DUMPSBOSS.

Microsoft 365 Administrator Exam

Microsoft MS-102

Version Demo

Total Demo Questions: 75

Total Premium Questions: 927

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Configure Microsoft 365 tenant and subscription management	117
Topic 2, Manage users, groups, and licenses	220
Topic 3, Manage security and compliance by using Microsoft Defender XDR and Microsoft Purview	442
Topic 4, Manage Microsoft 365 applications	135
Topic 5, Mix Questions	13
Total	927

QUESTION NO: 1

Which feature in Microsoft Defender for Endpoint provides full visibility of endpoints across the network?

A. Firewall management

B. Intrusion Detection System (IDS)

C. Network traffic analysis (NTA)

D. Endpoint Detection and Response (EDR)

ANSWER: D

Explanation:

Endpoint Detection and Response (EDR) provides the endpoint-level visibility needed to monitor, investigate, and respond to suspicious activity across an organization's managed device estate. Microsoft Defender for Endpoint continuously gathers endpoint telemetry, including information about processes, files, registry activity, network connections, users, and device events. That telemetry is analyzed to identify malicious or suspicious behaviors and is surfaced through alerts, incidents, device timelines, evidence, and investigation views in the Microsoft Defender portal.

This visibility is especially valuable when security teams need to understand the scope and progression of an attack. Analysts can review the activity history of an affected device, explore related entities and alerts, identify potentially impacted devices, and take response actions such as isolating a device or collecting an investigation package. EDR therefore goes beyond basic prevention by delivering the detection and investigative context required for endpoint security operations at scale. Microsoft describes Defender for Endpoint EDR as helping organizations detect, investigate, and respond to advanced threats that have bypassed preventive security controls. See Endpoint detection and response overview and Microsoft Defender for Endpoint overview.

QUESTION NO: 2

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, User2, User3, and User4

C. User1 only

D. User1 and User3 only

ANSWER: C

Explanation:

User1 only is correct. GPS-based named locations are evaluated through the location signal reported by the Microsoft Authenticator app during a supported authentication flow. Microsoft Entra Conditional Access can use GPS coordinates to determine whether a user is within or outside a configured country/region named location, but this capability depends on the user being able to supply GPS information from Microsoft Authenticator on a supported mobile device. The user must also

grant the app the required location permission; otherwise, Entra ID cannot obtain the GPS signal needed to evaluate the named-location condition. Based on the user and device details in the table, only User1 meets the prerequisites for GPS-based location evaluation. A Conditional Access policy using this named-location method can therefore protect User1. This control is particularly useful when an organization needs a stronger location indicator than IP address geolocation, which can be inaccurate or affected by VPNs and mobile networks. Microsoft documents the GPS-coordinate option as part of country/region named locations and describes the Microsoft Authenticator requirements for location-based Conditional Access evaluation. See Conditional Access network and location conditions and Use the location condition in Conditional Access.

QUESTION NO: 3

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 Microsoft Entra ID.

What should you use?

A. password hash synchronization

B. Microsoft Entra ID Protection

C. Microsoft Entra ID Seamless Single Sign-On (Microsoft Entra ID Seamless SSO)

D. pass-through authentication

ANSWER: D

Explanation:

pass-through authentication is the appropriate authentication method because it validates each user sign-in against the on-premises Active Directory Domain Services environment. The Microsoft Entra authentication agent securely forwards the password validation request to an on-premises domain controller, so the account state and password-related policies maintained in Active Directory are evaluated there rather than relying exclusively on a cloud-stored password hash. This supports an organization that requires its on-premises password controls to remain authoritative.

To enable Microsoft Entra self-service password reset for synchronized users while maintaining their on-premises passwords, password writeback must also be enabled in Microsoft Entra Connect Sync or Microsoft Entra Cloud Sync. Password writeback returns a password changed or reset through SSPR in Microsoft Entra ID to the on-premises AD DS directory in near real time. The on-premises directory can then apply its configured password policy when processing that password update. Microsoft documents pass-through authentication as a hybrid identity sign-in method and identifies it as a supported model for password writeback. See Microsoft Entra pass-through authentication and Enable SSPR password writeback.

QUESTION NO: 4

You have a Microsoft 365 subscription that uses Microsoft Intune.

You need to prevent personally owned Android devices and personally owned iOS/iPadOS devices from enrolling in Intune. Corporate-owned devices that use the same platforms must remain eligible for enrollment.

Which two enrollment restriction settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Block personally owned Android device enrollment.

B. Block personally owned iOS/iPadOS device enrollment.

C. Block Windows device enrollment.

D. Configure an app protection policy.

E. Configure a device compliance policy.

ANSWER: A B

Explanation:

Android device platform restrictions and **iOS/iPadOS device platform restrictions** are required. Intune enrollment restrictions can control whether devices on particular platforms can enroll, and the restrictions can distinguish between personally owned and corporate-owned devices for supported enrollment scenarios.

By creating platform restrictions that block personally owned enrollment for Android and iOS/iPadOS while allowing corporate-owned enrollment, the organization can prevent unmanaged personal devices from enrolling without preventing corporate device deployment. For more information, see Set enrollment restrictions.

QUESTION NO: 5

You have a Microsoft 365 E5 subscription.

You plan to ingest syslog data from a supported firewall device to Microsoft Defender for Cloud Apps.

You need to configure automatic log upload.

Which two components should you configure for the log collector? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. a connection string

B. the receiver type

C. the data source

D. the username and password

E. the host IP address or FQDN

ANSWER: C E

Explanation:

the data source and **the host IP address or FQDN** are required when configuring a log collector for automatic log upload in Microsoft Defender for Cloud Apps. A data source represents the appliance or service that produces the traffic logs, such as the supported firewall. Associating the relevant data source with the collector tells Defender for Cloud Apps which incoming logs the collector will receive and process for Cloud Discovery. The host IP address or fully qualified domain name identifies the Linux host on which the log collector is installed, allowing the Defender portal configuration to target and manage the appropriate collector endpoint. Together, these settings establish the relationship between the source of the syslog records and the collector host that receives and uploads those records to Defender for Cloud Apps. Microsoft documents creation of data sources and log collectors as the required portal-side configuration for automated log uploads. See Configure automatic log upload for continuous reports and Best practices for Cloud Discovery.

QUESTION NO: 6

You have a Microsoft 365 E5 subscription.

You need to be alerted when Microsoft 365 Defender detects high-severity incidents.

What should you use?

A. a custom detection rule

B. a threat policy

C. an alert policy

D. a notification rule

ANSWER: D

Explanation:

A notification rule is the appropriate mechanism for receiving email alerts about high-severity incidents in Microsoft Defender XDR (formerly Microsoft 365 Defender). Incident notification rules let security administrators specify the incident conditions that trigger an email, including severity. Configure a rule that applies to high-severity incidents and add the required recipients; Defender XDR then sends notifications when incidents meeting that condition are created. This supports timely operational awareness without requiring administrators or analysts to continually monitor the Defender portal.

Notification rules can also be scoped using relevant incident attributes, such as service source or device group, when an organization needs more targeted notification routing. The rule is managed from the Microsoft Defender portal's incident notification settings and is intended specifically for incident email notifications. An E5 subscription provides the Defender capabilities required for this integrated incident-management workflow. Microsoft describes the configuration process in Get email notifications about incidents. For context on how Defender XDR correlates alerts into incidents for investigation and response, see the Microsoft Defender XDR incidents overview.

QUESTION NO: 7

What are some benefits of using Azure AD for identity management?

A. It integrates with a wide range of non-Microsoft services.

B. All of the above.

C. It provides multi-factor authentication for increased security.

D. It enables single sign-on (SSO) to simplify user access to applications.

ANSWER: B

Explanation:

All of the above is correct because Azure AD, now called Microsoft Entra ID, provides each of the listed identity-management capabilities. Microsoft Entra ID is a cloud identity and access management service that supports application integration using common federation and authorization standards, including SAML, OAuth 2.0, and OpenID Connect. This allows organizations to centrally manage access not only to Microsoft services but also to many third-party SaaS and custom applications. It also includes Microsoft Entra multifactor authentication, which adds verification methods beyond a password to strengthen account protection and help secure sign-ins. In addition, single sign-on lets users authenticate with their organizational account and access connected applications without having to repeatedly enter credentials. These features reduce user friction while giving administrators centralized control over identities, authentication requirements, and application access. This combination of broad application integration, multifactor authentication, and SSO makes Microsoft Entra ID a foundational identity service for Microsoft 365 environments. See the Microsoft Entra ID overview and Microsoft Entra multifactor authentication documentation.

QUESTION NO: 8 - (HOTSPOT)

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

Name	Membership type	Membership rule
Group1	Assigned	*Not applicable*
Group2	Dynamic	(user.department -eq "Finance")
Group3	Dynamic	(user.department -eq "R&D")

The subscription contains the users shown in the following table.

Name	Department	Assigned group membership
User1	Finance	Group1
User2	Technical	*None*
User3	R&D	Group1

You have a Conditional Access policy that has the following settings:

• Assignments

o Users

■ Include: Group1

■ Exclude: Group2. Group3

o Target resources

■ Cloud apps

■ App1

■ Access controls

■ Grant

■ Block access

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can sign in to App1.	○	○
User2 can sign in to App1.	○	○
User3 can sign in to App1.	○	○

ANSWER:

Answer Area

Statements	Yes	No
User1 can sign in to App1.	○	○
User2 can sign in to App1.	○	○
User3 can sign in to App1.	○	○

Explanation:

The correct result is that User1, User2, and User3 can all sign in to App1. The Conditional Access policy targets members of Group1 and blocks access to App1, but it also explicitly excludes Group2 and Group3. Group2 is a dynamic group whose rule includes every user with a Department value of Finance. User1 has Finance as the department and is therefore dynamically included in Group2. Although User1 is also an assigned member of Group1, the Group2 exclusion means the Conditional Access policy does not apply to User1.

Group3 is also dynamic and includes users whose Department value is R&D. User3 has R&D as the department, so User3 is dynamically included in Group3. User3 is assigned to Group1, but Group3 is listed as an exclusion. In Conditional Access assignment processing, an exclusion takes precedence when a user is both included and excluded. As a result, the block-access control does not apply to User3.

User2 is not an assigned member of Group1 and does not meet either dynamic-group rule. Because User2 is outside the policy's included user scope, the policy does not apply to User2. Therefore, there is no block from this specific policy for any of the three users, and each can sign in to App1. This follows the Conditional Access user and group assignment behavior documented by Microsoft: Users and groups in Conditional Access policies and Dynamic membership rules for groups.

QUESTION NO: 9 - (DRAG DROP)

DRAG DROP

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.

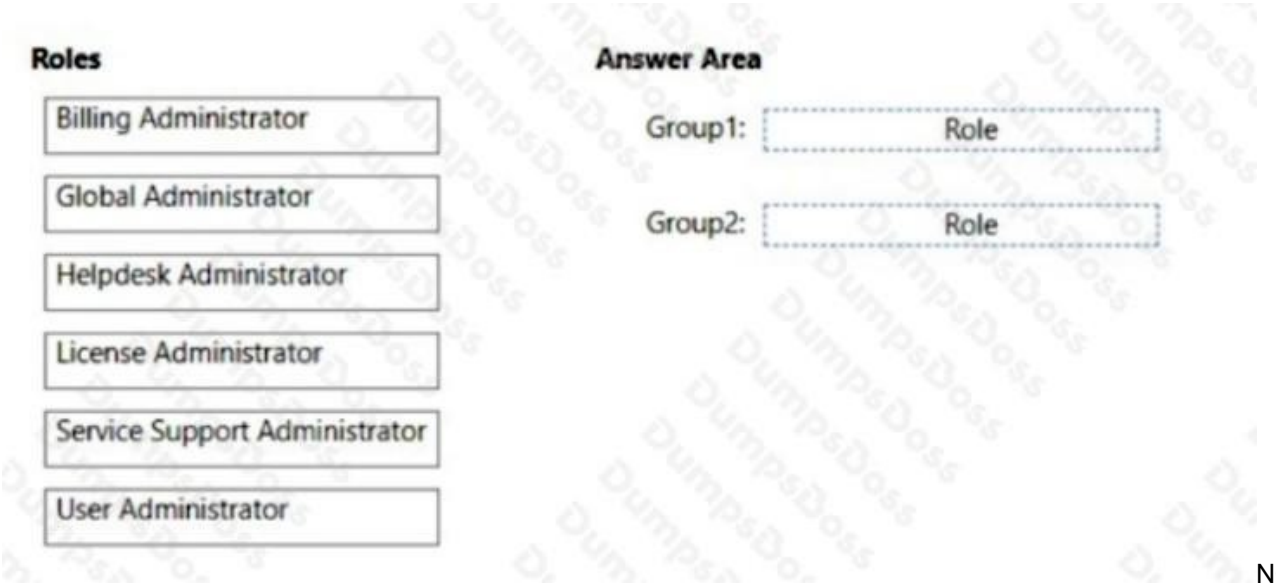
You need to ensure that each group can perform the tasks shown in the following table.

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.

