PassQueen
a.k.a dumpsqueen.com

Microsoft 365 Messaging

Microsoft MS-203

Version Demo

Total Demo Questions: 45

Total Premium Questions: 454

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Manage the Exchange Online environment	61
Topic 2, Manage mail flow	100
Topic 3, Manage recipients and devices	154
Topic 4, Manage messaging security and compliance	109
Topic 5, Mix Questions	1
Topic 6, Case Study 1	6
Topic 7, Case Study 2	3
Topic 8, Case Study 3	3
Topic 9, Case Study 4	2
Topic 10, Case Study 5	7
Topic 11, Case Study 6	4
Topic 12, Case Study 7	2
Topic 13, Case Study 8	2
Total	454

QUESTION NO: 1

You have a Microsoft Exchange Online tenant that uses Microsoft Defender for Office 365.

You create a new anti-phishing policy named Policy1.

You need to ensure that users are notified every five days about all the email messages quarantined by Policy1.

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

NOTE: Each correct selection is worth one point.

A. Modify the AdminOnlyAccessPolicy quarantine policy and assign the policy to Policy1.

B. Modify the DefaultFullAccessPolicy quarantine policy and assign the policy to Policy1.

C. Modify the global settings for quarantine policies.

D. Add a custom quarantine policy and assign the policy to Policy1.

E. Configure the User reported messages settings.

ANSWER: C D

Explanation:

To provide end users with periodic notifications for messages quarantined by an anti-phishing policy, configure both the quarantine policy assigned to the anti-phishing action and the tenant-wide notification schedule. “Add a custom quarantine policy and assign the policy to Policy1” is required because an anti-phishing policy’s quarantine action must reference a quarantine policy (quarantine tag). In that custom policy, end-user quarantine notifications can be enabled and the appropriate user access and release behavior can be defined. This makes messages quarantined as a result of Policy1 eligible to appear in users’ quarantine notifications.

“Modify the global settings for quarantine policies” is also required because notification frequency is a global quarantine notification setting, rather than a setting configured independently on each anti-phishing policy. Set the frequency to five days in the Microsoft Defender portal’s global quarantine notification settings. The resulting notification includes all eligible quarantined messages for each recipient since the previous notification, including messages quarantined through Policy1. Microsoft documents quarantine-policy assignment and the available user notification controls in Quarantine policies in Microsoft Defender for Office 365 and describes notification configuration in Quarantined email messages in Microsoft Defender for Office 365.

QUESTION NO: 2 - (DRAG DROP)

DRAG DROP

Your company named ADatum Corporation has a Microsoft 365 subscription.

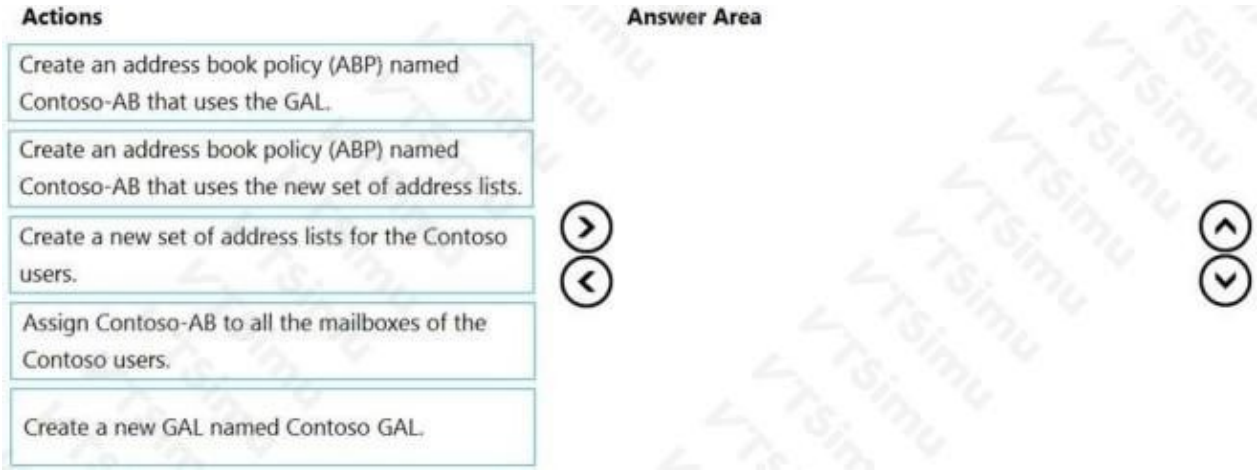
ADatum acquires a company named Contoso, Ltd.

In the subscription, you create a new mailbox for each user at Contoso.

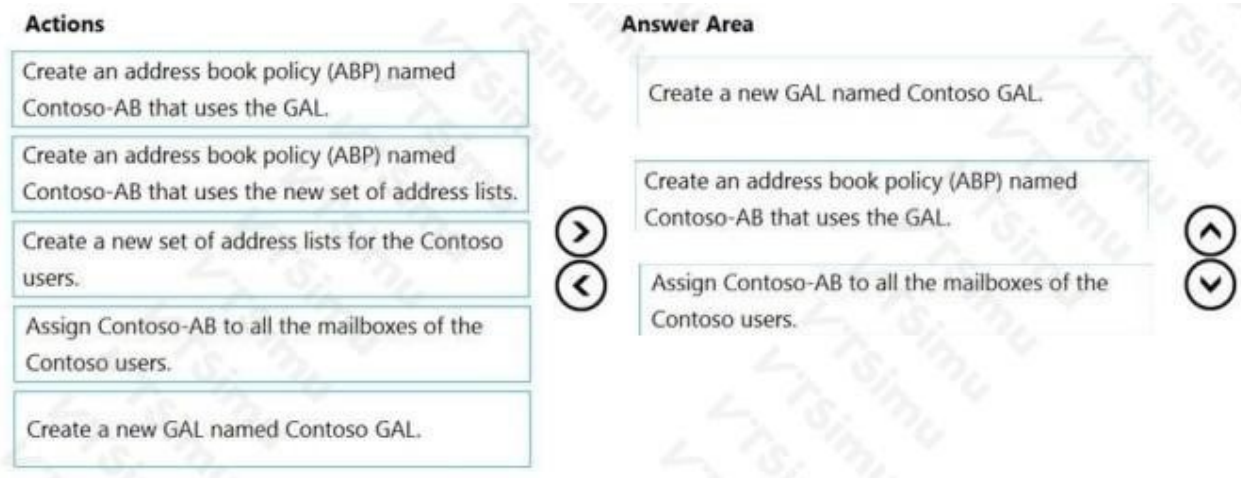
You need to provide the Contoso users with a global address list (GAL) that contains only their email addresses.

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

Select and Place:



ANSWER:



Explanation:

An address book policy is the Exchange Online feature used to provide separate address book views to different groups of users in the same Microsoft 365 organization. For Contoso users to see a global address list limited to Contoso recipients, the process begins by creating a dedicated global address list named Contoso GAL. In practice, that GAL is configured with an appropriate recipient filter so that it contains the intended Contoso mail-enabled recipients. This creates the distinct GAL that will be presented to the acquired company's users.

Next, create the address book policy named Contoso-AB and configure it to use Contoso GAL as its global address list. An address book policy is the assignment container that brings together the address book components presented to a mailbox, including its GAL. Using the Contoso GAL in that policy ensures that mailboxes receiving the policy use the Contoso-specific GAL rather than the organization-wide default GAL.

Finally, assign Contoso-AB to every Contoso user mailbox. Address book policies take effect on individual mailboxes only after the policy is assigned. Once assigned, Outlook and Outlook on the web use the policy's specified GAL for those users, giving the Contoso population the intended segregated address-list experience. Microsoft documents the creation and management of custom GALs at Create global address lists and explains how address book policies control the address lists visible to mailbox users at Address book policies in Exchange Online.

QUESTION NO: 3

Lynne Robbins and the users in the sales department plan to collaborate on a project with a partner company named Contoso, Ltd. that has an email domain named contoso.com.

You need to ensure that only the sales department users can share all their calendar free/busy information with the users in contoso.com.

How should you configure the organization relationship?

A. Select Calendar free/busy information with time only and enter Group1.

B. Select Calendar free/busy information with time, subject, and location and enter Group2.

C. Select Calendar free/busy information with time, subject, and location and enter Group3.

D. Select Calendar free/busy information with time only and enter Group3.

E. Select Calendar free/busy information with time only and enter Group2.

ANSWER: C

Explanation:

Select **Calendar free/busy information with time, subject, and location and enter Group3.** An organization relationship controls the calendar availability information that users in an external organization can obtain. The *Calendar free/busy information with time, subject, and location* sharing level corresponds to the LimitedDetails availability level. It exposes each calendar item's time, subject, and location, which meets the requirement to share all of the specified free/busy details with Contoso users.

The organization relationship must also be scoped to the group that contains the sales department users. Group3 is the designated sales group in this configuration, so entering it limits this external calendar-sharing relationship to that group rather than enabling the sharing level for every mailbox in the organization. This provides Contoso access only to the intended sales users' availability details while retaining the requested detail level for meetings.

Microsoft documents the available organization-relationship free/busy access levels, including `LimitedDetails`, and the ability to scope free/busy sharing by using the `FreeBusyAccessScope` setting. See Create an organization relationship in Exchange Online and Set-OrganizationRelationship.

QUESTION NO: 4

You have a Microsoft Exchange Online tenant that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

You need to track any modifications made to Policy! by the identifying following:

â€¢ The name of the user that modified the policy

â€¢ The old and new values of settings modified in Policy!

â€¢ How the modifications compare to the baseline settings of Standard Preset Security Policy

What should you use in the Microsoft 365 Defender portal?

A. Threat tracker

B. Threat analytics

C. Audit

D. Configuration analyzer

ANSWER: D

Explanation:

Configuration analyzer is the appropriate Microsoft 365 Defender portal feature because it is designed to analyze and compare the configuration of Defender for Office 365 security policies against the Standard and Strict preset security policy recommendations. It identifies policy-setting differences from the selected preset baseline, which directly satisfies the requirement to determine how the modified policy compares with the Standard Preset Security Policy.

Configuration analyzer also provides configuration change history for supported policies. Its change information includes the identity of the user who made the change and the relevant setting values before and after the update. This lets an

administrator investigate a policy modification in context: determine who performed it, understand precisely what setting was changed, and evaluate whether the resulting configuration aligns with Microsoft's recommended preset protection posture.

