QUESTION 206
Case Study: 3 - Fabrikam, Inc
Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal.
Fabrikam has a partnership with a company named Litware, Inc.
Existing Environment
Network Environment
The on-premises network of Fabrikam contains an Active Directory domain named fabrikam.com.
Fabrikam has a Microsoft 365 tenant named fabrikam.com. All users have Microsoft 365 Enterprise E5 licenses.
User accounts sync between Active Directory Domain Services (AD DS) and the Microsoft 365 tenant.
Fabrikam.com contains the users and devices shown in the following table.

User name	Department	Device name	Platform	Device owned by
User1	Sales	User1-Device	iOS	User
User2	Sales	User2-Device	Android	Fabrikam
User3	Marketing	User3-Device	iOS	Fabrikam

Fabrikam currently leases mobile devices from several mobile operators.
Microsoft Exchange Online Environment
All users are assigned an Outlook Web App policy named FilesPolicy.
In-Place Archiving is disabled for Exchange Online.
You have the users shown in the following table.

Name	Exchange Online role group
Admin1	Records Management
Admin2	Recipient Management
Admin3	Compliance Management
Admin4	Organization Management

User1 and User3 use Microsoft Outlook for iOS and Android to access email from their mobile device. User2 uses a native Android email app.
A Safe Links policy in Microsoft Defender for Office 365 is applied to the fabrikam.com tenant. The marketing department uses a mail-enabled public folder named FabrikamProject.
Default MRM Policy is disabled for the fabrikam.com tenant.
Problem Statements
Fabrikam identifies the following issues:
· Users report that they receive phishing emails containing embedded links.
· Users download and save ASPX files when they use Outlook on the web.
· Email between Fabrikam and Litware is unencrypted during transit.
· User2 reports that he lost his mobile device.
Requirements

Planned Changes

Fabrikam plans to implement the following changes:

・Configure FilesPolicy to prevent Outlook on the web users from downloading attachments that have the ASPX extension.

・Purchase a new smartboard and configure the smartboard as a booking resource in Exchange Online.

・Ensure that the new smartboard can only be booked for a maximum of one hour.

・Allow only Admin1 to accept or deny booking requests for the new smartboard.

・Standardize mobile device costs by moving to a single mobile device operator.

・Migrate the FabrikamProject public folder to Microsoft SharePoint Online.

・Enable In-Place Archiving for users in the marketing department.

・Encrypt all email between Fabrikam and Litware.

Technical Requirements

Fabrikam identifies the following technical requirements:

・Ensure that the planned Sharepoint site for FabrikamProject only contains content that was created during the last 12 months.

・Any existing file types that are currently configured as blocked or allowed in the FilesPolicy policy must remain intact.

・When users leave the company, remove their licenses and ensure that their mailbox is accessible to Admin1 and Admin2.

・Generate a report that identifies mobile devices and the mobile device operator of each device.

・Use the principle of least privilege.

・Minimize administrative effort.

Retention requirements

Fabrikam identifies the following retention requirements for all users:

・Enable users to tag items for deletion after one year.

・Enable users to tag items for deletion after two years.

・Enable users to tag items to be archived after one year.

・Automatically delete items in the Junk Email folder after 30 days.

・Automatically delete items in the Sent Items folder after 300 days.

・Ensure that any items without a retention tag are moved to the Archive mailbox two years after they were created and permanently deleted seven years after they were created.

You need to generate a report for the mobile devices that meets the technical requirements.

Which PowerShell cmdlet should you use?

A. Get-DevicePolicy
B. Get-MobileDevice
C. Get-MobileDeviceStatistics
D. Get-DeviceTenantPolicy

Answer: B
Explanation:
https://docs.microsoft.com/en-us/powershell/module/exchange/get-mobiledevice?view=exchange-ps

QUESTION 207
Case Study: 3 - Fabrikam, Inc
Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal.
Fabrikam has a partnership with a company named Litware, Inc.
Existing Environment
Network Environment
The on-premises network of Fabrikam contains an Active Directory domain named fabrikam.com.
Fabrikam has a Microsoft 365 tenant named fabrikam.com. All users have Microsoft 365 Enterprise E5 licenses.
User accounts sync between Active Directory Domain Services (AD DS) and the Microsoft 365 tenant.
Fabrikam.com contains the users and devices shown in the following table.

