DUMPSBOSS.

Microsoft 365 Administrator Exam

Microsoft MS-102

Version Demo

Total Demo Questions: 49

Total Premium Questions: 712

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Deploy and manage a Microsoft 365 tenant	176
Topic 2, Implement and manage identity and access in Microsoft Entra	244
Topic 3, Manage security and threats by using Microsoft Defender XDR	161
Topic 4, Manage compliance by using Microsoft Purview	115
Topic 5, Mix Questions	16
Total	712

QUESTION NO: 1

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:

To block access to a specific malicious website such as www.contoso.com by using Microsoft Defender for Endpoint, you use custom indicators for URLs or domains. “Enable Custom network indicators” is required because Defender for Endpoint must be allowed to enforce custom network-based indicators, such as URL, domain, and IP address indicators. After that capability is enabled, “Create an indicator” is required so that www.contoso.com can be added as a URL/domain indicator with a block action. Once the indicator is created and enforced, supported onboarded devices can block network access to that destination through Microsoft Defender for Endpoint’s network protection and indicator enforcement capabilities. Microsoft documents this workflow as creating indicators for IP addresses, URLs, or domains and using them to allow, audit, warn, or block access, provided the required Defender for Endpoint prerequisites are configured. For more information, see Create indicators for IPs and URLs/domains and Manage indicators.

QUESTION NO: 2

How does Microsoft Purview help organizations manage compliance?

A. It automates compliance tasks

B. It ensures that all employees are trained on compliance regulations

C. It provides a centralized dashboard for compliance reporting

D. It conducts regular compliance audits

ANSWER: A

Explanation:

It automates compliance tasks is correct because Microsoft Purview provides integrated compliance and governance capabilities that reduce the amount of manual work required to identify, protect, retain, and manage organizational data. In Microsoft 365 environments, Purview can automatically discover and classify sensitive information, apply sensitivity and retention labels, support data loss prevention policies, and provide compliance-related workflows through solutions such as Microsoft Purview Compliance Manager. These capabilities help administrators operationalize compliance requirements instead of relying only on manual review or ad hoc processes. Microsoft describes Purview as a family of data governance, risk, and compliance solutions that helps organizations manage and protect data across their environment. Compliance Manager also helps simplify compliance by providing assessments, improvement actions, and a compliance score that tracks progress against regulatory and organizational requirements. For more details, see Microsoft Purview and Microsoft Purview Compliance Manager.

QUESTION NO: 3

What service can be used to manage SharePoint data with Microsoft Graph?

A. Power BI

B. Microsoft Teams

C. OneDrive

D. SharePoint

ANSWER: D

Explanation:

SharePoint is correct because Microsoft Graph includes a dedicated SharePoint API surface for working with SharePoint data and resources. Through Microsoft Graph, administrators and developers can access SharePoint sites, lists, list items, pages, document libraries, and related permissions by using Graph endpoints such as the site and list resources. This provides a unified REST API model for managing Microsoft 365 data, including SharePoint content, without needing to rely only on older SharePoint-specific APIs. For example, Microsoft Graph can enumerate SharePoint sites, retrieve lists from a site, read or update list items, and work with files stored in SharePoint document libraries through the Drive and DriveItem resources. Microsoft's SharePoint and Microsoft Graph documentation describes SharePoint as one of the Microsoft 365 services exposed through Graph for this type of management and data access. See the Microsoft Graph SharePoint overview at Microsoft Graph SharePoint resources and the site resource documentation at Microsoft Graph site resource type.

QUESTION NO: 4

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer

authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and

computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as DNS servers.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere,

Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.

Microsoft 365 Apps for enterprise applications must be installed from a network share only.

Disruptions to email access must be minimized.

Application Requirements -

Fabrikam identifies the following application requirements:

An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the

My Apps portal.

The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -

Fabrikam identifies the following security requirements:

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

The principle of least privilege must be used.

You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.

Which authentication strategy should you implement for the pilot projects?

A. pass-through authentication

B. pass-through authentication and seamless SSO

C. password hash synchronization and seamless SSO

D. password hash synchronization

ANSWER: C

Explanation:

password hash synchronization and seamless SSO is correct because it satisfies both key authentication requirements for the pilot. Password hash synchronization lets Microsoft Entra ID authenticate users directly in the cloud by using synchronized password hashes from on-premises Active Directory. This is important for Fabrikam because users must still be able to access Microsoft 365 cloud services even if on-premises Active Directory becomes unavailable. Microsoft identifies password hash synchronization as a sign-in method that provides high availability for cloud authentication and is commonly recommended when federation is not required. See Microsoft Entra password hash synchronization.

Seamless SSO complements password hash synchronization by automatically signing in domain-joined users when they are on the corporate network, helping meet the requirement that users be signed in to on-premises and cloud-based applications automatically. It works with password hash synchronization and does not require Active Directory Federation Services, which aligns with Fabrikam's plan not to implement identity federation. Microsoft documents this integration in Microsoft Entra Seamless Single Sign-On.

QUESTION NO: 5

What is Conditional Access in Azure AD?

A. A way to grant access to specific resources to specific users

B. A feature that allows users to authenticate with their phone

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

D. A feature that enforces access policies based on conditions such as network location or device state

ANSWER: D

Explanation:

A feature that enforces access policies based on conditions such as network location or device state is correct. In Microsoft Entra ID, formerly Azure AD, Conditional Access is the policy engine that evaluates signals during an access attempt and then applies access controls. These signals can include the user or group, target cloud app, device platform, device compliance or hybrid join state, location, sign-in risk, and client app. Based on those conditions, administrators can allow access, block access, or require additional controls such as multifactor authentication, a compliant device, approved client app, or terms of use. This makes Conditional Access a core Zero Trust control because it helps enforce "verify explicitly" decisions at the time users try to access Microsoft 365 and other integrated applications. Microsoft describes Conditional Access as bringing signals together, making decisions, and enforcing organizational policies. For more details, see Microsoft Entra Conditional Access overview and Conditional Access policies.

QUESTION NO: 6

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 and Enable single sign-on are the correct selections for this hybrid identity requirement. Password Hash Synchronization synchronizes a hash of users' on-premises Active Directory password hashes to Microsoft Entra ID, allowing cloud authentication while still using the same user credentials. It is also important for Microsoft Entra ID Protection because certain risk detections, including leaked credential detection, require password hash synchronization to compare exposed credentials against the synchronized password hash data. This makes it the best authentication foundation when Identity Protection support is required. See Microsoft's guidance on password hash synchronization.

Enable single sign-on should also be selected because Microsoft Entra seamless single sign-on automatically signs in domain-joined users when they are on the corporate network, reducing repeated credential prompts when accessing Microsoft 365 resources. Seamless SSO is specifically designed to work with Password Hash Synchronization and can be enabled through Microsoft Entra Connect as part of the sign-in configuration. Microsoft documents this capability in Microsoft Entra seamless single sign-on.

QUESTION NO: 7

What is the difference between an Azure AD group and an Azure AD security group?

A. Azure AD groups are used to organize users and devices, while Azure AD security groups are used for access control.

B. Azure AD groups can be used to assign licenses to users, while Azure AD security groups cannot.

C. Azure AD security groups can be used to assign permissions to resources, while Azure AD groups cannot.

D. There is no difference between an Azure AD group and an Azure AD security group.

ANSWER: A

Explanation:

Azure AD groups, now referred to in Microsoft documentation as Microsoft Entra groups, are directory objects used to collect users, devices, service principals, and sometimes other groups so they can be managed together. Within that broader concept, a security group is specifically intended for access control scenarios, such as granting permissions to applications, assigning access to resources, or managing role-based access in services that support group-based authorization. The statement "Azure AD groups are used to organize users and devices, while Azure AD security groups are used for access control" is therefore the best answer because it captures the practical distinction being tested: grouping is the general organizational capability, while security groups are designed to control access. Microsoft describes groups as a way to manage access to resources for a collection of users, and specifically identifies security groups as being used to manage member and computer access to shared resources. See Microsoft's guidance on Microsoft Entra groups and creating and managing groups for more detail.