The feature is available in the Microsoft Defender portal under Email & collaboration policy configuration analysis and is intended to help organizations identify configuration drift and improve their email security settings over time. Microsoft documents the feature and its comparison and history capabilities at Configuration analyzer for security policies. For the baseline definitions used by the comparison, see Preset security policies in Microsoft Defender for Office 365.

QUESTION NO: 5

You manage a Microsoft Exchange Server 2019 hybrid deployment. All user mailboxes are located both on-premises and in the cloud. All public folders reside in Exchange Online.

You need to configure the deployment so that the on-premises mailboxes can access the public folders.

Which three commands should you run? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Sync-MailPublicFolders.ps1

B. Set-OrganizationConfig –PublicFoldersEnabled Remote

C. Import-PublicFolderMailboxes.ps1

D. Sync-MailPublicFoldersCloudToOnprem.ps1

E. Set-OrganizationConfig –PublicFoldersEnabled Local
-RemotePublicFolderMailboxes PfMailbox1

ANSWER: B C D

Explanation:

To provide users whose mailboxes remain on-premises with access to public folders hosted in Exchange Online, the on-premises Exchange organization must be configured to use remote public folders. `Set-OrganizationConfig -PublicFoldersEnabled Remote` establishes that the public-folder infrastructure used by the on-premises organization is remote rather than local.

The public-folder recipient and mailbox information also must be represented in the on-premises organization. `Import-PublicFolderMailboxes.ps1` imports the Exchange Online public-folder mailbox objects needed by the hybrid public-folder configuration. `Sync-MailPublicFoldersCloudToOnprem.ps1` then synchronizes mail-enabled public-folder objects from Exchange Online to the on-premises environment. This synchronization enables on-premises directory resolution and mail flow for public-folder mail-enabled objects while Exchange Online remains the public-folder location.

These steps are part of the supported Exchange hybrid public-folder procedure for an Exchange Online public-folder deployment. Run the scripts with the required permissions and parameters specified for the environment, and allow directory replication to complete before validating access from an on-premises mailbox. See Configure Exchange Online public folders for a hybrid deployment and Public folders in Exchange Server.

QUESTION NO: 6

Your company has a Microsoft Exchange Server 2019 hybrid deployment.

You are migrating mailboxes to Exchange Online by using remote mailbox move requests.

A recent security breach at the company required that the passwords of all privileged accounts be changed.

Since the password change, mailbox move requests are failing.

You need to ensure that the mailbox migration can resume.

What should you do first?

A. From Exchange Online, run Set-MigrationConfig.

B. From Exchange Online, run Set-MigrationEndpoint.

C. Run iisreset /noforce on all the Exchange servers that have MRSProxy enabled.

D. From Exchange on-premises, run Set-MigrationConfig.

E. From Exchange on-premises, run Set-MigrationEndpoint.

ANSWER: B

Explanation:

From Exchange Online, run Set-MigrationEndpoint. In a hybrid remote move, Exchange Online uses a migration endpoint to connect to the on-premises Exchange environment through the Mailbox Replication Service Proxy (MRS Proxy). The endpoint stores the credentials used for that remote connection. If the privileged account associated with the endpoint has had its password changed, the stored credentials are no longer valid, causing move requests to fail authentication when Exchange Online attempts to access the on-premises organization.

First, connect to Exchange Online PowerShell and update the affected migration endpoint with valid credentials, for example by supplying a new credential object to the `Credentials` parameter of `Set-MigrationEndpoint`. Once the endpoint has the current password, Exchange Online can again authenticate to the on-premises MRS Proxy and the existing migration requests can resume or be restarted as appropriate. This action directly addresses the dependency changed by the security incident without changing the migration configuration or unnecessarily restarting IIS.

For the available parameters and usage of this cmdlet, see Set-MigrationEndpoint. For hybrid mailbox move architecture and MRS Proxy requirements, see Move mailboxes between on-premises and Exchange Online organizations in hybrid deployments.

QUESTION NO: 7

Your network contains an Active Directory domain named corp.contoso.com. The domain contains client computers that have Microsoft Office 365 Apps installed.

You have a hybrid deployment that contains a Microsoft Exchange Online tenant and an on-premises Exchange Server 2019 server named Server1.

All recipients use an email address suffix of @contoso.com.

You migrate all the Exchange Server recipients to Exchange Online, and then decommission Server1.

Users connected to the internal network report that they receive an Autodiscover error when they open Microsoft Outlook.

You need to ensure that all users can connect successfully to their mailbox by using Outlook.

Which two actions should you perform? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Add an accepted domain.

B. From the domain, modify the Autodiscover service connection point (SCP).

C. From the contoso.com DNS zone, modify the Autodiscover alias (CNAME) record.

D. Modify the name of the TLS certificate.

E. From the corp.contoso.com DNS zone, modify the Autodiscover host (A) record.

ANSWER: B C

Explanation:

Domain-joined Outlook clients use the Autodiscover service connection point (SCP) published in Active Directory as a prioritized source of Autodiscover configuration. After Server1 is decommissioned, its SCP can still direct internal clients to the former on-premises Exchange Autodiscover endpoint. Modifying the Autodiscover SCP to remove the obsolete configuration prevents Outlook from attempting to use the retired server and allows it to continue with the appropriate Autodiscover lookup process.

The Autodiscover alias in the `contoso.com` DNS zone is also required because users' SMTP addresses use the `@contoso.com` suffix. The `autodiscover.contoso.com` CNAME should resolve to `autodiscover.outlook.com`, which is the Exchange Online Autodiscover service. This provides the correct cloud endpoint for Outlook mailbox discovery and profile connectivity. Together, removing or correcting the stale Active Directory SCP configuration and configuring the public-facing email namespace's CNAME ensure clients can discover Exchange Online after the on-premises Exchange server has been retired. For details, see Autodiscover service in Exchange Server and Microsoft 365 DNS records.

QUESTION NO: 8 - (HOTSPOT)

HOTSPOT

You have a Microsoft Exchange Server 2019 hybrid deployment.

You are migrating mailboxes from the on-premises organization to Exchange Online.

From the Exchange admin center, you create a new migration batch that includes 25 mailboxes, and then you select Manual Complete the batch.

Later, you must complete the migration of a mailbox named user1@litware.com in the batch as soon as possible. You discover that the status of the migration batch is Syncing, but the status of the move request for user1@litware.com is Synced.

You need to complete the migration of the user1@litware.com mailbox to Exchange Online as soon as possible.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

ANSWER:

Explanation:

The mailbox move for `user1@litware.com` has reached the `Synced` state, which means the initial data synchronization is complete and the mailbox is ready for its final completion phase. Because the migration batch was created with manual completion, the move is deliberately prevented from completing automatically. To complete only this mailbox as soon as possible, update that specific move request by using `Set-MoveRequest` with `-PreventCompletion $false`. This removes the completion block from the individual move request while leaving the rest of the batch under its existing manual-completion behavior.

After the completion block is removed, the provided `Resume-MoveRequest -Identity "user1@litware.com"` command resumes processing for that request, allowing Exchange to perform the final incremental synchronization and complete the move to Exchange Online. This approach is appropriately scoped to the mailbox that is already synchronized, rather than changing completion behavior for all 25 mailboxes in the migration batch. Microsoft documents that the `PreventCompletion` setting controls whether a move request is allowed to complete; setting it to `$false` permits the request to finish. See the Set-MoveRequest documentation and the Resume-MoveRequest documentation for the relevant Exchange PowerShell behavior.

QUESTION NO: 9

: 222

You have a hybrid deployment that contains a Microsoft Exchange Online tenant and an on-premises Exchange Server 2019 server named Server1. All users use an email address suffix of @contoso.com.

You migrate 200 mailboxes from Server1 to Exchange Online by using Exchange PowerShell cmdlets. Users hosted on Server1 can send email messages to the migrated mailboxes.

In Microsoft 365, you create a new mailbox that uses an email address of user1@contoso.com.

When email is sent from the mailboxes hosted on Server1 to user1@contoso.com, the senders receive a non-delivery report (NDR) that contains the following text:

"550 5.1.10 RESOLVER.ADR.RecipientNotFound;

Recipient not found by SMTP address lookup."

You verify that Microsoft 365 mailboxes can send email to user1@contoso.com successfully.

You delete the user account and mailbox of User1.

You need to ensure that when new mailboxes are created, all the users at your company can exchange email successfully

Which two actions should you perform? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. From Azure AD Connect, modify the synchronization settings

B. From Server1, run the New-RemoteMailbox cmdlet

C. From Server1, run the Enable-Mailbox cmdlet

D. From the on-premises network, create new mailboxes, and then migrate the mailboxes to Microsoft 365

E. From the Exchange admin center, modify the properties of the Outbound connector

ANSWER: B D

Explanation:

In an Exchange hybrid organization with directory synchronization, the on-premises Exchange organization must have a mail-enabled recipient object for an Exchange Online mailbox so that on-premises users can resolve the SMTP address and route messages correctly. Running `New-RemoteMailbox` from Server1 creates a remote mailbox object in on-premises Active Directory and mail-enables it for the Exchange Online target. Azure AD Connect then synchronizes that object to Microsoft Entra ID, preserving a consistent recipient representation across both environments. Microsoft documents `New-`

`RemoteMailbox` specifically for creating a mailbox in the cloud-based service while creating the associated on-premises remote mailbox object in a hybrid deployment.

Creating new mailboxes on-premises and then migrating the mailboxes to Microsoft 365 also provides a complete, supported lifecycle. The mailbox begins as an on-premises recipient known to Server1; after the migration, Exchange updates it to the appropriate remote recipient configuration. Consequently, users whose mailboxes remain on-premises can continue to resolve and send to the migrated user, while Exchange Online users can do the same. These approaches maintain the directory objects required for cross-premises mail flow. See New-RemoteMailbox and Move mailboxes in hybrid deployments.

QUESTION NO: 10

You need to ensure that Allan Deyoung can create a new public folder for the sales department.

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

NOTE: Each correct selection is worth one point.