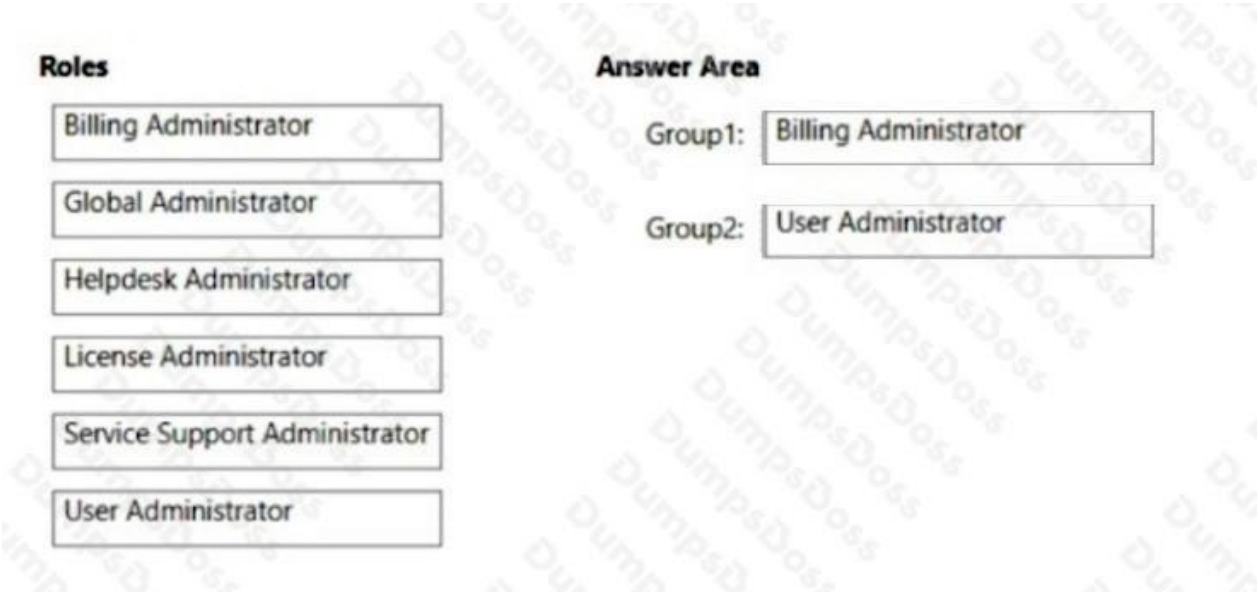
Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role may be used once, more than

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.

ANSWER:



Explanation:

The least-privilege assignments are **Billing Administrator** for Group1 and **User Administrator** for Group2. Billing Administrator is designed for people responsible for an organization's commercial Microsoft 365 administration. Its permissions support managing purchases and subscriptions, reviewing and handling billing-related information, creating and managing support requests, and monitoring service health. Those capabilities let Group1 perform the required subscription and billing operational work without granting broad tenant-wide control. This follows the separation of duties model Microsoft uses for administrative roles: a person who administers billing should receive a billing-focused role rather than permissions to manage unrelated identity, security, or configuration settings. Microsoft documents the billing role's scope in its Microsoft 365 admin roles guidance.

User Administrator is appropriate for Group2 because it is scoped to managing identities and directory objects needed for everyday user administration. The role can create and manage users and groups, update relevant user properties, manage user account settings, and assign licenses as part of user management. This enables the required user-focused administration while limiting access to billing configuration and broader Microsoft 365 tenant administration. Assigning the role to the group also allows role membership to be managed centrally, so administrators can add or remove people from the group as their job responsibilities change. Microsoft Entra documents the permissions and intended use of this role in the User Administrator permissions reference. Together, these assignments provide the required operational capabilities while avoiding unnecessary Global Administrator permissions.

QUESTION NO: 10 - (HOTSPOT)

You have a Microsoft 365 E5 subscription that contains two sensitivity labels named Label1 and Label2. The subscription contains a Windows device named Device1 that is onboarded to Microsoft Purview. Device1 contains the files shown in the following table:

Name

Location

Sensitivity label

File1.docx

C:\Temp\

Label1

File2.docx

C:\Temp\Folder1\

Label2

File3.docx

C:\Temp\Folder2\

Label1

You create a data loss prevention (DLP) policy named Policy1 that has the following configurations:

Locations: Devices: All users and groups

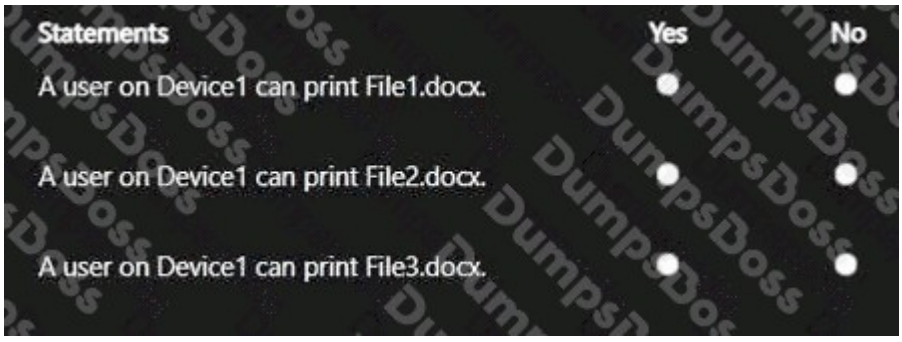
Conditions: Content contains sensitivity label Label1

Actions: Audit or restrict activities on devices

Print: Block

From the Data loss prevention settings, you configure a file path exclusion for C:\Temp\.

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



ANSWER:

Answer:

Answer:

Explanation:

A user on Device1 can print File1.docx.YesA user on Device1 can print File2.docx.YesA user on Device1 can print File3.docx.NoThe DLP rule blocks printing only when the file is subject to Endpoint DLP enforcement and the content matches the configured condition: sensitivity label Label1. Microsoft Purview Endpoint DLP can enforce protective actions on onboarded devices, and Microsoft lists Print as an auditable and restrictable endpoint activity for protected files.The path exclusion is the deciding detail. Microsoft states that file path exclusions turn off DLP monitoring, alerts, and policy enforcement for files in excluded locations. For Windows file path syntax, a path ending with a backslash, such as C:\Temp\, excludes only files directly under that specified folder. A path ending with * excludes files within subfolders, while a path without trailing \ or * excludes both the folder and all subfolders.Therefore, File1.docx can be printed because it has Label1 but is directly under C:\Temp\, so DLP enforcement does not apply. File2.docx can be printed because it is in a subfolder and not excluded, but it has Label2, so it does not match the Label1 blocking condition. File3.docx cannot be printed because it is in a subfolder, is not excluded by C:\Temp\, and has Label1, so the print action is blocked.

Explanation:

Endpoint DLP evaluates protected activity on onboarded Windows devices based on the policy rule and any globally configured exclusions. In this case, the rule is scoped to devices and matches content that has the sensitivity label named Label1. Its configured endpoint action blocks printing, so the block applies when a file is both subject to endpoint DLP monitoring and carries Label1.

The file path exclusion is important because the path is written as `C:\Temp\`, including the trailing backslash. For endpoint DLP exclusions, this format applies to files directly within that exact folder. It does not include files in child folders. Consequently, File1.docx is not evaluated or enforced by endpoint DLP because it is directly under the excluded Temp folder. The user can print it even though it has Label1.

File2.docx is located in Folder1, so it is outside the exact-folder exclusion and can be evaluated. However, it has Label2, while the rule condition requires Label1. Because the content does not meet the configured sensitivity-label condition, the printing restriction is not triggered and the user can print the file.

File3.docx is in Folder2 and is likewise outside the exact-folder exclusion. It has Label1, which meets the rule condition, and printing is configured as a blocked device activity. Therefore, endpoint DLP prevents the user from printing File3.docx. Microsoft documents endpoint DLP device activities and file-path exclusions at Endpoint activities you can monitor and take action on and Configure endpoint DLP settings.

QUESTION NO: 11

What is the purpose of Azure AD Application Proxy?

A. To connect on-premises web applications to Azure AD

B. To implement network security

C. To manage Azure resources

D. To synchronize on-premises identities to Azure AD

ANSWER: A

Explanation:

To connect on-premises web applications to Azure AD is correct. Azure AD Application Proxy, now named Microsoft Entra application proxy, provides secure remote access to on-premises web applications through Microsoft Entra ID. An organization installs a connector inside its private network, near the internal applications. The connector makes outbound connections to the Application Proxy cloud service, so the organization does not need to open inbound firewall ports or expose the application directly to the internet.

After an internal web application is published, users access it through an external URL and authenticate with their Microsoft Entra ID identities. This enables identity-based access features, including single sign-on where supported, multifactor authentication, Conditional Access, and user or group assignment. The service is particularly useful for securely extending access to internal line-of-business and legacy web applications for remote users while centralizing authentication and authorization in Microsoft Entra ID. Microsoft documents Application Proxy as a feature for publishing on-premises web applications and providing secure remote access through Entra ID. See What is Microsoft Entra application proxy? and Microsoft Entra application proxy documentation.

QUESTION NO: 12

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and Microsoft Intune.

All devices run Windows 11 and are Microsoft Entra joined.

You are alerted to a zero-day attack.

You need to identify which devices were affected by the attack and send a request to Intune administrators to update the affected devices.

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

NOTE: Each correct selection is worth one point.

A. From Incidents & alerts, select the latest incident.

B. From Vulnerability management, open the security recommendation.

C. Select the affected devices and request remediation.

D. From Threat analytics, view the list of vulnerable devices.

ANSWER: C D

Explanation:

From Threat analytics, view the list of vulnerable devices is the appropriate first action because threat analytics provides Microsoft Defender for Endpoint's analysis of significant emerging threats, including zero-day vulnerabilities. For a threat, the associated vulnerable-devices view identifies the devices in the organization that are exposed or affected, allowing the administrator to scope the remediation effort accurately. After identifying those devices, Select the affected devices and request remediation uses the Defender Vulnerability Management remediation workflow. A remediation request can be created for the selected devices and routed to Microsoft Intune administrators when the Defender for Endpoint–Intune integration is configured. The request includes the remediation task and affected-device context, enabling the Intune team to deploy the required update or configuration change through Intune and track the request's progress. This workflow connects threat intelligence, device exposure identification, and operational remediation without requiring manual device-list compilation. See Threat analytics in Microsoft Defender for Endpoint and Remediate vulnerabilities in Microsoft Defender Vulnerability Management.

QUESTION NO: 13

Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.

Your company purchases Microsoft 365 and creates an Azure AD tenant named contoso.onmicrosoft.com.

You plan to install Azure AD Connect on a member server and implement pass-through authentication.

You need to prepare the environment for the planned implementation of pass-through authentication.

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

NOTE: Each correct selection is worth one point.

A. From a domain controller, install an Authentication Agent.

B. From the Microsoft Entra admin center, configure an authentication method.

C. From Active Directory Domains and Trusts, add a UPN suffix.

D. Modify the email address attribute for each user account.

E. From the Microsoft Entra admin center, add a custom domain name.

F. Modify the User logon name for each user account.

ANSWER: C E F

Explanation:

Because `contoso.local` is a non-routable internal Active Directory DNS suffix, it cannot be verified as a Microsoft Entra ID custom domain for Microsoft 365 sign-in. The environment should therefore use an internet-routable domain, such as `contoso.com`, as the users' sign-in suffix. Adding a custom domain name in the Microsoft Entra admin center establishes the domain in the tenant and enables ownership verification. After verification, that domain becomes available for Microsoft Entra ID user sign-in.

Adding a UPN suffix through Active Directory Domains and Trusts makes the same routable suffix available in the on-premises Active Directory forest. Modifying the User logon name for each user account then assigns that suffix to each user's on-premises UPN. During Microsoft Entra Connect synchronization, those UPNs can synchronize to the verified tenant domain, providing users with a consistent Microsoft 365 sign-in identity. Pass-through authentication uses this synchronized identity and validates the password against on-premises Active Directory through the authentication agent installed as part of the Microsoft Entra Connect pass-through authentication configuration.

Microsoft documents domain verification and UPN alignment as key hybrid identity preparation activities. See Add a domain to Microsoft 365 and Microsoft Entra Connect prerequisites.

QUESTION NO: 14

What is the process called when a user signs in to an application or service with their Azure AD credentials?

A. Credential theft

B. Single sign-on

C. Authorization

D. Authentication

ANSWER: D

Explanation:

Authentication is the process through which Microsoft Entra ID, formerly Azure Active Directory, verifies the identity of a user who signs in to an application or service. It answers the fundamental identity question, "Who are you?" When a user supplies credentials such as a password, passkey, security key, certificate, or multifactor authentication response, Microsoft Entra ID validates the sign-in attempt. After successful verification, the identity platform can issue security tokens containing claims about the user, which the application uses to establish the signed-in session.

This process is central to access to Microsoft 365, Azure, and applications integrated with Microsoft Entra ID. Authentication may involve additional controls, including multifactor authentication and Conditional Access requirements, but its core purpose remains confirming the user's identity. Microsoft distinguishes authentication from subsequent access decisions by

defining authentication as proof of identity before an application determines the permissions or resources available to that identity. For details, see Microsoft's documentation on authentication and authorization in the Microsoft identity platform and the Microsoft Entra ID overview.

QUESTION NO: 15

Which PowerShell command can be used to connect to a Microsoft 365 tenant?

A. Connect-MsolService

B. Connect-AzureAD

C. Connect-ExchangeOnline

D. Connect-MicrosoftTeams

ANSWER: A

Explanation:

`Connect-MsolService` establishes an authenticated session to the Microsoft Online service directory for a Microsoft 365 tenant. It is the connection cmdlet in the MSOnline PowerShell module and, after interactive authentication, enables the administrator to run that module's tenant-directory management cmdlets for resources such as users, groups, domains, and license assignments. In the context of a general Microsoft 365 tenant connection question using the traditional Microsoft 365 administration modules, this is the expected command. Microsoft's cmdlet reference describes `Connect-MsolService` as connecting to Microsoft Entra ID, formerly Azure Active Directory, which provides the tenant identity directory used by Microsoft 365. See Connect-MsolService reference. For new scripts and automation, Microsoft recommends Microsoft Graph PowerShell rather than the legacy MSOnline module; however, that modernization guidance does not change the recognized answer among the commands provided. Microsoft's tenant PowerShell connection guidance is available at Connect to Microsoft 365 with PowerShell.