QUESTION NO: 8

Which report should the New York office auditors view?

A. DLP policy matches

B. DLP false positives and overrides

C. DLP incidents

D. Top Senders and Recipients

ANSWER: C

Explanation:

DLP incidents is the correct report for auditors when they need to review the actual content items that triggered data loss prevention policy activity. In Microsoft Purview, DLP reporting distinguishes between activity summarized by policy or rule and activity shown as incidents. The incidents view is intended for investigating specific items that caused DLP matches, such as messages or files that contain sensitive information and triggered a DLP rule. This makes it the most appropriate choice for an audit-focused review, because auditors typically need to identify and examine the individual events or content items that were flagged, rather than only seeing aggregate policy-match trends. Microsoft documentation explains that DLP reports help administrators investigate DLP rule matches, false positives, and overrides, and incident-level reporting is used to identify the specific pieces of content that are problematic for DLP policies. For more information, see Microsoft's guidance on viewing DLP reports and the overview of Microsoft Purview Data Loss Prevention.

QUESTION NO: 9

You need to create the Safe Attachments policy to meet the technical requirements.

Which option should you select?

A. Replace

B. Enable redirect

C. Block

D. Dynamic Delivery

ANSWER: D

Explanation:

Dynamic Delivery is the correct selection for a Microsoft Defender for Office 365 Safe Attachments policy when the goal is to let recipients receive and read email immediately while attachments are still being scanned. With Dynamic Delivery, the message body is delivered first, and attachments are temporarily replaced with placeholders until Safe Attachments scanning completes. If the attachments are found to be safe, they are reattached to the message; if a malicious attachment is detected, Defender for Office 365 takes the configured protection action. This approach is commonly used to reduce mail delivery delays while still maintaining attachment detonation and malware protection. Microsoft describes Dynamic Delivery as a Safe Attachments action that delivers messages immediately without attachments and then reattaches clean attachments after scanning completes. This behavior aligns well with technical requirements that prioritize both user productivity and attachment protection. See Microsoft's documentation on Safe Attachments in Microsoft Defender for Office 365 and configuring Safe Attachments policies.

QUESTION NO: 10

What is Azure AD Domain Services?

A. A feature that enables single sign-on (SSO) for cloud applications.

B. A feature that synchronizes on-premises Active Directory with Azure AD.

C. A tool for managing Azure AD domain names.

D. A cloud-based domain controller for managing domain-joined Azure VMs.

ANSWER: D

Explanation:

A cloud-based domain controller for managing domain-joined Azure VMs is correct. Azure AD Domain Services, now called Microsoft Entra Domain Services, provides managed domain services in Azure without requiring administrators to deploy, patch, monitor, or maintain traditional Windows Server domain controllers. It creates a managed domain that supports common Active Directory Domain Services capabilities such as domain join, Group Policy, LDAP, Kerberos authentication, and NTLM authentication. This is especially useful for legacy applications and Azure virtual machines that require traditional domain services but need to run in Azure using identities synchronized from Microsoft Entra ID. Microsoft manages the domain controllers as part of the service, while administrators manage the domain configuration, users, groups, and access patterns needed by workloads. In practice, organizations use it to join Azure VMs to a managed domain and allow those VMs and applications to use familiar AD DS authentication and management features. See Microsoft's overview of Microsoft Entra Domain Services and its managed domain concepts.

QUESTION NO: 11

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:

From Windows PowerShell, run the Register-AzureADConnectHealthSyncAgent cmdlet is correct because an Azure AD Connect Health agent must be registered with the Microsoft Entra Connect Health service before the server can appear in the portal and report health data. If the server entry was removed from the service, re-registering the sync health agent from the affected server restores the association with the tenant and allows health data for Server1 to be uploaded and displayed again. From Server1, reinstall the Azure AD Connect Health agent is also correct because installing the agent includes the registration process with Microsoft Entra ID and recreates the server's presence in the Connect Health blade. In practice,

reinstallation is a full remediation path when the existing agent registration is missing, damaged, or removed, while the registration cmdlet is a more direct repair method when the agent binaries are already present. Microsoft documents that Connect Health agents are installed on the monitored servers and must be registered to send monitoring data to the service. See Microsoft Entra Connect Health agent installation and Microsoft Entra Connect overview.

QUESTION NO: 12

What is Microsoft Defender for Office 365?

A. It's a cloud-based threat protection service for email, collaboration, and file-sharing services

B. It's an identity and access management (IAM) system

C. It's an endpoint protection platform

D. It's a network security platform

ANSWER: A

Explanation:

It's a cloud-based threat protection service for email, collaboration, and file-sharing services is correct because Microsoft Defender for Office 365 is designed to protect Microsoft 365 workloads such as Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams from advanced threats. It provides capabilities such as anti-phishing, Safe Links, Safe Attachments, threat investigation, automated response, attack simulation training, and security reporting. In practical Microsoft 365 administration, it helps organizations detect, prevent, investigate, and respond to malicious content and attacker activity that targets users through email and collaboration channels. Microsoft describes Defender for Office 365 as protection against threats such as phishing, business email compromise, and malware, with additional tools for hunting, investigation, and remediation depending on the plan. This aligns directly with the wording that it is a cloud-based threat protection service for email, collaboration, and file-sharing services. For more detail, see Microsoft's overview of Microsoft Defender for Office 365 and the Defender for Office 365 documentation.

QUESTION NO: 13

What is Azure AD B2B collaboration?

A. A way to provide single sign-on (SSO) to external users

B. A way to manage external users in your Azure AD tenant

C. A way to implement multi-factor authentication for external users

D. A way to grant access to external users to resources in your organization

ANSWER: D

Explanation:

A way to grant access to external users to resources in your organization is correct. Azure AD B2B collaboration, now part of Microsoft Entra External ID capabilities, is designed to let an organization securely collaborate with people outside its tenant, such as partners, vendors, contractors, or customers. Those external users are typically invited as guest users and can then be granted access to specific applications, Microsoft 365 resources, Teams, SharePoint sites, or other protected resources according to the organization's policies. The key purpose is controlled resource access for external identities while allowing the organization to retain governance through features such as Conditional Access, access reviews, entitlement management, and guest user permissions. Microsoft describes B2B collaboration as a capability that enables secure sharing of company applications and services with guest users from other organizations while maintaining control over corporate data. For more details, see Microsoft's overview of Microsoft Entra B2B collaboration and guidance for adding guest users for B2B collaboration.

QUESTION NO: 14

You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.

Which authentication strategy should you implement for the pilot projects?

A. pass-through authentication

B. pass-through authentication and seamless SSO

C. password hash synchronization and seamless SSO

D. password hash synchronization

ANSWER: C

Explanation:

password hash synchronization and seamless SSO is correct because it satisfies both key requirements for the pilot projects without requiring identity federation. Password hash synchronization allows users' on-premises Active Directory password hashes to be synchronized to Microsoft Entra ID, so the sales department users can authenticate to Microsoft 365 workloads such as Exchange Online, SharePoint Online, Teams, and Skype for Business Online by using the same UPN and password they use on-premises. This is a standard cloud authentication approach supported by Microsoft Entra Connect and is appropriate when federation is not planned. Seamless SSO complements password hash synchronization by automatically signing users in when they are on corporate, domain-joined devices connected to the organization's network. That meets the requirement that users be signed in automatically to both on-premises and cloud-based applications after the migration. Microsoft specifically supports Seamless SSO with password hash synchronization, making this combination a suitable strategy for the staged pilot involving mailbox migration followed by Teams and Skype for Business enablement. For more information, see Password hash synchronization and Microsoft Entra seamless single sign-on.

QUESTION NO: 15

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

You create the alert policy shown in the following exhibit.

User2 runs a script that modifies a file in a Microsoft SharePoint library once every four minutes and runs for a period of two hours.

How many alerts will User1 receive?

