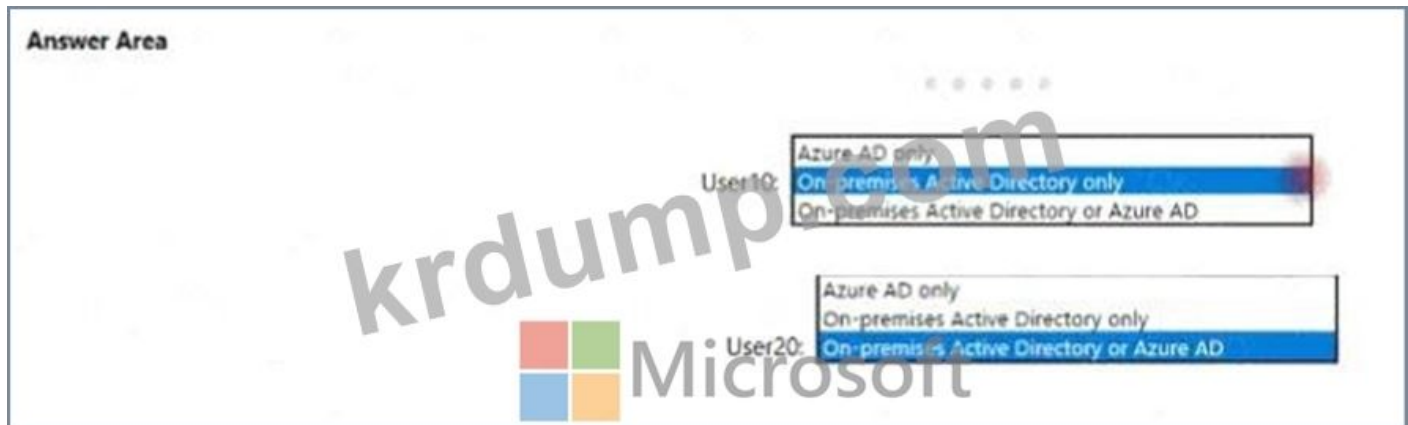


Microsoft.MS-100-KR.v2023-12-11.q186

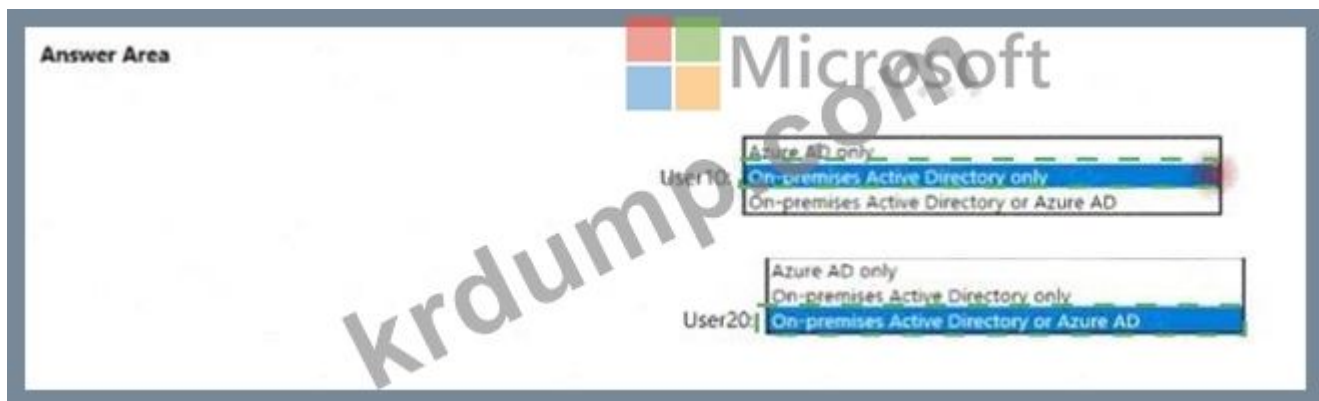
□□□□:	MS-100-KR
□□□□:	Microsoft 365 Identity and Services (MS-100 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	186
□□:	v2023-12-11
# □□ □:	667
# □□ □□□:	1860
https://www.krdump.com/Microsoft.MS-100-KR.v2023-12-11.q186.html	

NEW QUESTION: 1

□□□□□□ Contoso.com□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□ Microsoft 365 □□□ □□□□ □□ □□ □□□□ □□□□ Azure AD(Azure Active Directory)□ □□□□□ □□□ □□□□□. □□□□ □ □ □□□□ □□□ □□□□ □ □□ □□□ □□□□ □□□. □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□□. □□: □□□ □□□ □□□ □□□ □□□□□.



Answer:



NEW QUESTION: 2

□□□□ User1□□□□ □□□□ □□□□ contoso.onmicrosoft.com□□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.

□□□□ User1□ □□ □□□□ □□□□ Azure AD□ □□□□□□ □□□□ □□□□□□.

Admin1□□□□ □□□□ □□ User1□ □□ □□□ □□ □□□ □ □ □□□ □□□□ □□□□ □□□.

Admin1□ □□□□ □□ □ □□ □□□ □□□□□□? □ □□□ □□□ □□□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□□.

- A. □□ □□□
- B. □□ □□□
- C. □□□ □□□
- D. □□ □□ □□□
- E. □□□ □□
- F. □□ □□

Answer: (SHOW ANSWER)

Explanation

Users in the Security Administrator, Security Reader, Global Reader, and Report Reader roles can view the sign in details.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>

NEW QUESTION: 3

Microsoft 365 □□□ □□□□□.

App1□□□□ Microsoft Teams □□ □□□□□□.

□ □□□□□□ App1□ □□□□□ □□□□.

□□ □ □□ □□□ □□□□ □□□□ □□□□? □□□□□□ □□ □□□□ □□ □□□□ □□ □□

□□ □□□□ □□□ □□□ □□□□□□□□.

Actions

- Create an app package.
- Publish the app by using the Microsoft Teams admin center.
- Upload the app package by using the Teams App Submission API.
- Enable custom app uploading for Microsoft SharePoint Online.
- Sideload the app to Microsoft Teams.
- Upload the app package to Microsoft AppSource.

Answer Area

Answer:


Actions

- Create an app package.
- Publish the app by using the Microsoft Teams admin center.
- Upload the app package by using the Teams App Submission API.
- Enable custom app uploading for Microsoft SharePoint Online.
- Sideload the app to Microsoft Teams.
- Upload the app package to Microsoft AppSource.

Answer Area

- Create an app package.
- Publish the app by using the Microsoft Teams admin center.
- Sideload the app to Microsoft Teams.

Explanation

 Migration type to use:

▼
Cutover migration
Staged migration
Remote move migration
IMAP migration

Data to include in the migration:

▼
Email only
Email and calendar only
Email, calendar and contacts only
Email, calendar, contacts, and tasks

Answer:

Migration type to use:

▼
Cutover migration
Staged migration
Remote move migration
IMAP migration

Data to include in the migration:

▼
Email only
Email and calendar only
Email, calendar and contacts only
Email, calendar, contacts, and tasks

Explanation

Migration type to use:

▼
Cutover migration
Staged migration
Remote move migration
IMAP migration

Data to include in the migration:

▼
Email only
Email and calendar only
Email, calendar and contacts only
Email, calendar, contacts, and tasks

You'll need to use the IMAP migration method. You can use the setup wizard in the Microsoft 365 admin center for an IMAP migration to migrate mailboxes from Gmail to Microsoft 365.

