Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam

NEW QUESTION 1
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that contains the compliance policies shown in the following table.

Name	Require BitLocker	Require the device to be at or under the machine risk score
Policy1	Required	High
Policy2	Not configured	Medium
Policy3	Required	Low

The tenant contains the devices shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Microsoft Defender for Endpoint risk status	Policies applied
Device1	Configured	High	Policy1, Policy3
Device2	Not configured	Medium	Policy2, Policy3
Device3	Not configured	Low	Policy1, Policy2

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

Statements	Yes	No
Device1 is marked as compliant.	○	○
Device2 is marked as compliant.	○	○
Device3 is marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device1 is marked as compliant.	⊡	○
Device2 is marked as compliant.	⊡	○
Device3 is marked as compliant.	○	⊡

NEW QUESTION 2
- (Topic 6)
You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1. You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:
• Assign licenses to users.
• Procure apps from Microsoft Store.
• Manage private store availability for all items.
The solution must use the principle of least privilege.
Which Microsoft Store for Business role should you assign to User1?

A. Basic Purchaser
B. Device Guard signer
C. Admin
D. Purchaser

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

NEW QUESTION 3
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.
You need to ensure that each group can perform the tasks shown in the following table.

Group	Task
Group1	• Manage service requests. • Purchase new services. • Manage subscriptions. • Monitor service health.
Group2	• Assign licenses. • Add users and groups. • Create and manage user views. • Update password expiration policies.

The solution must use the principle of least privilege.
Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. 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

Billing Administrator

Global Administrator

Helpdesk Administrator

License Administrator

Service Support Administrator

User Administrator

Answer Area

Group1: | Role |

Group2: | Role |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Billing admin manage service request Purchase new services Etc.
Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.
Box 2: User admin User admin
Assign the User admin role to users who need to do the following for all users:
- Add users and groups
- Assign licenses
- Manage most users properties
- Create and manage user views
- Update password expiration policies
- Manage service requests
- Monitor service health

NEW QUESTION 4
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant
You create a data toss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.
To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 5
DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You need to automatically label the documents on Site1 that contain credit card numbers. 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
Create a sensitivity label.	
Create an auto-labeling policy.	
Create a sensitive information type.	
Wait 24 hours, and then turn on the policy.	
Publish the label.	
Create a retention label.	
Wait eight hours, and then turn on the policy.	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
Create a sensitivity label.	Create a sensitivity label.
Create an auto-labeling policy.	
Create a sensitive information type.	Publish the label.
Wait 24 hours, and then turn on the policy.	
Publish the label.	Create an auto-labeling policy.
Create a retention label.	
Wait eight hours, and then turn on the policy.	

NEW QUESTION 6
HOTSPOT - (Topic 6)
HOTSPOT
Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.
You need to implement Azure AD Connect cloud sync.
What should you install first and on which server? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Install:
- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:
- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: The Azure AD Connect provisioning agent Install the Azure AD Connect provisioning agent
How is Azure AD Connect cloud sync different from Azure AD Connect sync?
With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.
Box 2: Server1 or Server2 only.
Cloud provisioning agent requirements include:
* An on-premises server for the provisioning agent with Windows 2016 or later.
This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.
Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.

NEW QUESTION 7
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.
You need to remove User1 from the Restricted entities list. What should you use?

A. the Exchange admin center
B. the Microsoft Purview compliance portal
C. the Microsoft 365 admin center
D. the Microsoft 365 Defender portal
E. the Microsoft Entra admin center

Answer: D

Explanation:
Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.
Remove a user from the Restricted entities page in the Microsoft 365 Defender portal In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use https://security.microsoft.com/restrictedentities.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam

NEW QUESTION 8
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
You need to implement identity protection. The solution must meet the following requirements:
? Identify when a user's credentials are compromised and shared on the dark web.
? Provide users that have compromised credentials with the ability to self-remediate.
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 identify when users have compromised credentials, configure:

A registration policy
A sign-in risk policy
A user risk policy
A multifactor authentication registration policy
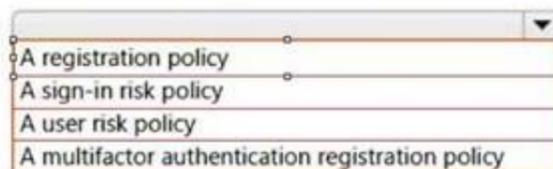
To enable self-remediation, select:

Generate a temporary password
Require multi-factor authentication
Require password change
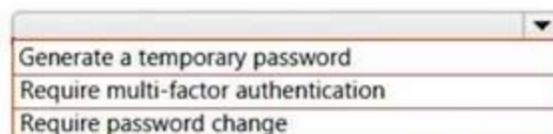
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: A user risk policy
Identify when a user's credentials are compromised and shared on the dark web.
User risk-based Conditional Access policy
Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:
Block access
Allow access but require a secure password change.
A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.
Box 2: Require password change
Provide users that have compromised credentials with the ability to self-remediate.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators

NEW QUESTION 9
- (Topic 6)
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 that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

NEW QUESTION 10
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to implement device configuration profiles in Microsoft Intune. Which platform can you manage by using the profiles?

A. Ubuntu Linux
B. macOS
C. Android Enterprise
D. Windows 8.1

Answer: D

NEW QUESTION 10
- (Topic 6)
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 an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

NEW QUESTION 15
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You plan to deploy 1.000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.
You need to recommend a Microsoft Intune enrollment option that meets the following requirements:
• Minimizes user interaction
• Minimizes administrative effort
• Automatically installs corporate apps What should you recommend?

A. Automated Device Enrollment (ADE)
B. bring your own device (BYOD) user and device enrollment
C. Apple Configurator enrollment

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll

NEW QUESTION 16
- (Topic 6)
You have a Microsoft 365 subscription.
You discover that some external users accessed center for a Microsoft SharePoint site. You modify the sharePoint sharing policy to prevent sharing, outside your organization. You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the Security $ Compliance admin center you create a threat management
policy.

Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 19
- (Topic 6)
Your company has 10,000 users who access all applications from an on-premises data center.
You plan to create a Microsoft 365 subscription and to migrate data to the cloud. You plan to implement directory synchronization.
User accounts and group accounts must sync to Azure AD successfully. You discover that several user accounts fail to sync to Azure AD.
You need to resolve the issue as quickly as possible. What should you do?

A. From Active Directory Administrative Center, search for all the users, and then modify the properties of the user accounts.
B. Run idfix.exe, and then click Edit.
C. From Windows PowerShell, run the start-AdSyncSyncCycle -PolicyType Delta command.
D. Run idfix.exe, and then click Complete.

Answer: B

Explanation:
IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for- synch-with-idfix

NEW QUESTION 23
- (Topic 6)
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 computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: At a command prompt, you run the winver.exe command. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

NEW QUESTION 25
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.
What should you use?

A. an attack surface reduction (ASR) policy
B. an app configuration policy
C. a device compliance policy
D. a device configuration profile

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

NEW QUESTION 28
- (Topic 6)
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 that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

NEW QUESTION 29
- (Topic 6)
You have a Microsoft 365 subscription.
You register two applications named App1 and App2 to Azure AD.
You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

A. From the Microsoft Entra admin center, create a conditional access policy
B. From the Microsoft 365 admin center, configure the Modem authentication settings.
C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.
D. From Multi-Factor Authentication, configure the service settings.

Answer: A

Explanation:
Use Conditional Access policies
If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication

NEW QUESTION 32
- (Topic 6)
Your company has a Microsoft 365 E5 tenant that contains a user named User1. You review the company's compliance score.
You need to assign the following improvement action to User1:Enable self-service password reset.
What should you do first?

A. From Compliance Manager, turn off automated testing.
B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

NEW QUESTION 35
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to configure a group naming policy.
Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Portal:	The Microsoft 365 admin center ▼
	The Microsoft 365 admin center
Group types:	The Microsoft 365 Defender portal
	The Microsoft Entra admin center
	The Microsoft Purview compliance portal

Group types:	Security only ▼
	Microsoft 365 only
	Security only
	Security and mail-enabled security only
	Microsoft 365 and distribution only
	Microsoft 365, mail-enabled security, and distribution only
	Security, Microsoft 365, mail-enabled security, and distribution

NEW QUESTION 36
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Configuration
Group1	Global security group
User1	Enabled user account
User2	Disabled user account

You configure Azure AD Connect to sync contoso.com to Azure AD.
Which objects will sync to Azure AD?

