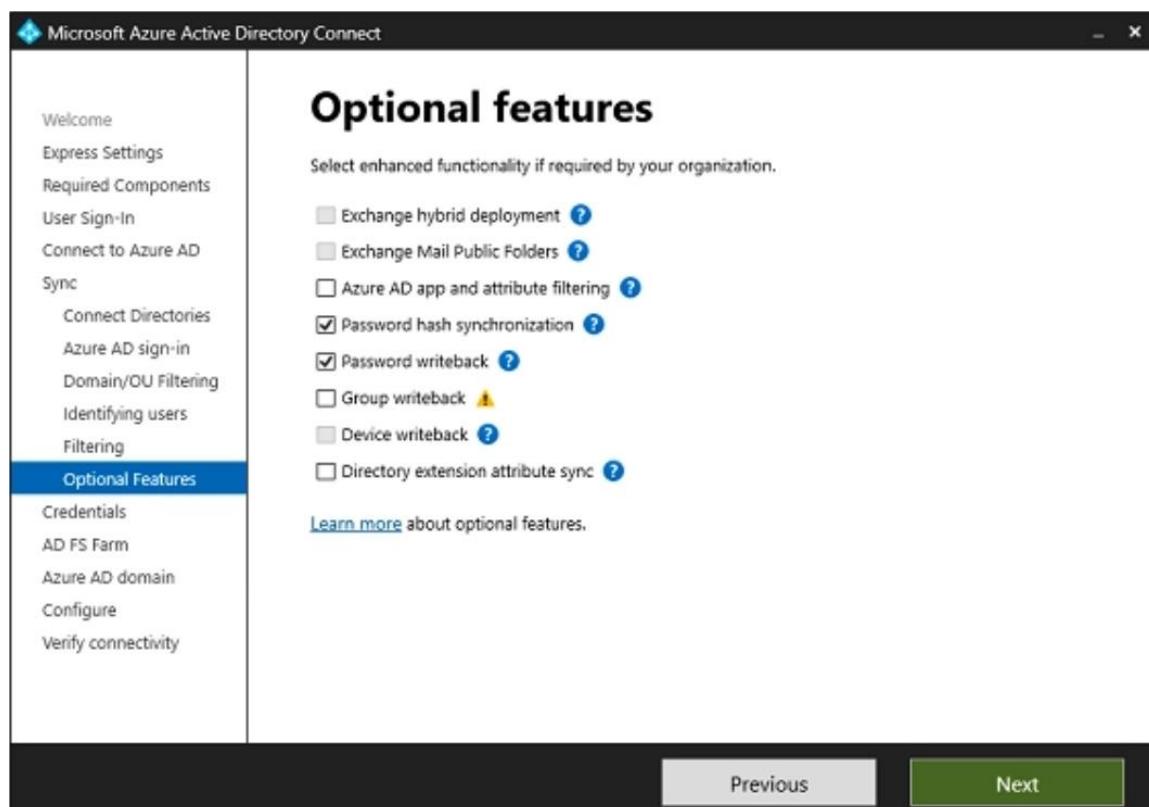
Hotspot Question

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named fabrikam.com. The domain contains an Active Directory Federation Services (AD FS) instance and a member server named Server1 that runs Windows Server. The domain contains the users shown in the following table.

Name	Description
User1	The user account has a six-character password and is enabled.
User2	The user account has a 12-character password and is enabled.
User3	The user account has an eight-character password and is disabled.

You have a Microsoft Entra tenant named contoso.com that is linked to a Microsoft 365 subscription.

You establish federation between fabrikam.com and contoso.com by using a Microsoft Entra Connect instance that is configured as shown in the following exhibit.



You perform the following tasks in contoso.com:

- Create a group named Group1.
- Disable User2.
- Enable 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 Area

Statements	Yes	No
You can add User1 to Group1.	<input type="radio"/>	<input type="radio"/>
User2 can sign in to Server1.	<input type="radio"/>	<input type="radio"/>
User3 can sign in to Microsoft 365.	<input type="radio"/>	<input type="radio"/>

Answer:
Answer Area

Statements	Yes	No
You can add User1 to Group1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in to Server1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can sign in to Microsoft 365.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

Group1 is created in the entra ID tenant, and the user is synced, so this is possible. It doesn't state that the group should be visible on-prem.