QUESTION NO: 16

You have a Microsoft 365 E3 subscription that uses Microsoft Intune.

You need to create a device compliance policy for Windows devices. Devices that do not meet the policy must be identified as noncompliant and can later be blocked from Microsoft 365 by using Conditional Access.

Which two settings can you configure in a Windows compliance policy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Require BitLocker.

B. Require a minimum operating system version.

C. Deploy a required application.

D. Configure an update ring.

E. Configure a device configuration profile.

ANSWER: A B

Explanation:

Requiring **BitLocker** is a supported Windows compliance-policy setting. Intune can evaluate whether a Windows device meets the organization's encryption requirement and mark the device noncompliant when it does not.

Requiring a **minimum operating system version** is also a supported compliance setting. This enables administrators to require that devices run a specified Windows version before they are considered compliant. A Conditional Access policy can then require a compliant device before granting access to cloud applications.

Application deployment and Windows Update ring configuration are managed by separate Intune policy types; they are not settings in a device compliance policy. For details, see Device compliance policies in Microsoft Intune and Require device compliance by using Conditional Access.

QUESTION NO: 17

Which tool is used to manage SharePoint Online in a Microsoft 365 tenant?

A. Yammer

B. Microsoft Teams

C. OneDrive Admin Center

D. Microsoft SharePoint Admin Center

ANSWER: D

Explanation:

Microsoft SharePoint Admin Center is the dedicated administration portal for managing SharePoint Online throughout a Microsoft 365 tenant. SharePoint administrators use it to manage active and deleted sites, configure organization-wide sharing and access controls, set site-storage limits, review usage and activity information, and apply SharePoint policies. It also provides tenant-level controls for areas such as site creation, external sharing, content services, and migration settings. The SharePoint admin center is accessed through the Microsoft 365 admin center by selecting *SharePoint* under Admin centers, or directly at the tenant's SharePoint admin URL. Appropriate permissions are required; users assigned the SharePoint Administrator role can manage SharePoint and OneDrive administration features without being granted unrestricted Global Administrator permissions. This makes Microsoft SharePoint Admin Center the appropriate tool for centralized SharePoint Online tenant administration. Microsoft describes the SharePoint Administrator role and its administrative capabilities at SharePoint Administrator role. For details about managing SharePoint sites and tenant settings through the portal, see Manage sites in the SharePoint admin center.

QUESTION NO: 18

What is Azure AD Privileged Identity Management?

A. A feature that allows users to reset their passwords

B. A feature that automatically locks accounts after failed sign-in attempts

C. A way to implement multi-factor authentication for privileged accounts

D. A way to manage user and group membership settings

E. A feature for managing, controlling, and monitoring privileged access to Microsoft Entra ID, Azure, and other Microsoft online services.

ANSWER: E

Explanation:

A feature for managing, controlling, and monitoring privileged access to Microsoft Entra ID, Azure, and other Microsoft online services is correct. Azure AD Privileged Identity Management (PIM) was renamed Microsoft Entra Privileged Identity Management. It is an identity governance capability that reduces the risk associated with permanent, highly privileged administrative assignments. Instead of making an administrator active indefinitely, PIM can assign the person as eligible for a role and allow them to activate that role only when needed, for a limited period. Organizations can require controls such as multifactor authentication, justification, ticket information, or approval before activation. PIM also provides visibility through

alerts, access reviews, and audit history for privileged role assignments and activations. These capabilities support least privilege by limiting both the number of people with active administrative rights and the time for which those rights remain active. PIM manages access to Microsoft Entra roles and Azure resource roles, and it can govern privileged access through groups in supported scenarios. Microsoft describes PIM as a service for managing, controlling, and monitoring access to important resources. See What is Microsoft Entra Privileged Identity Management? and Configure Microsoft Entra Privileged Identity Management.

QUESTION NO: 19

You have a Microsoft 365 subscription.

You suspect that several Microsoft Office 365 applications or services were recently updated.

You need to identify which applications or services were recently updated.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. From the Microsoft 365 admin center, review the Service health blade.

B. From the Microsoft 365 admin center, review the Message center blade.

C. From the Microsoft 365 admin center, review the Products blade.

D. From the Microsoft 365 Admin mobile app, review the messages.

ANSWER: B D

Explanation:

Reviewing the Message center in the Microsoft 365 admin center is a complete solution because Message center is Microsoft's central communication location for changes to Microsoft 365 services and features. Its posts identify the affected workload or application, describe the change, provide rollout and availability details, and state whether administrators need to take action. Administrators can filter and search posts to identify changes relevant to their organization and can view messages that were recently published or are associated with active feature rollouts.

Reviewing messages in the Microsoft 365 Admin mobile app is also a complete solution. The mobile app provides administrators with access to Message center communications and notifications while away from the web-based admin center. Therefore, it can be used to review the same type of service-change announcements and determine which Microsoft 365 applications or services have received updates. Message center communications are intended to help organizations prepare for, understand, and manage service updates that affect their tenant. For details, see Message center in the Microsoft 365 admin center and Microsoft 365 Admin mobile app.

QUESTION NO: 20

Your company has on-premises servers and an Azure AD tenant.

Several months ago, the Azure AD Connect Health agent was installed on all the servers.

You review the health status of all the servers regularly.

Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect

Servers list.

You suspect that another administrator removed Server1 from the list.

You need to ensure that you can view the health status of Server1.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. From Windows PowerShell, run the Register-AzureADConnectHealthSyncAgent cmdlet.

B. From Azure Cloud shell, run the Connect-AzureAD cmdlet.

C. From Server1, reinstall the Azure AD Connect Health agent.

D. From Server1, change the Azure AD Connect Health services Startup type to Automatic.

E. From Server1, change the Azure AD Connect Health services Startup type to Automatic (Delayed Start).

ANSWER: A C

Explanation:

Running `Register-AzureADConnectHealthSyncAgent` from Windows PowerShell is a complete solution because it registers the Microsoft Entra Connect Health synchronization agent installed on Server1 with the tenant's Connect Health service. Registration establishes the agent's service identity and enables it to send its monitoring and health telemetry to the portal. When the server's existing portal representation or registration association is no longer present, registering the installed agent again restores the server's ability to report and be displayed in the server list. The command must be run in the context of the affected synchronization server and with appropriate Microsoft Entra administrative credentials.

Reinstalling the Azure AD Connect Health agent on Server1 is also a complete remediation method. Installation of the synchronization agent includes its configuration and registration with the Connect Health service. Therefore, a reinstall recreates a functional local agent installation and registers it so that Server1 can resume uploading health information. This approach is appropriate where the existing agent registration is unavailable or the local installation needs to be rebuilt. Microsoft documents both agent installation and registration as required steps for monitored servers to communicate with Connect Health. See Install Microsoft Entra Connect Health agents and Register the agent for Microsoft Entra Connect Health.

QUESTION NO: 21

You have a Microsoft 365 E5 subscription.

You create the users shown in the following table.

You plan to use Microsoft Entra ID Protection.

Which users will be added automatically to the Users at risk detected alerts list?

A. Admin1 only

B. Admin2 only

C. Admin1 and Admin2 only

D. Admin1 and Admin3 only

E. Admin1, Admin2, and Admin3

ANSWER: D

Explanation:

Admin1 and Admin3 only is correct. Microsoft Entra ID Protection automatically includes members of the applicable built-in security-related directory roles in the recipients for Users at risk detected alert notifications. This behavior ensures that personnel with responsibility for identity security receive notification when Entra ID Protection detects a user account whose risk level reaches the configured alert threshold. Based on the role assignments in the table, Admin1 and Admin3 hold roles that are automatically included for these alerts, so they are added without an administrator manually selecting them as recipients.

This automatic recipient population is separate from risk-policy targeting. Risk policies determine which users are evaluated and what remediation is required, such as requiring secure password change or blocking access. Alert recipients instead receive security notifications so they can investigate, monitor, and respond to detected identity risk. Administrators can also configure additional notification recipients when their operational processes require it. Microsoft documents the automatic alert-recipient behavior and the available notification configuration in Configure notifications and alerts in Microsoft Entra ID Protection. For the built-in directory roles used to administer identity security, see Microsoft Entra built-in roles.

QUESTION NO: 22

Your network contains an Active Directory domain named adatum.com that is synced to Azure AD.

The domain contains 100 user accounts.

The city attribute for all the users is set to the city where the user resides.

You need to modify the value of the city attribute to the three-letter airport code of each city.

What should you do?

A. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.

B. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.

C. From Windows PowerShell on a domain controller, run the Get-MgUser and Update-MgUser cmdlets.

D. From Azure Cloud Shell, run the Get-MgUser and Update-MgUser cmdlets.

ANSWER: A

Explanation:

From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets. The accounts originate in the on-premises Active Directory domain and are synchronized to Microsoft Entra ID (formerly Azure AD). Consequently, on-premises Active Directory is the authoritative source for synchronized user attributes, including the City property, whose underlying LDAP attribute is `l`. Updates must therefore be made to the local user objects; Microsoft Entra Connect will synchronize those changes to Microsoft Entra ID during its next synchronization cycle.

The ActiveDirectory PowerShell module is designed for this administrative task. `Get-ADUser` can retrieve the users and the existing City values, and a script can use a city-to-airport-code mapping to set the appropriate new value for each account. `Set-ADUser` modifies the City property directly, allowing all 100 accounts to be processed consistently and efficiently. For example, the script can retrieve each user with the City property, determine its matching airport code, and apply that code using `Set-ADUser -City`.

Microsoft documents the available parameters and use of `Set-ADUser` at Set-ADUser. The synchronization model and role of on-premises Active Directory in hybrid identity are described in What is Microsoft Entra Connect?.

QUESTION NO: 23

You have a Microsoft 365 E5 subscription that contains devices onboarded to Microsoft Defender for Endpoint. You integrate Microsoft Defender for Cloud Apps with Defender for Endpoint. You need identify which cloud apps and services were used most during the last 30 days What should you do?

A. Generate a Cloud Discovery snapshot report.

B. Generate a monthly security summary report

C. Create a threat analytics alert notification.

D. Generate a Cloud Discovery executive report

ANSWER: D

Explanation:

Generate a Cloud Discovery executive report. This report is designed to provide a high-level, management-oriented view of cloud-app use discovered from integrated data sources such as Microsoft Defender for Endpoint. Its content highlights the cloud applications and services used most in the organization and summarizes their usage for the preceding 30 days. Therefore, it directly supplies the requested view without requiring manual analysis of raw discovery events or individual device activity.

Cloud Discovery uses traffic information collected through Defender for Endpoint to identify the cloud apps accessed by users. After Defender for Endpoint is connected as an app connector, Defender for Cloud Apps can aggregate this discovery data and present organizational insights. The executive report is the appropriate report format when the goal is to identify the most-used services over the defined 30-day reporting period and communicate that result at a summarized level. Microsoft documents Cloud Discovery reporting and its discovery data sources in Cloud Discovery dashboard and describes the Defender for Endpoint integration in Integrate Microsoft Defender for Endpoint with Defender for Cloud Apps.

QUESTION NO: 24

You have a Microsoft 365 subscription that uses 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 after you implemented the preservation lock? 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: A D

Explanation:

Add locations to the policy. and **Extend the duration of the policy.** are permitted after Preservation Lock is enabled because both changes strengthen the policy's retention protections rather than reducing them. Adding locations expands the scope of protected content, allowing the organization to apply the same immutable retention requirements to additional supported workloads or users. Extending the retention duration preserves content for a longer period, which is also a stricter compliance control.

Preservation Lock is intended for organizations that must meet regulatory recordkeeping obligations and need assurance that a retention policy cannot subsequently be weakened. Once enabled, the lock makes the retention configuration immutable with respect to changes that could reduce the policy's protection. Administrators can still make permitted changes that broaden coverage or increase the retention commitment. This supports a compliant operational model: retention can be made more restrictive as requirements evolve, while the organization remains protected from reducing the policy's existing preservation obligations.

Microsoft documents the permitted and restricted changes for locked policies in Preservation Lock for retention policies. For broader implementation guidance, see Learn about retention.

QUESTION NO: 25

Which programming language is recommended for developing collaborative app solutions with Microsoft 365?

A. JavaScript

B. C++

C. Java

D. Objective-C

ANSWER: A

Explanation:

JavaScript is the recommended choice because Microsoft 365 collaborative applications are primarily built on modern web technologies. Collaborative experiences commonly run in Microsoft Teams and Microsoft 365 surfaces as web-based tabs, message extensions, task modules, and integrations that use JavaScript or its strongly typed superset, TypeScript. JavaScript works naturally with client-side web frameworks and server-side Node.js services, enabling a single technology ecosystem for the user interface, app logic, authentication, and Microsoft 365 integration.

Microsoft's Teams development platform provides JavaScript and TypeScript project templates and tooling for creating collaborative apps. These applications can use Microsoft Graph to work with Microsoft 365 resources such as users, teams, chats, files, calendars, and documents. The Microsoft Graph JavaScript SDK further provides supported libraries for authenticating and making Graph requests from JavaScript-based applications. This close alignment with Teams, web application development, Teams Toolkit, and Microsoft Graph makes JavaScript the most appropriate answer for developing collaborative app solutions with Microsoft 365. See Microsoft Teams Toolkit fundamentals and Install the Microsoft Graph JavaScript SDK.