A. Group1 only
B. User1 and User2 only
C. Group1 and User1 only
D. Group1, User1, and User2

Answer: D

Explanation:
 Disabled accounts
Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.
The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts

NEW QUESTION 41
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Service Support Administrator
User3	Cloud Application Administrator
User4	None

You plan to provide User4 with early access to Microsoft 365 feature and service updates. You need to identify which Microsoft 365 setting must be configured, and which user can
modify the setting. The solution must use the principle of least privilege.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Microsoft 365 setting:

▼
Office installation options
Privileged access
Release preferences

User:

▼
User1 only
User2 only
User3 only
User1 and User2 only
User1 and User3 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Microsoft 365 setting:

▼
Office installation options
Privileged access
Release preferences

User:

▼
User1 only
User2 only
User3 only
User1 and User2 only
User1 and User3 only

NEW QUESTION 46
HOTSPOT - (Topic 6)
You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (default)	Device2	Group2

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

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	[○]
User2 can collect an investigation package from Device2.	○	[○]
User3 can isolate Device1.	[○]	○

NEW QUESTION 50
- (Topic 6)
You have a Microsoft 365 tenant that contains 500 Windows 10 devices and a Microsoft Endpoint Manager device compliance policy.
You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps.
Which policy type should you configure?

A. conditional access
B. account protection
C. attack surface reduction (ASR)
D. Endpoint detection and response

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION 55
- (Topic 6)
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.

Your network contains an Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the Azure AD credentials.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

The question states that "all the user account synchronizations completed successfully". Therefore, the Azure AD credentials are configured correctly in Azure AD Connect. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync- configure-filtering

NEW QUESTION 59
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains two users named Admin1 and Admin2.
All users are assigned a Microsoft 365 Enterprise E5 license and auditing is turned on.
You create the audit retention policy shown in the exhibit. (Click the Exhibit tab.)

After Policy1 is created, the following actions are performed:
? Admin1 creates a user named User1.
? Admin2 creates a user named User2.
How long will the audit events for the creation of User1 and User2 be retained? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User1:

| 0 days |
| 30 days |
| 90 days |
| 180 days |
| 365 days |

User2:

| 0 days |
| 30 days |
| 90 days |
| 180 days |
| 365 days |

A. Mastered
B. Not Mastered

Answer: A

Explanation:

User1:

| 0 days |
| 30 days |
| 90 days |
| 180 days |
| 365 days |

User2:

| 0 days |
| 30 days |
| 90 days |
| 180 days |
| 365 days |

NEW QUESTION 63
- (Topic 6)
You have a Microsoft 365 E5 subscription.
On Monday, you create a new user named User1.
On Tuesday, User1 signs in for the first time and perform the following actions:
• Signs in to Microsoft Exchange Online from an anonymous IP address
• Signs in to Microsoft SharePoint Online from a device in New York City.
• Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections
Which types of sign-in risks will Azure AD Identity Protection detect for User1?

A. anonymous IP address only
B. anonymous IP address and atypical travel
C. anonymous IP address, atypical travel, and unfamiliar sign-in properties
D. unfamiliar sign-in properties and atypical travel only
E. anonymous IP address and unfamiliar sign-in properties only

Answer: C

NEW QUESTION 67
- (Topic 6)

You have a Microsoft 365 tenant that contains the groups shown in the following table.

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

You plan to create a new Windows 10 Security Baseline profile. To which groups can you assign to the profile?

A. Group3 only
B. Group1 and Group3 only
C. Group2 and Group3 only
D. Group1. Group2. and Group3

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile
https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

NEW QUESTION 71
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription that contains the users in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.

Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	Group3

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 enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	⊙	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	⊙
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	⊙

NEW QUESTION 75
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to compare the current Safe Links configuration to the Microsoft recommended configurations.
What should you use?

A. Microsoft Purview
B. Azure AD Identity Protection
C. Microsoft Secure Score
D. the configuration analyzer

Answer: C

NEW QUESTION 77
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:
? Deploy a VPN connection by using a VPN device configuration profile.
? Configure security settings by using an Endpoint Protection device configuration profile.
You support the management tasks.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

VPN device configuration profile:
- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Endpoint Protection device configuration profile:
- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

A. Mastered
B. Not Mastered

Answer: A

Explanation:

VPN device configuration profile:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Endpoint Protection device configuration profile:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

NEW QUESTION 82
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You define a retention label that has the following settings:
• Retention period 7 years
• Start the retention period bated on: When items were created
You need to prevent the removal of the label once the label K applied to a lie What should you select in the retention label settings?

A. Retain items even If users delete
B. Mark items as a record
C. Mark items as a regulatory record
D. Retain items forever

Answer: B

NEW QUESTION 84
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You create a retention label named Retention1 as shown in the following exhibit.

Review your settings

Name   Edit
Retention1

Description for admins   Edit

Description for users   Edit

File plan descriptors   Edit
Reference Id:1
Business function/department Legal
Category: Compliance
Authority type: Legal

Retention   Edit
7 years
Retain only
Based on when it was created

Back	Create this label	Cancel

When users attempt to apply Retention1, the label is unavailable. You need to ensure that Retention1 is available to all the users. What should you do?

A. Create a new label policy
B. Modify the Authority type setting for Retention!
C. Modify the Business function/department setting for Retention 1.
D. Use a file plan CSV template to import Retention1.

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

NEW QUESTION 89
- (Topic 6)
Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 10.
You purchase a Microsoft 365 subscription.
You implement password hash synchronization and Azure AD Seamless Single Sign-On (Seamless SSO).
You need to ensure that users can use Seamless SSO from the Windows 10 computers. What should you do?

A. Join the computers to Azure AD.
B. Create a conditional access policy in Azure AD.
C. Modify the Intranet zone settings by using Group Policy.
D. Deploy an Azure AD Connect staging server.