Box 2: Yes

The user is a directory-synced user, so authority lies on-prem. Disabling it from the Entra ID portal will have no effect. The server is also an on-prem server. Disabling should be done in on-prem adds.

Box 3: No

You enable the account in the entra id tenant, but the account is directory synced, so authority lies with the on-prem AD, enabling from the portal is not possible.

QUESTION 276

Hotspot Question

You have a Microsoft Entra tenant that has a Microsoft Entra ID P2 service plan. The tenant contains the users shown in the following table.

Name	Role
Admin1	Cloud Device Administrator
Admin2	Microsoft Entra Joined Device Local Administrator
User1	None

You have the Device settings shown in the following exhibit.

Devices | Device settings ...

Default Directory - Azure Active Directory

Save Discard Got feedback?

- All devices
- Device settings**
- Enterprise State Roaming
- BitLocker keys (Preview)
- Diagnose and solve problems

Users may join devices to Azure AD ⓘ

All Selected None

Selected
No member selected

Activity

Users may register their devices with Azure AD ⓘ

All None

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication ⓘ

Yes No

⚠️ We recommend that you require Multi-Factor Authentication to register or join devices using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

Maximum number of devices per user ⓘ

5

Additional local administrators on all Azure AD joined devices

Manage Additional local administrators on all Azure AD joined devices

User1 has the devices shown in the following table.

Name	Operating system	Device identity
Device1	Windows 10	Microsoft Entra joined
Device2	iOS	Microsoft Entra registered
Device3	Windows 10	Microsoft Entra registered
Device4	Android	Microsoft Entra 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 Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Microsoft Entra ID.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to Yes .	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 is a local administrator on Device3.	<input type="radio"/>	<input checked="" type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Microsoft Entra ID.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to Yes.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 is a local administrator on Device3.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 277

You have an Azure subscription named Sub1 that contains a user named User1.

You need to ensure that User1 can purchase a Microsoft Entra Permissions Management license for Sub1. The solution must follow the principle of least privilege.

Which role should you assign to User1?

- A. Global Administrator
- B. Billing Administrator
- C. Permissions Management Administrator
- D. User Access Administrator

Answer: B

QUESTION 278

You have an Azure subscription that contains a user named User1 and two resource groups named RG1 and RG2.

You need to ensure that User1 can perform the following tasks:

- View all resources.
- Restart virtual machines.
- Create virtual machines in RG1 only.
- Create storage accounts in RG1 only.

What is the minimum number of role-based access control (RBAC) role assignments required?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: C

Explanation:

Assign User1 the "Reader" role at the subscription level to view all resources.

Assign User1 the "Virtual Machine Contributor" role at the RG1 level to restart virtual machines and create virtual machines in RG1 only.

Assign User1 the "Storage Account Contributor" role at the RG1 level to create storage accounts in RG1 only.

QUESTION 279

You work for a company named Contoso, Ltd. that has a Microsoft Entra tenant named contoso.com.

Contoso is working on a project with the following two partner companies:

- A company named A. Datum Corporation that has a Microsoft Entra tenant named adatum.com.
- A company named Fabrikam, Inc. that has a Microsoft Entra tenant named fabrikam.com.

When you attempt to invite a new guest user from adatum.com to contoso.com, you receive an error message.

You can successfully invite a new guest user from fabrikam.com to contoso.com.

You need to be able to invite new guest users from adatum.com to contoso.com.

What should you configure?

- A. Guest invite settings
- B. Verifiable credentials
- C. Named locations
- D. Collaboration restrictions

Answer: D

Explanation:

You need to add adatum.com to the list of domains on External Identities >> External Collab Settings >> Collaboration Restrictions >> Allow invitations only to the specified domains.

QUESTION 280

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named 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 package
- B. an access review
- C. a lifecycle workflow
- D. a Conditional Access policy

Answer: A

QUESTION 281

Hotspot Question

You have a Microsoft Entra tenant that contains multiple storage accounts.

You plan to deploy multiple Azure App Service apps that will require access to the storage accounts.

You need to recommend an identity solution to provide the apps with access to the storage accounts. The solution must minimize administrative effort.