QUESTION NO: 26

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 E5 subscription.

You plan to implement a hybrid configuration that has the following requirements:

• Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources

• Supports the use of Azure AD Identity Protection

You need to configure Azure AD Connect to support the planned implementation.

Which two options should you select? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Password Hash Synchronization

B. Password writeback

C. Directory extension attribute sync

D. Enable single sign-on

E. Pass-through authentication

ANSWER: A D

Explanation:

Password Hash Synchronization is required because it synchronizes a derived hash of each on-premises Active Directory password to Microsoft Entra ID, allowing users to authenticate to Microsoft 365 with their existing password. It also provides a key prerequisite for the fullest Microsoft Entra ID Protection capability: leaked-credential detections compare credentials

found in public breach data against synchronized password-hash information. This gives the organization cloud authentication resiliency while enabling Identity Protection to identify and remediate password-based risks.

Enable single sign-on is the complementary selection for reducing credential prompts. Microsoft Entra seamless single sign-on automatically signs in users from domain-joined corporate devices when they access Microsoft Entra ID-integrated applications, including Microsoft 365. It uses a computer account in on-premises Active Directory and Kerberos authentication to obtain the required sign-in token without requiring the user to repeatedly enter a password. Seamless SSO is supported with Password Hash Synchronization and can be enabled in the Microsoft Entra Connect configuration wizard. Together, these settings meet both the streamlined sign-in and Identity Protection requirements. For implementation details, see Microsoft Entra password hash synchronization and Microsoft Entra seamless single sign-on.

QUESTION NO: 27

What is Threat and Vulnerability Management and how does it benefit an organization?

A. Threat and Vulnerability Management is a tool that helps prevent phishing attacks

B. Threat and Vulnerability Management is a framework that guides an organization's security strategy

C. Threat and Vulnerability Management is a security capability that continuously identifies, assesses, and helps remediate vulnerabilities and misconfigurations.

D. Threat and Vulnerability Management is a tool for monitoring authentication and access control

ANSWER: C

Explanation:

Threat and Vulnerability Management is a security capability that continuously identifies, assesses, prioritizes, and supports remediation of vulnerabilities and misconfigurations. This gives an organization an actionable view of weaknesses that could be used to compromise devices, identities, applications, or data. Rather than treating every discovered issue with the same urgency, Microsoft Defender Vulnerability Management uses threat intelligence, exposure information, and asset context to help security teams focus remediation efforts on the issues that present the greatest risk.

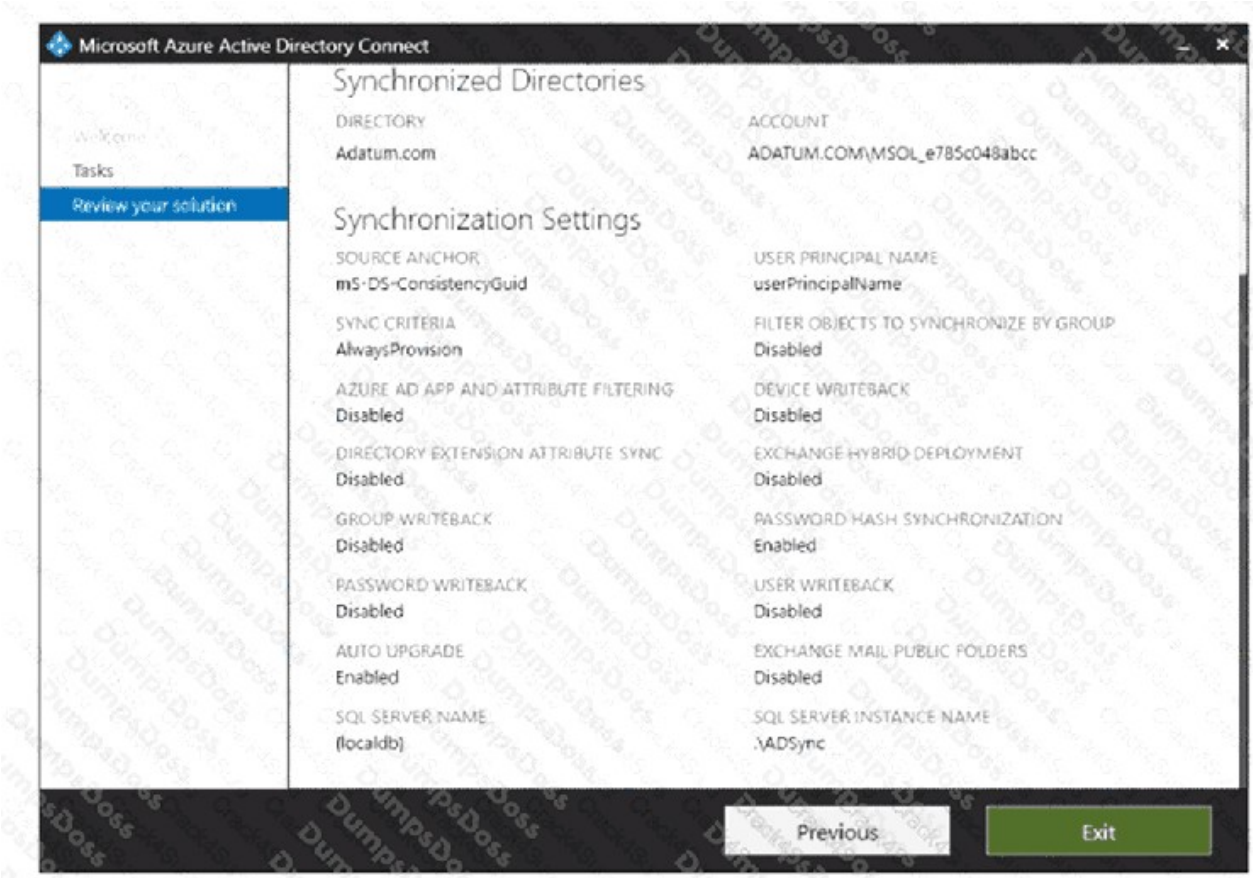
The key organizational benefit is a more proactive security posture. Administrators can discover outdated software, missing security updates, insecure configurations, and other exposure gaps before they are exploited. They can then use remediation recommendations and workflow tracking to reduce the attack surface efficiently. This continuous assessment also improves communication between security and IT operations teams by providing a common, risk-based basis for remediation decisions. Microsoft documents that Defender Vulnerability Management helps organizations discover, prioritize, and remediate vulnerabilities and misconfigurations across their environment. For further details, see Microsoft Defender Vulnerability Management and Threat and vulnerability management in Microsoft Defender for Endpoint.

QUESTION NO: 28 - (SIMULATION)

Your company has a hybrid deployment of Microsoft 365.

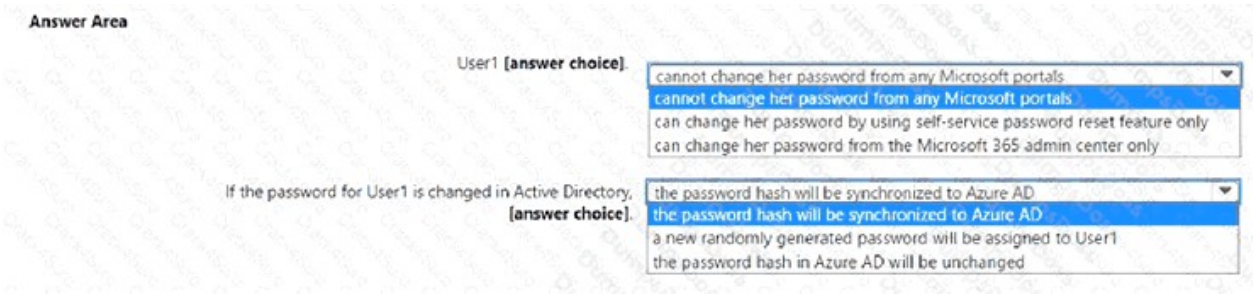
An on-premises user named User1 is synced to Microsoft Entra ID.

Microsoft Entra Connect Sync is configured as shown in the following exhibit



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



ANSWER: See the explanation for the answer

Explanation:

Selections:

The Entra Connect configuration has **Password hash synchronization** enabled, so an on-premises Active Directory password change results in an updated password hash being synchronized to Microsoft Entra ID. However, **Password writeback** is disabled, so password changes or resets performed in Microsoft cloud portals cannot be written back to the on-premises Active Directory account.

QUESTION NO: 29

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 E5 subscription.

You plan to implement a hybrid configuration that has the following requirements:

• Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources

• Supports the use of Microsoft Entra ID Protection

You need to configure Microsoft Entra Connect Sync to support the planned implementation. Which two options should you select? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Password Hash Synchronization

B. Password writeback

C. Directory extension attribute sync

D. Enable single sign-on

E. Pass-through authentication

ANSWER: A D

Explanation:

Password Hash Synchronization is required because it synchronizes a hash of each on-premises Active Directory password hash to Microsoft Entra ID. This enables cloud authentication and supports Microsoft Entra ID Protection capabilities that rely on password-hash data, including detection of leaked credentials and password-related risk evaluation. Microsoft recommends password hash synchronization as the cloud authentication method because it provides resiliency and enables identity-protection features. The synchronized hash is not the user's clear-text password and cannot be used to authenticate directly against the on-premises Active Directory environment.

Enable single sign-on refers to Seamless single sign-on. With Seamless SSO, users who are already signed in to domain-joined devices on the corporate network can be signed in automatically to Microsoft Entra ID and Microsoft 365 resources without repeatedly entering their credentials. It works with Password Hash Synchronization and is configured through Microsoft Entra Connect Sync. Together, these selections provide a cloud-authentication design that reduces credential prompts while retaining the password signals needed for Microsoft Entra ID Protection.

For configuration and feature details, see Microsoft Entra password hash synchronization and Microsoft Entra Seamless single sign-on.

QUESTION NO: 30

What are the three types of Microsoft 365 tenants?

A. Logging-only

B. All of the above

C. Trial

D. Paid

E. Developer, Trial, and Paid

ANSWER: E

Explanation:

Developer, Trial, and Paid are the three Microsoft 365 tenant types described in common Microsoft 365 administration and learning contexts. A paid tenant is an organization's licensed Microsoft 365 environment, used for ongoing business operations after the organization purchases subscriptions and assigns licenses. A trial tenant is provisioned when an organization starts a time-limited trial to evaluate Microsoft 365 capabilities before committing to a paid subscription. Microsoft provides guidance for starting trials, purchasing subscriptions, and managing the transition to paid licensing. A developer tenant, often called a developer sandbox, is available through the Microsoft 365 Developer Program for building,

testing, and learning with Microsoft 365 services and APIs. It is intended to provide a safe nonproduction environment with sample users and data, enabling developers to validate integrations without using an organization's production tenant. Together, these categories distinguish production licensing, evaluation use, and development/testing purposes. Microsoft's subscription guidance is available in Try or buy Microsoft 365 subscriptions, and details about developer sandboxes are in the Microsoft 365 Developer Program FAQ.

QUESTION NO: 31

What is the role of the Microsoft Global Reader in Microsoft Purview?

A. To manage metadata for specific data assets within an organization

B. To create and manage access policies within an organization

C. To view data catalogs across multiple Microsoft tenants

D. To view and edit all data within the organization

E. To view Microsoft Purview information and settings without making changes

ANSWER: E

Explanation:

To view Microsoft Purview information and settings without making changes is correct. Global Reader is a Microsoft Entra built-in role designed to provide broad read-only visibility across Microsoft 365 administration experiences. It is intended for personnel such as auditors, compliance reviewers, and support teams who must inspect tenant configuration and service information but must not be able to alter administrative settings.

In Microsoft Purview, this read-only access supports reviewing available compliance information and configuration without granting the ability to create, modify, or delete policies and other administrative objects. This follows the principle of least privilege: an organization can provide necessary oversight and visibility while protecting sensitive compliance configurations from unintended or unauthorized changes. Global Reader is therefore appropriate when the operational requirement is observation, review, and reporting rather than administration.

Microsoft describes Global Reader as having read-only access to administrative portals and services that support the role. Purview access is also governed through role-based access control, which enables organizations to assign only the permissions required for a user's responsibilities. See the Microsoft Entra Global Reader permissions reference and Microsoft Purview compliance portal permissions documentation.

QUESTION NO: 32

Which tool allows an administrator to quarantine or block a user when a threat is detected?

A. Microsoft Defender for Office 365

B. Microsoft Cloud App Security

C. Microsoft Defender for Endpoint

D. Azure Sentinel

ANSWER: B

Explanation:

Microsoft Cloud App Security is correct. This product has been renamed Microsoft Defender for Cloud Apps, but the former name remains recognizable in older Microsoft 365 training and exam material. Defender for Cloud Apps provides Cloud Access Security Broker capabilities to discover cloud-app usage, detect suspicious behavior through policies and anomaly detection, and apply governance controls when a policy match or threat is identified. Its governance capabilities can take action on affected users and content in connected cloud apps. Depending on the app integration and the configured policy,

an administrator can use actions such as suspending a user in Microsoft Entra ID, requiring the user to sign in again, revoking a user's app access, or quarantining files. These controls allow the organization to contain risk promptly while an investigation occurs. Policy-based governance actions can also be configured to run automatically for supported scenarios, which helps operationalize a response to detected threats rather than relying solely on manual review. Microsoft documents the available policy controls and remediation capabilities in Control cloud apps with policies and details user and file actions in Governance actions.

QUESTION NO: 33

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. Enable Custom network indicators.