IMAP migration will only migrate emails, not calendar and contact information. Users can import their own email, contacts, and other mailbox information to Office 365 after the mailboxes have been migrated.

Reference:

<https://docs.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/migrate-g-suite-mailbo>

NEW QUESTION: 6

□□□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□□ Windows 10 □ □□□□ 2,000□□ □□□□ □□□□.

Microsoft 365 □□□ □□□□□.

□□ □□ □□□ □ Azure AD(Azure Active Directory) Seamless Single Sign-On(Seamless SSO) □ □□□□□.

□□□□□ Windows 10 □□□□□ Seamless SSO□ □□□ □ □□□ □□□□ □□□□. □□□ □□ □□□?

A. Azure AD□□ □□□ □□□ □□□ □□□□.

B. Azure AD Connect □□ □□□ □□□□□.

C. □□□□□ Azure AD□ □□□□□.

D. □□ □□□ □□□□ □□□□ □□ □□ □□

Answer: D (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start>

NEW QUESTION: 7

□□□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Server name	Software	Configuration
Server1	Windows Server 2008	Domain controller
Server2	Windows Server 2012	Domain controller
Server3	Microsoft Exchange Server 2007	Not applicable
Server4	Microsoft SharePoint Server 2010	Not applicable
Server5	Microsoft Lync Server 2013	Not applicable

Microsoft 365 Enterprise E5□ □□□□ □□ □□□□□ □□ □□□□□ ID □□□ □ □□□□ □ □□□ □□□□ □□ □□□□□ Microsoft 365□ □□□ □□□□□.

Microsoft 365□ □□□□ □□ □□□□□□□ □□ □□□ □□□□ □□□□. □□□ □□□□ □ □□?

A. □□ 2

B. □□ 3

C. □□ 5

D. □□ 1

E. 4

Answer: (SHOW ANSWER)

Explanation

Exchange Server 2007 is not supported for a hybrid deployment.

Reference:

<https://docs.microsoft.com/en-us/exchange/hybrid-deployment-prerequisites>

NEW QUESTION: 8

Microsoft Azure AD Connect Express is used to connect an on-premises Active Directory to Azure AD(Azure Active Directory). The user User1 is created in the on-premises Active Directory. The password for User1 is Password.



Azure AD is used to connect the on-premises Active Directory to Azure AD.

Statements

User1 can sign in to Azure AD.

Yes

No

User1 can change the password immediately by using the My Apps portal.

From Azure AD, User1 must change the password every 90 days.

Answer:

Statements	Yes	No
User1 can sign in to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>
From Azure AD, User1 must change the password every 90 days.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation

Statements	Yes	No
User1 can sign in to Azure AD.	<input type="radio"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input type="radio"/>
From Azure AD, User1 must change the password every 90 days.	<input type="radio"/>	<input type="radio"/>

Box 1: Yes

The question states that User1 is synced to Azure AD. This tells us that the short password (Pass) meets the on-premise Active Directory password policy and you were able to create the on-premise account for User1.

The on-premise Active Directory password policy applies over the Azure AD password policy for synced user accounts.

Box 2: No

Self-Service Password Reset would need to be configured.

Box 3: Yes

The password for the Azure AD User1 account will expire after 90 days according to the Azure AD password policy. If the on-premise password policy has a shorter password expiration period, User1 would have to change his/her on-premise AD password. The new password would then sync to Azure AD.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express>

NEW QUESTION: 9

Microsoft 365 □□□ □□□□.

□□□□ AD FS(Active Directory Federation Services) □□□□ □□□□□.

AD FS □□□ □□□ □□□□□ □□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

A. □□ AD FS □□□□ audltpol.exe □ □□□□□.

- B. `set-AdminAuditLogConfig cmdlet -LogiLevel`
- C. `AD DS Azure AD Connect Health`
- D. `Register-AzureADConnectHealthSyncAgent cmdlet`
- E. `AD FS Azure AD Connect Health`

Answer: D,E (LEAVE A REPLY)

Explanation

To audit AD FS user authentication, you need to install Azure AD Connect Health for AD FS. The agent should be installed on an AD FS server. After the installation, you need to register the agent by running the `Register-AzureADConnectHealthSyncAgent` cmdlet.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install>
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-ads>

NEW QUESTION: 10

10,000 contoso.com Azure AD(Azure Active Directory) Microsoft 365 contoso.com Azure MFA(Multi-Factor Authentication) "SignInLogs" | ResultDescription == "MFA" Office 365 Analytics Azure Active Directory Azure Log Analytics

- A. Azure Active Directory Azure Storage
- B. Office 365 Analytics
- C. Office 365 Analytics
- D. Azure Active Directory Azure Log Analytics

Answer: D (LEAVE A REPLY)

Explanation

You can now send audit logs to Azure Log Analytics. This gives you much easier reporting on audit events and the ability to perform queries such as the one in this question.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-lo>

NEW QUESTION: 11

User1□□□ □□□□ Office Online□ □□□□ □□□ □□ □ □□□ □□□□ □□□.

User1□ □□ □□□□ □□ □ □□ Microsoft Office 365 □□□□ □□□ □□□□□? □□□□

□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Answer Area

License options

Microsoft Forms (Plan E5)	<input type="checkbox"/> Off	<input type="checkbox"/> On
Microsoft MyAnalytics (Full)	<input type="checkbox"/> Off	<input type="checkbox"/> On
Microsoft Planner	<input type="checkbox"/> Off	<input type="checkbox"/> On
Microsoft StaffHub	<input type="checkbox"/> Off	<input type="checkbox"/> On
Microsoft Stream for O365 E5 SKU	<input type="checkbox"/> Off	<input type="checkbox"/> On
Microsoft Teams	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office 365 Advanced eDiscovery	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office 365 Advanced Threat Protection (Plan 2)	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office 365 Cloud App Security	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office 365 Privileged Access Management	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office 365 ProPlus	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office Online	<input type="checkbox"/> Off	<input type="checkbox"/> On
Phone System	<input type="checkbox"/> Off	<input type="checkbox"/> On
Power BI Pro	<input type="checkbox"/> Off	<input type="checkbox"/> On
PowerApps for Office 365	<input type="checkbox"/> Off	<input type="checkbox"/> On
SharePoint Online (Plan 2)	<input type="checkbox"/> Off	<input type="checkbox"/> On
Skype for Business Online (Plan 2)	<input type="checkbox"/> Off	<input type="checkbox"/> On



Microsoft

Sway	<input type="checkbox"/> Off	<input type="checkbox"/> On
To-Do (Plan 3)	<input type="checkbox"/> Off	<input type="checkbox"/> On
Yammer Enterprise	<input type="checkbox"/> Off	<input type="checkbox"/> On

Answer:

Answer Area

License options

Microsoft Forms (Plan E5)	<input type="checkbox"/> Off	<input type="checkbox"/> On
Microsoft MyAnalytics (Full)	<input type="checkbox"/> Off	<input type="checkbox"/> On
Microsoft Planner	<input type="checkbox"/> Off	<input type="checkbox"/> On
Microsoft StaffHub	<input type="checkbox"/> Off	<input type="checkbox"/> On
Microsoft Stream for O365 E5 SKU	<input type="checkbox"/> Off	<input type="checkbox"/> On
Microsoft Teams	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office 365 Advanced eDiscovery	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office 365 Advanced Threat Protection (Plan 2)	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office 365 Cloud App Security	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office 365 Privileged Access Management	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office 365 ProPlus	<input type="checkbox"/> Off	<input type="checkbox"/> On
Office Online	<input type="checkbox"/> Off	<input type="checkbox"/> On
Phone System	<input type="checkbox"/> Off	<input type="checkbox"/> On
Power BI Pro	<input type="checkbox"/> Off	<input type="checkbox"/> On
PowerApps for Office 365	<input type="checkbox"/> Off	<input type="checkbox"/> On