Which type of identity should you recommend, and what should you recommend using to control access to the storage accounts? To answer, select the appropriate options in the answer area.

Answer Area

Identity type:

Microsoft Entra user
Service principal
System-assigned managed identity
User-assigned managed identity

To control access, use:

Microsoft Entra Domain Services
Role-based access control (RBAC)
Shared access signature (SAS) tokens
X.509 certificates

Answer:**Answer Area**

Identity type:

Microsoft Entra user
Service principal
System-assigned managed identity
User-assigned managed identity

To control access, use:

Microsoft Entra Domain Services
Role-based access control (RBAC)
Shared access signature (SAS) tokens
X.509 certificates

Explanation:

<https://learn.microsoft.com/en-us/azure/app-service/scenario-secure-app-access-storage?tabs=azure-portal>

QUESTION 282

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 Sub1, assign the Owner role.
- B. For DB1, assign the Azure Cosmos DB Account Reader Role role.
- C. For RG1, assign the Azure Cosmos DB Data Reader Role role.
- D. For RG1, assign the Reader role.

Answer: B

QUESTION 283

You have an Azure subscription that contains a storage account named storage1 and a web app named WebApp1. WebApp1 uses a system-assigned managed identity.

You need to ensure that WebApp1 can read and write files to storage1 by using the system-assigned managed identity.

What should you configure for storage1 in the Azure portal?

- A. data protection
- B. a shared access signature (SAS)
- C. the Access control (IAM) settings
- D. the File share settings
- E. access keys

Answer: C

QUESTION 284

You have a Microsoft 365 tenant.

In Microsoft Entra ID, you configure the terms of use.

You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.

What should you configure?

- A. Terms and conditions in Microsoft Intune
- B. an access policy in Microsoft Defender for Cloud Apps
- C. a conditional access policy in Microsoft Entra ID
- D. a compliance policy in Microsoft Intune

Answer: C

QUESTION 285

You have a Microsoft 365 E5 subscription that contains a user named User1. User1 is eligible for the Application Administrator role.

User1 needs to configure a new connector group for an application proxy.

What should you use to activate the role for User1?

- A. the Microsoft 365 Defender portal
- B. the Microsoft 365 admin center
- C. the Microsoft Intune admin center
- D. the Azure Active Directory admin center

Answer: D

QUESTION 286

Your on-premises network contains an Active Directory Domain Services (AD DS) domain and a certification authority (CA) named CA1.

You have an Azure AD tenant.

You need to implement certificate-based authentication in Azure AD. The solution must ensure that users can sign in by using certificates issued by CA1. What should you do first?

- A. Deploy an Azure key vault.
- B. Add CA1 as a Certificate Authority to the Microsoft Entra ID tenant.
- C. Enable auto-enrollment for CA1.
- D. Deploy Windows Hello for Business.

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-certificate-based-authentication>

QUESTION 287

You have accounts for the following cloud platforms:

- Azure
- Alibaba Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

You configure an Azure subscription to use Microsoft Entra Permissions Management to manage the permissions in Azure only.

Which additional cloud platforms can be managed by using Permissions Management?

- A. AWS only
- B. Alibaba Cloud and AWS only
- C. Alibaba Cloud and GCP only
- D. AWS and GCP only
- E. Alibaba Cloud, AWS, and GCP

Answer: D

Explanation:

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into permissions assigned to all identities. For example, over-privileged workload and user identities, actions, and resources across multicloud infrastructures in Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

QUESTION 288

You have three Azure subscriptions that are linked to a single Microsoft Entra tenant.

You need to evaluate and remediate the risks associated with highly privileged accounts. The solution must minimize administrative effort.

What should you use?

- A. Global Secure Access
- B. Privileged Identity Management (PIM)
- C. Microsoft Entra Permissions Management
- D. Microsoft Entra Verified ID

Answer: C

QUESTION 289

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 Role/Policy Template subtab, create a template.
- B. From the My Requests subtab, create a new request.
- C. From the Roles/Policies subtab, create a role.
- D. From the Permissions subtab, use a quick action.

Answer: D

Explanation:

There are four quick actions that can be used to manage users:

Revoke Unused Tasks
Revoke High-Risk Tasks
Revoke Delete Tasks
Assign Read-Only Status

<https://learn.microsoft.com/en-us/training/permissions-management/explore-features-of-permissions-management/9-act-on-your-findings-with-remediation-tab>

QUESTION 290

You have an Azure subscription that contains a user named User1. The subscription is

onboarded to Microsoft Entra Permissions Management.