C. Enable automated investigation.

D. Create an indicator.

E. Configure an enforcement scope.

ANSWER: B D

Explanation:

Enable Custom network indicators. is required to allow Microsoft Defender for Endpoint to apply organization-defined indicators for network destinations. This capability supports indicators for URLs, domains, and IP addresses, with actions such as allow, audit, warn, and block. Enabling it makes custom URL/domain block decisions available to the Defender for Endpoint protection stack on supported, onboarded devices.

Create an indicator. is then required to define the specific destination that must be blocked. Create a custom indicator for `www.contoso.com` (or the applicable domain/URL scope) and assign it the Block action. Defender for Endpoint distributes the indicator and enforces the requested block for devices that meet the relevant network-protection and platform prerequisites. Indicator configuration also permits specifying an expiration date, severity, title, description, and applicable device groups where appropriate, helping administrators limit the indicator's scope and manage it throughout its lifecycle.

Microsoft documents custom indicators as the mechanism for controlling access to specific IP addresses, URLs, and domains, and identifies enabling custom network indicators as a prerequisite for URL/domain indicator enforcement. See Create indicators for IPs and URLs/domains and Manage indicators.

QUESTION NO: 34

What is the recommended approach for customizing modern SharePoint list forms using SharePoint Framework?

A. Use InfoPath

B. Use SharePoint Designer

C. Use PowerApps

D. Use Flow

E. Use SharePoint Framework Form Customizer extensions

ANSWER: E

Explanation:

Use SharePoint Framework Form Customizer extensions is the recommended approach because Form Customizers are the supported SharePoint Framework extension type specifically intended to customize the modern New, Edit, and Display experiences for SharePoint list and library items. A developer can register a Form Customizer against a particular list and content type, then implement the required client-side user interface and behavior using supported SPFx development patterns. This provides a tailored form experience while retaining the modern SharePoint environment and integrating with Microsoft 365 identity, permissions, list data, and client-side APIs. Form Customizers are appropriate when the requirement explicitly calls for SharePoint Framework because they are built, packaged, deployed, and managed as SPFx solutions, rather than relying on legacy form technologies or a separate low-code customization platform. Microsoft documents the Form Customizer as an SPFx Extension that customizes list-form rendering and provides guidance for creating and associating it with a list. See Build a Form Customizer extension and SharePoint Framework Extensions overview.

QUESTION NO: 35

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.

You need to protect the mailbox of the CEO from messages that impersonate the CEO. Messages identified as impersonation attempts must be quarantined.

Which two settings should you configure in an anti-phishing policy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure user impersonation protection.

B. Configure domain impersonation protection.

C. Configure the impersonation action to quarantine the message.

D. Configure a Safe Attachments policy.

E. Configure a connection filter policy.

ANSWER: A C

Explanation:

User impersonation protection is required to identify messages that impersonate a specified user, such as the CEO. An anti-phishing policy can protect selected users by evaluating the sender display name and email address for impersonation attempts.

Quarantine the message is required to prevent the identified message from reaching the recipient's mailbox. Anti-phishing policies support configurable actions for detected impersonation and phishing messages, including moving the message to quarantine. For more information, see Anti-phishing policies in Microsoft Defender for Office 365.

QUESTION NO: 36

Your company has an on-premises Active Directory domain and a Microsoft 365 subscription.

You plan to synchronize users and groups to Microsoft Entra ID by using Microsoft Entra Cloud Sync.

You need to ensure that synchronization continues if a single synchronization server fails.

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

NOTE: Each correct selection is worth one point.

A. Install the Microsoft Entra provisioning agent on two servers.

B. Create a cloud sync configuration.

C. Install Microsoft Entra Connect Sync on each domain controller.

D. Configure Active Directory Federation Services (AD FS).

E. Enable password writeback.

ANSWER: A B

Explanation:

Install the Microsoft Entra provisioning agent on two servers provides high availability for Microsoft Entra Cloud Sync. Multiple active agents can be installed for the same Active Directory domain, and Cloud Sync can use another active agent if one agent becomes unavailable.

Create a cloud sync configuration is also required because the configuration defines the Active Directory domain, object scope, attribute mappings, and synchronization settings that the provisioning agents use. The agents provide the connection to Active Directory, while the cloud sync configuration defines what is synchronized to Microsoft Entra ID.

For more information, see What is Microsoft Entra Cloud Sync? and Install the Microsoft Entra provisioning agent.

QUESTION NO: 37

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:

No is correct. Creating an assessment in Microsoft Purview Compliance Manager requires permissions that include the Compliance Manager capabilities, such as membership in the appropriate Microsoft Purview role group or assignment of a role that grants Compliance Manager assessment-creation permissions. These permissions are managed through the Microsoft Purview portal's role-based access control model, where the applicable role group enables users to create and manage assessments, improvement actions, and related Compliance Manager content.

The Compliance data admin role assignment described in the solution is not the role assignment used to grant Compliance Manager assessment creation rights. Therefore, assigning that role from the Microsoft 365 admin center does not satisfy the stated requirement for User1. An administrator must instead assign User1 a supported Compliance Manager role or role group that includes assessment creation privileges. Microsoft documents the specific roles and permissions applicable to Compliance Manager in its Compliance Manager roles guidance. For broader context on assigning Microsoft Purview permissions and role groups, see Microsoft Purview permissions.

QUESTION NO: 38

What is the purpose of Microsoft Cloud App Security (MCAS)?

A. To monitor activity in cloud applications

B. To provide end-to-end encryption for all data in an organization

C. To provide security for on-premises network devices

D. To manage access to on-premises applications

ANSWER: A

Explanation:

To monitor activity in cloud applications is correct. Microsoft Cloud App Security (MCAS), now called Microsoft Defender for Cloud Apps, is a cloud access security broker solution. Its central purpose is to provide visibility into cloud application use, monitor activities and data movement, identify risky or anomalous behavior, and support investigation and policy-based controls across cloud services. It can discover cloud apps being used in an organization, including unsanctioned apps, and use signals from activity logs and analytics to help security teams detect threats and protect sensitive information.

Defender for Cloud Apps also integrates with Microsoft 365 and other supported SaaS applications to apply governance actions and real-time session controls where available. These capabilities make cloud-app activity monitoring the best concise description of the product's purpose. Microsoft's documentation describes Defender for Cloud Apps as providing visibility, control over data travel, and analytics to identify and combat cyberthreats across cloud services. See What is Microsoft Defender for Cloud Apps? and Get started with Microsoft Defender for Cloud Apps.

QUESTION NO: 39

You have a Microsoft 365 E5 subscription.

You need to use Microsoft Entra Privileged Identity Management (PIM) to reduce the standing access of users assigned to the Global Administrator role.

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

NOTE: Each correct selection is worth one point.

A. Make the users eligible for the Global Administrator role.

B. Require multifactor authentication for role activation.

C. Assign the Global Administrator role permanently.

D. Create a mail flow rule.

E. Assign a Microsoft 365 E5 license to each user.

ANSWER: A B

Explanation:

Make the users **eligible** for the Global Administrator role rather than permanently active. Eligible users do not receive the role's permissions until they activate the assignment when administrative work is required.

Configure a **role activation policy** that requires multifactor authentication. PIM can also require justification, approval, a ticket number, and a limited activation duration. These controls provide just-in-time privileged access and create an auditable activation process.

Creating a Conditional Access policy or assigning a Microsoft 365 license does not create just-in-time role assignments. For more information, see Assign Microsoft Entra roles in Privileged Identity Management and Configure Microsoft Entra role settings in PIM.

QUESTION NO: 40

What is the name of the group that defines the policies for data sources in Microsoft Purview?

A. Data source group

B. Data policy group

C. Data classification group

D. Data governance group

ANSWER: B

Explanation:

Data policy group is correct. In Microsoft Purview, data policy groups provide the organizational scope used to manage and apply data access policies to supported data sources. A group brings together one or more registered data sources that share policy-management requirements, allowing administrators to define and manage policies consistently for that collection rather than configuring equivalent policy scope independently for each source. This supports centralized governance of access to data assets while still allowing policies to be targeted to the appropriate sources and users. Data policy groups are part of the Microsoft Purview data policy capability, which enables organizations to create and manage access policies for data systems from Purview. The policies are then published to applicable data sources, where they can govern access according to the configured rules. This model helps ensure that a consistent policy definition can be managed centrally across a defined set of sources. For an overview of the feature and its purpose, see Microsoft Purview data policy overview. For information about configuring and managing these policies in Purview, see Create data access policies in Microsoft Purview.

QUESTION NO: 41

What is the maximum number of global administrators that can be assigned in a Microsoft 365 tenant?

A. 10 administrators

B. 1 administrator

C. 5 administrators

D. 3 administrators

E. No fixed maximum limit

F. 100 administrators

ANSWER: F

Explanation:

100 administrators is the maximum number of users that can be assigned the Global Administrator role in a Microsoft 365 tenant. This is a Microsoft 365 service limit, rather than merely a recommended operational threshold. The Global Administrator role provides broad administrative permissions across Microsoft 365 and Microsoft Entra ID, including the ability to manage users, subscriptions, domains, and other administrators. Consequently, this role should be assigned only when its extensive permissions are genuinely required.

Although a tenant can have as many as 100 Global Administrators, Microsoft recommends maintaining only a small set of permanent Global Administrators for security and operational resilience. In particular, organizations should retain multiple emergency-capable administrators so that access is not dependent on a single account, while using more narrowly scoped administrative roles for routine work. This supports least-privilege access and reduces the potential impact of a compromised privileged account. Microsoft documents both the maximum of 100 Global Administrators and its recommendation to maintain two to four of them in its Microsoft 365 administrator roles guidance. Additional privileged-access and role-assignment guidance is available in Microsoft Entra role-based access control best practices.

QUESTION NO: 42

What is an Asset in Microsoft Purview?

A. A software application used to process data

B. A hardware device used to store data

C. A user account with access to data

D. A piece of data or a collection of related data

ANSWER: D

Explanation:

In Microsoft Purview, an asset is a piece of data or a collection of related data that is represented in the Microsoft Purview Data Catalog. Assets are the cataloged data resources that users discover, search, understand, and govern across the organization. Depending on the source that is scanned or registered, an asset can represent items such as a database, table, file, folder, Power BI report, or other data entity. Purview captures and presents metadata for these assets, including descriptions, schema details, classifications, contacts, and lineage information where supported. This catalog-based representation helps data consumers identify relevant and trustworthy data without needing to know its underlying location or technical implementation in advance. The asset's metadata can also be enriched by data stewards to improve discoverability and clarify business context. Microsoft describes the Data Catalog as an environment for finding and understanding enterprise data assets, while its search and browse experience enables users to locate those assets and inspect their associated metadata. See the Microsoft Purview Data Catalog documentation and search and browse the Microsoft Purview Data Catalog.

QUESTION NO: 43

Your company has a Microsoft Entra tenant named contoso.com and a Microsoft 365 subscription. All users use Windows 10 devices to access Microsoft 365 apps. All the devices are in a workgroup.

You plan to implement passwordless sign-in to contoso.com.

You need to recommend changes to the infrastructure for the planned implementation. What should you include in the recommendation?

A. Deploy the Microsoft Entra Connect provisioning agent.

B. Join all the devices to contoso.com.

C. Deploy Microsoft Entra Application Proxy.

D. Deploy the Microsoft Authenticator app.

ANSWER: D

Explanation:

Deploy the Microsoft Authenticator app. Microsoft Entra ID supports passwordless authentication through Microsoft Authenticator phone sign-in. After users register the app and their organization enables the Microsoft Authenticator authentication method, users can approve sign-in requests with a biometric gesture, such as fingerprint or face recognition, or with the device PIN. This replaces entering the account password during supported sign-in flows while retaining strong, phishing-resistant multifactor verification through number matching and device-bound credentials.

The devices being in a workgroup does not prevent users from using Microsoft Authenticator for passwordless access to Microsoft 365. The essential infrastructure change for this approach is making the Authenticator app available on users' mobile devices and configuring the corresponding authentication method in the Microsoft Entra admin center. Administrators can scope the method to selected users or groups before broad deployment, and users must complete registration before they can use phone sign-in. Microsoft documents the setup and user registration process at Enable Microsoft Authenticator

passwordless phone sign-in. For supported passwordless methods and deployment considerations, see Passwordless authentication options.

QUESTION NO: 44

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

A Built-in protection preset security policy is applied to the subscription.

Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Anti-malware

B. Safe Attachments

C. Safe Links

D. Anti-phishing

E. Anti-spam

ANSWER: B C

Explanation:

Safe Attachments and Safe Links are applied by the Built-in protection preset security policy. Built-in protection is Microsoft's default Defender for Office 365 protection level for recipients who are not covered by Standard or Strict preset security policies or by custom Safe Links and Safe Attachments policies. It is designed to ensure baseline protection without requiring an administrator to configure or assign those policies manually.

Safe Attachments protects email recipients from malicious files by using detonation and analysis capabilities before potentially dangerous attachments are delivered. Safe Links provides time-of-click protection by evaluating URLs in supported email messages and Office applications, helping prevent users from reaching known malicious destinations even when a link was initially delivered as benign.

Microsoft documents that Built-in protection includes the Safe Links and Safe Attachments policy settings. The preset-policy model also ensures that its protection is automatically available where more specific preset or custom policies do not take precedence. See Preset security policies in Microsoft Defender for Office 365 and Ensure that everyone has Safe Links and Safe Attachments protection.

QUESTION NO: 45

What is Azure Active Directory in Microsoft 365?