Kroump.com

PowerApps for Office 365	Off	On
SharePoint Online (Plan 2)	Off	On
Skype for Business Online (Plan 2)	Off	On
Sway	Off	On
To-Do (Plan 3)	Off	On
Yammer Enterprise	Off	On

Explanation

License options

Microsoft Forms (Plan E5)	<input type="checkbox"/>	<input type="checkbox"/>
Microsoft MyAnalytics (Full)	<input type="checkbox"/>	<input type="checkbox"/>
Microsoft Planner	<input type="checkbox"/>	<input type="checkbox"/>
Microsoft StaffHub	<input type="checkbox"/>	<input type="checkbox"/>
Microsoft Stream for O365 E5 SKU	<input type="checkbox"/>	<input type="checkbox"/>
Microsoft Teams	<input type="checkbox"/>	<input type="checkbox"/>
Office 365 Advanced eDiscovery	<input type="checkbox"/>	<input type="checkbox"/>
Office 365 Advanced Threat Protection (Plan 2)	<input type="checkbox"/>	<input type="checkbox"/>
Office 365 Cloud App Security	<input type="checkbox"/>	<input type="checkbox"/>
Office 365 Privileged Access Management	<input type="checkbox"/>	<input type="checkbox"/>
Office 365 ProPlus	<input type="checkbox"/>	<input type="checkbox"/>
Office Online	<input type="checkbox"/>	<input type="checkbox"/>
Phone System	<input type="checkbox"/>	<input type="checkbox"/>
Power BI Pro	<input type="checkbox"/>	<input type="checkbox"/>
PowerApps for Office 365	<input type="checkbox"/>	<input type="checkbox"/>
SharePoint Online (Plan 2)	<input type="checkbox"/>	<input type="checkbox"/>
Skype for Business Online (Plan 2)	<input type="checkbox"/>	<input type="checkbox"/>
Sway	<input type="checkbox"/>	<input type="checkbox"/>
To-Do (Plan 3)	<input type="checkbox"/>	<input type="checkbox"/>
Yammer Enterprise	<input type="checkbox"/>	<input type="checkbox"/>

You need "Office Online" to be able to create documents by using Office Online. You also need an online location to save and store the documents. For this, you would use SharePoint online.

NEW QUESTION: 12

- Microsoft 365 □□□ □□□□.
- □□□ PST □□□ Microsoft Exchange Online □□□□□ □□□ □□□□□.
- PST □□□ □□ □□□□ □□□ □□□□ □□□.
- □□□ □□□□ □□ □□□□ □□ □ □□ □□□ □□□□□? □ □□□ □□□□ □ □□ □□□□□.
- : □ □□□ □□□ 1□□ □□□ □□□□.
- A. Microsoft Azure □□□ □□□ □□□□.
- B. Microsoft 365 □□ □ □□ □□□□ SAS □□ □□□□□.
- C. azcopy.exe □ □□□□ PST □□□ Microsoft Azure □□□□ □□□□□.
- D. Microsoft Azure Storage Explorer □ □□□□ PST □□□ Azure Storage □ □□□□□.
- E. PST □□□□ □□ □□□ □□□□□.

Answer: B,C,E (LEAVE A REPLY)

Explanation

The first step is to download and install the Azure AzCopy tool, which is the tool that you run in Step 2 to upload PST files to Office 365. You also copy the SAS URL for your organization. This URL is a combination of the network URL for the Azure Storage location in the Microsoft cloud for your organization and a Shared Access Signature (SAS) key. This key provides you with the necessary permissions to upload PST files to your Azure Storage location.

Now you're ready to use the AzCopy.exe tool to upload PST files to Office 365. This tool uploads and stores them in an Azure Storage location in the Microsoft cloud.

After the PST files have been uploaded to the Azure Storage location for your Office 365 organization, the next step is to create a comma-separated value (CSV) file that specifies which user mailboxes the PST files will be imported to. You'll submit this CSV file when you create a PST Import job.

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/use-network-upload-to-import-pst-files>

NEW QUESTION: 13

- □□□ SharePoint Online □□□ □□□□ □□ □□ □□ □ □□□ □□□□ □□□.
- □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□□.

Development model: ▼

Full-trust web parts
Sandboxed solutions
SharePoint Framework (SPFx)

IDE: ▼

Eclipse
Microsoft Visual Studio
Microsoft Visual Studio Code

Front-end framework: ▼

Bootstrap
Fluent UI
Material Design

Answer:

Development model: ▼

Full-trust web parts
Sandboxed solutions
SharePoint Framework (SPFx)

IDE: ▼

Eclipse
Microsoft Visual Studio
Microsoft Visual Studio Code

Front-end framework: ▼

Bootstrap
Fluent UI
Material Design

Explanation

Graphical user interface, text, application Description automatically generated

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) [Grant admin consent for nuborocks](#)

API / Permissions name	Type	Description
Microsoft Graph (2)		
Directory.AccessAsUser.All Group.Create Group.ReadWrite.All	Delegated	Read and write all groups
User.Read.All User.ReadBasic.All User.ReadWrite.All	Delegated	Read all users' basic profiles

Explanation

API / Permissions name	Type	Description
Microsoft Graph (2)		
Group.ReadWrite.All	Delegated	Read and write all groups
User.Read.All	Delegated	Read all users' basic profiles

MS-100-KR DumpTop MS-100-KR! DumpTop MS-100-KR, DumpTop MS-100-KR. DumpTop MS-100-KR. <https://www.dumptop.com/Microsoft/MS-100-KR-dump.html> (431 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 17

Microsoft Intune

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

Intune ☐ ☐☐☐☐ ☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐.

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

The device compliance policies have the assignment shown in the following table.

Name	Assigned to
Policy1	Group3
Policy2	Group2

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐.

☐☐: ☐☐☐☐☐☐ 1☐☐☐☐☐☐☐☐.

Statements	Yes	No
Device1 is compliant.	<input type="checkbox"/>	<input type="radio"/>
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation

Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Device 1:

No because Device1 is in group3 which has Policy1 assigned which requires BitLocker.

Device 2:

No because Device2 is in group3 which has Policy1 assigned which requires BitLocker. Device2 is also in Group2 which has Policy2 assigned but the BitLocker requirement is not configured in Policy2.

Device3:

Yes because Device3 is in Group2 which has Policy2 assigned but the BitLocker requirement is not configured in Policy2.

Reference:

<https://blogs.technet.microsoft.com/cbernier/2017/07/11/windows-10-intune-windows-bitlocker-management-ye>

NEW QUESTION: 18

□□ □□□ □□ Microsoft Azure Information Protection□ □□□□ □□□□ □□□ Microsoft OneDrive□ □□□□.