Answer: A

NEW QUESTION 93
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription.
A user named user1@contoso.com was recently provisioned.
You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

```
                          ▼   -Scopes User.ReadWrite.All, Organization.Read.All
 Connect-AzureAD
 Connect-MgGraph
 Connect-MSOLService


$E3 =        ▼   | Where SkuPartNumber -eq 'EnterprisePack'
      Get-AzureADUser
      Get-MgSubscribedSku
      Get-MSOLAccountSKU

$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$LicenseOptions= @(
    @{
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    }
)
                          ▼   -UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @()
 Set-AzureADUser
 Set-MgUserLicense
 Set-MSOLUser
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Connect-MgGraph
Assign Microsoft 365 licenses to user accounts with PowerShell Use the Microsoft Graph PowerShell SDK
First, connect to your Microsoft 365 tenant.
Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the 'Assign license'
Microsoft Graph API reference page.
The Organization.Read.All permission scope is required to read the licenses available in the tenant.
Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All Box 2: Get-MgSubscribedSku
Run the Get-MgSubscribedSku command to view the available licensing plans and the
number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.
Box 3: Set-MgUserLicense Assigning licenses to user accounts
To assign a license to a user, use the following command in PowerShell.
Set-MgUserLicense -UserId $userUPN -AddLicenses @{SkuId = "<SkuId>"} - RemoveLicenses @()
This example assigns a license from the SPE_E5 (Microsoft 365 E5) licensing plan to the unlicensed user belindan@litwareinc.com:
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId =
$e5Sku.SkuId} -RemoveLicenses @()

NEW QUESTION 98
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the resources shown in the following table.

Name	Type
Group1	Microsoft 365 group
Group2	Distribution group
Site1	Microsoft SharePoint site

You create a sensitivity label named Label1. To which resource can you apply Label1?

A. Group1 only
B. Group2 only
C. Site1 only
D. Group1 and Group2 only
E. Group1, Group2, and Site1

Answer: E

Explanation:
Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory
Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.
In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.
When you configure a label policy, you can:
Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams- groups-sites
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365- worldwide

NEW QUESTION 103
HOTSPOT - (Topic 6)
Your company has a Azure AD tenant named comoso.onmicrosoft.com that contains the users shown in the following table.

Name	Role
User1	Password Administrator
User2	Security Administrator
User3	User Administrator
User4	None

You need to identify which users can perform the following administrative tasks:
• Reset the password of User4.
• Modify the value for the manager attribute of User4.
Which users should you identify for each task? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Reset the password of User4: | User1 and User3 only ▼ |
  User1 only
  User2 only
  User1 and User2 only
  User1 and User3 only
  User1, User2, and User3

Modify the value for the manager attribute of User4: | User3 only ▼ |
  User2 only
  User3 only
  User1 and User3 only
  User2 and User3 only
  User1, User2, and User3

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Reset the password of User4: | User1 and User3 only ▼
- User1 only
- User2 only
- User1 and User2 only
- **User1 and User3 only**
- User1, User2, and User3

Modify the value for the manager attribute of User4: | User3 only ▼
- User2 only
- **User3 only**
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

NEW QUESTION 108
HOTSPOT - (Topic 6)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.

Configure
Microsoft Intune

☐ Save   ✕ Discard   🗑 Delete

MDM user scope ❶ | None | **Some** | All |

Groups
Select groups
Group1   ＞

MDM terms of use URL ❶   https://portal.manage.microsoft.com/TermsofUse.aspx

MDM discovery URL ❶   https://enrollment.manage.microsoft.com/enrollmentserver/discov ...

MDM compliance URL ❶   https://portal.manage.microsoft.com/?portalAction=Compliance

Restore default MDM URLs

MAM User scope ❶ | None | **Some** | All |

Groups
Select groups
Group2   ＞

MAM Terms of use URL ❶

MAM Discovery URL ❶   https://wip.mam.manage.microsoft.com/Enroll

MAM Compliance URL ❶

Restore default MAM URLs

You purchase a Windows 10 device named Device1.
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 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	⊙	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	⊙
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	⊙

NEW QUESTION 110
- (Topic 6)
You have a Microsoft 365 F5 subscription.
You plan to deploy 100 new Windows 10 devices.
You need to order the appropriate version of Windows 10 for the new devices. The version must
Meet the following requirements.
Be serviced for a minimum of 24 moths.
Support Microsoft Application Virtualization (App-V) Which version should you identify?

A. Window 10 Pro, version 1909
B. Window 10 Pro, version 2004
C. Window 10 Pro, version 1909
D. Window 10 Enterprise, version 2004

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/release-health/release-information
https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported- configurations

NEW QUESTION 111
- (Topic 6)
You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

The policies are assigned to Device1.
Which policy settings will be applied to Device1?

A. only the settings of Policy1
B. only the settings of Policy2
C. only the settings of Policy3
D. no settings

Answer: D

NEW QUESTION 116
HOTSPOT - (Topic 6)
HOTSPOT
You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1	Enforced

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs. The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Location1	131.107.20.0/24	Yes
Location2	131.107.50.0/24	Yes

You create a conditional access policy that has the following configurations:
? Users or workload identities assignments: All users
? Cloud apps or actions assignment: App1
? Conditions: Include all trusted locations
? Grant access: Require multi-factor authentication
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
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	◉	○
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
* 131.107.50.10 is in a Trusted Location so the conditional access policy applies. The policy requires MFA. However, User1's MFA status is disabled. The MFA requirement in the conditional access policy will override the user's MFA status of disabled. Therefore, User1 must use MFA.
Box 2: Yes.
* 131.107.20.15 is in a Trusted Location so the conditional access policy applies. The policy requires MFA so User2 must use MFA.
Box 3: No.
IP not from Trusted Location so Policy does not apply, Subnet 131.107.5.5 is not in the range of 131.107.50.0/24

NEW QUESTION 119
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Activation

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

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	15 day(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	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.

Answer Area

A user that is assigned the Global Administrator role as active [answer choice].

▼
will lose the role after eight hours
can reactivate the role every eight hours
can reactivate the role every 15 days
will lose the role after 15 days

You can make the Global Administrator role available to activation requests [answer choice].

▼
for up to eight hours
for up to three months
for up to 15 days
until the requests are revoked manually

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: will lose the role after eight hours
From exhibit: Activation, Activation maximum duration (hours): 8 hour(s)
Box 2: for up to three months
We see from exhibit: Assignment, Expire eligible assignment after: 3 month(s)

NEW QUESTION 120
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that has auditing turned on. The subscription contains the users shown in the following table.

Name	License
Admin1	Microsoft Office 365 E5
Admin2	None

New audit retention policy   ✕

Name *:
Policy1

Description

Record Types

AzureActiveDirectory ▾

Activities

Added user ▾

Users:
Show results for all users

Duration *:
○ 90 Days
◉ 6 Months
○ 1 Year

Priority *:
100

You plan to create a new user named User1.
How long will the user creation audit event be available if Admin1 or Admin2 creates User1? To answer, select the appropriate options in the answer area.
Each correct selection is worth one point.

Answer Area

Admin1: 6 months ▼
30 days
90 days
6 months
1 year

Admin2: 90 days ▼
30 days
90 days
6 months
1 year

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Admin1: 6 months ▼
30 days
90 days
6 months 1
1 year

Admin2: 90 days ▼
30 days
90 days
6 months
1 year

NEW QUESTION 125
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You plan to perform device discovery and authenticated scans of network devices. You install and register the network scanner on a device named Device1.
What should you do next?

A. Connect Defender for Endpoint to Microsoft Intune.
B. Apply for Microsoft Threat Experts - Targeted Attack Notifications.
C. Create an assessment job.
D. Download and run an onboarding package.

Answer: C

NEW QUESTION 130
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature. You need to block users from downloading a file named File1.exe.
What should you use?

A. an indicator
B. a suppression rule
C. a device configuration profile

Answer: A

NEW QUESTION 132
HOTSPOT - (Topic 6)
Your network contains an on-premises Active Directory domain that is synced to Azure AD as shown in the following exhibit.
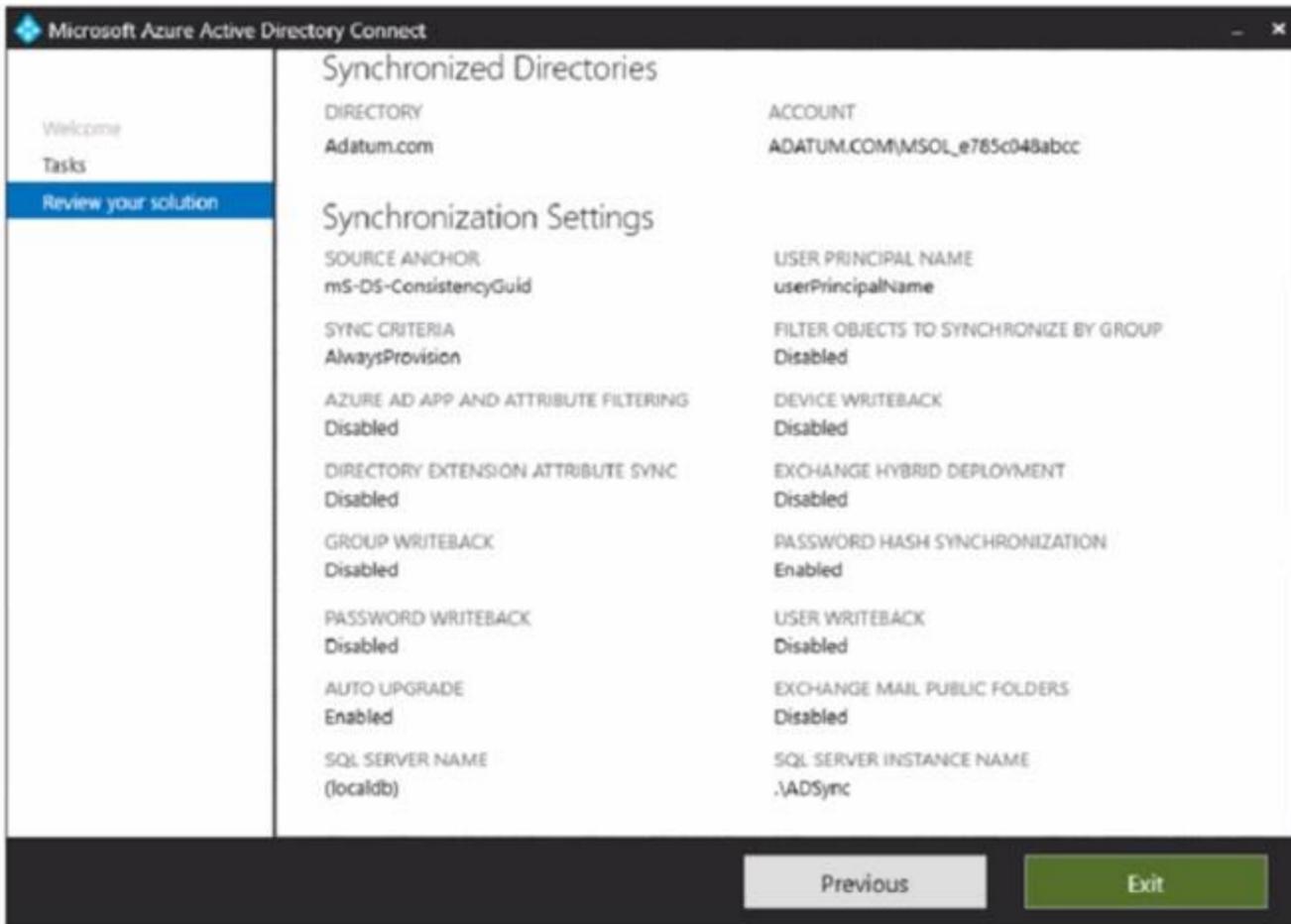
An on-premises Active Directory user account named Allan You is synchronized to Azure AD. You view Allan's account from Microsoft 365 and notice that his username is set to Allan @>ddatum.onmicrosoft.com.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 137
- (Topic 6)
Your network contains three Active Directory forests. There are forests trust relationships between the forests.
You create an Azure AD tenant.
You plan to sync the on-premises Active Directory to Azure AD.
You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.
What should you include in the recommendation?

A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode
B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode
C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode
D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

Answer: A

Explanation:

Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

NEW QUESTION 142