A. 2

B. 5

C. 10

D. 25

E. 30

ANSWER: D

Explanation:

25 is correct because the SharePoint file modification activity occurs 30 times during the two-hour period, but the alert policy's notification behavior limits how many notifications User1 receives. A modification every four minutes for 120 minutes produces 120 / 4 = 30 matching activities. When an alert policy is configured to notify a recipient each time the monitored activity matches, each qualifying SharePoint file modification can generate an alert notification. However, Microsoft Purview alert policies can include a daily notification limit, which caps the number of email notifications sent to the configured recipients for that policy in a single day. With the policy shown applying to User2's "file modified" activity and the daily notification limit set to 25, User1 receives only the first 25 alert notifications even though 30 matching events occur. This behavior aligns with Microsoft's alert policy configuration model, where email notification settings and daily notification limits control how many alert emails are delivered. For more details, see Microsoft's documentation on alert policies in Microsoft Purview and the related guidance for email notifications for alert policies.

QUESTION NO: 16

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

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

Azure AD Connect has the following settings:

Password Hash Sync: Enabled -

Pass-through authentication: Enabled

You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the

internet is lost.

Which users should you identify?

A. none

B. User1 only

C. User1 and User2 only

D. User1, User2, and User3

ANSWER: D

Explanation:

User1, User2, and User3 is correct because Password Hash Sync is enabled in the hybrid identity configuration. With password hash synchronization, Azure AD Connect synchronizes a hash of each synchronized user's on-premises password hash to Microsoft Entra ID. This allows Microsoft Entra ID to validate user credentials in the cloud without needing to contact an on-premises domain controller at sign-in time. Pass-through authentication can be used during normal operations to validate passwords against on-premises Active Directory through authentication agents, but Microsoft recommends enabling Password Hash Sync alongside pass-through authentication as a backup sign-in method for resilience during an on-premises outage. Therefore, when connectivity between the on-premises Active Directory environment and the internet is lost, Microsoft Entra ID can still authenticate the users whose password hashes are available in the cloud, and cloud-managed users are authenticated directly by Microsoft Entra ID as well. Microsoft documents Password Hash Sync as a supported cloud authentication method and as a backup option for pass-through authentication scenarios: Microsoft Entra Password Hash Synchronization and Microsoft Entra Pass-through Authentication.

QUESTION NO: 17

You have a Microsoft 365 E5 subscription.

You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:

• Support KQL for querying data.

• Retain report data for at least one year.

What should you include in the recommendation?

A. a security report in Microsoft 365 Defender

B. Endpoint analytics

C. Microsoft 365 usage analytics

D. Azure Monitor workbooks

ANSWER: D

Explanation:

Azure Monitor workbooks is the correct recommendation because it provides an interactive reporting and visualization layer over Azure Monitor data, including data stored in a Log Analytics workspace. For application access monitoring in Microsoft 365 and Microsoft Entra ID, sign-in and audit logs can be sent to Azure Monitor Logs, where administrators can query the data by using Kusto Query Language. Workbooks can then use those KQL queries to build dashboards, reports, charts, and investigation views for application access activity. This meets the requirement to support KQL-based querying. The retention requirement can also be met because Log Analytics workspace retention is configurable and can be set to retain analytics data for at least one year, subject to the selected retention settings and licensing/cost configuration. Microsoft documents that workbooks support querying Azure Monitor data sources and that Log Analytics workspaces support configurable data retention. See Azure Monitor workbooks and Configure data retention in Log Analytics.

QUESTION NO: 18

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:

After a preservation lock is applied to a Microsoft Purview retention policy, the policy becomes immutable in ways that would weaken or remove its retention protections. However, administrators can still make changes that increase or broaden protection. **Add locations to the policy.** is correct because adding more locations expands the scope of the locked retention policy and does not reduce the compliance protection already in place for existing locations. **Extend the duration of the policy.** is also correct because increasing the retention period makes the policy more restrictive by preserving content for longer. This aligns with the purpose of Preservation Lock, which is designed for regulatory and compliance scenarios where retention settings must not be weakened after the lock is enabled. Microsoft describes Preservation Lock as preventing actions such as turning off the policy, deleting it, removing locations, or reducing retention, while allowing changes that make the policy more restrictive. For details, see Microsoft's guidance on Preservation Lock for retention policies and the broader documentation for Microsoft Purview retention policies and retention labels.

QUESTION NO: 19

Which of the following is NOT a method to add a domain to a Microsoft 365 tenant?

A. Adding an MX record to the DNS

B. Adding a TXT record to the DNS

C. Adding an A record to the DNS

D. Adding a CNAME record to the DNS

ANSWER: C

Explanation:

Adding an A record to the DNS is the correct choice because it is not used as a supported method for adding and verifying a custom domain in a Microsoft 365 tenant. When you add a domain in the Microsoft 365 admin center, Microsoft must confirm that you own the domain before it can be associated with the tenant. The standard ownership verification process uses a DNS record that Microsoft provides during setup, most commonly a TXT record, and Microsoft also documents MX-based verification in supported scenarios. An A record maps a host name directly to an IPv4 address, which is useful for pointing web traffic to a server, but it does not provide the kind of Microsoft-specific ownership proof required during the Microsoft 365 domain-add process. Therefore, adding an A record is not considered a valid method to add or verify a domain for Microsoft 365. See Microsoft's guidance on adding a domain in the Microsoft 365 admin center and DNS record requirements in Create DNS records at any DNS hosting provider.

QUESTION NO: 20 - (DRAG DROP)

DRAG DROP

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

You need to configure policies to meet the following requirements:

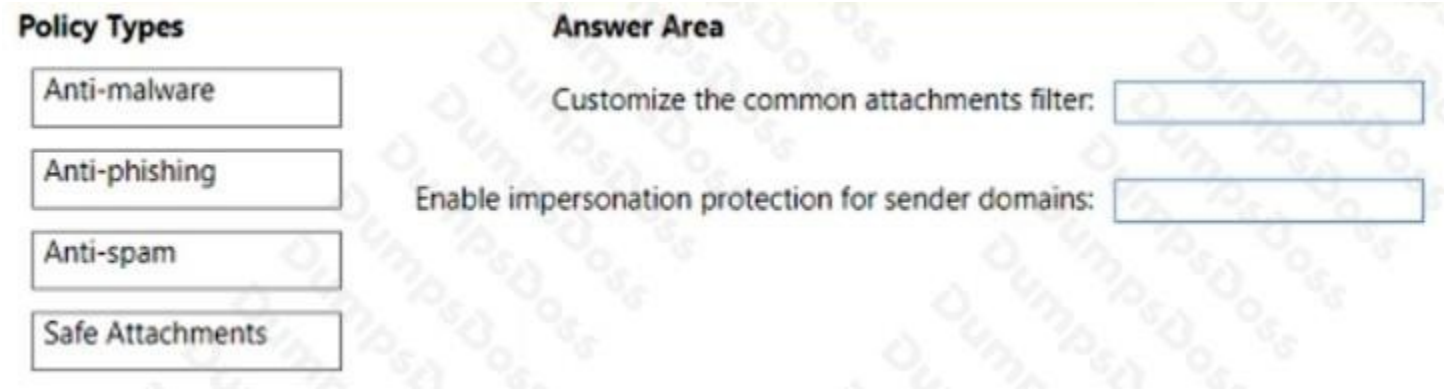
Customize the common attachments filter.

Enable impersonation protection for sender domains.