You need to provide User1 with access to Permissions Management. The solution must meet the following requirements:

- Follow the principle of least privilege.
- Minimize administrative effort.

What should you do first?

- A. From the Role/Policy Template subtab of Permissions Management, create a template.
- B. From the Microsoft Entra admin center, create a security group.
- C. From the My Requests subtab of Permissions Management, create a new request.
- D. From the Microsoft Entra admin center, assign a role to User1.

Answer: B

Explanation:

Permissions Management has its own group-based access system that provides granular control over what cloud environments, authorization systems, and permissions users have access to.

The settings to manage these areas are found under the User Management tab of the product, which is in your profile dropdown menu.

<https://learn.microsoft.com/en-us/training/permissions-management/explore-features-of-permissions-management/13-manage-access-to-microsoft-entra-permissions-management>

QUESTION 291

Drag and Drop Question

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

Name	Type	Description
User1	User	<i>Not applicable</i>
User2	User	<i>Not applicable</i>
Vault1	Azure Key Vault	Contains a secret named Secret1
Vault2	Azure Key Vault	Contains a secret named Secret2
Secret1	Secret	Stored in Vault1
Secret2	Secret	Stored in Vault2

The subscription uses Privileged Identity Management (PIM).

You need to configure the following access controls by using PIM:

- Ensure that User1 can read and update Secret1.
- Ensure that User2 can read the contents of the secrets stored in Vault2.

The solution must follow the principle of least privilege.

Which authorization method should you use for each user? To answer, drag the appropriate authorization methods to the correct users. Each authorization method 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.

Authorization methods

- The GET Secret Permissions Access Policy permission
- The Key Vault Secrets Officer RBAC role
- The Key Vault Reader RBAC role
- The Key Vault Secrets User RBAC role
- The LIST Secret Permissions Access Policy permission
- The SET Secret Permissions Access Policy permission

Answer Area

 User1:

 User2:
Answer:
Authorization methods

- The GET Secret Permissions Access Policy permission
- The Key Vault Reader RBAC role
- The LIST Secret Permissions Access Policy permission
- The SET Secret Permissions Access Policy permission

Answer Area

 User1:

 User2:
QUESTION 292
Hotspot Question

You have two Azure subscriptions named Sub1 and Sub2 that are linked to a Microsoft Entra tenant. The tenant contains three groups named Group1, Group2, and Group3.

The subscriptions contain the resources shown in the following table.

Name	Type	Subscription
VM1	Virtual machine	Sub1
VM2	Virtual machine	Sub2
Automation1	Azure Automation account	Sub2

The tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2, Group3
User3	Group3

You manage the subscriptions by using Microsoft Entra Permissions Management. Permissions Management is configured as shown in the following table.

Name	Roles	Authorization System Name	Requestor for Other Identities
Group1	Viewer	Sub1	None
Group2	Controller	Sub2	User1
Group3	Approver	All Current and Future	None

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 request access to VM2 by using Permissions Management.	<input type="radio"/>	<input type="radio"/>
User2 can create an access request to Automation1 on behalf of User1.	<input type="radio"/>	<input type="radio"/>
User3 can approve access requests for VM2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can request access to VM2 by using Permissions Management.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can create an access request to Automation1 on behalf of User1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can approve access requests for VM2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

No - User1 is part of the group that can request access to sub1, not sub2

No - User1 can request access to Sub1 on behalf of other identities, not user2

Yes - User3's group can approve access requests for all subscriptions

QUESTION 293

Hotspot Question

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.

Answer Area

Identify all the accounts that are assigned the Global Administrator role permanently:

Analytics
Audit
Azure AD Insights
Dashboard
Reports

Review the PCI of User1:

Analytics
Audit
Azure AD Insights
Dashboard
Reports

Answer:

Answer Area

Identify all the accounts that are assigned the Global Administrator role permanently:

Analytics
Audit
Azure AD Insights
Dashboard
Reports

Review the PCI of User1:

Analytics
Audit
Azure AD Insights
Dashboard
Reports