User name	Department	Device name	Platform	Device owned by
User1	Sales	User1-Device	iOS	User
User2	Sales	User2-Device	Android	Fabrikam
User3	Marketing	User3-Device	iOS	Fabrikam

Fabrikam currently leases mobile devices from several mobile operators.

Microsoft Exchange Online Environment

All users are assigned an Outlook Web App policy named FilesPolicy.

In-Place Archiving is disabled for Exchange Online.

You have the users shown in the following table.

Name	Exchange Online role group
Admin1	Records Management
Admin2	Recipient Management
Admin3	Compliance Management
Admin4	Organization Management

User1 and User3 use Microsoft Outlook for iOS and Android to access email from their mobile device. User2 uses a native Android email app.

A Safe Links policy in Microsoft Defender for Office 365 is applied to the fabrikam.com tenant. The marketing department uses a mail-enabled public folder named FabrikamProject.

Default MRM Policy is disabled for the fabrikam.com tenant.

Problem Statements

Fabrikam identifies the following issues:

‣ Users report that they receive phishing emails containing embedded links.

‣ Users download and save ASPX files when they use Outlook on the web.

‣ Email between Fabrikam and Litware is unencrypted during transit.

‣ User2 reports that he lost his mobile device.

Requirements

Planned Changes

Fabrikam plans to implement the following changes:

‣ Configure FilesPolicy to prevent Outlook on the web users from downloading attachments that have the ASPX extension.

‣ Purchase a new smartboard and configure the smartboard as a booking resource in Exchange Online.

‣ Ensure that the new smartboard can only be booked for a maximum of one hour.

‣ Allow only Admin1 to accept or deny booking requests for the new smartboard.

‣ Standardize mobile device costs by moving to a single mobile device operator.

‣ Migrate the FabrikamProject public folder to Microsoft SharePoint Online.

‣ Enable In-Place Archiving for users in the marketing department.

‣ Encrypt all email between Fabrikam and Litware.

Technical Requirements

Fabrikam identifies the following technical requirements:

‣ Ensure that the planned Sharepoint site for FabrikamProject only contains content that was created during the last 12 months.

‣ Any existing file types that are currently configured as blocked or allowed in the FilesPolicy policy must remain intact.

‣ When users leave the company, remove their licenses and ensure that their mailbox is accessible to Admin1 and Admin2.

‣ Generate a report that identifies mobile devices and the mobile device operator of each device.

‣ Use the principle of least privilege.

‣ Minimize administrative effort.

Retention requirements

Fabrikam identifies the following retention requirements for all users:

‣ Enable users to tag items for deletion after one year.

· Enable users to tag items for deletion after two years.
· Enable users to tag items to be archived after one year.
· Automatically delete items in the Junk Email folder after 30 days.
· Automatically delete items in the Sent Items folder after 300 days.
· Ensure that any items without a retention tag are moved to the Archive mailbox two years after they were created and permanently deleted seven years after they were created.
User3 leaves the company.
You need to ensure that Admin1 and Admin2 can access the mailbox of User3. The solution must meet the technical requirements.
What should you do?

A. Migrate the mailbox of User3 to a distribution group.
B. Migrate the mailbox of User3 to a Microsoft 365 group.
C. Convert the mailbox of User3 into a resource mailbox.
D. Convert the mailbox of User3 into a shared mailbox.

Answer: D
Explanation:
Fabrikam identifies the following technical requirements:
When users leave the company, remove their licenses and ensure that their mailbox is accessible to Admin1 and Admin2.
If you remove the license from User3, the mailbox will be deleted after 30 days. Converting the mailbox to a shared mailbox will ensure that the mailbox is not deleted. You would still need to give Admin1 and Admin2 permissions to access the mailbox.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/admin/email/convert-user-mailbox-to-shared-mailbox?view=o365-worldwide

QUESTION 208
Case Study: 3 - Fabrikam, Inc
Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal.
Fabrikam has a partnership with a company named Litware, Inc.
Existing Environment
Network Environment
The on-premises network of Fabrikam contains an Active Directory domain named fabrikam.com.
Fabrikam has a Microsoft 365 tenant named fabrikam.com. All users have Microsoft 365 Enterprise E5 licenses.
User accounts sync between Active Directory Domain Services (AD DS) and the Microsoft 365 tenant.
Fabrikam.com contains the users and devices shown in the following table.