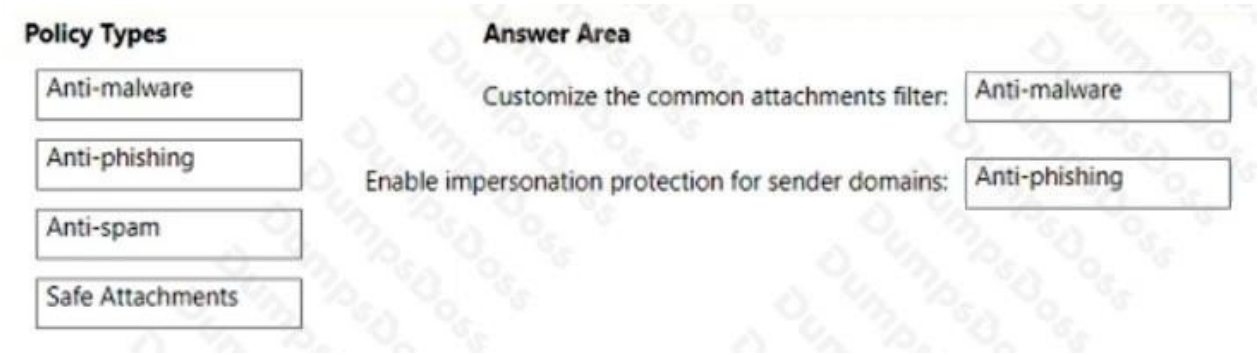
Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each

policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



ANSWER:



Explanation:

The correct configuration uses two different policy types in Microsoft Defender for Office 365 and Exchange Online Protection. The common attachments filter is part of anti-malware policy settings. In the Microsoft Defender portal, anti-malware policies include the ability to enable the common attachments filter and customize the file types that are blocked, such as executable or script-based attachment extensions. This is designed to stop potentially dangerous file attachments before they reach users' mailboxes. Microsoft documents this under anti-malware policies in Exchange Online Protection: Anti-malware protection in EOP.

Impersonation protection for sender domains is configured in anti-phishing policies. In Microsoft Defender for Office 365, anti-phishing policies can protect specific users and domains from impersonation attempts. Domain impersonation protection checks whether a sender is trying to look like a trusted domain and then applies the configured action when impersonation is detected. This feature is managed as part of anti-phishing policy configuration, not anti-malware, anti-spam, or Safe Attachments. Microsoft describes these controls in its guidance for anti-phishing policies: Anti-phishing policies in Microsoft Defender for Office 365.

QUESTION NO: 21

You need to configure Office on the web to meet the technical requirements.

What should you do?

A. Assign the Global reader role to User1.

B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.

C. Configure an auto-labeling policy to apply the sensitivity labels.

D. Assign the Office apps admin role to User1.

ANSWER: B

Explanation:

Enable sensitivity labels for Office files in SharePoint Online and OneDrive is correct because Office on the web relies on SharePoint Online and OneDrive integration with Microsoft Purview Information Protection to recognize, display, and enforce sensitivity labels on stored Office documents. When this integration is enabled, Word, Excel, and PowerPoint for the web can work with labeled files, including scenarios where labels apply protection such as encryption, and Microsoft 365 services can process labeled content more effectively for features such as coauthoring, search, eDiscovery, and data loss prevention. This is the required tenant-level configuration for enabling sensitivity label support for Office files stored in SharePoint and OneDrive, which is the storage platform behind Office on the web. Microsoft documents this capability in its guidance for enabling sensitivity labels for Office files in SharePoint and OneDrive and in the broader guidance for sensitivity labels in Office apps.

QUESTION NO: 22

You have a Microsoft 365 subscription.

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

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

You configure Tenant properties as shown in the following exhibit.

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

A. User1 only

B. User2 only

C. User3 only

D. User1 and User2 only

E. User2 and User3 only

ANSWER: B

Explanation:

User2 only is correct because Microsoft uses the Global privacy contact configured in Microsoft Entra tenant properties as the primary contact for privacy-related notifications, including data breach communications. In the tenant properties shown in the exhibit, User2 is configured as the Global privacy contact, so Microsoft will contact User2 for a tenant data breach notification. This setting is specifically intended for privacy and breach-related communications, and it takes precedence over relying on administrative role membership for this type of contact. Microsoft documentation states that the Global privacy contact is the person Microsoft contacts if there is a data breach; only if no Global privacy contact is listed does Microsoft contact the tenant's global administrators instead. You can find this behavior described in Microsoft's guidance for adding privacy information to an organization in Microsoft Entra ID: Add privacy info for your organization.

QUESTION NO: 23

What is the difference between Azure AD and Active Directory Domain Services (AD DS)?

A. Azure AD and AD DS are two different names for the same product.

B. Azure AD is a cloud-based directory service, while AD DS is a Windows Server-based directory service.

C. Azure AD is only available in the cloud, while AD DS can be deployed on-premises.

D. Azure AD is only for user authentication, while AD DS is for user authentication and resource management.

ANSWER: B

Explanation:

Azure AD is a cloud-based directory service, while AD DS is a Windows Server-based directory service. is correct because it captures the fundamental architectural and operational distinction between the two identity platforms. Azure AD, now Microsoft Entra ID, is Microsoft's cloud identity and access management service. It is designed for authentication and authorization to cloud services such as Microsoft 365, Azure, and SaaS applications, and it uses modern identity protocols such as OAuth 2.0, OpenID Connect, and SAML. Active Directory Domain Services, by contrast, is a traditional directory service role that runs on Windows Server domain controllers and provides domain join, Group Policy, Kerberos/NTLM authentication, LDAP directory services, and management of on-premises network resources. Microsoft's comparison guidance describes these as related but distinct identity services intended for different environments and scenarios. See Compare Active Directory to Microsoft Entra ID and Active Directory Domain Services overview for Microsoft's official descriptions.

QUESTION NO: 24

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 is the correct set of Microsoft 365 tenant types in this context. A paid tenant is the production Microsoft 365 environment an organization uses after purchasing subscriptions and assigning licenses to users. A trial tenant

is a temporary Microsoft 365 environment created to evaluate Microsoft 365 services before purchase; Microsoft documents the process to try or buy Microsoft 365 subscriptions and then move from evaluation to paid use. A developer tenant is typically provided through the Microsoft 365 Developer Program as a Microsoft 365 E5 developer sandbox, intended for development, testing, and learning rather than production workloads. These three tenant categories are commonly used when distinguishing between production use, evaluation use, and development/testing use in Microsoft 365 administration. See Microsoft's guidance on trying or buying Microsoft 365 subscriptions and the Microsoft 365 Developer Program.

QUESTION NO: 25

What is Microsoft Purview used for?

A. To manage compliance

B. To manage data storage

C. To manage security and threats

D. To manage identity and access

ANSWER: A

Explanation:

To manage compliance is the correct answer because Microsoft Purview provides Microsoft 365 organizations with a unified set of tools for understanding, governing, protecting, and managing data across the environment. In the Microsoft 365 administrator context, Purview is commonly associated with compliance capabilities such as data loss prevention, information protection, retention, eDiscovery, audit, insider risk management, communication compliance, and Compliance Manager. These features help administrators discover sensitive information, apply governance and protection policies, investigate compliance events, and assess the organization's alignment with regulatory and internal requirements. Microsoft describes Purview as a family of data governance, risk, and compliance solutions that helps organizations manage and protect data across Microsoft 365 and other locations. For MS-102, the key takeaway is that Purview is the Microsoft platform used for compliance and data governance administration. See Microsoft's overview of Microsoft Purview and Microsoft Purview Compliance Manager for more detail.

QUESTION NO: 26

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

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Exchange Administrator

You need to compare the permissions of each role. The solution must minimize administrative effort.

Which portal should you use?

A. the Microsoft Purview compliance portal

B. the Microsoft 365 admin center

C. the Microsoft 365 Defender portal

D. the Microsoft Entra admin center

ANSWER: D

Explanation:

the Microsoft Entra admin center is correct because Azure AD is now Microsoft Entra ID, and Microsoft Entra administrator roles are managed from the Entra admin experience. To compare role permissions with the least administrative effort, you can use the built-in role management experience under Identity > Roles & admins. This area is designed for reviewing Microsoft Entra built-in roles, their permissions, assignments, and administrative scope, making it the appropriate place to compare what each directory role can do. Microsoft's role permissions reference documents the permissions included in Microsoft Entra roles and supports the same role-based access control model used in the admin center. Using this portal avoids manually checking permissions across separate service-specific admin portals and keeps the comparison focused on tenant-level Microsoft Entra role permissions. For more information, see Microsoft's documentation on Microsoft Entra built-in role permissions and managing Microsoft Entra roles in the portal.