Protection settings ⓘ

Azure (cloud key)

HYOK (AD RMS)

Select the protection action type ⓘ

- Set permissions
- Set user-defined permissions (Preview)

USERS

PERMISSIONS

M365x901434.onmicrosoft.com

Co-Owner

+ Add permissions

Content expiration

Always

Never

By days

Number of days the content is valid

30

Allow offline access

Balance security requirements (includes access after revocation) with the flexibility to open protected content without an Internet connection. [More information and recommended settings](#)

Always

Never

By days

Number of days the content is available without an Internet connection

7

Protection template ID - template id is automatically generated after template is saved

□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□ □□□□□
□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

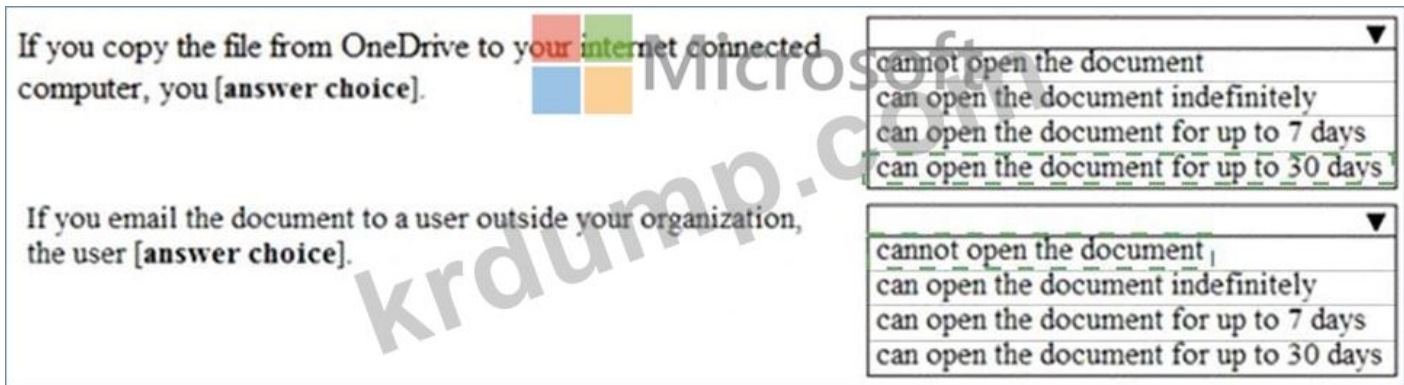
If you copy the file from OneDrive to your internet connected computer, you [answer choice].

If you email the document to a user outside your organization, the user [answer choice].

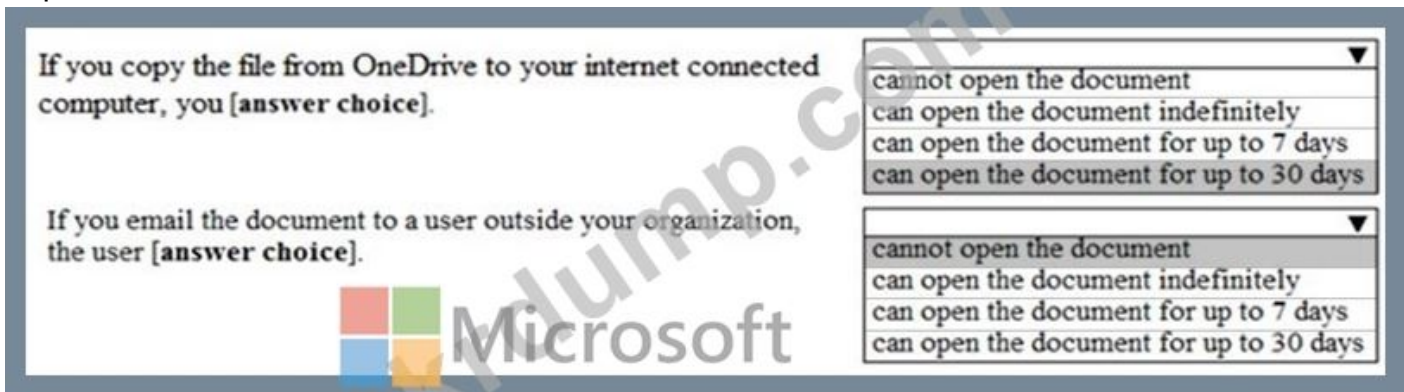
cannot open the document
can open the document indefinitely
can open the document for up to 7 days
can open the document for up to 30 days

cannot open the document
can open the document indefinitely
can open the document for up to 7 days
can open the document for up to 30 days

Answer:



Explanation



Box 1:

If you copy the file from OneDrive to your internet connected computer, you can open the document for up to 30 days. This is because the "Number of days the content is valid" setting is set to 30 days.

Box 2:

If you email the document to a user outside your organization, the user cannot open the document. To open the document, the user would need to be added to the Users list and assigned permission. With the configuration in the exhibit, only the user listed in the Users list and the creator of the document can open the document.

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection>

NEW QUESTION: 19

<https://app.contoso.local> URL is blocked by Microsoft 365. URL is blocked by Microsoft 365. URL is blocked by Microsoft 365.

Microsoft 365 blocks the URL.

The URL is blocked by Microsoft 365.

The URL is blocked by Microsoft 365. The URL is blocked by Microsoft 365. The URL is blocked by Microsoft 365.

The URL is blocked by Microsoft 365. The URL is blocked by Microsoft 365.

The URL is blocked by Microsoft 365.

A. Microsoft 365 blocks the URL.

B. Azure Active Directory blocks the URL.

C. Azure Active Directory blocks the URL.

D. The URL is blocked by Microsoft 365.



□□□ □□ □□□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□□

□□□□ □□ □□□□ □□□□ □□ □□□ □□□□□ □ Lee Gu□ □□□ □□□ □□ □□

□□□ □□□□ Microsoft 365 □□□ □□□□□□□.

Answer:

See explanation below.

Explanation

Create an activity alert

1. Go to <https://protection.office.com/managealerts>.
2. Sign in to Office 365 using your work or school account.
3. On the Activity alerts page, click + New. The flyout page to create an activity alert is displayed.

The screenshot shows the configuration page for an activity alert in Microsoft 365. It features several sections:

- Name:** A text input field with a blue 'A' icon.
- Description:** A larger text input field with a blue 'B' icon.
- Alert type:** A dropdown menu currently set to 'Custom' with a blue 'C' icon.
- Send this alert when...:** A section with a blue 'D' icon containing:
 - Activities:** A dropdown menu labeled 'Choose activities for alert'.
 - Users:** A dropdown menu labeled 'Show results for all users'.
- Send this alert to...:** A section with a blue 'E' icon containing a dropdown menu labeled 'Show results for all users'.

4. Complete the following fields to create an activity alert:

- * Name - Type a name for the alert. Alert names must be unique within your organization.
- * Description (Optional) - Describe the alert, such as the activities and users being tracked, and the users that email notifications are sent to. Descriptions provide a quick and easy way to describe the purpose of the alert to other admins.
- * Alert type - Make sure the Custom option is selected.
- * Send this alert when - Click Send this alert when and then configure these two fields:
 - Activities - Click the drop-down list to display the activities that you can create an alert for. This is the same activities list that's displayed when you search the Office 365 audit log. You can select one or more specific activities or you can click the activity group name to select all activities in the group. For a description of these activities, see the "Audited activities" section in Search the audit log. When a user performs any of the activities that you've added to the alert, an email notification is sent.
 - Users - Click this box and then select one or more users. If the users in this box perform the activities that you added to the Activities box, an alert will be sent. Leave the Users box blank to send an alert when any user in your organization performs the activities specified by the alert.
- * Send this alert to - Click Send this alert, and then click in the Recipients box and type a name to add a users who will receive an email notification when a user (specified in the Users box)

performs an activity (specified in the Activities box). Note that you are added to the list of recipients by default. You can remove your name from this list.