User name	Department	Device name	Platform	Device owned by
User1	Sales	User1-Device	iOS	User
User2	Sales	User2-Device	Android	Fabrikam
User3	Marketing	User3-Device	iOS	Fabrikam

Fabrikam currently leases mobile devices from several mobile operators.
Microsoft Exchange Online Environment
All users are assigned an Outlook Web App policy named FilesPolicy.
In-Place Archiving is disabled for Exchange Online.
You have the users shown in the following table.

Name	Exchange Online role group
Admin1	Records Management
Admin2	Recipient Management
Admin3	Compliance Management
Admin4	Organization Management

User1 and User3 use Microsoft Outlook for iOS and Android to access email from their mobile device. User2 uses a native Android email app.

A Safe Links policy in Microsoft Defender for Office 365 is applied to the fabrikam.com tenant. The marketing department uses a mail-enabled public folder named FabrikamProject.

Default MRM Policy is disabled for the fabrikam.com tenant.

Problem Statements

Fabrikam identifies the following issues:

・Users report that they receive phishing emails containing embedded links.

・Users download and save ASPX files when they use Outlook on the web.

・Email between Fabrikam and Litware is unencrypted during transit.

・User2 reports that he lost his mobile device.

Requirements

Planned Changes

Fabrikam plans to implement the following changes:

・Configure FilesPolicy to prevent Outlook on the web users from downloading attachments that have the ASPX extension.

・Purchase a new smartboard and configure the smartboard as a booking resource in Exchange Online.

・Ensure that the new smartboard can only be booked for a maximum of one hour.

・Allow only Admin1 to accept or deny booking requests for the new smartboard.

・Standardize mobile device costs by moving to a single mobile device operator.

・Migrate the FabrikamProject public folder to Microsoft SharePoint Online.

・Enable In-Place Archiving for users in the marketing department.

・Encrypt all email between Fabrikam and Litware.

Technical Requirements

Fabrikam identifies the following technical requirements:

・Ensure that the planned Sharepoint site for FabrikamProject only contains content that was created during the last 12 months.

・Any existing file types that are currently configured as blocked or allowed in the FilesPolicy policy must remain intact.

・When users leave the company, remove their licenses and ensure that their mailbox is accessible to Admin1 and Admin2.

・Generate a report that identifies mobile devices and the mobile device operator of each device.

・Use the principle of least privilege.

・Minimize administrative effort.

Retention requirements

Fabrikam identifies the following retention requirements for all users:

・Enable users to tag items for deletion after one year.

・Enable users to tag items for deletion after two years.

・Enable users to tag items to be archived after one year.

・Automatically delete items in the Junk Email folder after 30 days.

・Automatically delete items in the Sent Items folder after 300 days.

・Ensure that any items without a retention tag are moved to the Archive mailbox two years after they were created and permanently deleted seven years after they were created.

You need to identify which users clicked the links in the phishing emails.

What should you do?

A. Run a message trace and review the results.

B. Query the mailbox audit log.
C. Use the URL trace reporting feature.
D. Review the quarantine mailbox.

Answer: C
Explanation:
https://docs.microsoft.com/en-us/powershell/module/exchange/get-maildetailatpreport?view=exchange-ps

QUESTION 209
Case Study: 3 - Fabrikam, Inc
Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal.
Fabrikam has a partnership with a company named Litware, Inc.
Existing Environment
Network Environment
The on-premises network of Fabrikam contains an Active Directory domain named fabrikam.com.
Fabrikam has a Microsoft 365 tenant named fabrikam.com. All users have Microsoft 365 Enterprise E5 licenses.
User accounts sync between Active Directory Domain Services (AD DS) and the Microsoft 365 tenant.
Fabrikam.com contains the users and devices shown in the following table.