A. A cloud-based identity and access management service

B. A file storage service

C. A virtualization service for hosting virtual machines

D. A feature for configuring user access to Microsoft 365 services

ANSWER: A

Explanation:

A cloud-based identity and access management service is correct. Azure Active Directory was renamed Microsoft Entra ID and is the cloud-based directory and identity platform that underpins authentication and authorization for Microsoft 365. It stores and manages organizational identities, including users, groups, devices, and application service principals. When a

user signs in to Microsoft 365, Microsoft Entra ID validates the identity and provides the access controls needed to use services such as Exchange Online, SharePoint Online, Microsoft Teams, and integrated software-as-a-service applications.

Administrators use this service to manage user accounts and group membership, enable single sign-on, configure multifactor authentication, apply Conditional Access policies, and govern access to organizational resources. Its identity and access management capabilities allow an organization to determine who can sign in, under which conditions they can sign in, and which cloud resources they can access. Microsoft describes Microsoft Entra ID as a cloud-based identity and access management service that helps users access both Microsoft resources and external applications. See the Microsoft Entra ID overview and Microsoft's Microsoft 365 identity and device access overview.

QUESTION NO: 46

Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages

and documents. Users in other departments must not be restricted.

What should you do?

A. Create a data loss prevention (DLP) policy that has a Content is shared condition.

B. Modify the safe links policy Global settings.

C. Create a data loss prevention (DLP) policy that has a Content contains condition.

D. Create a new safe links policy.

ANSWER: D

Explanation:

Create a new safe links policy is correct because Safe Links in Microsoft Defender for Office 365 provides time-of-click protection for URLs in email messages and supported Office applications. When a protected user selects a hyperlink, Safe Links checks the destination against Microsoft threat intelligence at that time, including URLs whose reputation may have changed after the email or document was delivered. Access can be blocked when the destination is malicious or otherwise determined to be unsafe.

A separate Safe Links policy can be targeted to the research department by assigning the policy to the appropriate users, groups, or accepted domains. This provides the required scoped protection without applying the restriction to users in other departments. Policy targeting and priority enable an organization to use different Safe Links settings for distinct groups of users. Microsoft 365 E5 includes Microsoft Defender for Office 365 Plan 2, which supports Safe Links protection. For implementation details, see Safe Links in Microsoft Defender for Office 365 and Set up Safe Links policies.

QUESTION NO: 47

Which PowerShell command can be used to enable or disable a user's access to Microsoft 365 services?

A. Set-MsolUser

B. Set-MsolUserLicense

C. Set-MsolGroup

D. Set-MsolRoleMember

ANSWER: A

Explanation:

Set-MsolUser can enable or disable a user's sign-in access to Microsoft 365 services through its `BlockCredential` parameter. An administrator sets `-BlockCredential $true` to block the account from authenticating to Microsoft online services. This is useful when an employee leaves the organization, when an account is suspected of compromise, or whenever access must be stopped immediately without deleting the user or removing their data. Setting `-BlockCredential $false` removes that sign-in block and allows the user to authenticate again, provided the account meets all other access requirements, such as having an appropriate license and satisfying any applicable Conditional Access policies.

For example, `Set-MsolUser -UserPrincipalName user@contoso.com -BlockCredential $true` blocks the specified user's credentials. The cmdlet updates properties of a user object in the Microsoft Online (MSOnline) service, including the credential-blocking setting. Microsoft's reference documents the `BlockCredential` parameter and its use for preventing sign-in. For current administrative guidance on blocking and unblocking users in the Microsoft 365 admin center, see Set-MsolUser and Block user accounts in Microsoft 365.

QUESTION NO: 48

What is a Privileged Access Management (PAM)?

A. It's a machine-learning algorithm that detects and blocks threats to privileged accounts.

B. It's a security feature that controls access to privileged resources in Microsoft 365 services.

C. It's a proactive technique that allows organizations to monitor and control privileged access across their environment.

D. It's a feature of Azure AD that manages user and group access to resources.

ANSWER: B

Explanation:

It's a security feature that controls access to privileged resources in Microsoft 365 services. Privileged Access Management in Microsoft 365 is a security capability designed to provide granular, just-in-time control over highly sensitive administrative tasks. Rather than permanently assigning powerful permissions, an administrator can request access to perform a protected operation. The request is evaluated against the applicable access policy and can require approval before access is activated. When approved, the elevation is limited to the authorized task and a defined time period.

This model implements least privilege by reducing persistent administrative access, sometimes described as zero standing access. It also provides governance and accountability for actions that could have a significant organizational impact, including certain privileged tasks in Exchange Online. PAM is therefore specifically about controlling and governing access to privileged resources and operations; its essential characteristics are policy-based requests, optional approvals, scoped access, and time-limited elevation. Microsoft documents PAM as providing granular access control over privileged admin tasks in Microsoft 365. For implementation details and the supported workload scope, see Privileged access management in Microsoft 365 and Configure privileged access management.

QUESTION NO: 49

You have a Microsoft 365 subscription.

You need to configure a compliance solution that meets the following requirements:

Defines sensitive data based on existing data samples

Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a trainable classifier

B. a sensitive info type

C. an insider risk policy

D. an adaptive policy scope

E. a data loss prevention (DLP) policy

ANSWER: A E

Explanation:

A trainable classifier is required to define the data of concern from existing sample content. In Microsoft Purview, trainable classifiers use example items to learn and recognize a category of content, including content that may not have a consistent pattern such as a fixed identifier or regular expression. After training and publishing, the classifier becomes available for use as a condition in supported Purview compliance policies.

A data loss prevention (DLP) policy provides the enforcement mechanism. A DLP policy can evaluate content in Exchange email and SharePoint, use a trainable classifier in its rule conditions, and apply protective actions when content matches the classifier. Those actions can restrict access to SharePoint content or block email messages, including scenarios intended to prevent external sharing. This combines sample-based detection with automatic protection in the required Microsoft 365 workloads. Microsoft documents the classifier lifecycle and its use in DLP at Microsoft Purview trainable classifiers. For DLP policy capabilities and supported protection across Exchange and SharePoint, see Learn about data loss prevention.

QUESTION NO: 50

What is Azure AD Application Proxy?

A. A tool that enables on-premises applications to be published securely to users outside the corporate network

B. A tool that enables IT administrators to manage user accounts and groups

C. A service that provides real-time threat detection and remediation

D. An authentication mechanism that uses multi-factor authentication

ANSWER: A

Explanation:

A tool that enables on-premises applications to be published securely to users outside the corporate network is correct. Now named Microsoft Entra Application Proxy, Azure AD Application Proxy is a Microsoft Entra ID feature that provides remote access to private, on-premises web applications. Organizations deploy lightweight connectors within their internal network. The connectors create outbound connections to the Application Proxy service, so administrators do not need to open inbound firewall ports or expose the application directly to the internet.

When a user accesses a published application, Microsoft Entra ID authenticates the user and applies the organization's identity and access controls before brokering the connection to the internal application. This enables capabilities such as single sign-on, Conditional Access, and multifactor authentication for eligible applications. It is particularly useful for providing secure external access to legacy or line-of-business web applications while retaining centralized identity governance and security controls. Microsoft documents Application Proxy as a secure way to publish on-premises applications for remote users through Microsoft Entra ID. See What is Microsoft Entra Application Proxy? and Microsoft Entra Application Proxy documentation.

QUESTION NO: 51

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's

Microsoft SharePoint site.

What should you do?

A. From the SharePoint admin center, modify the sharing settings.

B. From the SharePoint site, create an alert.

C. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.

D. From the Microsoft 365 Defender portal, create an alert policy.

ANSWER: D

Explanation:

From the Microsoft 365 Defender portal, create an alert policy. An alert policy is designed for monitoring defined Microsoft 365 user and administrator activities and generating an alert, including email notifications to designated recipients, when those activities occur. For this requirement, the policy can be scoped to the relevant SharePoint workload and configured around SharePoint sharing activity, such as creating a sharing invitation or sharing a file or folder. The policy can also be narrowed by the user accounts in the Human Resources department and the relevant SharePoint site, so the HR manager receives notifications only for the required events. This directly addresses an operational notification requirement: detect a sharing event and notify a responsible person. Microsoft documents that alert policies use conditions based on activities and can send email notifications when an alert is generated. SharePoint sharing operations are also recorded Microsoft 365 audit activities, providing the events that can be monitored. See Alert policies in Microsoft Purview and Sharing and access-request audit activities.

QUESTION NO: 52

Which PowerShell command can be used to retrieve a list of all licenses available in a Microsoft 365 tenant?

A. Get-MsolAccountSku

B. Get-OnPremisesOrganizations

C. Get-TeamFunSettings

D. Get-MsolGroup

ANSWER: A

Explanation:

Get-MsolAccountSku retrieves the Microsoft 365 subscription SKUs held by a tenant when connected through the MSOnline PowerShell module. A SKU represents a license product or subscription available to the organization. The cmdlet returns tenant licensing inventory information such as the account SKU identifier and unit counts, including enabled (ActiveUnits), assigned (ConsumedUnits), and warning units. Administrators can use those values to identify the license products the tenant owns and determine licensing capacity before assigning services to users.

This cmdlet is the established answer for environments and exam material using the MSOnline module. Microsoft has since shifted license-management automation toward the Microsoft Graph PowerShell SDK, where `Get-MgSubscribedSku` provides the current Graph-based method to retrieve subscribed SKUs. Nevertheless, Get-MsolAccountSku directly fulfills the question's request and remains the appropriate selection among the supplied commands. For Microsoft's licensing-inventory guidance and the modern API equivalent, see View licenses and services with Microsoft 365 PowerShell and List subscribedSkus.

QUESTION NO: 53

You have a Microsoft 365 E5 subscription.

Your company s Microsoft Secure Score recommends the actions shown in the following exhibit.

You select Create Safe Links policies for email messages and change Status to Risk accepted in the Status & action plan settings.

How does the change affect the Secure Score?

A. remains the same

B. increases by 1 point

C. increases by 9 points

D. decreases by 1 point

E. decreases by 9 points

ANSWER: A

Explanation:

remains the same is correct. Microsoft Secure Score measures an organization's security posture by awarding points when Microsoft can detect that a recommended security configuration or activity has been implemented. Changing an improvement action's tracking status to *Risk accepted* documents an administrative decision to acknowledge and accept the risk associated with not implementing that recommendation. It does not enable Safe Links protection, create a Safe Links policy, or otherwise satisfy the technical signals Secure Score uses to award points.

The Status & action plan setting is therefore useful for governance: it lets administrators record the organization's decision and, where applicable, document a plan or rationale for handling the recommendation. However, it is not a compensating control and does not alter the achieved security configuration. Consequently, the Secure Score does not gain or lose points merely because the recommendation is marked as risk accepted. Points change when the underlying improvement action is implemented and detected, or when the relevant security state changes. Microsoft describes the available improvement-action statuses and their purpose in Manage improvement actions in Microsoft Secure Score. For the Safe Links configuration that would provide the protective control, see Safe Links in Microsoft Defender for Office 365.

QUESTION NO: 54

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: B D

Explanation:

A compliance policy is required to define the minimum device-health conditions that Windows devices must satisfy. In Microsoft Intune, Windows compliance policies can evaluate password requirements, encryption status, and Microsoft Defender Antimalware settings, including whether real-time protection is enabled. Intune uses the results of these checks to assign a compliance state to each enrolled device. This directly provides the mechanism for identifying devices that satisfy the organization's required security posture. See Windows device compliance settings in Intune.

A conditional access policy is required to enforce the access consequence based on that compliance state. The policy can target the relevant users and cloud applications, then require a device to be marked as compliant before access is granted. When Intune reports that a device does not meet one or more configured requirements, Conditional Access can block that device from accessing the protected Microsoft 365 tenant resources. This pairing lets Intune assess device compliance and Microsoft Entra Conditional Access use that assessment during sign-in and resource access decisions. For implementation guidance, see Require device compliance with Conditional Access.

QUESTION NO: 55

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 Defender XDR portal, create a device group.

C. From the Microsoft Endpoint Manager admin center, create a device category.

D. From the Microsoft Entra ID admin center, create a dynamic device group.

ANSWER: B

Explanation:

From the Microsoft Defender XDR portal, create a device group. Device groups in Microsoft Defender for Endpoint provide a direct way to logically scope devices by using membership rules based on device properties, including the operating system. Create a group whose membership criteria identifies Windows 10 devices, then use that device group when configuring the incident email notification rule. This lets Defender evaluate alerts against the group automatically, so future Windows 10 devices that meet the defined rule are included without requiring individual device selection or ongoing manual updates. Device groups are also the native Defender for Endpoint mechanism for organizing and filtering devices for security operations and access-related scenarios. The incident email notification configuration supports limiting notifications to alerts associated with selected device groups, which satisfies the requirement to notify only for incidents involving Windows 10 devices. Creating the device group first establishes the reusable scope that the notification rule requires. For configuration details, see Create and manage device groups and Configure email notifications for alerts and vulnerabilities.

QUESTION NO: 56

You have a Microsoft 365 E5 subscription.

You need to configure a Microsoft Purview eDiscovery solution for a legal investigation. The solution must prevent selected users from permanently deleting Exchange Online mailbox content and SharePoint Online files that are relevant to the investigation.

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

NOTE: Each correct selection is worth one point.

A. Create an eDiscovery case.

B. Create a hold policy.

C. Create a sensitivity label.

D. Create an audit retention policy.

E. Create a data loss prevention (DLP) policy.

ANSWER: A B

Explanation:

Create an **eDiscovery case** to organize the investigation and its associated custodians, searches, holds, and review sets. A case provides the management boundary for legal and compliance personnel working on the matter.