A. Add Allan Deyoung to the Organization Management role group

B. Create a new public folder mailbox

C. Add Allan Deyoung to the Recipient Management role group

D. Create a new shared mailbox

E. Modify Sales Policy

ANSWER: A B

Explanation:

Creating a public folder in Exchange Online requires both an available public folder mailbox and appropriate administrative permissions. A public folder mailbox is the storage hierarchy that hosts public folder content. Therefore, creating a new public folder mailbox establishes the required public-folder infrastructure before a new folder can be created. If the organization already had a suitable public folder mailbox, this step would not be necessary; however, when setting up public folders, it is an initial prerequisite.

Adding Allan Deyoung to the Organization Management role group grants the Exchange management permissions needed to administer public folders. This role group includes the Public Folders management role, which permits members to create, modify, and remove public folders and manage related public-folder settings. After membership is assigned, Allan may need to sign out and back in for the updated role-based access control permissions to apply.

Microsoft documents public folder mailbox creation and public-folder administration in its public folder guidance, and identifies the permissions associated with Exchange features and role groups. See Public folders in Exchange Online and Feature permissions in Exchange Online.

QUESTION NO: 11

You have a Microsoft Exchange Online subscription.

You need to generate a CSV file containing all the email messages that failed to send from the user1@contoso.com email address during the last 30 days.

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

NOTE: Each correct selection is worth one point.

A. From the Security & Compliance center, run a message trace.

B. From the Exchange admin center, run a message trace.

C. From Exchange Online PowerShell, run the Get-MessageTrace cmdlet.

D. From the Security & Compliance center, export the mailbox audit logs.

E. From Exchange Online PowerShell, run the Get-MessagetraceDetail cmdlet.

ANSWER: B C

Explanation:

From the Exchange admin center, run a message trace is correct because message trace provides a searchable record of mail-flow events for messages sent through Exchange Online. An administrator can specify user1@contoso.com as the sender, set a date range covering the previous 30 days, filter or review results for failed delivery status, and export the returned results to a CSV file. This is the portal-based method for collecting the requested evidence.

From Exchange Online PowerShell, run the Get-MessageTrace cmdlet is also correct because it retrieves message-trace records programmatically. The cmdlet supports sender and time-range filtering, allowing the administrator to request trace records for user1@contoso.com during the required period. The resulting PowerShell objects can then be filtered for failed messages as needed and piped to `Export-Csv` to create the required CSV output. Message trace data is retained long enough for a 30-day query, subject to the trace reporting and query capabilities available to the tenant.

For Microsoft guidance on using message trace in the Exchange admin center, see Message trace in the modern Exchange admin center. Cmdlet syntax and supported filtering parameters are documented at Get-MessageTrace.

QUESTION NO: 12

You have a Microsoft Exchange Online tenant named contoso.com.

Several users report that email messages sent to the users at another company named fabrikam.com contain a Winmail.dat attachment.

You need to prevent the fabrikam.com users from receiving Winmail.dat attachments.

What should you do?

A. Create an Outbound connector that has the ValidationRecipients parameter set to fabrikam.com.

B. Create an Outbound connector that has the ValidationRecipients parameter set to contoso.com.

C. Configure a remote domain that has the TrustedMailOutboundEnabled parameter set to $False.

D. Configure a remote domain that has the TNEFEnabled parameter set to $False.

ANSWER: D

Explanation:

Configure a remote domain that has the TNEFEnabled parameter set to $False. Winmail.dat is commonly created when Exchange sends messages using Transport Neutral Encapsulation Format (TNEF), which packages Outlook-rich formatting and certain MAPI properties into a format that recipients using non-Exchange-compatible mail clients may see as a Winmail.dat attachment. In Exchange Online, remote domain settings let administrators apply message-formatting behavior to a specific external recipient domain rather than changing the format for every external recipient. Create or modify the remote domain for fabrikam.com and disable TNEF by setting `TNEFEnabled` to `$false`. Exchange Online will then avoid using TNEF for messages sent to that remote domain, preventing the unwanted Winmail.dat attachment while preserving the ability to use other formatting behavior for different destinations. Microsoft documents that the `TNEFEnabled` remote-domain setting controls whether TNEF is used for messages sent to recipients in that domain. The configuration can be managed in Exchange Online PowerShell, for example with `Set-RemoteDomain -Identity fabrikam.com -TNEFEnabled $false`, after ensuring that the relevant remote-domain object exists. See Set-RemoteDomain and Remote domains in Exchange Online.

QUESTION NO: 13

You have a Microsoft Exchange Online tenant that contains a user mailbox named User1.

User1 leaves the company. The user's manager requires continued access to User1's existing email, but no one will sign in directly to User1's account.

You need to change User1's mailbox to a shared mailbox.

Which cmdlet should you run?

A. Set-Mailbox -Type Shared

B. Enable-Mailbox

C. New-Mailbox

D. Set-CASMailbox

ANSWER: A

Explanation:

You should run `Set-Mailbox -Type Shared`. The `Type` parameter of the Set-Mailbox cmdlet converts an existing user mailbox to a shared mailbox while retaining the mailbox content and email addresses. Administrators can then assign mailbox permissions to users who require access.

The `Enable-Mailbox` cmdlet enables mailbox functionality for an existing recipient, but it does not convert a user mailbox to a shared mailbox. `New-Mailbox` creates a new mailbox, and `Set-CASMailbox` configures client access settings.

For more information, see Set-Mailbox and Convert a user mailbox to a shared mailbox.

QUESTION NO: 14

You have a Microsoft Exchange Server 2019 organization.

You plan to implement a hybrid deployment between Exchange Online and Exchange Server. The deployment must meet the following requirements:

- Support Outlook for iOS and Android.
- Support 500 on-premises mailboxes.
- Support Modern Authentication.

Which hybrid configuration topology should you recommend?

A. Classic Full

B. Modern Minimal

C. Modern Full

D. Classic Minimal

ANSWER: A

Explanation:

Classic Full is the appropriate topology because the organization requires Hybrid Modern Authentication and support for Outlook for iOS and Android while retaining a substantial on-premises mailbox population. Hybrid Modern Authentication enables Exchange on-premises users to authenticate through Microsoft Entra ID and is the prerequisite for modern-authentication-capable clients, including Outlook mobile, to access on-premises Exchange mailboxes in a hybrid environment. Microsoft documents Hybrid Modern Authentication for Exchange Server hybrid deployments using the classic hybrid topology.

A full hybrid configuration establishes the complete hybrid feature set required for ongoing coexistence between Exchange Server and Exchange Online. This includes the organization relationship and OAuth-based capabilities used for cross-premises client and service functionality. It is suitable for an environment with 500 on-premises mailboxes because it is designed for sustained hybrid coexistence rather than a migration-only scenario. The Hybrid Configuration Wizard uses the classic topology when the deployment needs capabilities that require direct published Exchange connectivity and the full hybrid feature set.

For Microsoft's hybrid-topology guidance, see Hybrid Agent and modern hybrid topology. For Hybrid Modern Authentication requirements and configuration, see Using Hybrid Modern Authentication with Outlook for iOS and Android.

QUESTION NO: 15 - (DRAG DROP)

Your company has three departments name Dept1, Dept2. and Dept3 and a Microsoft Exchange Online tenant.

You need to increase security for the email messages sent from the departments. The solution must meet the following requirements:

« Users in Dept1 must be able to digitally sign and encrypt email messages as required.

+ Email messages sent from Dept2 to an external email domain must be encrypted automatically during transit only.

« Email messages sent from Dept3 to an external email domain must be encrypted until the recipient opens the message.

« Implementation costs must be minimized.

'Which type of encryption should you use for each department? To answer, drag the appropriate encryption types to the correct departments. Each encryption type may be used

ANSWER:

Explanation:

The correct mapping is Dept1 to S/MIME, Dept2 to TLS, and Dept3 to Microsoft Purview Message Encryption. S/MIME is the appropriate solution for Dept1 because it supports both required capabilities at the user-message level: a sender can digitally sign an email to provide authenticity and integrity, and can encrypt the email so its contents are protected for intended recipients. Exchange Online supports S/MIME for these signing and encryption scenarios when the required certificates are deployed to users.

TLS is appropriate for Dept2 because the stated scope is encryption during transit only. Exchange Online uses TLS to establish an encrypted SMTP transport session between mail systems. As a result, the message is protected while it travels across the connection to the external domain, without requiring an ongoing protected-message experience after delivery. This directly fits a transport-only requirement and avoids introducing unnecessary persistent message-protection administration.

Microsoft Purview Message Encryption is appropriate for Dept3 because its protection remains associated with the message after it leaves the organization. The recipient must authenticate or otherwise use the supported secure viewing experience to open protected content, allowing the organization to apply encryption and usage controls that persist through delivery and recipient access. This is the intended Microsoft 365 approach when mail must remain encrypted until the recipient opens it, including messages addressed to external recipients.

Using TLS for the limited transport requirement and reserving the more comprehensive message-level protections for the departments that explicitly require them meets the security objectives while keeping implementation effort proportionate to each use case. Microsoft documentation for S/MIME in Exchange Online, TLS configuration in Exchange Online, and Microsoft Purview Message Encryption describes these respective capabilities.

QUESTION NO: 16

You have a Microsoft Exchange Online tenant that contains a group named Group1.

The members of Group1 need to create user mailboxes. The solution must use the principle of least privilege.

To which role group should you add Group1?

A. Recipient Management

B. Security Operator

C. Help Desk

D. Organization Management

ANSWER: A

Explanation:

Recipient Management is the appropriate Exchange Online role group for this requirement. It is designed to delegate recipient administration tasks, including creating and managing mailbox recipients, without granting broad tenant-wide administrative permissions. Adding Group1 to this role group allows its members to perform the required user mailbox management work while keeping their permissions scoped to Exchange recipient operations.

This aligns with least privilege because the role group includes the recipient-management capabilities needed for tasks such as creating and modifying mailboxes, mail users, contacts, and distribution groups. The assigned users do not need access to unrelated organization-level configuration, security operations, or other Microsoft 365 administrative functions in order to create user mailboxes. Role-based access control in Exchange Online assigns permissions through management roles and role groups, enabling administrators to grant only the operational rights required for a delegated task.

Microsoft documents Recipient Management as the built-in role group for managing Exchange Online recipients. For further details, see Manage role groups in Exchange Online and Permissions in Exchange Online.

QUESTION NO: 17

You have a hybrid deployment that contains a Microsoft Exchange Online tenant and an on-premises Exchange Server 2019 server named Server1.