5. Click Save to create the alert. The new alert is displayed in the list on the Activity alerts page.

Name	Recipients	Status ▲	Date modified
Executive mailbox alert	compliance@contoso.com	On	2016-06-08 14:42:02
SharePoint upload alert	admin@contoso.com	Off	2016-06-08 14:23:39
External sharing alert	admin@contoso.com	Off	2016-06-08 14:24:08

The status of the alert is set to On. Note that the recipients who will received an email notification when an alert is sent are also listed.

References:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-activity-alerts?view=o365-worldwide>

NEW QUESTION: 21

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □ □□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□ □□□ □□□□ □□ □ □□□ □□ □ □□□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□ □□□□ □□□□.

Microsoft 365 □□□ □□□□.

□□□□ □□□□□ □□□□□ □□□□ □□ □□□ □□□□ Microsoft SharePoint Online □ □□□ □□□□□ □□□□ □□ □□□.

□□□: Azure Active Directory □□ □□□□ □□□ □ □□ □□□ □□□ □□□ □□□ □□□ □□□ □□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

Explanation

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online>

SharePoint-Online

NEW QUESTION: 22

Contoso.com Azure AD(Azure Directory) Microsoft 365 .

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

user5 .

User5 .

.

A. Azure AD .

B. Azure AD .

C. User2 User4 .

D. User4 .

E. User1, User2 User4 .

F. User2 User4 .

Answer: (SHOW ANSWER)

Explanation

Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).

Only on users who are non-admins or in any of the following limited admin roles:

- * Directory Readers
- * Guest Inviter
- * Helpdesk Administrator
- * Message Center Reader
- * Reports Reader
- * User Administrator

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#availab>

NEW QUESTION: 23

Microsoft 365 .

Name	Role
User1	Helpdesk admin
User2	Global Administrator
User3	None
User4	None
User5	None

.

Name	Type	Members
Group1	Microsoft 365	User2, User3
Group2	Mail-enabled security	User1, Group3
Group3	Distribution list	User4, User5

□□ □□□ □□ □□ □□□□□.

Deploy your app



□□ □ □□□ □□ □□□ □□ □□□□□□. □□□ □□□ □□□□ □□□□□.



Answer:



Explanation





Microsoft Office 365 is a suite of products and services from Microsoft. It includes the following apps:

- A. Microsoft Endpoint Manager (formerly Intune) is a cloud-based service that helps organizations manage their devices and applications.
- B. Microsoft Dynamics 365 is a set of business management solutions that help organizations manage their sales, customer service, and marketing.
- C. Microsoft 365 is a subscription-based service that provides access to all the Office 365 apps and services.
- D. Microsoft 365 is a subscription-based service that provides access to all the Office 365 apps and services, including Windows Defender, Office, OneDrive, and Microsoft Exchange Online.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 27

Microsoft 365 is a cloud-based suite of productivity and business applications. It includes the following apps and services:

- Word, Excel, PowerPoint, and OneNote: Office productivity applications.
- Outlook: Email and calendar management.
- OneDrive: Cloud storage for documents and files.
- SharePoint: Collaboration and content management.
- Teams: Communication and collaboration hub.
- Yammer: Enterprise social network.
- Microsoft Exchange Online: Cloud email and calendaring.
- Microsoft Dynamics 365: Business management solutions.
- Microsoft Defender: Security and compliance solutions.

Microsoft 365 is a subscription-based service that provides access to all the Office 365 apps and services.

Microsoft 365 admin@LODSe426243.onmicrosoft.com

Microsoft 365 ID: 3&YWyjse-6-d

Microsoft 365 Admin Center: CTRL-K to search for users.

Grady Archie is a user in the organization.

Grady Archie ID: 10887751

Grady Archie is currently assigned the Billing Administrator role.

Grady Archie is currently assigned the Billing Administrator role.

Grady Archie is currently assigned the Billing Administrator role.

Grady Archie is currently assigned the Billing Administrator role.

Answer:

See explanation below.

Explanation

You need to assign the 'Billing Administrator' role to Grady Archie.

1. Go to the Azure Active Directory admin center.
2. Select Users.
3. Select the Grady Archie account to open the account properties page.
4. Select 'Assigned roles'.
5. Click the 'Add Assignments' button.
6. Select Billing Administrator then click the Add button.

References:

<https://docs.microsoft.com/en-us/office365/admin/add-users/about-admin-roles?view=o365-worldwide>

NEW QUESTION: 28

Microsoft 365 Enterprise E5 user.

Microsoft Azure Active Directory(Azure AD) App1 user.

App1 user is currently assigned the Billing Administrator role.

App1 user is currently assigned the Billing Administrator role.

New	Users and groups
Info	Include Exclude
*Name <input type="text" value="App1 policy"/>	<input type="radio"/> None
Assignments	<input checked="" type="radio"/> All users
<input type="text" value="Users and groups"/> All users	<input type="radio"/> Select users and groups
<input type="text" value="Cloud apps"/> 0 cloud apps selected	<input type="checkbox"/> All guest users
<input type="text" value="Conditions"/> 0 conditions selected	<input type="checkbox"/> Directory roles
Access controls	<input type="checkbox"/> Users and groups
<input type="text" value="Grant"/> 0 controls selected	
<input type="text" value="Session"/> 0 controls selected	
Enable policy	
<input type="button" value="On"/> <input checked="" type="button" value="Off"/>	

Answer:

New x	Users and groups □ x
Info	Include Exclude
*Name	
<input type="text" value="App1 policy"/>	<input type="radio"/> None
Assignments	<input checked="" type="radio"/> All users
<input type="text" value="Users and groups"/> All users	<input type="radio"/> Select users and groups
<input type="text" value="Cloud apps"/> 0 cloud apps selected	<input type="checkbox"/> All guest users
<input type="text" value="Conditions"/> 0 conditions selected	<input type="checkbox"/> Directory sales
Access controls	<input type="checkbox"/> Users and groups
<input type="text" value="Grant"/> 0 controls selected	
<input type="text" value="Session"/> 0 controls selected	
Enable policy	
<input type="button" value="On"/> <input checked="" type="button" value="Off"/>	

Explanation

In the Cloud Apps section, you need to select the name of the app (App1) that the policy will apply to.

In the Grant section under Access Controls, there is a checkbox named "Require Multi-factor Authentication".

That checkbox needs to be ticked.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/best-practices>

<https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Conditional-Access-now-in-the-new-Azur>

NEW QUESTION: 29

□□ □□ □□□ □□□□ □□□□ Microsoft 365□ □□□□□ □□□ □□□□.

Name	Azure Active Directory (Azure AD) role	On-premises Active Directory group membership
User1	Cloud application administrator	None
User2	Application administrator	None
User3	Service administrator	None
User4	None	Domain Admins

Azure AD □□□□□□ □□□□ □□□□ App1□□□□ □□□□□□ □□ □□ □□□□ □□□□ □□□□□□. App1□ User4□ □□□□□□. □□□□□□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□. □□ □□□□ □□□□ □□□□?

- A. □□□1
- B. □□□2
- C. □□□3
- D. □□□4

Answer: B ([LEAVE A REPLY](#))

Explanation

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-add-on-premisesapplicat>

NEW QUESTION: 30

□□ □□□ □□□□ □ Microsoft Teams □□ □□□□ □□□□□.