Create a **hold policy** in the eDiscovery case and apply it to the relevant custodians and data sources. A hold preserves matching content in supported Microsoft 365 locations, including Exchange mailboxes and SharePoint sites, even when users edit or delete the original content. Retention policies and sensitivity labels have separate information-governance purposes and do not provide the case-specific preservation workflow required for an investigation.

For more information, see Microsoft Purview eDiscovery solutions and Create and manage eDiscovery cases.

QUESTION NO: 57

You have a Microsoft 365 subscription.

You need to configure a Microsoft Entra Conditional Access policy that requires multifactor authentication when users access Microsoft 365 from outside the corporate network.

Which two policy components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure the Locations condition.

B. Configure the Require multifactor authentication grant control.

C. Configure a device filter.

D. Configure an app enforced restrictions session control.

E. Configure a sign-in frequency session control.

ANSWER: A B

Explanation:

Configure a **Locations** condition and exclude the named location that represents the corporate network. This causes the policy to apply to sign-ins originating outside that trusted location.

Configure the **Require multifactor authentication** grant control. When targeted users access the selected cloud applications and the location condition is met, Microsoft Entra ID requires the additional authentication factor before access is granted.

Device filters and session controls can be used for other access requirements, but they do not define the required network-based MFA behavior. For more information, see Conditional Access conditions and Conditional Access grant controls.

QUESTION NO: 58

You have a Microsoft 365 E5 subscription.

You are evaluating Microsoft Defender for Cloud Apps.

Which two types of policy rely on Conditional Access App Control? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. app discovery policy

B. OAuth app policy

C. access policy

D. file policy

E. session policy

F. activity policy

ANSWER: C E

Explanation:

access policy and **session policy** rely on Conditional Access App Control in Microsoft Defender for Cloud Apps. Conditional Access App Control works with Microsoft Entra Conditional Access to route a user's browser session through Defender for Cloud Apps, where controls can be applied in real time to supported cloud applications. An access policy uses this integration to control whether a session can access an app based on conditions such as the user, device state, network location, or risk-related criteria. This enables organizations to allow or block access at the point a user attempts to open an app.

A session policy uses the same Conditional Access App Control integration to monitor and govern actions during an active browser session. For example, it can prevent downloading sensitive files to an unmanaged device, require files to be protected before download, or monitor specific user activities. The Conditional Access policy is the mechanism that brings the applicable web session into the Defender for Cloud Apps reverse-proxy control path, after which the selected access or session policy is enforced. For implementation details, see Conditional Access App Control deployment and access and session policies documentation.

QUESTION NO: 59

You have a Microsoft 365 E5 subscription that uses Microsoft Defender Vulnerability Management.

You identify a critical software vulnerability on several devices.

You need to assign the remediation work to the IT operations team and track the remediation status from the Microsoft Defender portal.

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

NOTE: Each correct selection is worth one point.

A. Create a remediation request.

B. Assign the remediation request to the IT operations team.

C. Configure a Safe Links policy.

D. Create a Microsoft Purview retention policy.

E. Configure an access review.

ANSWER: A B

Explanation:

Create a remediation request is required to create a tracked remediation activity from a vulnerability or security recommendation in Microsoft Defender Vulnerability Management. A remediation request can include a due date, priority, notes, and a list of affected devices.

Assign the remediation request to the IT operations team is required to identify the team responsible for completing the work. Defender Vulnerability Management supports remediation tracking in the Microsoft Defender portal and can integrate with supported ticketing workflows for operational follow-up.

For more information, see Remediate vulnerabilities in Microsoft Defender Vulnerability Management.

QUESTION NO: 60

You have a Microsoft 365 E5 subscription.

You need to create a Microsoft Purview sensitivity label for documents and email messages that contain highly confidential information.

The label must ensure that only members of a specific Microsoft Entra ID group can open protected content. Access to protected content must expire after 30 days.

Which two label settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure encryption and assign permissions to the specified group.

B. Set user access to expire after 30 days.

C. Configure a retention period of 30 days.

D. Configure a watermark.

E. Configure external sharing settings for SharePoint sites.

ANSWER: A B

Explanation:

Configure encryption and assign permissions to the specified group is required because encryption in a sensitivity label controls who can open protected documents and email. Permissions can be assigned to users, groups, or domains, allowing the organization to restrict access to the designated Microsoft Entra ID group.

Set user access to expire after 30 days is required to limit how long recipients can access content protected by the label. The encryption settings for a sensitivity label include an option to set an access expiration period.

For more information, see Encryption for sensitivity labels.

QUESTION NO: 61

What is the maximum number of allowed Exchange ActiveSync devices per user in Microsoft 365?

A. 5 devices

B. 1 device

C. 25 devices

D. 10 devices

E. 100 devices

ANSWER: E

Explanation:

The maximum number of allowed Exchange ActiveSync devices per user mailbox in Exchange Online is **100 devices**. Exchange ActiveSync creates a device partnership between a mailbox and each mobile device or app that connects by using the protocol. The limit applies individually to each mailbox, not across the Microsoft 365 tenant. Consequently, a user can have up to 100 retained ActiveSync device partnerships associated with their mailbox.

Device partnerships may remain in the mailbox after a user replaces, resets, or stops using a phone or tablet. Administrators can review and remove obsolete mobile-device partnerships when needed, which frees capacity for new Exchange ActiveSync connections. This limit is specifically relevant to clients using Exchange ActiveSync; it is not a general limit on every type of Outlook or Microsoft 365 client connection. Microsoft documents the 100-device value in its Exchange Online service limits under Exchange ActiveSync limits. For details, see Exchange Online limits and Exchange ActiveSync in Exchange Online.

QUESTION NO: 62

You have a Microsoft 365 E5 subscription.

You need to use Microsoft Purview Audit to investigate changes to a user's mailbox permissions and identify who performed the changes.

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

NOTE: Each correct selection is worth one point.

A. Search the Audit solution in the Microsoft Purview portal.

B. Filter for Exchange mailbox permission activities.

C. Run a message trace.

D. Create an eDiscovery hold.

E. Create a retention label.

ANSWER: A B

Explanation:

Search the **Audit** solution in the Microsoft Purview portal. Audit records activities across Microsoft 365 services and includes details such as the user or administrator who performed an operation, the workload, the affected object, and the time of the event.

Filter the audit search by the relevant **Exchange mailbox permission activities** and specify the investigation time range. This narrows the results to operations associated with mailbox permission changes, such as adding or removing mailbox access, and helps identify the actor responsible for the change.

Message trace is used to investigate mail flow, and eDiscovery holds preserve content for legal matters. Neither is the appropriate source for determining who changed mailbox permissions. For more information, see Search the audit log and Audited activities.

QUESTION NO: 63

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named site1.

You need to ensure that site1 meets the following requirements:

• Retains all data for 10 years

• Prevents the sharing of data outside the organization

Which two items should you create and apply to site1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a retention policy

B. a data loss prevention (DLP) policy

C. a retention label policy

D. a sensitive info type

E. a retention label

F. a sensitivity label

ANSWER: A F

Explanation:

A retention policy and a sensitivity label provide the required controls for site1. A Microsoft Purview retention policy can be configured to retain SharePoint content for a fixed duration of 10 years and scoped specifically to the target SharePoint site. During that retention period, the policy preserves content even if users edit or delete files, helping the organization satisfy its records-retention requirement. Retention policies are appropriate when the retention setting must broadly cover content in a selected SharePoint location rather than depend on users manually classifying individual documents.

A sensitivity label configured for the Groups & sites scope can be applied to a SharePoint site and used to set the site's external-sharing control. The label can enforce an internal-only sharing setting, preventing site content from being shared with external users. This is a container-level setting, so it protects the sharing posture of the SharePoint site itself while the retention policy independently governs how long its content is retained. See Retention for SharePoint and OneDrive and Use sensitivity labels for Teams, Microsoft 365 groups, and SharePoint sites.

QUESTION NO: 64

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 Defender XDR portal

E. the Microsoft Entra admin center

ANSWER: D

Explanation:

The Microsoft Defender XDR portal is the appropriate portal to remove User1 from the Restricted entities list. Microsoft 365 restricts users who exceed outbound email-sending limits to help protect the service and recipients from spam, compromised-account activity, and other abusive sending patterns. An administrator can investigate and remediate this restriction from the Restricted entities page in the Defender portal. Navigate to **Email & collaboration**, then **Review**, and select **Restricted entities**; the direct URL is https://security.microsoft.com/restrictedentities. After selecting the restricted user, an authorized administrator can choose to unblock the account. Before unblocking, the administrator should verify that the account is secure, including reviewing recent sign-in and sending activity and resetting credentials or revoking sessions if compromise is suspected. The restricted-entities workflow is part of Microsoft Defender for Office 365 security operations, which centralizes investigation and response for email-related protections. Microsoft documents the process and the required permissions in Remove users from the Restricted entities page.

QUESTION NO: 65

What is the purpose of Microsoft Defender for Identity?

A. To protect against data loss and leaks

B. To protect against unauthorized access to on-premises resources

C. To protect against malware and phishing attacks

D. To monitor user activity and detect suspicious behavior

ANSWER: D

Explanation:

Microsoft Defender for Identity is designed to monitor identity-related signals and detect suspicious behavior that could indicate identity compromise or an advanced attack. It gathers data primarily from on-premises Active Directory Domain Services domain controllers and evaluates users, devices, and activities using behavioral analytics, threat intelligence, and detections. This helps security teams identify threats such as reconnaissance, credential theft, suspicious authentication activity, compromised accounts, and lateral movement in hybrid identity environments.

Therefore, **To monitor user activity and detect suspicious behavior** accurately describes its central purpose. Defender for Identity provides alerts and investigation context in the Microsoft Defender portal, allowing analysts to assess identity-related risks and respond to potentially malicious behavior. It is particularly relevant to protecting identity infrastructure because identities and credentials are frequent targets in enterprise attacks. Microsoft describes Defender for Identity as a cloud-based security solution that monitors and analyzes user behavior and information across an organization to identify suspicious activities and advanced threats. For implementation and product details, see What is Microsoft Defender for Identity? and Understand Microsoft Defender for Identity security alerts.

QUESTION NO: 66

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

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: A E

Explanation:

The User Administrator role grants User5 broad user-lifecycle administration capabilities, including deleting user accounts and resetting passwords, but its authority is constrained when the target account has higher privileged administrative permissions. Based on the roles shown in the table, User2 and User4 are within the management scope of a User Administrator. Therefore, User5 can delete User2 and User4, and can reset the passwords for those same accounts.

Microsoft documents that a User Administrator can manage users and groups and can reset passwords for non-administrators and certain limited administrator roles. This supports both permitted actions in the scenario: deletion is a standard user-management operation for manageable accounts, while password reset is explicitly granted for eligible users and limited admin targets. The privileged-role boundary remains important because it prevents this role from taking equivalent control over accounts holding more highly privileged directory roles. See the Microsoft Entra built-in roles permissions reference and Microsoft's privileged role permissions guidance for the applicable role-management and password-reset scope.

QUESTION NO: 67

What is the process for implementing Microsoft Purview?

A. Purchase a Microsoft 365 subscription

B. Create an Azure Active Directory tenant

C. Install the Microsoft Purview app on your computer

D. Deploy Microsoft Purview in your environment

ANSWER: D

Explanation:

Deploy Microsoft Purview in your environment is correct because Microsoft Purview implementation is an organizational deployment and configuration process, not a standalone product installation. An administrator starts by ensuring that the tenant has the required licensing and that the appropriate users have the necessary Microsoft Purview roles. The organization then enables and configures the Purview solutions that address its governance, risk, compliance, and information-protection requirements. Depending on the intended scope, this can include configuring sensitivity labels and label publishing, retention and records-management policies, audit capabilities, eDiscovery, data loss prevention policies, data classification, insider risk management, and relevant data connections. Administrators also define role groups and permissions so that compliance, security, legal, and records-management staff can administer only the capabilities appropriate to their responsibilities. Microsoft Purview is managed through cloud-based administrative experiences, principally the Microsoft Purview portal, and its deployment should be planned around the organization's data locations, regulatory obligations, and operational processes. Microsoft describes Purview as a family of governance, risk, and compliance solutions for managing and protecting data across Microsoft 365, Azure, and other environments. See the Microsoft Purview documentation and Microsoft Purview portal documentation.

QUESTION NO: 68

Which tool is used to manage Microsoft 365 licenses?

A. Microsoft Teams

B. Microsoft 365 admin center

C. Microsoft Intune

D. Azure Active Directory

ANSWER: B

Explanation:

Microsoft 365 admin center is the primary portal for managing Microsoft 365 subscription licenses. Administrators use it to see the licenses purchased by the organization, review how many are assigned or still available, and assign, remove, or update license assignments for users. License management is part of the standard user lifecycle process: when a user needs access to Microsoft 365 services, an administrator can assign an appropriate product license; when access is no longer required, the license can be removed and made available for reassignment. The admin center also supports assigning licenses to multiple users and managing the products and subscriptions that provide those licenses. Although identity information is integrated with Microsoft Entra ID, the Microsoft 365 admin center is the expected central management interface for Microsoft 365 licensing tasks in a Microsoft 365 administrator context. Microsoft documents the process for assigning licenses through the Users section of the Microsoft 365 admin center, including selecting users and choosing the licenses and service plans to enable. It also documents subscription and license management under the Billing area. See Assign licenses to users in the Microsoft 365 admin center and Manage licenses in the Microsoft 365 admin center.

QUESTION NO: 69

You have a Microsoft 365 E5 tenant.

Users store data in the following locations:

Microsoft Teams -

Microsoft OneDrive -

Microsoft Exchange Online -

Microsoft SharePoint -

You need to retain Microsoft 365 data for two years.