Server1 uses a certificate from a third-party certification authority (CA). The certificate is enabled for the SMTP service.

You replace the certificate with a new certificate.

You discover that delivery fails for all email messages sent from Server1 to your Microsoft 365 tenant.

You receive the following error message for all the queued email messages: “450 4.4.101 Proxy session setup failed on Frontend with 451 4.4.0 Primary target IP address responded with 451 5.7.3 STARTTLS is required to send mail.”

You need to ensure that the messages are delivered successfully from Server1 to the Microsoft 365 tenant.

What should you do?

A. From the Exchange admin center, update the TLS certificate name in the properties of the connector

B. From Server1, regenerate the certificate and select **Make private keys exportable**

C. From the firewall, disable SMTP content inspection

D. From Server1, enable the new certificate for the IMAP4 service

ANSWER: A

Explanation:

Update the TLS certificate name configured on the hybrid outbound connector to reference the replacement certificate. In an Exchange hybrid deployment, secure mail flow between on-premises Exchange and Exchange Online uses TLS. The Send connector used for outbound mail to Microsoft 365 can be configured with a `TlsCertificateName` value that identifies the certificate Exchange must present during the TLS negotiation. Replacing a certificate does not automatically update this connector setting if it still references certificate identity information from the former certificate.

Assigning the new certificate to SMTP is necessary, but it is not sufficient when the connector explicitly selects a certificate for TLS. Update the connector configuration with the TLS certificate name generated from the new certificate's issuer and subject, or rerun the Hybrid Configuration Wizard so that it updates the hybrid mail-flow configuration. This lets Server1 establish the required STARTTLS session with Exchange Online and resume delivery of queued messages.

Microsoft documents the hybrid certificate requirements and explains that the certificate must be enabled for SMTP and used by the hybrid connectors. See Hybrid deployment prerequisites and Set-SendConnector.

QUESTION NO: 18

You have a Microsoft Exchange Server 2019 organization.

You need to provide a user named User1 with the ability to create and manage transport rules.

To which management role group should you add User1?

A. Compliance Management

B. Server Management

C. Records Management

D. Hygiene Management

ANSWER: D

Explanation:

Hygiene Management is the appropriate built-in Exchange Server 2019 role group because it includes the *Transport Rules* management role. This role grants the permissions required to create, view, modify, enable, disable, and remove mail-flow (transport) rules in the Exchange organization. Transport rules are processed on messages while they are in transit through the Exchange transport pipeline and are commonly used to apply organization-wide mail-flow controls, such as adding disclaimers, redirecting messages, restricting delivery, or applying message handling conditions.

Adding User1 to Hygiene Management follows the principle of least privilege: the user receives the transport-rule administration capability without requiring broad, organization-wide administrative rights. Exchange uses role-based access control (RBAC), in which management role groups collect related management roles and assign their permissions to group members. Membership changes are made through the Exchange admin center or Exchange Management Shell and may require the user to sign out and sign in again before the new permissions are available.

Microsoft documents the Transport Rules role and its assignment to the Hygiene Management role group in its Exchange RBAC role documentation. See Permissions in Exchange Server and Understanding management role groups.

QUESTION NO: 19

You have a Microsoft 365 subscription that contains a user named User1.

You need to ensure that User1 can only manage eDiscovery cases that she creates and export the search results. The solution must use the principle of least privilege.

To which role should you add User1?

A. eDiscovery Manager

B. eDiscovery Administrator

C. Communications Compliance

D. Compliance Administrator

ANSWER: A

Explanation:

eDiscovery Manager is the appropriate role because it provides the scoped eDiscovery case-management permissions required while adhering to least privilege. A member of the eDiscovery Manager role group can create and manage eDiscovery cases, but is limited to accessing and managing cases that they created themselves. This directly meets the requirement that User1 must manage only her own cases rather than all cases in the organization.

The role group also provides the permissions needed to work with eDiscovery content within those cases, including creating and managing searches, placing content on hold where applicable, and exporting search results. Therefore, User1 can perform the required export operation without being granted broad tenant-wide compliance or eDiscovery administrative authority. Microsoft describes the eDiscovery Manager role group as intended for users who manage eDiscovery cases, with eDiscovery Managers restricted to the cases they create. This makes it the least-privileged built-in role assignment for the stated scenario.

For details, see Assign eDiscovery permissions and Microsoft Purview eDiscovery.

QUESTION NO: 20

Your company has a Microsoft Exchange Server 2019 organization.

You are auditing the Litigation Hold on the mailboxes of the company's research and development

department.

You discover that the mailbox of a user named User1 has a Litigation Hold enabled.

You need to discover who placed the Litigation Hold on the mailbox of User1, and when the Litigation Hold was enabled.

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

NOTE: Each correct selection is worth one point.

A. From the Exchange admin center, run an In-place eDiscovery and Hold report.

B. From PowerShell, run the Get-Mailbox cmdlet.

C. From the Exchange admin center. run a per-mailbox Litigation Hold report.

D. From PowerShell, run the Get-MailboxStatistics cmdlet.

ANSWER: B C

Explanation:

Running the `Get-Mailbox` cmdlet for User1 is an appropriate way to inspect the mailbox's Litigation Hold configuration. The mailbox object includes the `LitigationHoldOwner` and `LitigationHoldDate` properties. These properties identify the account recorded as the hold owner and the date and time that Litigation Hold was enabled. For a focused result, an administrator can run `Get-Mailbox -Identity User1 | Format-List LitigationHoldOwner,LitigationHoldDate`. Microsoft documents these Litigation Hold-related mailbox properties as part of the `Get-Mailbox` output: Get-Mailbox cmdlet.

The per-mailbox Litigation Hold report in the Exchange admin center provides the corresponding administrative view for auditing hold details for an individual mailbox. It enables the administrator to review the mailbox-specific Litigation Hold information, including the hold owner and the time the hold was applied, without needing to interpret broader discovery-case results. This aligns with Exchange Litigation Hold administration, where hold metadata is maintained with the mailbox configuration. For the Exchange Server Litigation Hold workflow and administration concepts, see Create or remove a Litigation Hold.

QUESTION NO: 21

You have a Microsoft Exchange Server 2019 organization.

You plan to migrate to Exchange Online incrementally during a 12-month period.

You need to ensure that during the migration, the following features continue to work for all users:

Free/Busy synchronization

Microsoft Teams calendar integration

The Microsoft Outlook mobile app for Android

Which hybrid configuration should you implement?

A. Modern Hybrid Configuration

B. Minimal Hybrid Configuration

C. Classic Hybrid

ANSWER: C

Explanation:

Classic Hybrid is correct because it provides the full Exchange hybrid coexistence feature set needed for an extended, staged migration. A classic hybrid deployment uses hybrid configuration between the on-premises Exchange organization and Exchange Online, enabling organization relationships and availability sharing so users can retrieve free/busy information across mailbox locations. This allows scheduling to remain consistent while some mailboxes are on-premises and others have moved to Exchange Online.

It also supports the service integration required for a productive coexistence period, including Microsoft Teams calendar access and Outlook mobile connectivity for users whose mailboxes remain on-premises or have been migrated. Microsoft documents that full hybrid deployments are intended for organizations that require rich coexistence features during longer migrations, rather than merely a short-term mailbox move. Exchange Server 2019 is supported for hybrid connectivity with Exchange Online, provided that the organization meets the applicable Exchange hybrid requirements and uses the Hybrid Configuration Wizard.

For implementation guidance and supported coexistence capabilities, see Hybrid deployment prerequisites and Hybrid Agent and hybrid deployment options.

QUESTION NO: 22

You need to ensure that Alex Wilber can recover deleted items when using Outlook on the web.

Which two actions should you perform? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Assign Sales Policy to Alex Wilbur.

B. Modify Marketing Policy.

C. Remove Alex Wilbur from all groups.

D. Assign Policy2 to Alex Wilbur.

E. Modify Policy1

ANSWER: B D

Explanation:

Deleted-item recovery in Outlook on the web depends on the mailbox's Exchange retention configuration. The applicable retention policy must include a retention tag for the Deleted Items folder that uses the *Delete and allow recovery* retention action. This action moves items out of the Deleted Items folder after the defined retention age while keeping them available in the Recover Deleted Items location for the mailbox's deleted-item retention period. Therefore, *Modify Marketing Policy.* is a complete solution when that modification adds or configures the required Deleted Items retention tag. *Assign Policy2 to Alex Wilbur.* is also a complete solution because Policy2 is the policy that provides the required recoverable-deletion behavior, and assigning it makes that policy apply to Alex's mailbox. Retention policies are assigned per mailbox, and the mailbox can have one retention policy at a time; the policy's linked retention tags determine the actions available for mailbox folders. Microsoft documents the Deleted Items retention tag and its recovery-capable action in its retention-tag guidance. See Retention tags and retention policies in Exchange Server and Recover deleted messages in Outlook on the web.

QUESTION NO: 23

You manage an Exchange Online tenant.

You plan to migrate on-premises Microsoft Exchange Server mailboxes by using a cutover migration.

You need to grant the required permissions to the migration administrator account to complete the migration. The solution must use the principle of least privilege.

Which three permissions should you grant? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. the FullAccess permission on each on-premises mailbox and the WriteProperty permission to modify the TargetAddress property of the on-premises user account

B. the Receive As permission on the on-premises mailbox database that stores the user mailboxes and the WriteProperty permission to modify the TargetAddress property of the on-premises user account

C. Domain Admins group member in Active Directory Domain Services (AD DS) of the on-premises Exchange organization

D. the FullAccess permission on each on-premises mailbox

E. the Receive As permission on the on-premises mailbox database that stores the user mailboxes

ANSWER: C D E

Explanation:

For a cutover migration, the migration administrator account must be able to access the contents of every source mailbox in the on-premises Exchange organization. Membership in the Domain Admins group supplies the broad Active Directory and Exchange-related access that enables the account to perform the required source-side operations. Alternatively, mailbox access can be delegated more directly by granting FullAccess on every on-premises mailbox. This allows the migration service to open and copy mailbox data without assigning broader administrative rights across the domain. A third supported delegation model is to grant Receive As on the mailbox database or databases that contain the mailboxes being migrated. Receive As provides mailbox-level access for all mailboxes hosted in the applicable database, avoiding the administrative

overhead of assigning FullAccess individually to each mailbox. These are alternative complete source-permission approaches for the migration account; in a least-privilege implementation, use the narrowest approach that covers all mailboxes in scope, such as individual FullAccess permissions or Receive As scoped to only the required databases. Microsoft documents these supported permission paths for Exchange mailbox migrations in Assign permissions for mailbox migration and provides the cutover migration process in Cutover migration to Microsoft 365 or Office 365.