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Reports Reader
User2	Exchange Administrator
User3	User Experience Success Manager

Which users can review the Adoption Score in the Microsoft 365 admin center?

A. User! only
B. User2onry
C. User1 and User2 only
D. User! and User3 only
E. User1, User2. and User3

Answer: E

NEW QUESTION 146
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.
You need to prevent users from copying data from App1 and pasting the data into other apps.
Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Policy to create in Microsoft Endpoint Manager:

- An app configuration policy
- An app protection policy
- A conditional access policy
- A device compliance policy

Minimum number of required policies:

- 1
- 2
- 3
- 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Policy to create in Microsoft Endpoint Manager:

An app configuration policy
An app protection policy
A conditional access policy
A device compliance policy

Minimum number of required policies:

1
2
3
5

NEW QUESTION 149
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

The devices are managed by using Microsoft Intune.
You plan to use a configuration profile to assign the Delivery Optimization settings. Which devices will support the settings?

A. Device1 only
B. Device1 and Device4
C. Device1, Device3, and Device4
D. Device1, Device2, Device3, and Device4

Answer: A

NEW QUESTION 151
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	None

You create an administrative unit named AU1 that contains the members shown in the following exhibit.

AU1

Members   Role assignments

Add users and groups, or select and remove them. The administrators assigned to this unit will manage these users and groups. Adding groups doesn't add users to the unit, it lets the assigned admins manage group settings.

Add users   Add groups   Upload users   ···   Filter   Search this list

	Members	Email address	Last sign-in	Member type
☐	User1	User1@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:25 PM	User
☐	User3	User3@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:27 PM	User

General   **Assigned**   Permissions

You can assign this role to users and groups, and select users and groups to remove or manage them.

Learn more about assigning admin roles

Add users   Add groups

	Admin name	Last sign-in	Scope ⓘ
☐	**Group1**	Unavailable for groups	Organization
☐	**Group2**	Unavailable for groups	AU1

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 reset the password of User3.	○	○
User2 can reset the password of User3.	○	○
User2 can reset the password of User1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	○	☐
User2 can reset the password of User3.	○	☐
User2 can reset the password of User1.	○	☐

NEW QUESTION 153
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You have the devices shown in the following table.

Name	TPM version	Operating system	BIOS/UEFI	BitLocker Drive Encryption (BitLocker)
Device1	TPM 1.2	Windows 10 Pro	BIOS	Enabled
Device2	TPM 2	Windows 10 Home	BIOS	**Not applicable**
Device3	TPM 2	Windows 8.1 Pro	UEFI	Enabled

You plan to join the devices to Azure Active Directory (Azure AD)

What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, of 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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 156
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You onboard all devices to Microsoft Defender for Endpoint
You need to use Defender for Endpoint to block access to a malicious website at www.contoso.com.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

A. Create a web content filtering policy.
B. Configure an enforcement scope.
C. Enable Custom network indicators.
D. Create an indicator.
E. Enable automated investigation.

Answer: AC

NEW QUESTION 160
- (Topic 6)
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.
Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1. Solution: You raise the forest functional level to Windows Server 2016. You copy the Group
Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.
Does this meet the goal?

A. yes
B. No

Answer: B

NEW QUESTION 161
HOTSPOT - (Topic 6)
HOTSPOT
Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.
You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)

Microsoft Azure Active Directory Connect _ ✕

Domain and OU filtering

Directory: fabrikam.com ▾   **Refresh Ou/Domain** ❓

○ Sync all domains and OUs
● Sync selected domains and OUs

▲ ☐ fabrikam.com
  ▷ ☐ Builtin
  ▷ ☐ Computers
  ▷ ☐ Domain Controllers
  ▷ ☐ ForeignSecurityPrincipals
  ▷ ☐ Infrastructure
  ▷ ☐ LostAndFound
  ▷ ☐ Managed Service Accounts
  ▷ ☐ OU1
  ▷ ☑ OU2
  ▷ ☐ Program Data
  ▷ ☐ System
  ▷ ☐ Users

Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
  Connect Directories
  Azure AD sign-in
  Domain/OU Filtering
  Identifying users
  Filtering
  Optional Features
Configure

[Previous] [**Next**]

You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)

Microsoft Azure Active Directory Connect _ ✕

Filter users and devices

For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.

○ Synchronize all users and devices
● Synchronize selected ❓

FOREST   GROUP
fabrikam.com   CN=Group2,OU=OU2,DC=fabrikam,DC=com   [Resolve] ✅

Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
  Connect Directories
  Azure AD sign-in
  Domain/OU Filtering
  Identifying users
  Filtering
  Optional Features
Configure

[Previous] [**Next**]

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
User2 will synchronize to Azure AD.	○	○
Group2 will synchronize to Azure AD.	○	○
User3 will synchronize to Azure AD.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.
User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD.
Box 2: Yes
Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.
Box 3: Yes
User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD.

NEW QUESTION 165
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

Defender for Endpoint has the device groups shown in the following table.

Rank	Name	Matching rule
1	Group1	Tag Contains Inventory And OS in Android
2	Group2	Name Starts with Device And Tag Contains Inventory
Last	Ungrouped devices (default)	Not applicable

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@contoso.com

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 a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	○
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	○
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.
Box 2: No
Computer1 does not belong to either Group1 or Group2
Box 3: Yes
Device3 belongs to both Group1 and Group2.
Note: Understanding alert severity
Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.
The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

NEW QUESTION 168
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.
All the devices in your organization are onboarded to Microsoft Defender for Endpoint.
You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.
What should you do?

A. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
B. From Alerts queue, create a suppression rule and assign an alert.
C. From Advanced hunting, create a query and a detection rule.
D. From the Microsoft Purview compliance portal, create an audit log search.

Answer: C

NEW QUESTION 171
- (Topic 6)
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 an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

NEW QUESTION 172
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert
occurs only on a Windows 10 device. The solution must minimize administrative effort. What should you do first?

A. From the Microsoft 365 admin center, create a mail-enabled security group.
B. From the Microsoft 365 Defender portal, create a device group.
C. From the Microsoft Endpoint Manager admin center, create a device category.
D. From the Azure Active Directory admin center, create a dynamic device group.

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide

NEW QUESTION 176
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations: Name: Policy1
Assignments:
- Users and groups: Group1

- Cloud aps or actions: All cloud apps
? Access controls:
? Grant, require multi-factor authentication
? Enable policy: Report-only
You set Enabled Security defaults to Yes for the tenant.
For each of the following settings select Yes, if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:
? Conditional Access policies can be enabled in report-only mode.
? During sign-in, policies in report-only mode are evaluated but not enforced.
? Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
? Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

NEW QUESTION 181
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:
? MDM user scope: Some
? uk.co.certification.simulator.questionpool.PList@184e72e0
? MAM user scope: Some
? uk.co.certification.simulator.questionpool.PList@184e7360 You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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 enroll Device1 in Intune by using automatic enrollment	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	⊙	○
User1 can enroll Device2 in Intune by using automatic enrollment	⊙	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	⊙

NEW QUESTION 186
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You need to meet the following requirements:
• Report a Microsoft 365 service issue.
• Request help on how to add a new user to an Azure AD tenant.
What should you use in the Microsoft 365 admin center? 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

Message center
New service request
Product feedback
Service health

Answer Area

To report issues regarding a Microsoft 365 service: _____

To request help on how to add a new user to the tenant: _____

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Features

Message center
New service request
Product feedback
Service health

Answer Area

To report issues regarding a Microsoft 365 service: | New service request |

To request help on how to add a new user to the tenant: | Message center |

NEW QUESTION 187
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Role
User1	Group1	User Administrator
User2	Group1	None
User3	Group2	None
User4	None	Global Administrator

You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.
Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.
NOTE; Each correct selection is worth one point.

Answer Area

Users that can use SSPR:	User1, User2, and User4 only ▼
	User1 and User2 only
	User1, User2, and User3 only
	User1, User2, and User4 only
	User1, User2, User3, and User4
Users that must answer security questions to reset their password:	User1 and User2 only ▼
	User1 only
	User2 only
	User1 and User2 only
	User1, User2, and User3 only
	User1, User2, and User4 only
	User1, User2, User3, and User4

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Users that can use SSPR:	User1, User2, and User4 only ▼
	User1 and User2 only