- * □ □□ □□
- * □□□□□□ □□ □□□□□□ □□□□□ □□□□□□.
- * Microsoft Graph API□ □□□□□□.
- * □□ □□ □□□□ □□□□□□□□.

□ □□□□ □□□□□ □□□□ □ □□ □ □□ □□□ □□□□□□□□? □ □□□ □□□□□ □□□□ □□ □□□□. □□: □ □□□ □□□□ 1□□ □□□□ □□□□□.

- A. □□ □□ □□□□ □□□□□□□.
- B. □ □□ □□
- C. □□□□□ □□ □□□□□□ □□□□□ □□□□□□.
- D. Microsoft Graph API □□□ □□□□□.

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 31

contoso.com□□□ Azure AD(Azure Active Directory) □□□□□ □□□□ □□□□ Microsoft 365 E5 □□□□ □□□□□. □□□□□□ Site1□□□□□ Microsoft SharePoint Online □□□□□ □□ □□ □□□□ □□□□ □□□□□ □□□□□.

□□□.

* App1□ □□□□ □□□□ □□ □ □□□ □□□□□□□.

* □□ □ □□□ □□ □□□ □□□□□□□.

* App1□ □□□ □□ □□□ □□□ □□□□ □□□ □□□.

□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□□.

```
function authCallback(error, response) {
}
userAgentApplication.handleRedirectCallback(authCallback);
const accessTokenRequest: AuthenticationParameters = {
  scopes: ["user.read"]
}
use {
  scopes: ["user.read.all"]
  scopes: ["people.read"]
  scopes: ["people.read.all"]
}
let accessToken = acc
}).catch(function (error) {
  acquireTokenRedirect
  acquireTokenSilent
  acquireTokenPopup
})
userAgentApplication.
  acquireTokenRedirect
  acquireTokenSilent
  acquireTokenPopup
  (accessTokenRequest);
});
```

Answer:

```
function authCallback(error, response) {
}
userAgentApplication.handleRedirectCallback(authCallback);
const accessTokenRequest: AuthenticationParameters = {
  scopes: ["user.read"]
}
use {
  scopes: ["user.read.all"]
  scopes: ["people.read"]
  scopes: ["people.read.all"]
}
let accessToken = acc
}).catch(function (error) {
  acquireTokenRedirect
  acquireTokenSilent
  acquireTokenPopup
})
userAgentApplication.
  acquireTokenRedirect
  acquireTokenSilent
  acquireTokenPopup
  (accessTokenRequest);
});
```

Explanation

```
function authCallback(error, response) {
}
userAgentApplication.handleRedirectCallback(authCallback);
const accessTokenRequest: AuthenticationParameters = {
  scopes: ["user.read"]
}
userAgentApplication. acquireTokenSilent (accessTokenRequest).then(function(accessTokenResponse) {
  let accessToken = accessTokenResponse.accessToken;
}).catch(function (error) {
  if (error.errorMessage.indexOf("interaction_required") !== -1) {
    userAgentApplication. acquireTokenPopup (accessTokenRequest);
  }
});
```



NEW QUESTION: 33

□□ □□□ □□□□ □□ □□ □□□ □□□□. □□□□ □ □□□□ □□□ □ □□□□. □
□□□ □ □ □□ □ □□□ □ □□□ □□ □□ □□□ □□□□ □□□□ □□□□.
□□ □□□ □□□ □ □□□ □□□□ □□ □□□ □□□□□□. □ □□□□□ □□□ □□□
□ □□□ □□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□□ □□□ □ □□□
□□ □□(□: □□ □ □□□□, □□ □ □□□ □□ □□)□ □□□ □□□□□□□.
□□□ □□□ □□□ □□□ □□□ □□□ □□□ □□□. □, □□□ □□□ □□□□□□ □
□□□ □□□ □□□□□ □□□□ □□ □□□ □□ □□□□ □□ □□□.
□□ □□□ □□□ □□□□ □□□ □ □□□□ □□□□ □□ □□□ □ □ □□ □□ □ □□□
□. □ □□□ □□□□ □ □□□ □□ □□□ □□□ □ □□□□. □□□ □□□ □□ □□ □□
□□□ □□ □□ □□□ □□□ □ □□□ □□□ □□□□ □□□□ □□□□ □□□.
□ □□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □ □□□□.
□□ □□□ □□□□ □□□ □□□ □ □□□□.
□□□ □□
□□□ □□ □□ □□□ □□ □□□ □□□□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□ □□□ □□□ □□□□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□□□.
Microsoft 365 □□□ □□: admin@LODSe878763.onmicrosoft.com
Microsoft 365 □□: m3t^We\$Z7&xy
Microsoft 365 □□□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□
□ □□□ □□ □□□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□□.
□ □□□□: 11440873



Sign in

Email, phone, or Skype

No account? [Create one!](#)



Sign-in options

Next

□□□ □□□ □□□ □ □□ □□□□□□□ □□ □□□ □□□ □□□ □□ □□□□□ □□
 □ □□□□□.

□□□ □□□□□ □□ Microsoft Teams□□ □□ □□□□ □□□. □□□ □□□ □□ □□□
 □□□ □□□.

Project1□□□ □□□ □□□□□.

□□□□ □□□ □□□□.

Channel1□□□ □□□ □□□□.

□□□□□ Microsoft 365 □□□ □□□□□□.

Answer:

See explanation below.

Explanation

You need to create a team. You can create a team in the Microsoft Teams Admin Center or in the Microsoft Teams app. However, to be able to specify the team owner when creating the team, you need to use the Teams Admin Center.

1. Go to the Microsoft Teams Admin Center.
2. In the left navigation pane, expand the Teams section and select 'Manage Teams'.
3. Click the '+ Add' link to add a new team.
4. Give the team the name Project1.
5. In the Team Owner field, remove your name which is there by default and add Lee Gu.
6. Click the 'Create a team' button to create the team.
7. In the teams list, select the Project1 team.
8. Click on 'Channels'.
9. Click the '+ Add' link to add a new channel.
10. Give the channel the name Channel1.
11. Click the Apply button to create the channel.

NEW QUESTION: 34

□□□□ Microsoft Teams□□ □□□ □□□□ □□ □□□ □□□ □ □□□ HRApp□ □□□
 □ □□□. □□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□
 □ □□ □□□□ □□□□ □□□ □□□ □□□□□□□.

Actions

- Implement a handler for the `jobsearch` command in the Microsoft Bot Framework app.
- In the HRApp manifest, configure the `botId` value in the `bot` section to match the `botId` value of the bot registration.
- Implement a handler for the `query` command in the Microsoft Bot Framework app.
- Create a bot registration and a Microsoft Bot Framework app.
- In the HRApp manifest, configure the `botId` value in the `ComposeExtensions` section to match the `botId` value of the bot registration.

Answer Area

Navigation: > <

Answer:

Actions

- Implement a handler for the `jobsearch` command in the Microsoft Bot Framework app.
- In the HRApp manifest, configure the `botId` value in the `bot` section to match the `botId` value of the bot registration.
- Implement a handler for the `query` command in the Microsoft Bot Framework app.
- Create a bot registration and a Microsoft Bot Framework app.
- In the HRApp manifest, configure the `botId` value in the `ComposeExtensions` section to match the `botId` value of the bot registration.