QUESTION NO: 24

You must prevent HelpDeskUser1 from repeating the same mistake.

You need to identify which management role provided HelpDeskUser1 with the necessary permissions to make the mistake identified in the problem statement.

Which two cmdlets should you run? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Get-ManagementRoleEntry

B. Get-RoleGroupMember

C. Get-ManagementRole

D. Get-ManagementRoleAssignment

E. Get-RoleGroup

ANSWER: A D

Explanation:

`Get-ManagementRoleAssignment` is used to examine Exchange RBAC role assignments and determine which management roles are assigned to, or effective for, HelpDeskUser1. Role assignments connect management roles to role assignees such as users, role groups, security groups, or assignment policies. In particular, the cmdlet can be used with effective-user output to identify assignments that grant permissions to a specified user. This establishes the role or roles through which HelpDeskUser1 receives administrative capability.

`Get-ManagementRoleEntry` is then used to inspect the cmdlet entries contained in the identified management role. A management-role entry represents a permitted cmdlet and, where applicable, its permitted parameters. Querying the role entries lets an administrator confirm that the role includes the specific command or parameter required to perform the problematic action. Together, these cmdlets trace the permission path from the user's effective RBAC assignment to the exact management-role permission that enabled the action, providing the information needed to adjust assignments or role entries appropriately. Microsoft documents this RBAC investigation workflow in Find the permissions required to run Exchange cmdlets and documents role-assignment discovery at Get-ManagementRoleAssignment.

QUESTION NO: 25

You need to recommend a solution for the public folders that supports the planned changes and meets the technical requirements.

What should you recommend?

A. Microsoft SharePoint site mailboxes

B. Office 365 groups

C. Resource mailboxes

D. Public folder replicas

ANSWER: B

Explanation:

Office 365 groups is the appropriate recommendation because Microsoft 365 Groups provide a modern collaboration workspace that can replace common public-folder usage scenarios. A group includes a shared Exchange mailbox and calendar, and can be connected to additional Microsoft 365 services such as a SharePoint site, Planner, Teams, and OneNote. This gives users a centrally managed membership model and collaboration features that extend beyond the email-centric capabilities of public folders.

Microsoft provides a supported process to migrate public folders to Microsoft 365 Groups. The migration process creates groups from the public-folder hierarchy and transfers supported content, enabling the organization to modernize the collaboration experience while retaining relevant folder data. Group owners can manage membership and access, and administrators can apply Microsoft 365 governance and compliance capabilities appropriate to group-connected resources. Therefore, Office 365 groups supports a planned move away from public folders while providing the shared conversations, calendar, files, and membership functionality expected for modern team collaboration.

See Migrate public folders to Microsoft 365 Groups and Compare Microsoft 365 groups.

QUESTION NO: 26

You have a Microsoft 365 E3 subscription that uses Microsoft Exchange Online. You need to retain audit log entries for users in the legal department for up to one year. Which two actions should you perform? Each Correct answer presents part of the solution.

Note: Each Correct Selection is worth one point.

A. For the default audit log retention policy, set Duration to 1 Year.

B. Assign a Microsoft Office 365 E5 license to each legal department user.

C. Create a retention policy that has a one-year retention tag and apply the policy to the user mailboxes in the legal department.

D. Create a new audit log retention policy and assign the policy to the legal department.

E. Assign a Microsoft Office 365 E5 license to each user in the tenant.

ANSWER: B D

Explanation:

Assigning a Microsoft Office 365 E5 license to each legal department user provides the Audit Premium entitlement needed for extended audit-record retention beyond the standard Audit retention period included with E3. Licensing must be assigned to the users whose audit records require the extended retention, so assigning it specifically to the legal department meets the stated scope without unnecessarily licensing the entire tenant.

Creating a new audit log retention policy and assigning the policy to the legal department then defines how long the applicable audit records are retained. Audit retention policies can be scoped to specified users and can retain their audit records for up to one year under the Audit Premium licensing capability. The policy should be configured with a one-year retention duration and the legal users included in its scope. This approach protects the audit events generated by those users—such as mailbox, SharePoint, Teams, and other audited Microsoft 365 activities—rather than applying an Exchange mailbox retention configuration, which governs mailbox content rather than Microsoft Purview Audit records.

Microsoft documents the licensing and retention capabilities for Audit Premium in Audit Premium and explains how to configure scoped audit retention policies in Manage audit log retention policies.

QUESTION NO: 27

You have a Microsoft Exchange Server 2019 organization.

You purchase a Microsoft Office 365 E5 subscription.

You plan to implement Exchange Modern Hybrid and free/busy sharing.

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

NOTE: Each correct selection is worth one point.

A. a sharing policy

B. a federation trust

C. an organization relationship

D. a relying party trust

E. Active Directory Lightweight Directory Services (AD LDS)

ANSWER: B C

Explanation:

A federation trust and an organization relationship provide the Exchange configuration that supports cross-organization availability sharing in a hybrid coexistence deployment. The federation trust establishes Exchange's trust with the Microsoft federation service, allowing the on-premises Exchange organization to authenticate and share availability information with Exchange Online. In a hybrid environment, this trust is normally created or validated as part of running the Hybrid Configuration Wizard.

The organization relationship defines the specific relationship between the on-premises Exchange organization and the Exchange Online organization. It includes the external domain namespace and availability settings that determine how free/busy requests are sent and what calendar detail can be returned. Exchange uses this relationship to locate the remote organization's availability service and apply the intended sharing scope for users.

Together, these components establish the trust and the organization-specific availability configuration needed for users in Exchange Server 2019 and Exchange Online to view each other's calendar availability. Microsoft's hybrid deployment guidance identifies organization relationships and federation configuration as key elements for cross-premises free/busy coexistence. See Hybrid deployment prerequisites in Exchange Server and Create an organization relationship in Exchange Server.

QUESTION NO: 28

You plan to use the Microsoft Office 365 Import service to import PST files.

You need to create a new user account to perform the import. The solution must use the principle of least privilege.

Which two roles should you assign to the user account? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. the Recipient Management role in Office 365

B. the Organization Management role in Office 365

C. the Mailbox Import Export role in Office 365

D. the Global reader role in Azure Active Directory (Azure AD)

E. the Global administrator role in Office 365

ANSWER: A C

Explanation:

The correct least-privilege assignment combines **the Recipient Management role in Office 365** with **the Mailbox Import Export role in Office 365**. Recipient Management provides the limited Exchange recipient-administration scope needed

when working with mailbox recipients that are the targets of the PST import. This avoids granting broad tenant-wide administrative permissions merely to perform a mailbox-data migration task.

The Mailbox Import Export role is the Exchange RBAC management role that authorizes mailbox import and export operations, including the PST import capability used by the Office 365 Import service. Microsoft treats this as a sensitive role and does not generally include it in broad default administrative assignments; it should be granted explicitly to the account or a narrowly scoped role group that performs the import. Assigning these two permissions to the dedicated import account supplies the recipient-management and mailbox-import capabilities required for the operation while following least privilege.

For Exchange Online RBAC role-group guidance, see Manage role groups in Exchange Online. For PST import-service procedures and permission requirements, see Import PST files to Microsoft 365.

QUESTION NO: 29

You have a Microsoft 365 subscription.

A safe attachments policy that uses Dynamic Delivery is applied to all recipients who match your SMTP domains.

You need to prevent attachments from being scanned when internal users send email to one another.

What should you do?

A. From the Exchange admin center, create a transport rule.

B. From the Exchange admin center, modify the malware filter.

C. From the Security & Compliance admin center, modify the safe attachments policy.

D. From the Security & Compliance admin center, modify the Service assurance settings.

ANSWER: A

Explanation:

From the Exchange admin center, create a transport rule. is correct because mail flow rules can identify messages that are sent internally and stamp them with the Exchange organization header that bypasses Safe Attachments processing. Configure the rule to match messages where both the sender and recipient are internal to the organization, then set the `X-MS-Exchange-Organization-SkipSafeAttachmentProcessing` message header to `1`. This prevents Safe Attachments from scanning attachments on those internal messages while allowing the existing Safe Attachments policy, including Dynamic Delivery, to continue protecting messages that require scanning.

This approach provides a targeted exception based on message flow instead of changing the recipient scope of the Safe Attachments policy. Consequently, the organization can retain its policy coverage for mail sent from external sources and other applicable traffic. Exchange mail flow rules support adding message headers as rule actions, and Safe Attachments supports this specific header as a mechanism for bypassing its attachment-processing workflow when an intentional exception is required. See Safe Attachments in Microsoft Defender for Office 365 and Mail flow rules in Exchange Online.

QUESTION NO: 30

You have a Microsoft Exchange Online tenant that contains a distribution group named ProjectTeam.

A consultant named User1 works for a partner organization and has an email address of user1@fabrikam.com.

You need to add User1 to ProjectTeam without creating a user account in the tenant.

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 mail contact for User1.

B. Add the mail contact to ProjectTeam.

C. Create a remote mailbox for User1.

D. Create a shared mailbox for User1.

E. Create an organization relationship with fabrikam.com.

ANSWER: A B

Explanation:

Create a mail contact for User1 and specify user1@fabrikam.com as the external email address. A mail contact is an Exchange recipient object that represents a person outside the organization and provides an external SMTP address for mail delivery.

After the mail contact is created, add the mail contact as a member of ProjectTeam. Distribution groups can contain mail contacts as members, allowing the consultant to receive messages sent to the group while avoiding the creation and licensing of a Microsoft 365 user account. A mail user would require an associated Microsoft Entra user account, and a remote mailbox is used for hybrid recipient management.

For more information, see Manage mail contacts in Exchange Online and Manage distribution groups in Exchange Online.