	User1, User2, and User3 only
	User1, User2, and User4 only
	User1, User2, User3, and User4
Users that must answer security questions to reset their password:	User1 and User2 only ▼
	User1 only
	User2 only
	User1 and User2 only
	User1, User2, and User3 only
	User1, User2, and User4 only
	User1, User2, User3, and User4

NEW QUESTION 191
HOTSPOT - (Topic 6)
You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.
You need to centrally monitor System log events from the computers.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

In Azure:	▼
	Add and configure the Diagnostics settings for the Azure Activity Log.
	Add and configure an Azure Log Analytics workspace.
	Add an Azure Storage account and Azure Cognitive Search
	Add an Azure Storage account and a file share.
On the computers:	▼
	Create an event subscription.
	Modify the membership of the Event Log Readers group.
	Enroll in Microsoft Endpoint Manager.
	Install the Microsoft Monitoring Agent.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

In Azure: ▼

Add and configure the Diagnostics settings for the Azure Activity Log.
Add and configure an Azure Log Analytics workspace.
Add an Azure Storage account and Azure Cognitive Search
Add an Azure Storage account and a file share.

On the computers: ▼

Create an event subscription.
Modify the membership of the Event Log Readers group.
Enroll in Microsoft Endpoint Manager.
Install the Microsoft Monitoring Agent.

NEW QUESTION 193
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.
You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard.
ASR2 will be used to configure Microsoft Defender SmartScreen.
Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

ASR1: ▼

Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

ASR2: ▼

Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

A. Mastered
B. Not Mastered

Answer: A

Explanation:

ASR1: ▼

Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

ASR2: ▼

Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

NEW QUESTION 196
- (Topic 6)
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.
Where can you store data from the LinkedIn connector?

A. a Microsoft OneDrive for Business folder
B. a Microsoft SharePoint Online document library
C. a Microsoft 365 mailbox
D. Azure Files

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin- data?view=o365-worldwide

NEW QUESTION 198
- (Topic 6)
You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Exchange Administrator
User2	User Administrator
User3	Global Administrator
User4	None

You add another user named User5 to the User Administrator role. You need to identify which two management tasks User5 can perform.
Which two tasks should you identify? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Delete User2 and User4 only.
B. Reset the password of User4 only
C. Reset the password of any user in Azure AD.
D. Delete User1, User2, and User4 only.
E. Reset the password of User2 and User4 only.
F. Delete any user in Azure AD.

Answer: AE

Explanation:
Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).
Only on users who are non-admins or in any of the following limited admin roles:
• Directory Readers
• Guest Inviter
• Helpdesk Administrator
• Message Center Reader
• Reports Reader
• User Administrator Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#available-roles

NEW QUESTION 199
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 security center. Which Microsoft service source will appear on the Incidents page of the Microsoft 365
security center?

A. Microsoft Cloud App Security
B. Azure Sentinel
C. Azure Web Application Firewall
D. Azure Defender

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate- alerts?view=o365-worldwide

NEW QUESTION 203
HOTSPOT - (Topic 6)
HOTSPOT

			progress	actions	actions			
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	O	O
The SP800 assessment score will increase by 54 points.	O	O
The Data Protection Baseline score will increase by 9 points.	O	O

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	O	☑
The SP800 assessment score will increase by 54 points.	O	☑
The Data Protection Baseline score will increase by 9 points.	O	☑

NEW QUESTION 204
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 tenant
You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM)
The device type restriction are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

The device limit restriction are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

Answer Area

Device limit:
5
10
15

Allowed platform
Android only
iOS only
All platforms

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restriction-priority
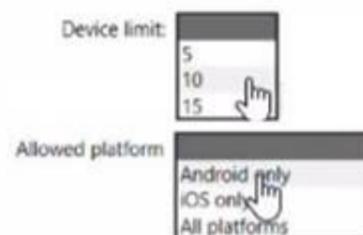
NEW QUESTION 208
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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.
Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the filtering settings.
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 211
DRAG DROP - (Topic 6)
You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.
All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.
You plan to implement self-service password reset (SSPR).
You need to ensure that when a user resets or changes a password, the password syncs with AD DS.
Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action 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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 215
- (Topic 6)
You have a Microsoft 365 E5 subscription. You need to create a mail-enabled contact. Which portal should you use?

A. the Microsoft 365 admin center
B. the SharePoint admin center
C. the Microsoft Entra admin center
D. the Microsoft Purview compliance portal

Answer: A

NEW QUESTION 216
- (Topic 6)
You have a Microsoft 365 subscription.
You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.
What is the maximum number of onmicrosoft.com domains the subscription can contain?

A. 1
B. 2
C. 5
D. 10

Answer: C

Explanation:
You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to

create a new one.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq

NEW QUESTION 217
- (Topic 6)
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 222
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription.
Your network uses an IP address space of 51.40.15.0/24.
An Exchange Online administrator recently created a role named Role1 from a computer on the network.
You need to identify the name of the administrator by using an audit log search.
For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Activities to search for:
- Exchange mailbox activities
- Site administration activities
- Show results for all activities
- Role administration activities

Field to filter by:
- Item
- User
- Detail
- IP address

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Activities to search for:
- Exchange mailbox activities
- Site administration activities
- **Show results for all activities**
- Role administration activities

Field to filter by:
- Item
- User
- **Detail**
- IP address

NEW QUESTION 227
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

You need to enable user access to the partner company's portal. Which Microsoft Defender for Endpoint setting should you modify?

A. Alert notifications
B. Alert suppression
C. Custom detections
D. Advanced hunting
E. Indicators

Answer: E

Explanation:
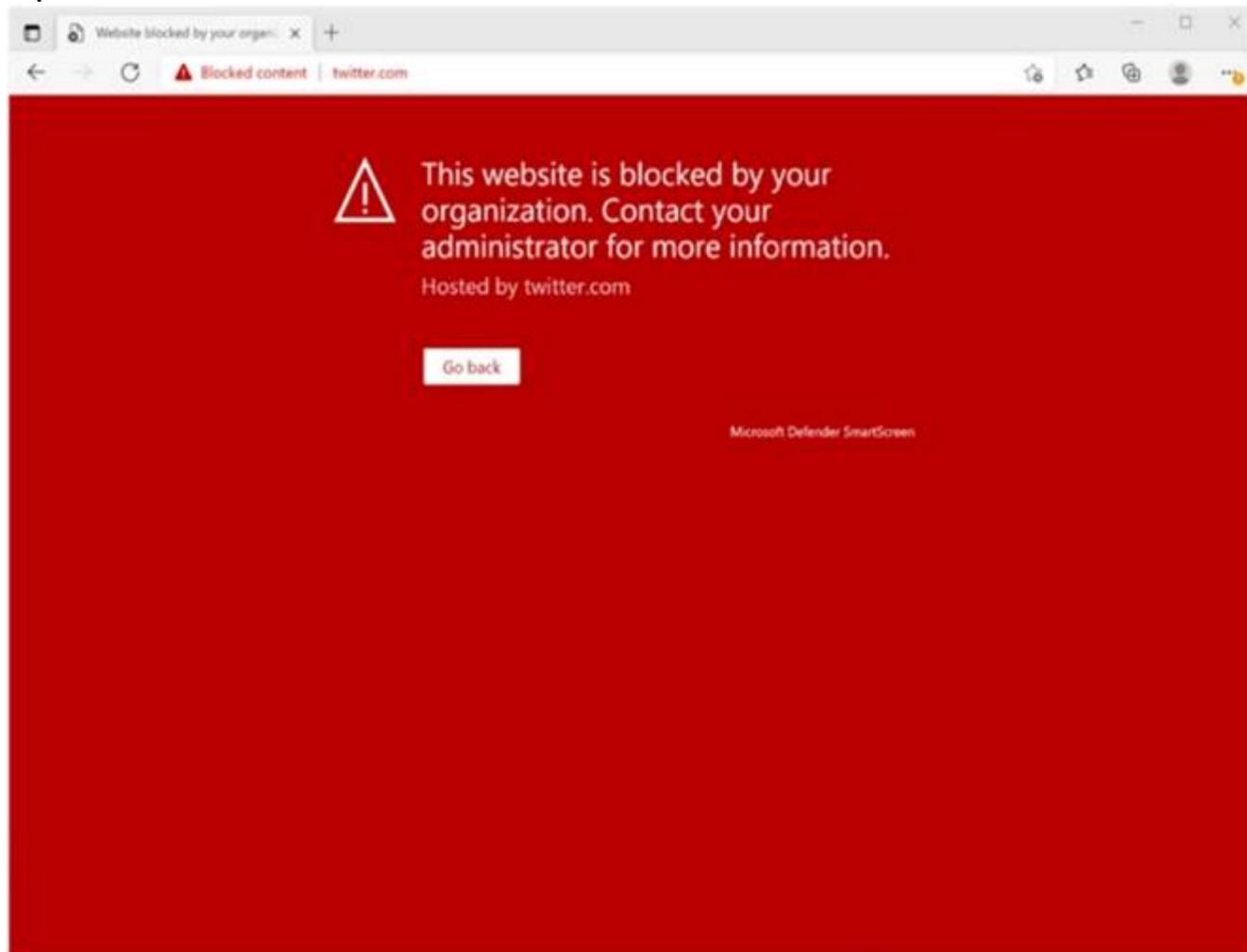
This Website Is Blocked By Your Organization
Custom indicators will block malicious IPs, URLs, and domains. Then, they will display the above message for the user.
Reference: https://jadexstrategic.com/web-protection/

NEW QUESTION 230
- (Topic 6)
You have a Microsoft 365 subscription.
You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Global Administrator
User3	Service Support Administrator

You configure Tenant properties as shown in the following exhibit.

Technical contact

| User1@contoso.com | ✓ |

Global privacy contact

| | ✓ |

Privacy statement URL

| http://contoso.com/privacy | ✓ |

Which users will be contacted by Microsoft if the tenant experiences a data breach?

A. Used only
B. User2 only
C. User3 only
D. Used and User2 only
E. User2 and User3 only

Answer: B

Explanation:
Microsoft 365 is committed to notifying customers within 72 hours of breach declaration.
The customer's tenant administrator will be notified.
Reference:
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365

NEW QUESTION 235
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Passwordless authentication	Multi-factor authentication (MFA) method registered
User1	Not configured	Microsoft Authenticator app (push notification)
User2	Configured	Microsoft Authenticator app (push notification)
User3	Not configured	Mobile phone
User4	Not configured	Email

You plan to create a Conditional Access policy that will use GPS-based named locations. Which users can the policy protect?

A. User2 and User4 only
B. User1 and User3 only
C. Userl1 only
D. User1, User2. User3. and User4

Answer: C

NEW QUESTION 236
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Operating system	Microsoft Intune
Device1	Windows 11 Enterprise	Enrolled
Device2	iOS	Enrolled
Device3	Android	Not enrolled

You install Microsoft Word on all the devices.
You plan to configure policies to meet the following requirements:
• Word files created by using Windows devices must be encrypted automatically.
• If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
• For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.
Which type of polio/ should you configure for each device? To answer, drag the appropriate policy types to the correct devices. 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

App configuration policy

App protection policy

Compliance policy

Conditional Access policy

Answer Area

Device1: [   ]

Device2: [   ]

Device3: [   ]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Policy Types		Answer Area		
App configuration policy			Device1:	App protection policy
App protection policy			Device2:	Conditional Access policy
Compliance policy			Device3:	Compliance policy
Conditional Access policy				

NEW QUESTION 238
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Conditional Access is configured to block high-risk sign-ins for all users.
All users are in France and are registered for multi-factor authentication (MFA). Users in the media department will travel to various countries during the next month.
You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention.
What should you configure?

A. an exclusion group
B. the MFA registration policy
C. named locations
D. self-service password reset (SSPR)

Answer: D

Explanation:
Self-remediation with self-service password reset
If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock

NEW QUESTION 242
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.
You need to deploy the policy. What should you do first?