User name	Department	Device name	Platform	Device owned by
User1	Sales	User1-Device	iOS	User
User2	Sales	User2-Device	Android	Fabrikam
User3	Marketing	User3-Device	iOS	Fabrikam

Fabrikam currently leases mobile devices from several mobile operators.
Microsoft Exchange Online Environment
All users are assigned an Outlook Web App policy named FilesPolicy.
In-Place Archiving is disabled for Exchange Online.
You have the users shown in the following table.

Name	Exchange Online role group
Admin1	Records Management
Admin2	Recipient Management
Admin3	Compliance Management
Admin4	Organization Management

User1 and User3 use Microsoft Outlook for iOS and Android to access email from their mobile device. User2 uses a native Android email app.
A Safe Links policy in Microsoft Defender for Office 365 is applied to the fabrikam.com tenant. The marketing department uses a mail-enabled public folder named FabrikamProject.
Default MRM Policy is disabled for the fabrikam.com tenant.
Problem Statements
Fabrikam identifies the following issues:
・Users report that they receive phishing emails containing embedded links.
・Users download and save ASPX files when they use Outlook on the web.
・Email between Fabrikam and Litware is unencrypted during transit.
・User2 reports that he lost his mobile device.
Requirements
Planned Changes
Fabrikam plans to implement the following changes:
・Configure FilesPolicy to prevent Outlook on the web users from downloading attachments that have the ASPX extension.
・Purchase a new smartboard and configure the smartboard as a booking resource in Exchange Online.
・Ensure that the new smartboard can only be booked for a maximum of one hour.
・Allow only Admin1 to accept or deny booking requests for the new smartboard.

· Standardize mobile device costs by moving to a single mobile device operator.

· Migrate the FabrikamProject public folder to Microsoft SharePoint Online.

· Enable In-Place Archiving for users in the marketing department.

· Encrypt all email between Fabrikam and Litware.

Technical Requirements

Fabrikam identifies the following technical requirements:

· Ensure that the planned Sharepoint site for FabrikamProject only contains content that was created during the last 12 months.

· Any existing file types that are currently configured as blocked or allowed in the FilesPolicy policy must remain intact.

· When users leave the company, remove their licenses and ensure that their mailbox is accessible to Admin1 and Admin2.

· Generate a report that identifies mobile devices and the mobile device operator of each device.

· Use the principle of least privilege.

· Minimize administrative effort.

Retention requirements

Fabrikam identifies the following retention requirements for all users:

· Enable users to tag items for deletion after one year.

· Enable users to tag items for deletion after two years.

· Enable users to tag items to be archived after one year.

· Automatically delete items in the Junk Email folder after 30 days.

· Automatically delete items in the Sent Items folder after 300 days.

· Ensure that any items without a retention tag are moved to the Archive mailbox two years after they were created and permanently deleted seven years after they were created.

Hotspot Question

You need to modify FilesPolicy to prevent users from downloading ASPX files. The solution must meet the technical requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area

Set-SafeLinksPolicy ▼	-id FilesPolicy -BlockedFileTypes	.aspx ▼
Set-SafeLinksPolicy		.aspx
Set-OwaMailboxPolicy		*.aspx
Set-ActiveSyncMailboxPolicy		@{Add = ".aspx"}
Set-HostedContentFilterPolicy		@{Remove = ".aspx"}

Answer:

Answer Area

▼	-id FilesPolicy -BlockedFileTypes	.aspx ▼
Set-SafeLinksPolicy		.aspx
Set-OwaMailboxPolicy		*.aspx
Set-ActiveSyncMailboxPolicy		**@{Add = ".aspx"}**
Set-HostedContentFilterPolicy		@{Remove = ".aspx"}

Explanation:

https://docs.microsoft.com/en-us/powershell/module/exchange/set-owamailboxpolicy?view=exchange-ps

QUESTION 210
Case Study: 3 - Fabrikam, Inc
Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal.
Fabrikam has a partnership with a company named Litware, Inc.
Existing Environment
Network Environment
The on-premises network of Fabrikam contains an Active Directory domain named fabrikam.com.
Fabrikam has a Microsoft 365 tenant named fabrikam.com. All users have Microsoft 365 Enterprise E5 licenses.
User accounts sync between Active Directory Domain Services (AD DS) and the Microsoft 365 tenant.