QUESTION NO: 31 - (HOTSPOT)

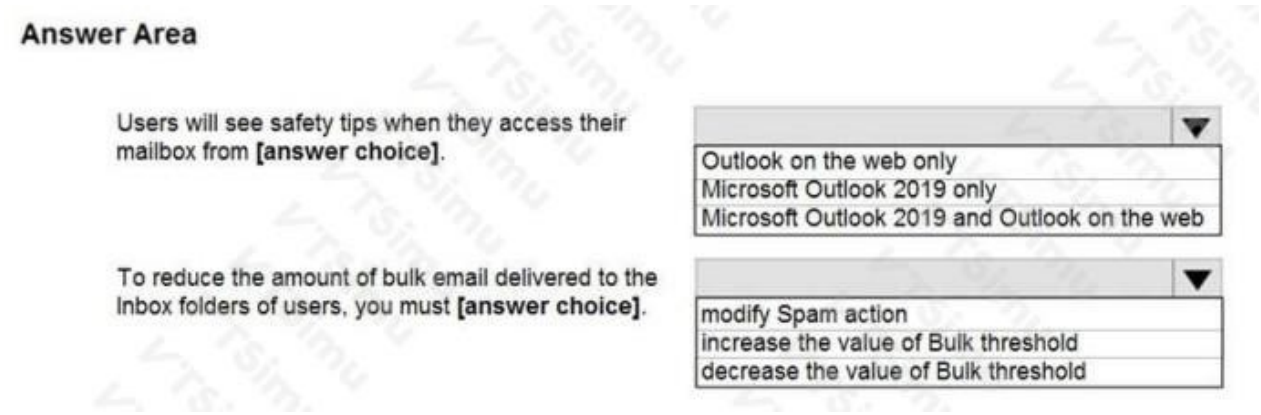
HOTSPOT

You have an Exchange Online tenant that has the anti-spam settings configured as shown in the following exhibit.

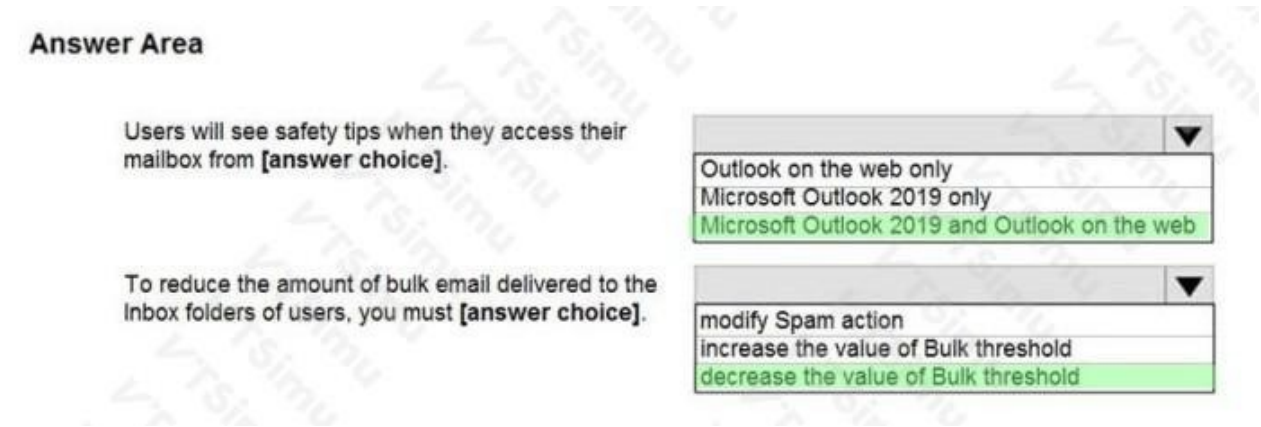
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

Safety tips are visual messages in the mail client that help users recognize potentially suspicious messages before they interact with them. In Exchange Online and Microsoft Defender for Office 365, these tips can communicate conditions such as an unverified sender, a first-time sender, or a message that has characteristics associated with phishing. The relevant client support includes Outlook on the web and Outlook 2019, so users can see the applicable safety-tip indicators when accessing their mailboxes through either of those clients. Microsoft documents the available safety-tip behavior and user experience in its safety tips and indicators documentation.

The Bulk Complaint Level, commonly called BCL or Bulk threshold in anti-spam policy settings, is a numerical measure of how likely a message is to be considered bulk mail. A lower threshold causes messages with lower BCL scores to meet the bulk-mail classification criterion. Consequently, lowering the Bulk threshold increases the volume of mail processed as bulk. The anti-spam policy's configured bulk-mail action then determines how those messages are handled, such as moving them to Junk Email or quarantining them, thereby reducing the amount of bulk email that reaches users' Inbox folders. Microsoft describes the threshold and its relationship to bulk-mail handling in the Bulk Complaint Level values guidance. Therefore, the correct completed statements identify Microsoft Outlook 2019 together with Outlook on the web for safety tips, and decreasing the Bulk threshold to reduce Inbox delivery of bulk email.

QUESTION NO: 32

You have a Microsoft Exchange Online tenant that contains a room mailbox named ConferenceRoom1.

Users report that meeting requests sent to ConferenceRoom1 remain in the room mailbox Inbox until an administrator responds manually.

You need to ensure that ConferenceRoom1 automatically accepts available meeting requests and declines conflicting requests.

What should you configure?

A. Set AutomateProcessing to AutoAccept.

B. Set AutomateProcessing to None.

C. Enable mailbox forwarding.

D. Assign the Mail Recipients role.

ANSWER: A

Explanation:

You should configure `AutomateProcessing` as `AutoAccept` for ConferenceRoom1. The AutoAccept setting causes the Calendar Attendant to process meeting requests automatically. It accepts requests when the room is available and declines requests that conflict with existing reservations or violate booking policies.

Changing the mailbox's forwarding settings or granting users Full Access permissions does not configure calendar processing. The setting can be configured by using `Set-CalendarProcessing`, for example: `Set-CalendarProcessing -Identity ConferenceRoom1 -AutomateProcessing AutoAccept`.

For more information, see Set-CalendarProcessing.

QUESTION NO: 33

You have a Microsoft Exchange Online tenant that has Office 365 Advanced Threat Protection (ATP) enabled.

The tenant contains a user named Ben Smith who has a UPN of ben.smith@fabrikam.com. Ben Smith is protected by using an ATP anti-phishing policy.

Ben Smith reports that emails sent from his personal account of ben.smith@relecloud.com are not delivered to his work email account.

You need to ensure that personal emails are delivered to the ben.smith@fabrikam.com

What should you do?

A. Create a transport rule to assign the MS-Exchange-Organization-PhishThresholdLevel header a value of 2 for the message received from ben.smith@relecloud.com

B. Add ben.smith@fabrikam.com as a trusted sender to the ATP anti-phishing policy.

C. Add ben.smith@relecloud.com as a trusted sender to the ATP anti-phishing policy.

D. Add relecloud.com to the ATP anti-phishing list of misted domains.

ANSWER: C

Explanation:

Add **ben.smith@relecloud.com** as a trusted sender in the ATP anti-phishing policy. Anti-phishing policies in Microsoft Defender for Office 365 provide impersonation and spoofing protection, which can identify messages as suspicious when a sender address resembles a protected user or organization. In this case, Ben's personal address contains the same name as the protected work identity, so it can be evaluated by the policy's phishing protections.

The policy's trusted senders and domains settings provide an explicit exception for mail from a known, legitimate external sender. Adding the full personal email address is appropriately narrow: it allows messages sent specifically from **ben.smith@relecloud.com** to reach Ben's work mailbox while retaining anti-phishing protection for other senders at relecloud.com and elsewhere. Configure this exception in the anti-phishing policy that applies to Ben, and ensure the policy remains assigned to the intended recipient scope. Microsoft documents trusted senders and domains as anti-phishing policy settings used to exclude recognized senders from phishing evaluation. See Anti-phishing policies in Microsoft Defender for Office 365 and Configure anti-phishing policies.

QUESTION NO: 34

All the users in your company are licensed for Microsoft 365 and connect to their mailbox from client computers that run Windows 10.

The users connect to Outlook on the web by using the following browsers:

You apply restrictions for Outlook on the web sessions by using app protection policies in Microsoft Endpoint Manager, and then you deploy several Outlook Web App policies.

You need to ensure that the users can continue to connect successfully to their mailbox by using Outlook on the web.

What should you do?

A. Enroll all the computers in Microsoft Intune

B. Instruct all the users to connect by using Microsoft Edge only

C. From Microsoft Cloud App Security, configure a sanctioned application

ANSWER: B

Explanation:

Instruct all the users to connect by using Microsoft Edge only. Outlook on the web session restrictions that integrate Microsoft Intune app protection policies rely on the Microsoft Edge browser on Windows devices. This integration enables Exchange Online Outlook on the web mailbox policies to apply the intended protection controls to a browser session, such as restrictions governing data transfer from the session. Standardizing users on Microsoft Edge ensures that the browser can receive and enforce the applicable Intune app protection settings while users access their Exchange Online mailboxes through Outlook on the web.

This approach is specifically about browser-based access and app-level data protection; it does not require Windows computers to be enrolled in Intune merely for users to access Outlook on the web under these protections. The Outlook on the web policy is deployed through Exchange Online, while Intune provides the app-protection-policy component for the supported browser experience. Microsoft documents the Outlook on the web and Intune integration, including the requirement to use Microsoft Edge for supported protected browser sessions, in its guidance for app protection policies for Outlook on the web. Additional details about configuring and using these protections are available in Microsoft Intune app protection policies.