Answer Area

- Create a bot registration and a Microsoft Bot Framework app.
- In the HRApp manifest, configure the `botId` value in the `ComposeExtensions` section to match the `botId` value of the bot registration.
- Implement a handler for the `jobsearch` command in the Microsoft Bot Framework app.

Navigation: > <

Explanation

Graphical user interface, text, application Description automatically generated

- Create a bot registration and a Microsoft Bot Framework app.
- In the HRApp manifest, configure the `botId` value in the `ComposeExtensions` section to match the `botId` value of the bot registration.
- Implement a handler for the `jobsearch` command in the Microsoft Bot Framework app.

Step 1: Create a bot registration..

Step 2: In the HRApp manifest, configure the `botId` value in the `ComposeExtensions` section to match the `botId` value of the bot registration.

Scenario: HRApp must include a messaging extension that enables users to search jobs by job title or job ID.

Step 3: Implement a handler

Reference:

Microsoft 365 User: m3t^We\$Z7&xy

Microsoft 365 User: m3t^We\$Z7&xy CTRL-K
 Microsoft 365 User: m3t^We\$Z7&xy
 Microsoft 365 User: m3t^We\$Z7&xy
 Microsoft 365 User: m3t^We\$Z7&xy
 Microsoft 365 User: m3t^We\$Z7&xy



Lynne Robbins Microsoft Office 365 User: Lynne Robbins
 Microsoft Office 365 User: Lynne Robbins
 Microsoft Office 365 User: Lynne Robbins
 Microsoft Office 365 User: Lynne Robbins

Answer:

See explanation below.

Explanation

You need to enable Multi-Factor Authentication for Lynne Robbins.

1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Users section and select Active Users.
3. Click the 'Multi-factor authentication' link.
4. Select Lynne Robbins.
5. In the right navigation pane, select the 'Enable' link to enable MFA for the account.
6. Confirm the setting by clicking the 'Enable multi-factor authentication' button.
7. Click the Close button to close the confirmation window.

NEW QUESTION: 37

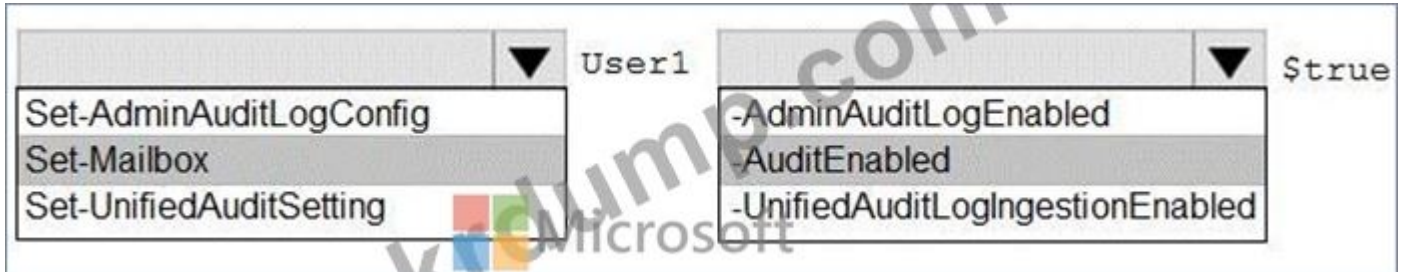
Microsoft 365 User: User1
 User1 Microsoft Exchange Online User: User1
 User1 Microsoft Exchange Online User: User1
 User1 Microsoft Exchange Online User: User1
 User1 Microsoft Exchange Online User: User1



Answer:



Explanation



To enable auditing for a single mailbox (in this example, belonging to Holly Sharp), use this PowerShell command: Set-Mailbox username -AuditEnabled \$true
 References:
<https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins>
<https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps>

NEW QUESTION: 38

2022-03-05 Package1

* 0000

* 00:001

* 00:00 0 0

* 00:00

* 000000

o 000 000 00 00: 00 f 00 00 00: 2022-03-20 2022-03-05 00 00 0
 00 000 00000 Package1 000000.

Name	Email address
Guest3	Guest3@outlook.com
Guest4	Guest4@outlook.com

2022-03-06 Guest3

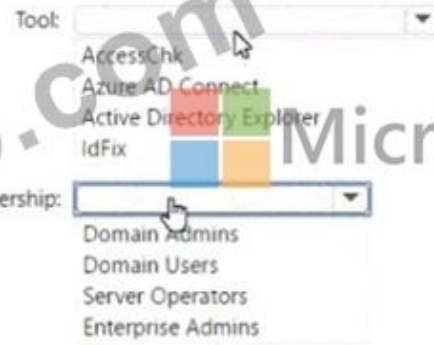
00 0 000 00 000 000 00 000000. 000 000 00000 000000.

00: 0 000 000 100 000 00000.

Statements	Yes	No
On April 10, 2022, Guest2 will be able to sign in to contoso.com.	<input type="radio"/>	<input type="radio"/>
On April 25, 2022, Guest3 will be able to sign in to contoso.com.	<input type="radio"/>	<input type="radio"/>
On May 1, 2022, Guest1 will be able to sign in to contoso.com.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area



Answer:



Explanation



NEW QUESTION: 41

□□ □□□ □□□□ □□ □□ □□□ □□□□. □□□□ □ □□□□ □□□ □ □□□□. □
□□□ □ □ □□ □□□ □ □□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□.
□□ □□□ □□□ □ □□□ □□□□ □□ □□□ □□□□□□. □ □□□□□ □□□ □□□
□ □□□ □□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□□ □□□ □ □□□
□□ □□(□: □□ □ □□□□, □□ □ □□□ □□ □□)□ □□□ □□□□□□.
□□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□. □, □□□ □□□ □□□□□□□ □
□□□ □□□ □□□□□ □□□□ □□ □□ □□□□ □□ □□ □□ □□ □□.
□□ □□□ □□□ □□□□ □□□ □ □□□□ □□□□ □□ □□□ □ □ □□ □□ □ □□□
□. □ □□□ □□□□ □ □□□ □□ □□□ □ □□□□. □□□ □□□ □□ □□ □□
□□□ □□ □□ □□□ □□□ □ □□□ □□□ □□□□ □□□□ □□□□ □□□.
□ □□□ □□ □□□ □□□□ □□□ □□□□ □□□□ □□□ □□ □□□□.
□□ □□□ □□□□ □□□ □□□ □□ □□□□.
□□□ □□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□□.

Microsoft 365 :

admin@LODSe1211885.onmicrosoft.com

Microsoft 365 : oL9z0=?Nq@ox

Microsoft 365 CTRL-K

.

: 11098651



Microsoft 365 .

Answer:

See explanation below.

Explanation

You need to edit the Data Loss Prevention Policy to disable the email notifications.

- 1. Go to <https://protection.office.com> or navigate to the Security & Compliance admin center.
- 2. In the left navigation pane, expand Data Loss Protection and select Policy.
- 3. Select the Data Loss Prevention policy and click the Edit Policy button.
- 4. Click Policy Settings in the left navigation pane of the policy.
- 5. Select the policy rule and click the Edit Rule button.
- 6. Scroll down to the 'User notifications' section.
- 7. Toggle the slider labelled "Use Notifications to inform users...." to Off.

- Click Save to save the changes to the policy rule.
- Click Save to save the changes to the policy.

NEW QUESTION: 42

HR app is a Microsoft Teams app. The app is currently in the HRApp section of the app catalog. You need to ensure that the app is available to all users in the organization. What should you do?