QUESTION NO: 27

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 named Microsoft Entra ID, provides all the listed identity-management benefits. It supports integration with a broad ecosystem of cloud and SaaS applications, including many non-Microsoft services, through standards such as SAML, OAuth, and OpenID Connect, enabling centralized identity management across an organization's application portfolio. It also provides Microsoft Entra multifactor authentication, which strengthens sign-in security by requiring additional verification beyond a password. In addition, Microsoft Entra ID enables single sign-on so users can access multiple connected applications with one identity and a streamlined sign-in experience. Together, these capabilities make it a core identity platform for Microsoft 365 administration, helping administrators improve security, simplify user access, and manage identities consistently across Microsoft and third-party applications. For more details, see Microsoft's overview of Microsoft Entra ID and the documentation for Microsoft Entra multifactor authentication.

QUESTION NO: 28

What is the recommended approach to maintain and update a custom app solution in Microsoft 365?

A. Make changes to the app solution in the original source code

B. Make changes to the app solution in a separate instance and test it in a staging environment before deploying it again.

C. Update the app solution in the production environment

D. Redeploy the app solution from scratch

ANSWER: B

Explanation:

Make changes to the app solution in a separate instance and test it in a staging environment before deploying it again. is correct because Microsoft recommends using a controlled application lifecycle management approach for business and custom solutions. In practice, this means changes should be made outside the live production environment, validated in a development or staging/test environment, and only then promoted or deployed to production. This approach helps administrators confirm that updates do not break existing functionality, introduce security issues, or disrupt users who rely on the app. It also supports rollback planning, version control, and proper change management, which are important

operational practices for Microsoft 365 environments. Microsoft's ALM guidance emphasizes separating development, testing, and production environments so that solutions can be validated before users are affected. Similarly, environment strategy guidance for Microsoft business applications recommends structured environment use to support safe deployment and governance. See Microsoft's guidance on application lifecycle management and environment strategy for ALM.

QUESTION NO: 29 - (HOTSPOT)

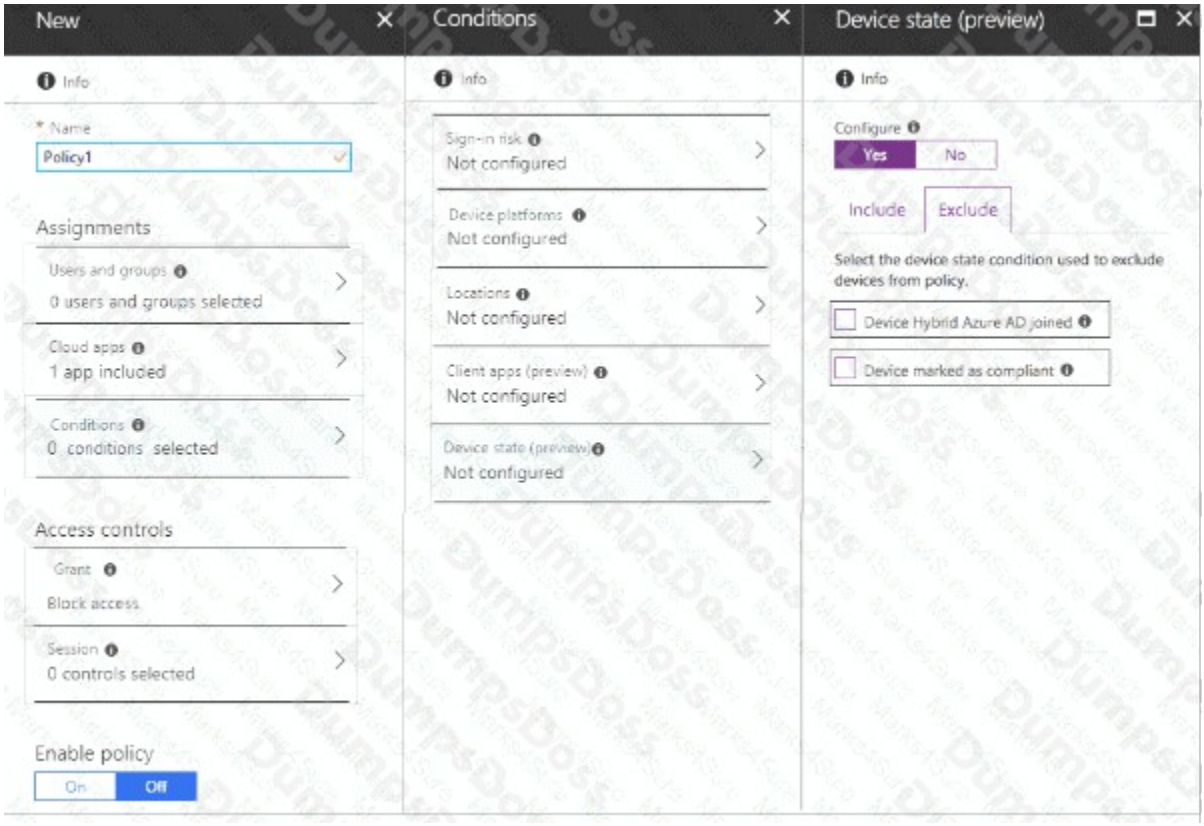
HOTSPOT

You need to configure a conditional access policy to meet the compliance requirements.

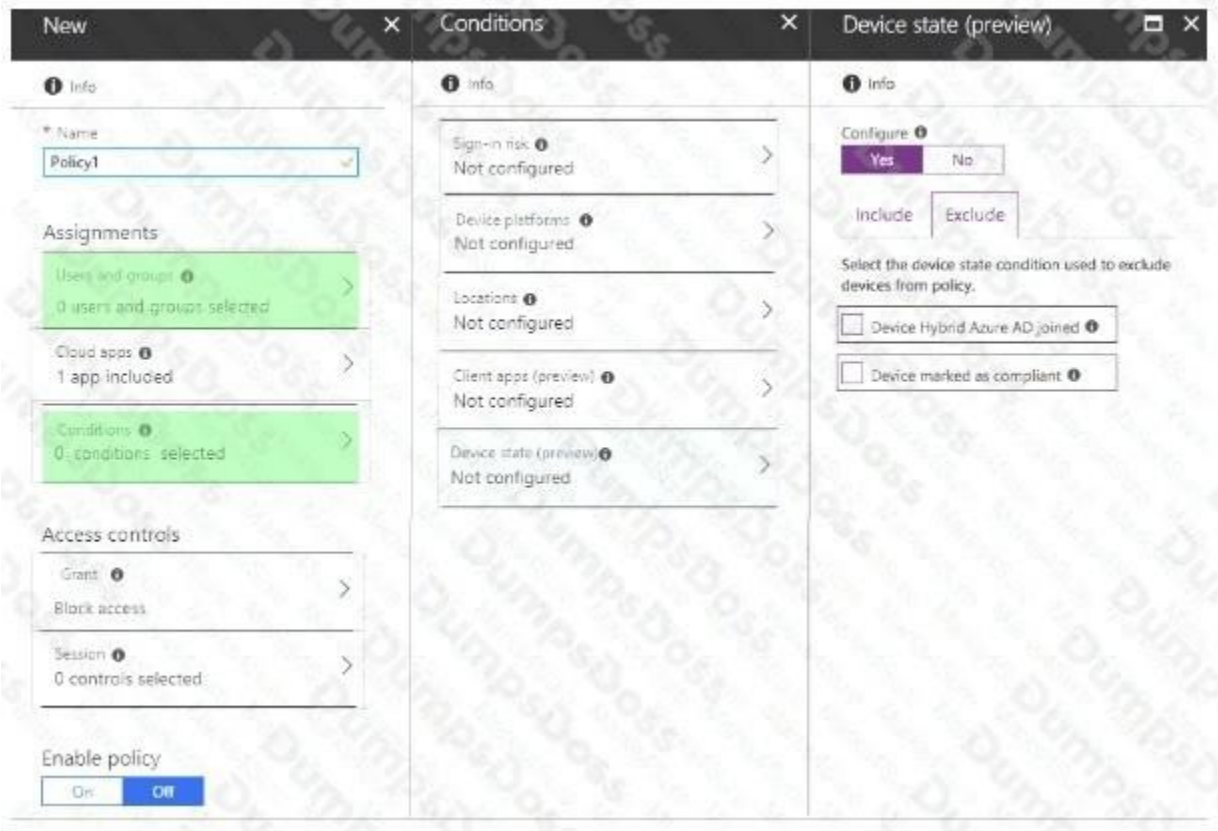
You add Exchange Online as a cloud app.

Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



ANSWER:



Explanation:

After Exchange Online is selected as the target cloud app, the conditional access policy still needs to define who the policy applies to and under what circumstances it applies. In the screenshot, the policy shows that no users or groups have been selected and no conditions have been selected. A conditional access policy without a user or group assignment will not target anyone, and without the required condition it will not enforce the intended compliance requirement in the right scenario. Therefore, the two additional areas to configure are **Users and groups** and **Conditions**.

In Microsoft Entra Conditional Access, assignments are the core of a policy: they define the users, groups, apps, and conditions that must be evaluated before the configured access control is applied. Since Exchange Online has already been added as the cloud app and the grant control is already shown as blocking access, the missing configuration is to assign the policy to the appropriate users or groups and configure the relevant condition, such as the device-state-related condition shown in the answer area. Microsoft documents these policy assignment components in the Conditional Access policy structure, including users/groups and conditions, in Conditional Access policies.

QUESTION NO: 30

On which server should you install the Azure ATP sensor?

A. Server 1

B. Server 2

C. Server 3

D. Server 4

E. Server 5

F. A domain controller.

ANSWER: F

Explanation:

A domain controller is correct because the Azure ATP sensor, now known as the Microsoft Defender for Identity sensor, is designed to be installed on servers that handle Active Directory authentication and directory activity. Installing the sensor directly on a domain controller allows it to inspect domain controller network traffic, collect relevant Windows events, and analyze authentication protocols such as Kerberos and NTLM. This visibility is what enables Defender for Identity to detect suspicious identity-based activity, lateral movement, credential theft attempts, and other attacks that target Active Directory. Microsoft's deployment guidance states that the sensor can be installed directly on domain controllers, and this is the standard deployment model when you want complete visibility into on-premises identity activity. For environments that include AD FS or AD CS, sensors can also be deployed there for those specific workloads, but for Azure ATP/Defender for Identity monitoring of Active Directory, the key target server is a domain controller. See Microsoft's sensor installation guidance at Install Microsoft Defender for Identity sensor and the architecture overview at Microsoft Defender for Identity architecture.

QUESTION NO: 31

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 is correct because Microsoft Purview retention policies can be scoped to specific SharePoint sites and configured to retain content for a defined period, such as 10 years. When applied to a SharePoint site, the policy helps ensure that documents and other site content are preserved according to the configured retention settings, including content that users modify or delete during the retention period. See Microsoft's guidance on retention for SharePoint and OneDrive.

A sensitivity label is also correct because sensitivity labels can be configured for the "Groups & sites" scope and applied to SharePoint sites. For SharePoint sites, a sensitivity label can control site-level external sharing settings, including restricting sharing so that content can be shared only with people inside the organization. This directly addresses the requirement to prevent data in site1 from being shared externally. Microsoft documents these container-level label capabilities in use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites.

QUESTION NO: 32

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:

From Active Directory Domains and Trusts, add a UPN suffix, From the Microsoft Entra admin center, add a custom domain name, and Modify the User logon name for each user account are correct. Because the on-premises Active Directory domain is contoso.local, its default UPN suffix is not an internet-routable, verifiable domain for Microsoft Entra ID. Before synchronizing identities for Microsoft 365 sign-in, you should add and verify a custom domain name in Microsoft Entra ID, such as contoso.com, so users can sign in with a routable UPN that matches an accepted tenant domain. You then add the same UPN suffix in Active Directory Domains and Trusts and update each user's User logon name to use that suffix. This aligns the on-premises user principal names with the verified Microsoft Entra custom domain, which is a standard preparation step for Microsoft Entra Connect synchronization and pass-through authentication. Pass-through authentication validates the user's password against on-premises Active Directory, but the sign-in identity still needs to be represented correctly in Microsoft Entra ID. Microsoft documents custom domain configuration and UPN preparation as part of identity setup for Microsoft 365 and Microsoft Entra hybrid identity. References: Add a domain to Microsoft 365 and Microsoft Entra Connect prerequisites.

QUESTION NO: 33

What is the purpose of Azure AD Application Proxy?

A. To manage access to administrative roles in Azure

B. To provide secure access to cloud-based web applications

C. To monitor user access to your Azure resources

D. To provide domain services to Azure virtual machines

E. To provide secure remote access to on-premises web applications

ANSWER: E

Explanation:

To provide secure remote access to on-premises web applications is correct. Azure AD Application Proxy, now known as Microsoft Entra application proxy, is designed to publish internal, on-premises web applications so users can access them securely from outside the corporate network. It uses an outbound connector installed on an internal server, so organizations do not need to open inbound firewall ports or place applications directly on the internet. Users authenticate through Microsoft Entra ID, which allows administrators to apply modern identity controls such as Conditional Access, multifactor authentication, and single sign-on to legacy or internal web apps.

This service is especially useful when an organization wants to reduce reliance on traditional VPN access for browser-based internal applications while still enforcing centralized identity and security policies. Microsoft describes Application Proxy as a

feature that provides secure remote access to on-premises web applications through Microsoft Entra ID. See Microsoft Entra application proxy overview and Microsoft Entra application proxy documentation.

QUESTION NO: 34 - (HOTSPOT)

HOTSPOT

As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

ANSWER:

Explanation:

The correct selections are based on Microsoft's Windows feature update servicing lifecycle. For supported Enterprise and Education editions, feature updates released in the second half of the year, such as September releases, receive 30 months of servicing from the release date. Feature updates released in the first half of the year, such as March releases, receive 18 months of servicing. Since the question asks "as of March," the Seattle computers are treated as being on the September feature update cycle. By March, six months of that 30-month servicing period have already elapsed, so those computers have 24 months of Microsoft support remaining. The New York computers are on the March feature update cycle, so they begin with the standard 18 months of servicing remaining as of March.

This aligns with Microsoft's published Windows release health and lifecycle guidance, where servicing timelines are determined by the feature update release period and edition. Microsoft documents these lifecycle rules in the Windows release information and lifecycle resources, including Windows 10 release information and Windows 10 Enterprise and Education lifecycle information. Therefore, Seattle should be set to 24 months, and New York should be set to 18 months.

QUESTION NO: 35

What is Microsoft Cloud App Security?

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

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

C. It's an endpoint protection platform

D. It's a cloud access security broker (CASB) that provides visibility, control, and protection for your cloud applications

ANSWER: D

Explanation:

It's a cloud access security broker (CASB) that provides visibility, control, and protection for your cloud applications is correct. Microsoft Cloud App Security, now known as Microsoft Defender for Cloud Apps, is Microsoft's CASB solution. Its

purpose is to help organizations discover cloud apps in use, assess risk, monitor user activity, enforce policies, detect suspicious behavior, and protect sensitive information across sanctioned and unsanctioned cloud services. In a Microsoft 365 administration context, this service is important because it extends security and compliance controls beyond core Microsoft 365 workloads to a broader cloud app environment. Defender for Cloud Apps can integrate with Microsoft Entra ID, Microsoft Defender XDR, Microsoft Purview Information Protection, and other services to provide session control, app governance, threat detection, and data protection for cloud-based activity. Microsoft describes it as a CASB that supports visibility, data control, threat protection, and compliance capabilities for cloud apps. See What is Microsoft Defender for Cloud Apps? and Microsoft Defender for Cloud Apps licensing.

QUESTION NO: 36

Which Microsoft tool is used to detect, investigate, and respond to advanced threats in Microsoft 365?

A. Microsoft Endpoint Manager

B. Microsoft Azure Active Directory

C. Microsoft Defender for Endpoint

D. Microsoft Intune

ANSWER: C

Explanation:

Microsoft Defender for Endpoint is the correct tool because it is Microsoft's endpoint security platform for preventing, detecting, investigating, and responding to advanced threats across devices in a Microsoft 365 environment. It provides endpoint detection and response capabilities, threat and vulnerability management, attack surface reduction, automated investigation and remediation, and advanced hunting. These capabilities help security teams identify suspicious activity, investigate alerts, understand the scope of an attack, and take response actions such as isolating devices or remediating threats. Microsoft Defender for Endpoint is also integrated into Microsoft Defender XDR, allowing endpoint signals to be correlated with identity, email, collaboration, and cloud app signals for broader Microsoft 365 security operations. Microsoft describes Defender for Endpoint as a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats, which directly matches the wording of the question. See Microsoft's overview of Microsoft Defender for Endpoint and the Microsoft Defender XDR documentation for more details.