QUESTION NO: 35 - (SIMULATION)

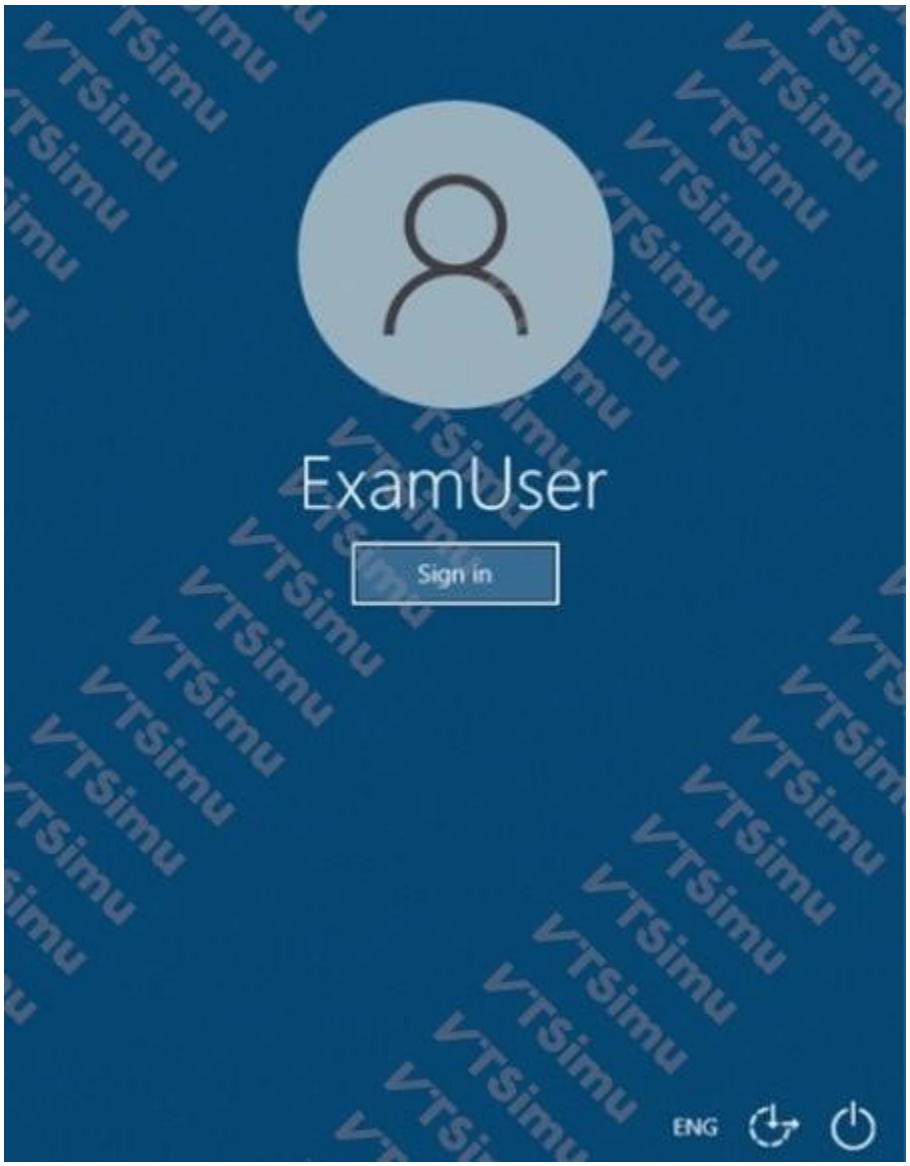
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@abc.com

Microsoft 365 Password: xxxxxx

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only.

Lab Instance: XXXXXX

Users report that email disclaimers are no longer being appended to email messages sent to external recipients.

You need to ensure that all email sent to external recipients contains your corporate disclaimer.

To complete this task, sign in to the Microsoft 365 admin center.

ANSWER: See the explanation for the answer

Explanation:

Enable the existing external-recipient disclaimer mail-flow rule.

1. Sign in to the Microsoft 365 admin center as `admin@abc.com`.
2. Open the **Exchange admin center** (Admin centers > Exchange).
3. Go to **Mail flow** > **Rules**.
4. Select the rule that appends the corporate disclaimer to messages sent externally (for example, a rule named *Corporate Disclaimer* or *Append disclaimer to external messages*).
5. Edit the rule and turn it **On/Enabled** (ensure its mode is **Enforce**, not Test or Disabled).
6. Confirm that the rule applies when the recipient is **outside the organization** and that its action is to **append/apply the corporate disclaimer**.
7. Click **Save**.

This restores the transport (mail-flow) rule responsible for adding the disclaimer to all outbound email addressed to external recipients.

Reference: Mail flow rule actions for disclaimers, signatures, footers, or headers

QUESTION NO: 36

You recently migrated all the on-premises mailboxes from Microsoft Exchange Server 2019 to Exchange Online.

You decommission the on-premises Exchange Server 2019 servers.

The finance department at your company reports that email delivery from several printers fails after Exchange Server 2019 is decommissioned.

You need to ensure that the printers can deliver email successfully to the users in the finance department.

What should you do?

A. Create a resource mailbox for each printer.

B. Create an Inbound connector that has certificate validation disabled.

C. Create an Inbound connector that is configured to allow SMTP relay.

D. Create an Office 365 group for each printer.

ANSWER: C

Explanation:

Create an Inbound connector that is configured to allow SMTP relay. The printers previously depended on the on-premises Exchange servers as an SMTP relay endpoint. Once those servers were decommissioned, the devices no longer had an authorized relay service through which they could submit messages to Exchange Online recipients.

An inbound connector in Exchange Online identifies and trusts the organization's SMTP relay source, typically by its public IP address or, where supported, a TLS certificate. The connector provides the controlled mail-flow path that allows the printers to send messages using Exchange Online Protection and have them delivered to the finance users' Exchange Online mailboxes. The printers must be configured to send SMTP traffic to the Microsoft 365 endpoint and the connector must be scoped to the organization's known sending source. This approach is intended for devices and applications that cannot use authenticated client SMTP submission but need to relay mail to internal Microsoft 365 recipients.

Microsoft documents this pattern as SMTP relay through an Exchange Online connector and recommends restricting the connector to known IP addresses or certificates to prevent unauthorized relay. See How to set up a multifunction device or application to send email using Microsoft 365 and Use connectors to configure mail flow.

QUESTION NO: 37

Your network contains an Active Directory domain named fabrikam.com.

You have a Microsoft Exchange Server 2019 organization that contains two Mailbox servers. The servers are members of a database availability group (DAG).

You plan to implement an Exchange hybrid deployment.

You are evaluating the use of the Exchange Modern Hybrid connection option during the hybrid deployment.

What are two benefits of using Exchange Modern Hybrid instead of Exchange Classic Hybrid? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. allows the use of Microsoft Azure Multi-Factor Authentication (MFA) for on-premises users

B. eliminates the need to purchase publicly trusted certificates for communication between the on-premises organization and Exchange Online

C. preserves mailbox quotas when mailboxes are moved between the on-premises organization and Exchange Online

D. uses Organization Configuration Transfer to configure Exchange Online

E. allows federated sharing between the on-premises organization and Exchange Online

ANSWER: B D

Explanation:

Exchange Modern Hybrid uses the Hybrid Agent to establish outbound connectivity from the on-premises Exchange organization to Microsoft 365. Because this agent-based connection is brokered through Microsoft's service, the hybrid deployment does not require an externally published on-premises Exchange endpoint for the supported hybrid features. Consequently, the organization does not need to acquire and deploy a publicly trusted certificate specifically for communication between the on-premises organization and Exchange Online. This simplifies the required external DNS, certificate, and inbound network configuration.

Modern Hybrid also uses Organization Configuration Transfer as part of the Hybrid Configuration Wizard experience to transfer supported Exchange organization settings to Exchange Online. This automates configuration that otherwise must be created and maintained separately, helping establish the cloud-side organization configuration needed for a hybrid deployment and mailbox migration scenario. The transfer capability reduces manual setup effort while maintaining supported configuration consistency between the on-premises Exchange organization and Exchange Online.

For implementation details, see Hybrid Agent and Organization Configuration Transfer in Microsoft Learn.

QUESTION NO: 38

You have a hybrid deployment between a Microsoft Exchange Online tenant and an on-premises Exchange Server 2019 organization.

The tenant uses an email domain named @contoso.com.

You recently purchased an email domain named fabrikam.com.

You need to ensure that all the users in the tenant can receive email messages by using the @fabrikam.com email domain. The solution must ensure that the users can continue to receive email by using the @contoso.com email domain.

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

NOTE: Each correct selection is worth one point.

A. From Azure AD Connect, add a domain for fabrikam.com.

B. From the on-premises Exchange admin center, modify the email address policy.

C. From the on-premises Exchange admin center, add an accepted domain for fabrikam.com.

D. From the Microsoft 365 admin center, verify the fabrikam.com email domain.

E. From Azure Cloud Shell, create a script that runs the Set-Mailbox cmdlet.

F. From the Microsoft 365 admin center, add the fabrikam.com email domain.

ANSWER: D E F

Explanation:

To provide every Exchange Online mailbox with an additional fabrikam.com receiving address while retaining its existing contoso.com address, first add fabrikam.com as a custom domain in the Microsoft 365 admin center. Adding the domain starts the Microsoft 365 domain onboarding process and makes the domain available for use by the tenant. The domain must then be verified in the Microsoft 365 admin center by publishing the required DNS verification record. Verification proves ownership of fabrikam.com and enables Microsoft 365 to use it for email addresses and mail flow.

After the domain is available, use Exchange Online PowerShell to run `Set-Mailbox` for each relevant cloud mailbox, adding a fabrikam.com SMTP proxy address. This can be automated in a script run from Azure Cloud Shell. Adding the new address as an alias preserves the existing contoso.com address, so mail continues to be delivered for both domains. The primary SMTP address can remain contoso.com unless there is a separate requirement to change the primary reply address. Microsoft documents adding and verifying custom domains at Add a domain to Microsoft 365 and managing mailbox email addresses through Exchange Online PowerShell at Set-Mailbox.

QUESTION NO: 39

You have a Microsoft 365 subscription that uses a default domain named contoso.com.

Users report that email messages from a domain named fabrikam.com are identified as spam even though the messages are legitimate.

You need to prevent messages from fabrikam.com from being identified as spam.

What should you do?

A. Enable the Zero-hour auto purge (ZAP) email protection feature.

B. Enable the safe list on a connection filter.

C. Edit the default mail flow rule to bypass the spam filter.

D. Modify the IP Allow list of a connection filter policy.

E. Add fabrikam.com to the allowed domains list in the inbound anti-spam policy.

ANSWER: E

Explanation:

Add fabrikam.com to the allowed domains list in the inbound anti-spam policy. This configuration is designed for known, trusted sending domains whose legitimate messages are being incorrectly classified as spam. The allowed sender and allowed domain settings are evaluated by Exchange Online Protection during inbound anti-spam processing, enabling administrators to account for recurring false positives from approved external correspondents.

The domain entry should be limited to the specific trusted domain, fabrikam.com, rather than applying a broad mail-flow bypass. A domain-based allow entry addresses the stated requirement directly without requiring knowledge of the sender's outbound IP addresses, which can change or be shared by multiple senders. Microsoft also recommends using the Tenant Allow/Block List where appropriate for managing allow and block entries; however, the inbound anti-spam policy's allowed domains setting is the direct policy setting represented by this scenario and is appropriate for allowing mail from a trusted domain.