Fabrikam.com contains the users and devices shown in the following table.

User name	Department	Device name	Platform	Device owned by
User1	Sales	User1-Device	iOS	User
User2	Sales	User2-Device	Android	Fabrikam
User3	Marketing	User3-Device	iOS	Fabrikam

Fabrikam currently leases mobile devices from several mobile operators.
Microsoft Exchange Online Environment
All users are assigned an Outlook Web App policy named FilesPolicy.
In-Place Archiving is disabled for Exchange Online.
You have the users shown in the following table.

Name	Exchange Online role group
Admin1	Records Management
Admin2	Recipient Management
Admin3	Compliance Management
Admin4	Organization Management

User1 and User3 use Microsoft Outlook for iOS and Android to access email from their mobile device. User2 uses a native Android email app.
A Safe Links policy in Microsoft Defender for Office 365 is applied to the fabrikam.com tenant. The marketing department uses a mail-enabled public folder named FabrikamProject.
Default MRM Policy is disabled for the fabrikam.com tenant.
Problem Statements
Fabrikam identifies the following issues:
· Users report that they receive phishing emails containing embedded links.
· Users download and save ASPX files when they use Outlook on the web.
· Email between Fabrikam and Litware is unencrypted during transit.
· User2 reports that he lost his mobile device.
Requirements
Planned Changes
Fabrikam plans to implement the following changes:
· Configure FilesPolicy to prevent Outlook on the web users from downloading attachments that have the ASPX extension.
· Purchase a new smartboard and configure the smartboard as a booking resource in Exchange Online.
· Ensure that the new smartboard can only be booked for a maximum of one hour.
· Allow only Admin1 to accept or deny booking requests for the new smartboard.
· Standardize mobile device costs by moving to a single mobile device operator.
· Migrate the FabrikamProject public folder to Microsoft SharePoint Online.
· Enable In-Place Archiving for users in the marketing department.
· Encrypt all email between Fabrikam and Litware.
Technical Requirements
Fabrikam identifies the following technical requirements:
· Ensure that the planned Sharepoint site for FabrikamProject only contains content that was created during the last 12 months.
· Any existing file types that are currently configured as blocked or allowed in the FilesPolicy policy must remain intact.
· When users leave the company, remove their licenses and ensure that their mailbox is accessible to Admin1 and Admin2.
· Generate a report that identifies mobile devices and the mobile device operator of each device.
· Use the principle of least privilege.
· Minimize administrative effort.
Retention requirements
Fabrikam identifies the following retention requirements for all users:

・Enable users to tag items for deletion after one year.
・Enable users to tag items for deletion after two years.
・Enable users to tag items to be archived after one year.
・Automatically delete items in the Junk Email folder after 30 days.
・Automatically delete items in the Sent Items folder after 300 days.
・Ensure that any items without a retention tag are moved to the Archive mailbox two years after they were created and permanently deleted seven years after they were created.

Hotspot Question
You need to configure the new smartboard to support the planned changes.
Which three settings should you configure?To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Booking options

Assign settings for the booking policy that defines when this resource can be scheduled

☐ Allow repeating meetings

☐ Allow scheduling only during work hours

☐ Auto-accepts meeting request

Set to "Off" if you want to specify users who want to accept meetings manually

Booking delegates

Search a mail or email

☐ Automatically decline meetings outside of limits below

Booking window (days)

Maximum duration (hours)

If the organizer needs a reply enter message below

Answer:

Answer Area

Booking options

Assign settings for the booking policy that defines when this resource can be scheduled

☐ Allow repeating meetings

☐ Allow scheduling only during work hours

☐ Auto-accepts meeting request

Set to "Off" if you want to specify users who want to accept meetings manually

Booking delegates

Search a mail or email

☐ Automatically decline meetings outside of limits below

Booking window (days)