QUESTION NO: 37

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 correct tasks are **Delete User2 and User4 only.** and **Reset the password of User2 and User4 only.** The User Administrator role in Microsoft Entra ID is intended for day-to-day user lifecycle administration. A user assigned this role can create, update, and delete users that are within the role's management scope, and can reset passwords for non-privileged users and some limited administrator roles. In this scenario, User2 and User4 fall within the set of accounts that a User Administrator can manage, so User5 can both delete those accounts and reset their passwords.

Microsoft's role permissions reference describes the User Administrator role as being able to manage all aspects of users and groups, including resetting passwords for limited administrators, while still being constrained from managing more highly privileged administrator accounts. That privilege boundary is why the valid management actions are limited to User2 and User4 in the provided tenant table. For more detail, see the Microsoft Entra built-in role documentation for User Administrator permissions and Microsoft's guidance on privileged role permissions.

QUESTION NO: 38

What is the main purpose of Microsoft Purview?

A. To manage security and threats by using Microsoft 365 Defender

B. To implement and manage identity and access in Azure

C. To manage compliance by using Microsoft Purview

D. To deploy and manage a Microsoft 365 tenant

ANSWER: C

Explanation:

To manage compliance by using Microsoft Purview is correct because Microsoft Purview is Microsoft's integrated family of data governance, risk, and compliance solutions. In the Microsoft 365 administrator context, Purview is used to help organizations protect sensitive information, manage compliance requirements, govern data, and reduce compliance risk across Microsoft 365 services and other connected data sources. It includes capabilities such as data loss prevention, information protection and sensitivity labels, retention and records management, eDiscovery, audit, communication compliance, insider risk management, and compliance assessment through Compliance Manager. These features are centered on helping organizations understand their data, apply protection and governance controls, and demonstrate compliance with regulatory or organizational requirements. Microsoft describes Purview as a solution that brings together data security, data governance, and compliance management, which aligns directly with the purpose stated in the option. For more details, see Microsoft Purview documentation and Microsoft Purview Compliance Manager.

QUESTION NO: 39

What is Microsoft's solution for passwordless authentication?

A. Windows Hello

B. Microsoft Hello for Business

C. Microsoft Authenticator

D. All of the above

ANSWER: D

Explanation:

All of the above is correct because Microsoft's passwordless authentication strategy is not limited to a single user experience. Microsoft supports multiple passwordless sign-in methods across Microsoft Entra ID and Windows, including Windows Hello/Windows Hello for Business for device-based biometric or PIN sign-in and Microsoft Authenticator for phone-based passwordless sign-in. These methods are designed to replace traditional passwords with stronger authentication approaches that use something the user has, such as a trusted device or phone, combined with something the user is or knows, such as biometrics or a PIN. In Microsoft 365 administration, these passwordless methods are commonly managed through Microsoft Entra authentication methods policies and are part of Microsoft's broader identity security recommendations. Microsoft documentation describes passwordless authentication options such as Windows Hello for Business and the Microsoft Authenticator app as supported passwordless methods for Microsoft Entra ID. See Passwordless authentication options for Microsoft Entra ID and Enable passwordless sign-in with Microsoft Authenticator.

QUESTION NO: 40

What type of users can be added to Azure AD using the Azure portal?

A. Guest users

B. Service accounts

C. Users with Microsoft accounts

D. Global administrators

ANSWER: A

Explanation:

Guest users is correct because Microsoft Entra ID, formerly Azure AD, supports adding external identities to a tenant by inviting them as B2B collaboration users through the Azure portal or Microsoft Entra admin center. These invited external users are represented in the directory with the user type Guest, which allows administrators to grant access to Microsoft 365 resources, apps, groups, Teams, SharePoint sites, and other protected resources while still letting the users authenticate with their own external identity provider. Microsoft's documentation describes this as inviting an external user to the tenant and managing that user as a guest account in Microsoft Entra ID. The key point is that "guest" is the directory user type that can be added through the portal; the guest may authenticate with a Microsoft account, work or school account, or another supported identity depending on the collaboration configuration. See Microsoft's guidance on adding guest users in the portal and the overview of Microsoft Entra B2B collaboration.

QUESTION NO: 41

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

Name	Microsoft 365 admin role	Microsoft Exchange Online admin role
User1	Global Administrator	*None*
User2	Exchange Administrator	*None*
User3	Service Support Administrator	*None*
User4	*None*	Organization Management

You plan to use Exchange Online to manage email for a DNS domain.

An administrator adds the DNS domain to the subscription.

The DNS domain has a status of Incomplete setup.

You need to identify which user can complete the setup of the DNS domain. The solution must use the principle of least privilege.

Which user should you identify?

A. User1

B. User2

C. User3

D. User4

ANSWER: A

Explanation:

User1 is correct because the least-privileged role for completing setup of a custom DNS domain in Microsoft 365 is the Domains administrator, also known in Microsoft Entra ID as the Domain Name Administrator role. Completing a domain setup typically involves verifying domain ownership and configuring or confirming the required DNS records for Microsoft 365 services such as Exchange Online. Microsoft documentation states that adding, modifying, or removing domains requires either a Global Administrator or Domain Name Administrator, and the Domain Name Administrator role is the more limited permission set for this task. Since the requirement is to use the principle of least privilege, the user assigned the domain management role should be selected instead of a broader administrative role. For Exchange Online mail flow, completing domain setup ensures records such as MX, Autodiscover, SPF, and related service records can be configured or validated for the domain. See Microsoft's guidance on adding a custom domain in Microsoft 365 at Add a domain to Microsoft 365 and the Microsoft Entra built-in role description at Domain Name Administrator.

QUESTION NO: 42

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:

The correct ways to identify recently updated Microsoft 365 applications or services are **From the Microsoft 365 admin center, review the Message center blade.** and **From the Microsoft 365 Admin mobile app, review the messages.** Message center is the Microsoft 365 admin location designed to communicate service changes, new and changed features, updates, and other actionable announcements that can affect your tenant. It includes posts for specific Microsoft 365 workloads and apps, often with details such as the affected service, rollout timing, user impact, and any admin action

required. Microsoft documents Message center as the place to track upcoming and recent changes in Microsoft 365: Message center in the Microsoft 365 admin center. The Microsoft 365 Admin mobile app also provides access to admin messages and notifications, allowing administrators to review Message center communications from a mobile device rather than using the web admin center. Microsoft describes the mobile app as a way to manage Microsoft 365 and receive important service health and message center notifications: Microsoft 365 Admin mobile app.

QUESTION NO: 43

What is Azure AD Premium?

A. An upgraded version of Azure Active Directory

B. An authentication service for Windows servers

C. A standalone identity and access management product

D. A free version of Azure Active Directory

ANSWER: A

Explanation:

An upgraded version of Azure Active Directory is correct because Azure AD Premium, now represented in Microsoft's current naming as Microsoft Entra ID Premium P1 and P2, is a paid licensing tier that extends the capabilities of the base directory service. It adds advanced identity and access management features such as Conditional Access, self-service password reset with enhanced controls, Microsoft Entra ID Protection capabilities depending on the tier, Privileged Identity Management in P2, access reviews, and more comprehensive security and governance functionality. In other words, it is not a separate directory technology from Azure Active Directory; it is a premium edition of the same cloud identity platform that provides additional administrative, security, and compliance features for organizations that need more than the free tier provides. Microsoft documents these capabilities in its Microsoft Entra ID licensing guidance and feature comparison resources. See What is Microsoft Entra ID? and Microsoft Entra ID licensing for Microsoft's current product naming and licensing details.

QUESTION NO: 44

What is the difference between Microsoft Defender for Endpoint and Microsoft Defender for Office 365?