For details on configuring anti-spam policy allow lists, see Configure anti-spam policies in Microsoft Defender for Office 365. For Microsoft guidance on managing allow and block entries, see Tenant Allow/Block List in Microsoft Defender for Office 365.

QUESTION NO: 40

You need to recommend an Office 365 solution that meets the technical requirements for email from adatum.com.

Which two components should you recommend configuring from the Exchange admin center in Exchange Online? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. a malware filter

B. a connection filter

C. data loss prevention (DLP) policies

D. DKIM signatures

E. a spam filter

ANSWER: B E

Explanation:

A connection filter and a spam filter are the appropriate Exchange Online Protection components to configure for controlling unwanted email sent to adatum.com. Connection filtering evaluates the source of inbound messages before normal content filtering occurs. Administrators can use the IP Allow List and IP Block List to explicitly trust known sending infrastructure or block known unwanted sources. This is particularly useful when the stated email requirements involve accepting messages from approved external systems or preventing mail from identified source IP addresses.

A spam filter complements that source-based control by evaluating the message itself and applying anti-spam policy actions. Exchange Online Protection can identify spam, bulk mail, phishing-related spam signals, and related unwanted content, then apply the organization's selected handling action, such as moving the message to Junk Email or quarantining it. Together, these controls provide both connection-level and message-level anti-spam protection for inbound mail.

Microsoft documents connection filtering, including configuration of allowed and blocked IP addresses, at Configure connection filter policies. Configuration and behavior of Exchange Online Protection anti-spam policies are documented at Configure anti-spam policies.

QUESTION NO: 41

Your company has a Microsoft Exchange Server 2019 organization.

You are auditing the Litigation Hold on the mailboxes of the company's research and development

department.

You discover that the mailbox of a user named User1 has a Litigation Hold enabled.

You need to discover who placed the Litigation Hold on the mailbox of User1, and when the Litigation Hold was enabled.

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

NOTE: Each correct selection is worth one point.

A. From the Exchange admin center, run an In-place eDiscovery and Hold report.

B. From PowerShell, run the Get-Mailbox cmdlet.

C. From the Exchange admin center, view the per-mailbox Litigation Hold information.

D. From PowerShell, run the Get-MailboxStatistics cmdlet.

ANSWER: B C

Explanation:

Run the Get-Mailbox cmdlet and inspect User1's Litigation Hold properties. Exchange stores the key audit-style metadata directly on the mailbox object: `LitigationHoldOwner` identifies the administrator or account that enabled the hold, and `LitigationHoldDate` records when it was enabled. For example, administrators can retrieve the relevant values with `Get-Mailbox -Identity User1 | Format-List LitigationHoldEnabled,LitigationHoldOwner,LitigationHoldDate`. This is the authoritative PowerShell method because it reads the properties maintained for that mailbox's Litigation Hold configuration.

Viewing the per-mailbox Litigation Hold information in the Exchange admin center provides the corresponding graphical administrative view for the mailbox. The mailbox's Litigation Hold settings are accessed through the recipient mailbox features, allowing an administrator to review the hold configuration for the individual mailbox while auditing it. Using both the Exchange admin center mailbox view and Get-Mailbox provides the requested information through the graphical interface and a precise, scriptable command-line query. Microsoft documents the mailbox properties exposed by Get-Mailbox and the Exchange mailbox-feature management experience in Manage mailbox features in Exchange Server.

QUESTION NO: 42

NO: 29

You have a Microsoft Exchange Server 2019 organization named contoso.com and an Exchange Online tenant.

You plan to implement a hybrid deployment.

You have the certificates shown in the following table.

You need to identify which certificates can be assigned in the Microsoft Office 365 Exchange Hybrid Configuration wizard.

Which certificates should you identify?

A. Cert4 and Cert5 only

B. Cert2 and Cert3 only

C. Cert1 only

D. Cert3 and Cert5 only

E. Cert2 and Cert4 only

F. Cert2, Cert3, Cert4, and Cert5 only

ANSWER: E

Explanation:

Cert2 and Cert4 only can be used for the hybrid configuration because a certificate selected by the Hybrid Configuration wizard must support the externally published Exchange namespace used for hybrid mail flow and services. The certificate must be valid, include a private key, be trusted by a public certification authority, and contain the required external fully qualified domain name in either its subject name or a subject alternative name. A wildcard certificate can satisfy the name requirement for a matching host under the domain, provided it is otherwise valid and trusted. These requirements allow Exchange Online to establish trusted TLS connections to the on-premises Exchange organization and enable secure hybrid functionality. Microsoft recommends using a certificate from a trusted third-party certification authority for hybrid deployments, rather than a self-signed certificate. The certificate must also be available on the applicable Exchange server and enabled for the services required by the hybrid configuration, including SMTP for secure mail transport. For the certificate selection requirements used by hybrid deployments, see Microsoft Learn: Hybrid deployment prerequisites and Microsoft Learn: Exchange certificate requirements.

QUESTION NO: 43

You plan to use the Hybrid Agent to integrate your Microsoft Exchange Server 2016 organization and Exchange Online.

The installation of the Hybrid Agent fails.

You validate the following Exchange virtual directory settings.

```
Get-WebServicesVirtualDirectory | fl

ExternalAuthenticationMethods: {Ntlm, WindowsIntegrated, WSSecurity, OAuth}
InternalURL : https//mail.contoso.com/EWS/Exchange.asmx
ExternalURL: https://mail.contoso.com/EWS/Exchange.asmx
MRSProxyEnabled: False
Server : EX01

Get-MAPIVirtualDirectory | fl

InternalURL : https://autodiscover.contoso.com/mapi
ExternalURL: https//Autodiscover.contoso.com/mapid
Server: EX01

Get-OWAVirtualDirectory | fl

InternalURL : https://mail.contoso.com/owa
ExternalURL: https://mail.contoso.com/owa
Server: EX01
```

You need to install the Hybrid Agent successfully.

What should you do first?

A. Update the server parameter of WebServicesVirtualDirectory to the FQDN of Exchange instead of the host name.

B. Set MRSProxyEnabled to True.

C. Remove WindowsIntegrated from ExternalAuthenticationMethods.

D. Change the ExternalURL parameter of MAPIVirtualDirectory to https://mail.contoso.com instead of https://autodiscover.contoso.com.

ANSWER: B

Explanation:

Set MRSProxyEnabled to True. The Mailbox Replication Service (MRS) Proxy is exposed through the Exchange Web Services virtual directory and is required for hybrid mailbox move operations between the on-premises Exchange organization and Exchange Online. The Hybrid Agent installation and configuration process validates the selected Exchange server's hybrid connectivity prerequisites, including availability of the MRS Proxy. If MRS Proxy is disabled, the agent cannot support the required migration functionality and the installation validation fails.

Enable the setting on the appropriate Exchange Web Services virtual directory, for example by using `Set-WebServicesVirtualDirectory -Identity "<server>\EWS (Default Web Site)" -MRSProxyEnabled $true`. After enabling it, allow the configuration to apply and rerun the Hybrid Configuration Wizard or Hybrid Agent installation. Microsoft documents MRS Proxy as a required component for remote mailbox moves in hybrid deployments and includes it among the Hybrid Agent setup requirements. For implementation guidance, see Hybrid Agent deployment and Move mailboxes between on-premises and Exchange Online organizations.

QUESTION NO: 44 - (SIMULATION)

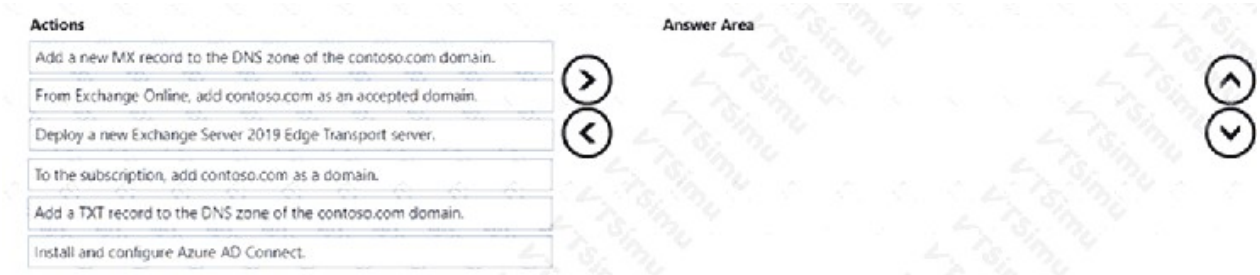
Your network contains an Active Directory domain named contoso.com. The domain contains a Microsoft Exchange Server 2016 server named Server1.

All users have an email address with a suffix of ©contoso.com.

You have a new Microsoft 365 subscription.

You plan to configure an Exchange hybrid deployment.

You need to complete the prerequisites to run the Hybrid Configuration wizard.



ANSWER: See the explanation for the answer

Explanation:

Add the following actions to the Answer Area, in this order:

To the subscription, add contoso.com as a domain.

Add a TXT record to the DNS zone of the contoso.com domain.

Install and configure Azure AD Connect.

The custom domain must first be added to Microsoft 365 and verified through the DNS TXT record. Azure AD Connect is then required to synchronize the on-premises Active Directory users to Microsoft 365 before configuring the hybrid relationship.

Do not add a new MX record, deploy an Edge Transport server, or manually add the domain as an Exchange Online accepted domain. Domain verification makes the domain available in Exchange Online.

QUESTION NO: 45

You have a Microsoft Exchange Online tenant that contains a shared mailbox named Support.

A user named User1 must be able to open the Support mailbox and send email messages that appear to be sent directly from support@contoso.com.

Which two permissions should you assign to User1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Full Access

B. Send As

C. Send on Behalf

D. ApplicationImpersonation

E. Owner

ANSWER: A B

Explanation:

Full Access permission enables User1 to open the Support shared mailbox and access its contents. Full Access does not, by itself, grant permission to send messages by using the shared mailbox address.

Send As permission enables User1 to send messages that display `support@contoso.com` as the sender. Recipients see the message as originating from the shared mailbox rather than as being sent on behalf of User1.

Send on Behalf permission is not appropriate because it causes recipients to see that User1 sent the message on behalf of the Support mailbox. For more information, see Manage permissions for recipients in Exchange Online and Add-RecipientPermission.