Maximum duration (hours)

If the organizer needs a reply enter message below

Explanation:
https://docs.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-resource-mailboxes

QUESTION 211
Case Study: 3 - Fabrikam, Inc
Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal.
Fabrikam has a partnership with a company named Litware, Inc.
Existing Environment
Network Environment
The on-premises network of Fabrikam contains an Active Directory domain named fabrikam.com.
Fabrikam has a Microsoft 365 tenant named fabrikam.com. All users have Microsoft 365 Enterprise E5 licenses.
User accounts sync between Active Directory Domain Services (AD DS) and the Microsoft 365 tenant.
Fabrikam.com contains the users and devices shown in the following table.

User name	Department	Device name	Platform	Device owned by
User1	Sales	User1-Device	iOS	User
User2	Sales	User2-Device	Android	Fabrikam
User3	Marketing	User3-Device	iOS	Fabrikam

Fabrikam currently leases mobile devices from several mobile operators.

Microsoft Exchange Online Environment

All users are assigned an Outlook Web App policy named FilesPolicy.

In-Place Archiving is disabled for Exchange Online.

You have the users shown in the following table.

Name	Exchange Online role group
Admin1	Records Management
Admin2	Recipient Management
Admin3	Compliance Management
Admin4	Organization Management

User1 and User3 use Microsoft Outlook for iOS and Android to access email from their mobile device. User2 uses a native Android email app.

A Safe Links policy in Microsoft Defender for Office 365 is applied to the fabrikam.com tenant. The marketing department uses a mail-enabled public folder named FabrikamProject.

Default MRM Policy is disabled for the fabrikam.com tenant.

Problem Statements

Fabrikam identifies the following issues:

· Users report that they receive phishing emails containing embedded links.

· Users download and save ASPX files when they use Outlook on the web.

· Email between Fabrikam and Litware is unencrypted during transit.

· User2 reports that he lost his mobile device.

Requirements

Planned Changes

Fabrikam plans to implement the following changes:

· Configure FilesPolicy to prevent Outlook on the web users from downloading attachments that have the ASPX extension.

· Purchase a new smartboard and configure the smartboard as a booking resource in Exchange Online.

· Ensure that the new smartboard can only be booked for a maximum of one hour.

· Allow only Admin1 to accept or deny booking requests for the new smartboard.

· Standardize mobile device costs by moving to a single mobile device operator.

· Migrate the FabrikamProject public folder to Microsoft SharePoint Online.

· Enable In-Place Archiving for users in the marketing department.

· Encrypt all email between Fabrikam and Litware.

Technical Requirements

Fabrikam identifies the following technical requirements:

· Ensure that the planned Sharepoint site for FabrikamProject only contains content that was created during the last 12 months.

· Any existing file types that are currently configured as blocked or allowed in the FilesPolicy policy must remain intact.

· When users leave the company, remove their licenses and ensure that their mailbox is accessible to Admin1 and Admin2.

· Generate a report that identifies mobile devices and the mobile device operator of each device.

· Use the principle of least privilege.

· Minimize administrative effort.

Retention requirements

Fabrikam identifies the following retention requirements for all users:

· Enable users to tag items for deletion after one year.

・Enable users to tag items for deletion after two years.

・Enable users to tag items to be archived after one year.

・Automatically delete items in the Junk Email folder after 30 days.

・Automatically delete items in the Sent Items folder after 300 days.

・Ensure that any items without a retention tag are moved to the Archive mailbox two years after they were created and permanently deleted seven years after they were created.

Hotspot Question

You need to perform a remote wipe of the devices of User2 and User3.

You run the following commands.

```
Clear-MobileDevice -id User2-Device
-NotificationEmailAddress "admin@Fabrikam.com"
Clear-MobileDevice -id User3-Device
-NotificationEmailAddress "admin@Fabrikam.com"
```

What occurs on each device?To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

On the device of User2:

All data is deleted.
Only email messages are deleted.
Only email messages and calendar, contact, and file data are deleted.

On the device of User3:

All data is deleted.
Only email messages are deleted.
Only email messages and calendar, contact, and file data are deleted.