What is the minimum number of retention policies that you should create?

A. 1

B. 2

C. 3

D. 4

ANSWER: A

Explanation:

1 is correct. A single Microsoft Purview retention policy can apply the same retention configuration across multiple Microsoft 365 locations. For this requirement, configure one policy to retain content for two years and select the relevant locations: Exchange mailboxes, SharePoint sites, OneDrive accounts, Teams channel messages, and Teams chats. The policy's retention period is consistently applied to all included locations, which meets the stated requirement without needing separate policies per workload.

Although Teams content has distinct storage and processing architecture, Purview exposes Teams channel messages and Teams chats as selectable locations in a retention policy. Including these locations ensures that Teams messages are retained according to the policy, while selecting Exchange, SharePoint, and OneDrive protects data in those services. Separate policies are appropriate only when different locations require different retention periods, retention actions, scopes, or administrative configurations. Because every listed workload has the identical requirement of retaining data for two years, one policy is the minimum supported and manageable configuration. See Learn about retention policies and retention labels and Learn about retention for Microsoft Teams.

QUESTION NO: 70 - (SIMULATION)

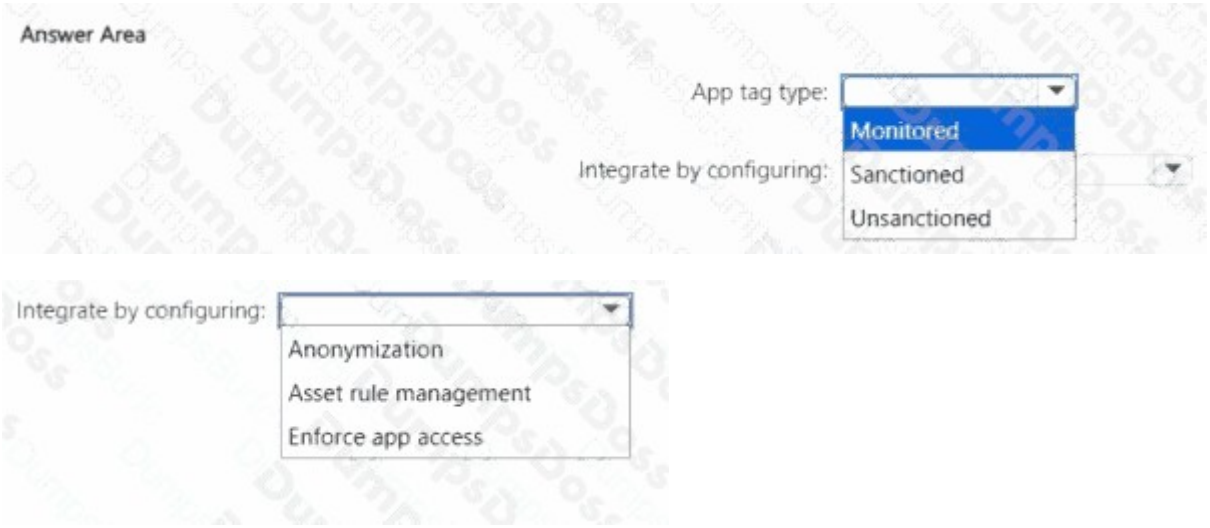
You have a Microsoft 365 E5 subscription.

The subscription contains users that have devices onboarded to Microsoft Defender for Endpoint. Defender for Endpoint is configured to forward signals to Microsoft Defender for Cloud Apps.

Cloud Discovery identifies a risky web app named App1.

You need to block users from connecting to App1 from Microsoft Edge. Users must be able to bypass the restriction.

Which type of app tag should you use, and what should you configure to integrate Defender for Endpoint with Defender for Cloud



ANSWER: See the explanation for the answer

Explanation:

App tag type: `Unsanctioned`

Integrate by configuring: `Enforce app access`

Tagging App1 as **Unsanctioned** identifies it as an application that should be restricted. Configuring **Enforce app access** for the Microsoft Defender for Endpoint integration enables Defender for Cloud Apps to enforce the unsanctioned-app restriction in Microsoft Edge. The Edge block experience permits users to bypass the warning when appropriate.

QUESTION NO: 71

You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.

Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. advanced hunting

B. security reports

C. digital certificate assessment

D. device discovery

E. attack surface reduction (ASR)

ANSWER: B E

Explanation:

security reports and **attack surface reduction (ASR)** are available with Microsoft Defender for Endpoint Plan 1, which is included with Microsoft 365 E3. Plan 1 is focused on preventive endpoint security: it provides visibility into the endpoint security posture and applies controls that reduce the opportunities for threats to execute, spread, or access protected resources.

Security reports provide administrators with centralized reporting in the Microsoft Defender portal. This helps them monitor the protection state of onboarded devices, review security-related information, and use that visibility to manage endpoint protection across the organization. ASR is a core Plan 1 capability that hardens endpoints against common attack techniques. It includes protections and controls such as attack surface reduction rules, network protection, web protection, exploit protection, controlled folder access, and device-control capabilities, depending on the applicable platform and configuration.

These capabilities align with the Plan 1 emphasis on next-generation protection, attack-surface reduction, centralized management, and security reporting. Microsoft documents the Plan 1 feature set at Microsoft Defender for Endpoint Plan 1 and provides configuration guidance at Attack surface reduction.

QUESTION NO: 72

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: B

Explanation:

Device1 and Device4 is correct. Delivery Optimization is a Windows client feature that controls the way devices obtain Microsoft content, including Windows updates, Microsoft Store app updates, and other downloads. Its policies include controls for peer-to-peer downloading, download mode, bandwidth limits, cache behavior, and peer selection. In Intune, these policies are deployed by using a Windows device configuration profile, specifically the Settings catalog or Delivery Optimization template for the Windows 10 and later platform.

Based on the operating systems shown in the device table, Device1 and Device4 are the supported Windows client devices. Because they are Intune-managed and run supported Windows 10 or Windows 11 client versions, they can receive and enforce the Delivery Optimization policy settings assigned through Intune. This is device-level configuration: after the profile is targeted to an appropriate device group, the Windows Delivery Optimization service applies the configured settings locally and uses them when handling eligible content downloads.

Microsoft documents both Intune's Delivery Optimization policy configuration and the Windows feature's supported behavior in Delivery Optimization settings in Microsoft Intune and Delivery Optimization for Windows.

QUESTION NO: 73

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 Microsoft Entra tenant.

Another administrator configures the domain to synchronize to Microsoft Entra ID.

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

You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Microsoft Entra ID.

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:

No is correct. The fact that every other user synchronizes successfully and that the excluded accounts are all located in one organizational unit strongly indicates that the OU has not been selected in Microsoft Entra Connect's domain and OU filtering configuration. OU filtering determines which Active Directory containers Microsoft Entra Connect imports into its connector space. If an OU is excluded, its users are not imported for synchronization processing, regardless of whether an outbound synchronization rule exists.

Outbound synchronization rules apply attribute and provisioning behavior after an object has been imported and evaluated by the synchronization engine. They do not add objects from an OU that the Active Directory connector is not configured to synchronize. To meet the goal, an administrator should modify the Microsoft Entra Connect configuration and include the relevant OU in the selected synchronization scope, then allow or initiate a synchronization cycle. Microsoft documents OU-based filtering as the mechanism for selecting the Active Directory OUs that are synchronized: Configure Microsoft Entra Connect Sync filtering. The synchronization architecture and connector-space processing model are also described in Microsoft Entra Connect Sync architecture.

QUESTION NO: 74 - (DRAG DROP)

: 219 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:

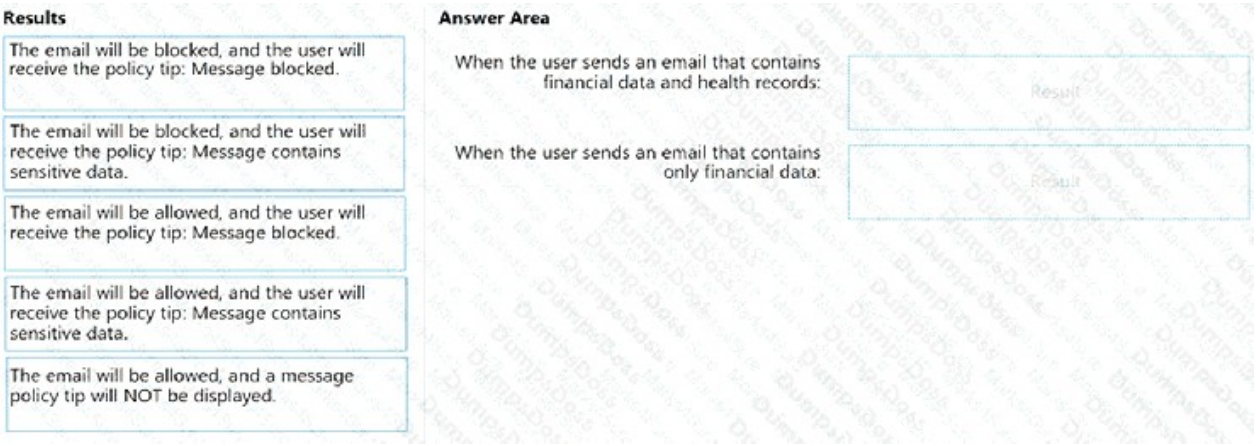
Use the following location: Exchange email.

Display the following policy tip text: Message contains sensitive data.

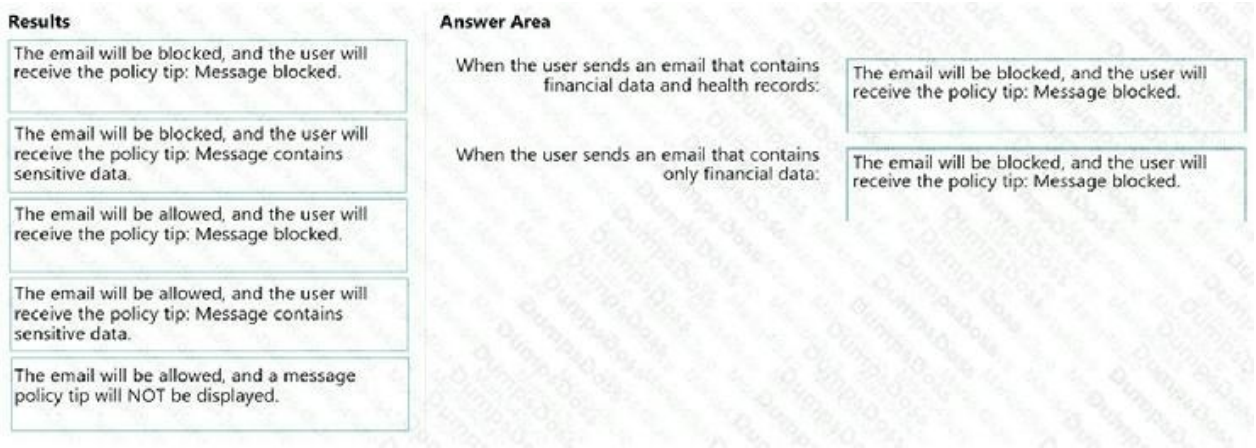
When a user sends an email, notify the user if the email contains health records.

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.



ANSWER:



Explanation:

Policy1 applies whenever an outgoing email contains financial data. Its configured action is to block the email, and its configured policy tip is “Message blocked.” Both described messages contain financial data: the first contains financial data

together with health records, and the second contains financial data without health records. Consequently, Policy1 produces the same block result and policy tip in both cases.

For the message that contains both financial data and health records, the health-record condition in Policy2 is also relevant. However, Policy2 is configured to notify the sender when health records are detected; it does not supersede the blocking action already configured by Policy1 for financial data. The blocking result from Policy1 remains the effective result for the message, and the user receives the “Message blocked.” policy tip.

For the message containing only financial data, the health-record notification condition does not apply because health records are absent. Policy1 still directly matches the financial-data condition and blocks the email. Therefore, the user receives the policy tip specified by Policy1, “Message blocked.” Exchange mail flow and DLP processing enforce the configured protective action for detected sensitive information. Microsoft documents the behavior and configuration of Exchange DLP policies at Data loss prevention in Exchange Server, and documents policy tips at Policy tips in Microsoft Purview Data Loss Prevention.

QUESTION NO: 75

What is Microsoft Cloud App Security?

A. It's a cloud-based threat protection service for corporate identities and accounts

B. It's a cloud access security broker (CASB)

C. It's a cloud platform for hosting Microsoft 365

D. It's an endpoint protection platform

ANSWER: B

Explanation:

Microsoft Cloud App Security, which has been renamed Microsoft Defender for Cloud Apps, is Microsoft’s cloud access security broker (CASB). A CASB provides visibility, control, and protection for an organization’s use of cloud applications and services. Defender for Cloud Apps helps administrators discover cloud app usage, including unsanctioned apps that can represent shadow IT, assess the risk of those apps, and apply governance actions. It also protects data and detects suspicious behavior across supported cloud services.

The service supports key CASB capabilities through several deployment approaches, including API connectors for cloud apps, traffic-log collection for cloud discovery, and Conditional Access App Control, which provides real-time session monitoring and controls. These capabilities enable organizations to investigate cloud activity, apply policies that protect sensitive information, and respond to threats involving cloud applications. Its role therefore extends across SaaS applications rather than being limited to identity protection or endpoint protection. Microsoft documents Defender for Cloud Apps as a CASB solution that provides visibility, control, and protection for cloud apps and data. See the Microsoft Defender for Cloud Apps overview and Conditional Access App Control documentation.