A. Review the sensitive information in Activity explorer
B. Turn on the policy
C. Run the policy in simulation mode
D. Configure Azure Information Protection analytics

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

NEW QUESTION 247
- (Topic 6)
You have Windows 10 devices that are managed by using Microsoft Endpoint Manager. You need to configure the security settings in Microsoft Edge.
What should you create in Microsoft Endpoint Manager?

A. an app configuration policy
B. an app
C. a device configuration profile
D. a device compliance policy

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

NEW QUESTION 250
- (Topic 6)
You have a Microsoft 365 subscription that uses Security & Compliance retention policies.
You implement a preservation lock on a retention policy that is assigned to all executive users.
Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point?

A. Add locations to the policy
B. Reduce the duration of policy
C. Remove locations from the policy
D. Extend the duration of the policy
E. Disable the policy

Answer: AB

NEW QUESTION 253
- (Topic 6)
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.
Your network contains an Active Directory forest. You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
• Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
• User passwords must be 10 characters or more.
Solution: implement password hash synchronization and configure password protection in the Azure AD tenant.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 256
HOTSPOT - (Topic 6)
You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

If User1 creates a team in Microsoft Teams, the event is [answer choice].

| not retained |
| retained for 90 days |
| retained for six months |
| retained for one year |

If User2 adds a channel in Microsoft Teams, the event is [answer choice].

| not retained |
| retained for 90 days |
| retained for six months |
| retained for one year |

NEW QUESTION 258
DRAG DROP - (Topic 6)
Your company purchases a cloud app named App1.
You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls.
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

- Deploy Azure Active Directory (Azure AD) Application Proxy.
- From the Cloud App Security admin center, add an app connector.
- Sign in to App1.
- Create a conditional access policy.
- From the Azure Active Directory admin center, configure the Diagnostic settings.
- From the Azure Active Directory admin center, add an app registration for App1.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

- Deploy Azure Active Directory (Azure AD) Application Proxy.
- From the Cloud App Security admin center, add an app connector.
- Sign in to App1.
- Create a conditional access policy.
- From the Azure Active Directory admin center, configure the Diagnostic settings.
- From the Azure Active Directory admin center, add an app registration for App1.

Answer Area

1. From the Cloud App Security admin center, add an app connector.
2. Create a conditional access policy.
3. Sign in to App1.

NEW QUESTION 259
- (Topic 6)
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.
Your network contains an Active Directory forest. You deploy Microsoft 365.

You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
• Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
• User passwords must be 10 characters or more.
Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 263
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.
Which two policies can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. a data loss prevention (DLP) policy
B. a sensitivity label policy
C. a Microsoft Cloud App Security file policy
D. a communication compliance policy
E. a retention label policy

Answer: AD

NEW QUESTION 265
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:
? Scope type: Directory
? Selected members: Group1
? Assignment type: Active
? Assignment starts: Mar 15, 2023
? Assignment ends: Aug 15, 2023
You add the following assignment for the Exchange Administrator role:
? Scope type: Directory
? Selected members: Group2
? Assignment type: Eligible
? Assignment starts: Jun 15, 2023
? Assignment ends: Oct 15, 2023
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 July 15, 2023, Admin1 can reset the password of a user.	◉	○
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	○	◉
On May 1, 2023, Admin3 can reset the password of a user.	○	◉

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
Admin1 is member of Group1.
The User Administrator role assignment has Group1 as a member. The assignment type: Active
July 15, 2023 is with the assignment period.
A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.
Box 2: No
Admin2 is member of Group2.
The Exchange Administrator role assignment has Group2 as a member. The assignment type: Eligible
June 20, 2023 is with the assignment period. The assignment must be approved.

Note: Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.
Box 3: Yes
Admin3 is member of Gropu1 and Group2.
The User Administrator role assignment has Group1 as a member. The assignment type: Active
May 1, 2023 is with the assignment period.

NEW QUESTION 269
DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Type	Number of devices	Operating system	Enrollment status
Corporate	150	Windows 11	Azure AD-joined, Microsoft Intune-managed
Bring your own device (BYOD)	25	Windows 11	Unmanaged

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must minimize administrative effort.
What should you use to onboard each type of device? To answer, drag the appropriate onboarding methods to the correct device types. Each onboarding 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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 271
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.
What should you use to onboard each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Device1: | Microsoft Endpoint Manager | ▼ |
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Device2: | A local script | ▼ |
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Device1: | Microsoft Endpoint Manager | ▼ |
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Device2: | A local script | ▼ |
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

NEW QUESTION 276
- (Topic 6)
You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels   Label policies   Auto-labeling (preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

+ Create a label   📺 Publish labels   ↻ Refresh

Name ↑		Order	Created by	Last modified
Label1	...	0 - highest	Prvi	04/24/2020
— Label2	...	1	Prvi	04/24/2020
Label3	...	0 - highest	Prvi	04/24/2020
Label4	...	0 - highest	Prvi	04/24/2020
— Label5	...	5	Prvi	04/24/2020
Label6		0 - highest	Prvi	04/24/2020

Which labels can users apply to content?

A. Label1, Label2, and Label5 only
B. Label3. Label4, and Label6 only
C. Label1, Label3, Labe2, and Label6 only
D. Label1, Label2, Label3, Label4, Label5. and Label6

Answer: C

NEW QUESTION 278
HOTSPOT - (Topic 6)
HOTSPOT
Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Device group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped devices (default)	*Not applicable*

You onboard a computer named computer1 to Microsoft Defender for Endpoint as shown in the following exhibit.

Settings > Endpoints > computer1

computer1

Device summary

Risk level ⓘ
▬▬▬ None

Device details

Domain
adatum.com

OS
Windows 10 64-bit
Version 21H2
Build 19044.2130

Use the drop-down menus to select the answer choice that completes each statement.
NOTE: Each correct selection is worth one point.

Answer Area

Computer1 will be a member of **[answer choice]**.

| Group3 only |
| Group4 only |
| Group3 and Group4 only |
| Ungrouped devices |

If you add the tag demo to Computer1, the computer will be a member of **[answer choice]**.

| Group1 only |
| Group1 and Group2 only |
| Group1, Group2, Group3, and Group4 |
| Ungrouped devices |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Group3 and Group4 only Computer1 has no Demo Tag.
Computer1 is in the adatum domain and OS is Windows 10. Box 2: Group1, Group2, Group3 and Group4

NEW QUESTION 279
- (Topic 6)
You have the sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels   Label policies   Auto-labeling(preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

+ Create a label   ⬚ Publish labels   ⟳ Refresh

Name ↑		Order	Created by	Last modified
Label1	...	0-highest	Prvi	04/24/2020
— **Label2**	...	1	Prvi	04/24/2020
Label3	...	0-highest	Prvi	04/24/2020
Label4	...	0-highest	Prvi	04/24/2020
— **Label5**	...	5	Prvi	04/24/2020
Label6		0-highest	Prvi	04/24/2020

Which labels can users apply to content?

A. Label3, Label4, and Label6 only
B. Label1, Label2. Label3. Label4. Label5. and Label6
C. Label1, Label2, and Label5 only
D. Label1, Label3, Label4, and Label6 only

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

NEW QUESTION 282
- (Topic 6)
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 computer that runs Windows 10.
You need to verify which version of Windows 10 is installed. Solution: From Device Manager, you view the computer properties. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

NEW QUESTION 286
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.
You need to configure Defender for Endpoint to meet the following requirements:
? Block a vulnerable app until the app is updated.
? Block an application executable based on a file hash.
The solution must minimize administrative effort.
What should you configure for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Block a vulnerable app until the app is updated:
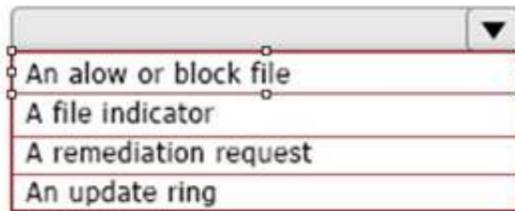
An alow or block file
A file indicator
A remediation request
An update ring

Block an application executable based on a file hash:

An alow or block file
A file indicator
A remediation request
An update ring

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: A remediation request
Block a vulnerable app until the app is updated.
Block vulnerable applications
How to block vulnerable applications
? Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.
? Select a security recommendation to see a flyout with more information.
? Select Request remediation.
? Select whether you want to apply the remediation and mitigation to all device groups or only a few.
? Select the remediation options on the Remediation request page. The remediation options are software update, software uninstall, and attention required.
? Pick a Remediation due date and select Next.
? Under Mitigation action, select Block or Warn. Once you submit a mitigation action, it is immediately applied.
? Review the selections you made and Submit request. On the final page you can
choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.
Box 2: A file indicator
Block an application executable based on a file hash.
While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.
The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