A. Microsoft Defender for Endpoint provides protection for all endpoints in an organization, while Microsoft Defender for Office 365 focuses on protecting email and other communication tools.

B. Microsoft Defender for Office 365 is only available for Windows devices, while Microsoft Defender for Endpoint provides protection for multiple platforms.

C. Microsoft Defender for Endpoint is only available for on-premises use, while Microsoft Defender for Office 365 is a cloud-based solution.

D. Microsoft Defender for Endpoint and Microsoft Defender for Office 365 are the same thing.

ANSWER: A

Explanation:

Microsoft Defender for Endpoint provides protection for all endpoints in an organization, while Microsoft Defender for Office 365 focuses on protecting email and other communication tools. Microsoft Defender for Endpoint is Microsoft's endpoint security platform for protecting user devices and servers through capabilities such as vulnerability management, attack surface reduction, next-generation protection, endpoint detection and response, automated investigation, and advanced hunting. It is intended to help organizations prevent, detect, investigate, and respond to threats on endpoints across supported platforms. Microsoft describes these capabilities in its Defender for Endpoint overview: Microsoft Defender for Endpoint.

Microsoft Defender for Office 365, by contrast, is focused on protecting Microsoft 365 collaboration workloads, especially email and collaboration services. It helps defend against phishing, business email compromise, malware, unsafe links, and unsafe attachments across services such as Exchange Online, SharePoint, OneDrive, and Microsoft Teams. Microsoft's overview explains this workload-focused protection here: Microsoft Defender for Office 365. So the key distinction is endpoint/device protection versus Microsoft 365 email and collaboration protection.

QUESTION NO: 45

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 and a data loss prevention (DLP) policy are the correct components for this requirement. A trainable classifier is designed to identify content by learning from sample items that represent the type of information you want Microsoft Purview to detect. After the classifier is trained and published, it can be used as a condition in compliance workflows to detect matching content across Microsoft 365 services. A data loss prevention (DLP) policy then provides the enforcement layer: it can evaluate content in locations such as Exchange email and SharePoint, detect content that matches the configured classifier, and automatically apply protective actions such as blocking external sharing, restricting access, or preventing messages from being sent. Together, the classifier defines what should be detected from the samples, and the DLP policy enforces the business rule that matching data must not be shared externally. Microsoft documents trainable classifiers as sample-trained classification tools in Purview and DLP as the Microsoft 365 control used to identify, monitor, and protect sensitive information across services. See Microsoft Purview trainable classifiers and Learn about data loss prevention.

QUESTION NO: 46

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 correct because the Built-in protection preset security policy in Microsoft Defender for Office 365 is designed to provide baseline protection for eligible users by automatically applying core Defender for Office 365 protections. Microsoft documents Built-in protection as a preset security policy that specifically includes Safe Links protection and Safe Attachments protection. Safe Attachments helps protect users by opening email attachments in a detonation environment before delivery, helping detect malicious files. Safe Links helps protect users from malicious URLs by checking links at time of click and applying URL protection across supported workloads. This built-in policy is intended to ensure organizations have a default level of protection without requiring administrators to manually create those Defender for Office 365 policies for every recipient. Microsoft's documentation for preset security policies identifies Built-in protection as including Safe Links and Safe Attachments settings, and the Safe Links and Safe Attachments protection guidance also describes using Built-in protection to ensure users receive those protections.

QUESTION NO: 47

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

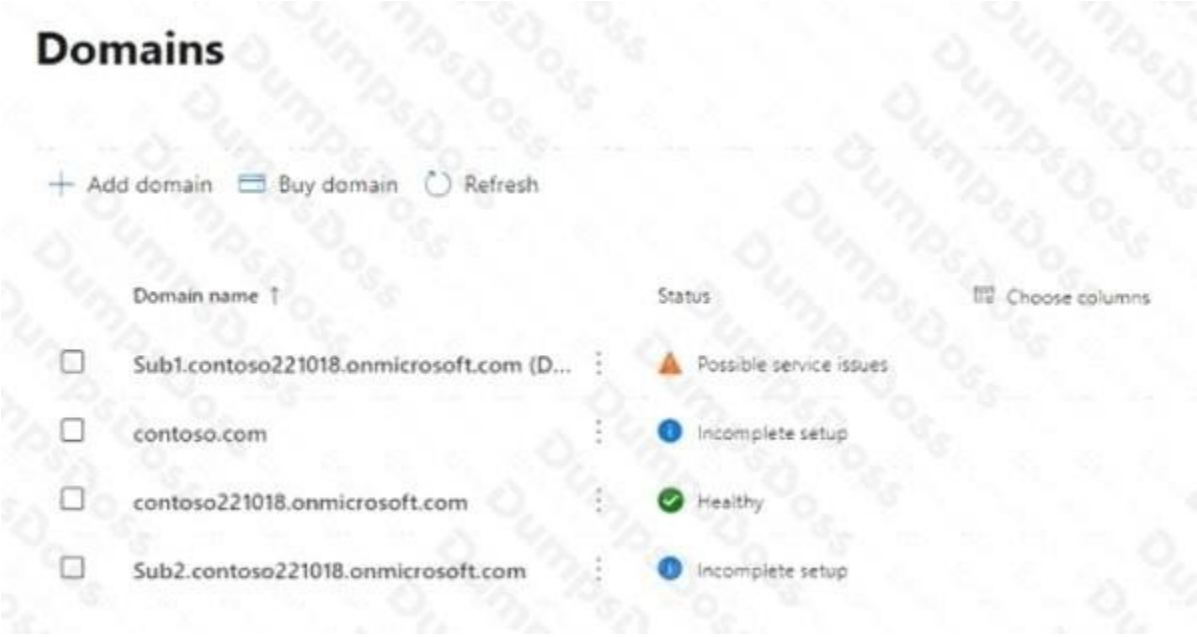
Explanation:

Microsoft Defender for Endpoint Plan 1 is designed to provide foundational endpoint protection and prevention capabilities for Microsoft 365 environments. **security reports** is correct because Plan 1 includes centralized security reporting in the Microsoft Defender portal, allowing administrators to view endpoint protection status, security recommendations, and related visibility for managed devices. **attack surface reduction (ASR)** is also correct because Plan 1 includes attack surface reduction capabilities such as ASR rules, network protection, web protection, controlled folder access, exploit protection, and device control-related protections. These capabilities are core prevention and hardening features intended to reduce common attack paths before endpoint detection and response investigation capabilities are needed. Microsoft's Defender for Endpoint plan comparison identifies Plan 1 as including next-generation protection, attack surface reduction, centralized management, and security reports, while reserving more advanced investigation and vulnerability-management capabilities for higher plans. For details, see Microsoft's Microsoft Defender for Endpoint Plan 1 overview and the Microsoft Defender for Endpoint documentation.

QUESTION NO: 48 - (SIMULATION)

SIMULATION

You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.



Which domain name suffixes can you use when you create users?

ANSWER: See the explanation for the answer

QUESTION NO: 49

Which PowerShell command can be used to retrieve information about a specific user in Microsoft 365?

A. Get-MsolGroup

B. Get-MsolRole

C. Get-MsolUser

D. Get-MsolAccountSku

ANSWER: C

Explanation:

Get-MsolUser is correct because it is the MSOnline PowerShell cmdlet used to retrieve Microsoft 365 user objects from Microsoft Entra ID. When used by itself, it can return a list of users in the tenant, and when used with identifying parameters such as `-UserPrincipalName` or `-ObjectId`, it retrieves information for a specific user account. The returned user object can include common administrative details such as the display name, user principal name, license status, block credential status, usage location, and other directory-related properties that are useful for Microsoft 365 administration. For example, an administrator can run `Get-MsolUser -UserPrincipalName user@contoso.com` to retrieve that individual user's account information. Microsoft documents this cmdlet as part of the MSOnline module and describes its purpose as getting individual users or a list of users. See the official Microsoft reference for Get-MsolUser and Microsoft's broader PowerShell guidance for managing Microsoft 365 users at Manage user accounts and licenses with Microsoft 365 PowerShell.