Answer:

Answer Area

On the device of User2:

All data is deleted.
Only email messages are deleted.
Only email messages and calendar, contact, and file data are deleted.

On the device of User3:

All data is deleted.
Only email messages are deleted.
Only email messages and calendar, contact, and file data are deleted.

Explanation:
https://docs.microsoft.com/en-us/exchange/clients/exchange-activesync/remote-wipe?view=exchserver-

QUESTION 212
You have a Microsoft Exchange Online tenant that contains the groups shown in the following table.

Name	Type	Owner	Number of members	Member of
Group1	Distribution list	Admin1	200	*none*
Group2	Dynamic distribution list	*None*	50	*Not applicable*
Group3	Security group	Admin1	50	*none*
Group4	Distribution list	Admin1	150	Group3

Which groups can you upgrade to a Microsoft 365 group?

A. Group1 only
B. Group1, Group2, Group3, and Group4
C. Group2 and Group3 only
D. Group3 only
E. Group1 and Group4 only

Answer: AE
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/admin/manage/upgrade-distribution-lists?view=o365-worldwide

QUESTION 213
You have a Microsoft Exchange Server 2019 organization.
Users access their email by using Microsoft Outlook 2019.
The users report that when a mailbox is provisioned for a new user, there is a delay of many hours before the new user appears in the global address list (GAL). From Outlook on the web, the users can see the new user in the GAL immediately.
You need to reduce the amount of time it takes for new users to appear in the GAL in Outlook 2019.
What should you do?

A. Create a scheduled task that runs the Update-GlobalAddressList cmdlet.
B. Create an address book policy (ABP).
C. Modify the default email address policy.
D. Modify the offline address book (OAB) schedule.

Answer: D
Explanation:
https://docs.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/change-oab-generation-schedule?view=exchserver-2019

QUESTION 214
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft Exchange Online tenant that uses an email domain named contoso.com.
You need to prevent all users from performing the following tasks:
- Sending out-of-office replies to an email domain named fabrikam.com.
- Sending automatic replies to an email domain named adatum.com.
The solution must ensure that all the users can send out-of-office replies and automatic replies to other email domains on the internet.
Solution: You create one mail flow rule.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/remote-domains/remote-domains

QUESTION 215
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft Exchange Online tenant that uses an email domain named contoso.com.
You need to prevent all users from performing the following tasks:
- Sending out-of-office replies to an email domain named fabrikam.com.
- Sending automatic replies to an email domain named adatum.com.
The solution must ensure that all the users can send out-of-office replies and automatic replies to other email domains on the internet.
Solution: You create two new remote domains.
Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/remote-domains/remote-domains

QUESTION 216
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft Exchange Online tenant that uses an email domain named contoso.com.
You need to prevent all users from performing the following tasks:
- Sending out-of-office replies to an email domain named fabrikam.com.
- Sending automatic replies to an email domain named adatum.com.
The solution must ensure that all the users can send out-of-office replies and automatic replies to other email domains on the internet.
Solution: You modify the default remote domain.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/remote-domains/remote-domains

QUESTION 217
You have a Microsoft Exchange Online tenant that uses a third-party email gateway device.
You discover that inbound email messages are delayed.
The gateway device receives the following error message when sending email to the tenant.
4.7.500 Server busy, please try again later.
You need to prevent inbound email delays.
What should you configure?

A. Organization Sharing

B. an MX record for the domain
C. a transport rule
D. a connector

Answer: D
Explanation:
https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/ use-connectors-to-configure-mail-flow

QUESTION 218
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft Exchange Online tenant that contains the following email domains:
- `Adatum.com`
- `Contoso.com`
- `Fabrikam.com`
When external recipients receive email messages from the users in the tenant, all the messages are delivered by using the @contoso.com email domain.
You need to ensure that the users send email by using the @fabrikam.com email domain.
Solution: You modify the properties of the fabrikam.com accepted domain.
Does this meet the goal?

A. No
B. Yes

Answer: A
Explanation:
https://docs.microsoft.com/en-us/exchange/mail-flow/accepted-domains/accepted-domains?view=exchserver-2019