NEW QUESTION 287
- (Topic 6)
You have a Microsoft 365 subscription.
You need to receive a notification each time a user in the service desk department grants Full Access permissions for a user mailbox.
What should you configure?

A. a data loss prevention (DLP) policy
B. an alert policy
C. an audit search
D. an insider risk management policy

Answer: B

NEW QUESTION 288
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected.
What should you use to create the policy?

A. the Microsoft 365 admin center
B. the Microsoft Purview compliance portal
C. the Microsoft Defender for Cloud Apps portal
D. the Microsoft Apps admin center

Answer: C

NEW QUESTION 291
HOTSPOT - (Topic 6)
Your company uses Microsoft Defender for Endpoint.
The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

The alerts visible in the Microsoft Defender for Endpoint alerts queue are shown in the following table.

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:
• Triggering IOC: Any IOC
• Action: Hide alert
• Suppression scope: Alerts on ATP1 device 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

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	○	○
After you create the suppression rule, Alert3 is visible in the alerts queue.	○	○
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	⊡	○
After you create the suppression rule, Alert3 is visible in the alerts queue.	⊡	○
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	○	⊡

NEW QUESTION 295
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.
From Azure AD Identity Protection, you enable a sign-in risk policy.
Users report that when they use the VDI solution, they are regularly blocked when they attempt to access Microsoft 365.
What should you configure?

A. the Tenant restrictions settings in Azure AD
B. a trusted location
C. a Conditional Access policy exclusion
D. the Microsoft 365 network connectivity settings

Answer: B

Explanation:
There are two types of risk policies in Azure Active Directory (Azure AD) Conditional Access you can set up to automate the response to risks and allow users to self-remediate when risk is detected:
Sign-in risk policy User risk policy
Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity- protection-configure-risk-policies
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location- condition

NEW QUESTION 298
- (Topic 6)
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 an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp

NEW QUESTION 301
FILL IN THE BLANK - (Topic 6)
You have a Microsoft 365 tenant.
You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Save the audit logs to: [▼]

Azure Active Directory admin center blade to use to view the saved audit logs: [▼]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Save the audit logs to: [Azure Log Analytics ▼]

Azure Active Directory admin center blade to use to view the saved audit logs: [Audit logs ▼]

NEW QUESTION 305
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to configure Microsoft Defender for Office 365 to meet the following requirements:
• A user's email sending patterns must be used to minimize false positives for spoof protection.
• Documents uploaded to Microsoft Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365.
What should you configure for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection: [Domains to protect ▼]
- Domains to protect
- Mailbox intelligence
- Users to protect

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365: [Global settings for safe attachments ▼]
- Global settings for safe attachments
- The Safe Attachments policy settings
- The Safe Links policy settings

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection: [Domains to protect ▼]
- Domains to protect
- Mailbox intelligence
- Users to protect

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365: [Global settings for safe attachments ▼]
- Global settings for safe attachments
- The Safe Attachments policy settings
- The Safe Links policy settings

NEW QUESTION 306
- (Topic 6)
You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Source	Last sign in
User1	Azure AD	Yesterday
User2	Active Directory Domain Services (AD DS)	Two days ago
User3	Active Directory Domain Services (AD DS)	Never

Azure AD Connect has the following settings:
? Password Hash Sync: Enabled
? Pass-through authentication: Enabled
You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.
Which users should you identify?

A. none
B. Used only1
C. User1 and User2 only
D. User1. User2, and User3

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn¨

NEW QUESTION 308
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You need to ensure that when a document containing a credit card number is added to the tenant, the document is encrypted.
Which policy should you use?

A. a retention policy
B. a retention label policy
C. an auto-labeling policy
D. an insider risk policy

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

NEW QUESTION 312
- (Topic 6)
Your company has a Microsoft E5 tenant.
The company must meet the requirements of the ISO/IEC 27001:2013 standard. You need to assess the company's current state of compliance.
What should you use?

A. eDiscovery
B. Information governance
C. Compliance Manager
D. Data Subject Requests (DSRs)

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

NEW QUESTION 313
- (Topic 6)
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.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

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	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
This is not a permissions issue so you do not need to assign the Security Reader role. The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

NEW QUESTION 315
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:
? Show app and profile configuration progress: Yes
? Allow users to collect logs about installation errors: Yes
? Only show page to devices provisioned by out-of-box experience (OOBE): No
? Assignments: Group2
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	[○]
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	[○]	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	[○]

NEW QUESTION 317
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 subscription.
In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:
? Block emails that contain financial data.
? Display the following policy tip text: Message blocked.
From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:
? Use the following location: Exchange email.
? Display the following policy tip text: Message contains sensitive data.
? When a user sends an email, notify the user if the email contains health records.
What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result 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.

Results

The email will be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and the user will receive the policy tip: Message blocked.

The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records: Result

When the user sends an email that contains only financial data: Result

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked. If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.
Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

NEW QUESTION 322
- (Topic 6)
Your on-premises network contains an Active Directory domain.
You have a Microsoft 365 subscription.
You need to sync the domain with the subscription. The solution must meet the following requirements:

On-premises Active Directory password complexity policies must be enforced. Users must be able to use self-service password reset (SSPR) in Azure AD. What should you use?

A. password hash synchronization
B. Azure AD Identity Protection
C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
D. pass-through authentication

Answer: D

Explanation:
Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.
This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations
wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.
Note: Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time by using either Azure AD Connect or Azure AD Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.
Password writeback is supported in environments that use the following hybrid identity models:
Password hash synchronization Pass-through authentication
Active Directory Federation Services
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback

NEW QUESTION 324
- (Topic 6)
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 computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select Update & Security to view the update history. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 329
HOTSPOT - (Topic 6)
You have several devices enrolled in Microsoft Endpoint Manager.
You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

The device type restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	○
User2 can enroll Android devices in Endpoint Manager.	○	○
User3 can enroll iOS devices in Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	☐○
User2 can enroll Android devices in Endpoint Manager.	○	☐○
User3 can enroll iOS devices in Endpoint Manager.	☐○	○

NEW QUESTION 332
- (Topic 6)
You have a Microsoft 365 tenant.
Company policy requires that all Windows 10 devices meet the following minimum requirements:
? Require complex passwords.
? Require the encryption of data storage devices.
? Have Microsoft Defender Antivirus real-time protection enabled.
You need to prevent devices that do not meet the requirements from accessing resources in the tenant.
Which two components should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a configuration policy
B. a compliance policy
C. a security baseline profile
D. a conditional access policy
E. a configuration profile

Answer: BD

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION 333
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.

Group1

G

Private group   ● 1 owner   ● 1 member

🗑

General   Members   **Settings**   Microsoft Teams

General settings

☐ Allow external senders to email this group

☑ Send copies of group conversations and events to group members

☐ Hide from my organization's global address list

Privacy

◉ Private

○ Public

An external user named User1 has an email address of user1@outlook.com. You need to add User1 to Group1.
What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Action: ▼

- Add User1 to the subscription as an active user.
- For Group1, change the Privacy setting to Public.
- For Group1, select Allow external senders to email this group.
- Invite User1 to collaborate with your organization as a guest.

Portal: ▼

- The Microsoft Entra admin center
- The Exchange admin center
- The Microsoft 365 admin center
- The Microsoft Purview compliance portal

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Invite User1 to collaborate with your organization as a guest.
To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.
Navigate with your Web browser to https://admin.microsoft.com. On the left pane, click on "Users", then click "Guest Users".
On the "Guest Users" page, to create a new guest user, click on either the "Add a guest user" link on the top of the page or click on "Go to Azure Active Directory to add guest users" link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at https://aad.portal.azure.com.
On the "New user" page in the Microsoft Azure portal, you must choose to either "Create user" or "Invite user". If you choose the "Create user" option, this will create a new user in your organization, which will have a login address with format username@tenantdomain,dot,com. If you choose the "Invite user" option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the "Invite user" option.
Box 2: The Microsoft Entra admin center
Microsoft Entra admin center unites Azure AD with family of identity and access products
Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.
Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).

NEW QUESTION 336
- (Topic 6)
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.
Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The question states that "all the user account synchronizations completed successfully". Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync- configure-filtering

NEW QUESTION 340
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Office 365 role group
User1	None	Compliance Data Administrator
User2	Global Administrator	None

You create a retention label named Label 1 that has the following configurations:
• Retains content for five years
• Automatically deletes all content that is older than five years
You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:
• Applies to content that contains the word Merger
• Specifies the OneDrive accounts and SharePoint sites locations You run the following command.
Set-RetentionConpliancePolicy Policy1 -RestrictiveRetention Strue -Force
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 add Exchange email as a location to Policy1.	○	○
User2 can remove SharePoint sites from Policy1.	○	○
User2 can add the word Acquisition to Policy1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	○	○
User2 can remove SharePoint sites from Policy1.	○	○
User2 can add the word Acquisition to Policy1.	○	○

NEW QUESTION 341
HOTSPOT - (Topic 6)
Your network contains an Active Directory domain and an Azure AD tenant.
You implement directory synchronization for all 10.000 users in the organization. You automate the creation of 100 new user accounts.
You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.
Which command should you run? To answer, select the appropriate options in the answer area.

Answer Area

Start-ADSyncSyncCycle ▼	-PolicyType	Delta ▼
Start-ADSyncSyncCycle		Delta
Set-ADSyncScheduler		Initial
Invoke-ADSyncRunProfile		Full

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Start-ADSyncSyncCycle ▼	-PolicyType	Delta ▼
Start-ADSyncSyncCycle		Delta
Set-ADSyncScheduler		Initial
Invoke-ADSyncRunProfile		Full

NEW QUESTION 345
- (Topic 6)
You have a Microsoft 365 subscription.
Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers
followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de- fghij.
You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.
D18912E1457D5D1DDCBD40AB3BF70D5D

What should you create to ensure that the DLP policy can detect the customer IDs?

A. a sensitive information type
B. a sensitivity label
C. a supervision policy
D. a retention label

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide

NEW QUESTION 349
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview policies to meet the following requirements: Identify documents that are stored in Microsoft Teams and SharePoint that contain
Personally Identifiable Information (PII). Report on shared documents that contain PII. What should you create?

A. a data loss prevention (DLP) policy
B. a retention policy
C. an alert policy
D. a Microsoft Defender for Cloud Apps policy

Answer: A

Explanation:
Demonstrate data protection
Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.
There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.
In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.
? From the Security & Compliance tab of your browser, click Home.
? Click Data loss prevention > Policy.
? Click + Create a policy.
? In Start with a template or create a custom policy, click Custom > Custom policy > Next.
? In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b. Description: Protect the personally identifiable information of European citizens
? Etc.
Reference:
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-test-environment

NEW QUESTION 352
HOTSPOT - (Topic 6)
Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD) Password hash synchronization is disabled.
You plan to implement co-management.
You need to configure Azure AD Connect and the domain to support co-management. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
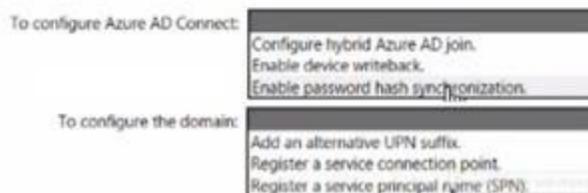
A. Mastered
B. Not Mastered

Answer: A

Explanation:
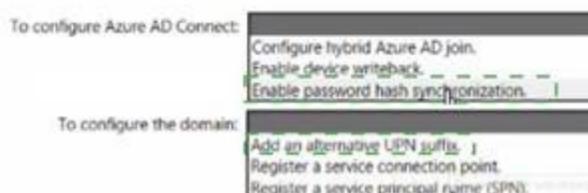
NEW QUESTION 354
- (Topic 6)

You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that Used can place a hold on all mailbox content. What permission should you assign to User1?

A. the Information Protection administrator ide from the Azure Active Directory admin center.
B. the eDiscovery Manager tote from the Microsoft 365 compliance center.
C. the Compliance Management role from the Exchange admin center.
D. the User management administrator role from the Microsoft 365 admin center.

Answer: B

NEW QUESTION 355
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to create a policy that will generate an email alert when a banned app is detected requesting permission to access user information or data in the subscription.
What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
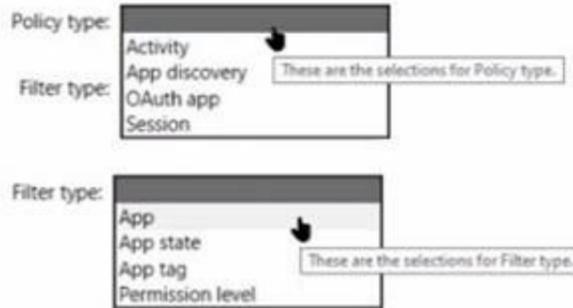
A. Mastered
B. Not Mastered

Answer: A

Explanation:
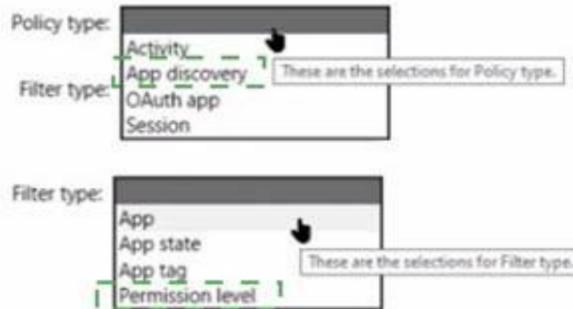
NEW QUESTION 358
HOTSPOT - (Topic 6)
You work at a company named Contoso, Ltd.
Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.
Contoso purchases a company named Fabrikam, Inc.
Contoso plans to add the following domains to the Microsoft 365 subscription:
• fabrikam.com
• east.fabrikam.com
• west.contoso.com
You need to ensure that the devices in the new domains can register by using Autodiscover.
How many domains should you verify, and what is the minimum number of enterprise registration DNS records you should add? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 362
- (Topic 6)
You have a Microsoft 365 subscription.
You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.
Which type of group should you use to assign the Reports Reader role and to access App1?

A. a Microsoft 365 group that has assigned membership
B. a Microsoft 365 group that has dynamic user membership
C. a security group that has assigned membership
D. a security group that has dynamic user membership

Answer: C

Explanation:
To grant permissions to assignees to manage users and group access for a specific enterprise app, go to that app in Azure AD and open in the Roles and Administrators list for
that app. Select the new custom role and complete the user or group assignment. The assignees can manage users and group access only for the specific app.
Note: You can add the following types of groups:
Assigned groups - Manually add users or devices into a static group.
Dynamic groups (Requires Azure AD Premium) - Automatically add users or devices to user groups or device groups based on an expression you create.
Note:
Security groups
Security groups are used for granting access to Microsoft 365 resources, such as SharePoint. They can make administration easier because you need only administer the group rather than adding users to each resource individually.
Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.
Security groups can be configured for dynamic membership in Azure Active Directory, allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device attributes such as operating system version.
Security groups can be added to a team.
Microsoft 365 Groups can't be members of security groups. Microsoft 365 Groups
Microsoft 365 Groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 Group, members get a group email and shared workspace for conversations, files, and calendar events, Stream, and a Planner.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups? https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy

NEW QUESTION 365
- (Topic 6)
You purchase a new computer that has Windows 10, version 21H1 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

A. Install all the feature updates released since version 21H1 and the latest quality update only.
B. Install the latest feature update and all the quality updates released since version 21H1.
C. Install the latest feature update and the latest quality update only.
D. Install all the feature updates released since version 21H1 and all the quality updates released since version 21H1 only.

Answer: C

NEW QUESTION 366
- (Topic 6)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.
The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	**None**	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User3 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 367
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You need to review reports to identify the following:
• The storage usage of files stored in Microsoft Teams
• The number of active users per team
Which report should you review for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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

Report		Requirements	
The device usage report in Teams		The storage usage of files stored in Microsoft Teams:	
The OneDrive usage report		Number of active users per Microsoft Team:	
The SharePoint site usage report			
The Teams usage report in Teams			
The User activity report in Teams			

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Report		Requirements	
The device usage report in Teams		The storage usage of files stored in Microsoft Teams:	The SharePoint site usage report
The OneDrive usage report		Number of active users per Microsoft Team:	The Teams usage report in Teams
The SharePoint site usage report			
The Teams usage report in Teams			
The User activity report in Teams			

NEW QUESTION 371
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

MS-102 Practice Exam Features:

* MS-102 Questions and Answers Updated Frequently

* MS-102 Practice Questions Verified by Expert Senior Certified Staff

* MS-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* MS-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The MS-102 Practice Test Here