Options:

- Change the app's visibility to Public.
- Change the app's visibility to MyOrg.
- Change the app's visibility to MyOrg and Public.
- Change the app's visibility to MyOrg and MyOrg and Public.

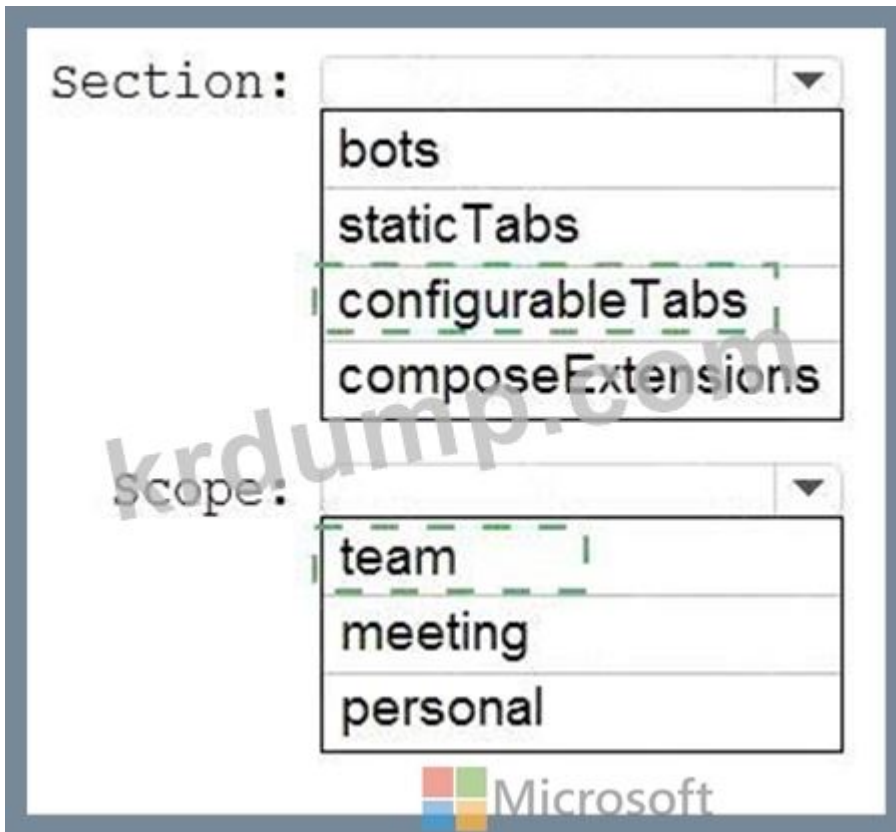
Section:

- bots
- static Tabs
- configurable Tabs
- compose Extensions

Scope:

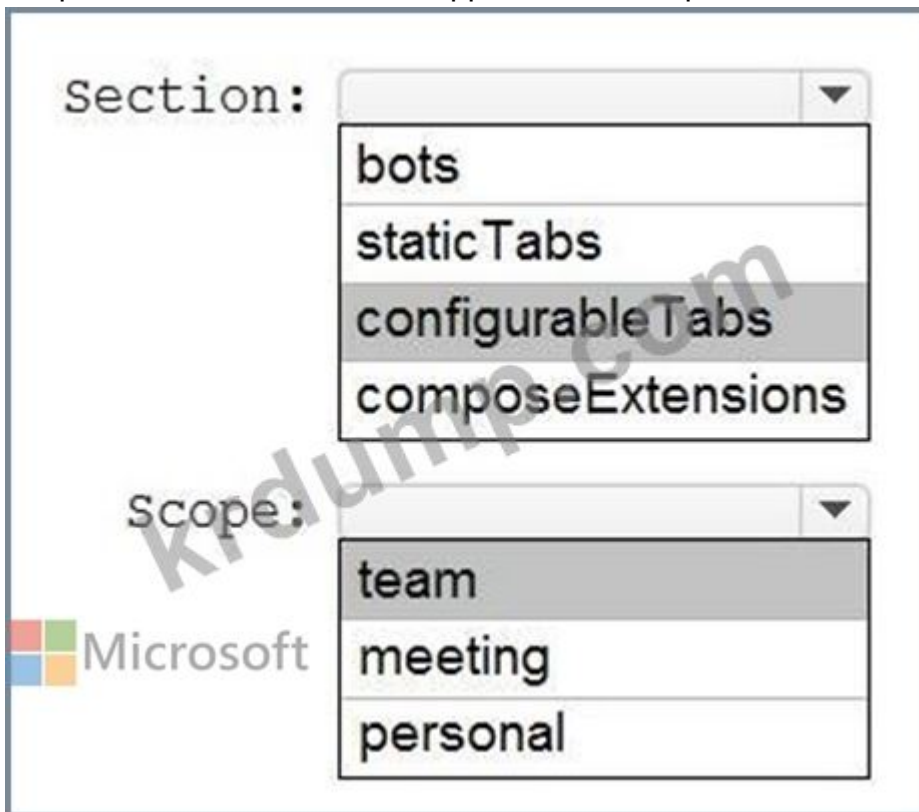
- team
- meeting
- personal

Answer:



Explanation

Graphical user interface, text, application Description automatically generated



Reference:

<https://docs.microsoft.com/en-us/microsoftteams/platform/resources/schema/manifest-schema#composeextensio>

NEW QUESTION: 43

Microsoft Exchange Server 2013 .
 100 .
 Microsoft 365 .- .
 Active Directory Microsoft Azure Active Directory(Azure AD) .
 Exchange Online .
 ?

- A.
- B. IMAP
- C.
- D.

Answer: A (LEAVE A REPLY)

Explanation

References:

<https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365> A cutover migration and an IMAP migration do not require the company to sync the on-premises Active Directory domain to Microsoft Azure Active Directory (Azure AD). Only a cutover migration meets the requirements in this question.

With a cutover migration, user accounts will need to be created in Azure Active Directory for each user. The mailboxes are all migrated in one go and MX records configured to redirect email to Microsoft 365.

NEW QUESTION: 44

Microsoft Endpoint Manager Windows 10 .

Name	CPU	Member of	Installed apps
Device1	x86	Group1	Microsoft Office 2016
Device2	x86	Group1	None
Device3	x64	Group1	Microsoft Office 2019
Device4	x64	Group1	None

Microsoft 365 Suite (Exhibit) Group1 . Microsoft 365 ?

- A. 2
- B. 1 2
- C. Device2 Device4
- D. 1, 2. Device4
- E. 1, 2, 3 4

Answer: E (LEAVE A REPLY)

NEW QUESTION: 45

Active Directory Microsoft Azure Active Directory(Azure AD)

□□□ □□□□.

□□□□□ □□□ □□□□□ □□□ □□□ □□□ □□□□□ □□□□□.

□□□□ □□□□ □□□□ □□□□□□.

□□□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □□□□ □□□ □□□□□□□.

* *.microsof.com

* *.office.com

□□□□ □□□□ □□□□□.

□□□□ □□□□ □□□□□ □□□□□□ □□□□ □□□.

□□□ □□□□ □□ □□□ □□ □□□ □□□□□□? □□ □□□ □□ □□□ □□□ □□□ □□□ □

□□□□. □□ □□ □□ □□□□□.

A. □□□□□ □□□□□ □□□ □□ Azure □□□□ □□□ IP □□ □□□ □□□□□.

B. Azure AD Connect□□ □□□ □□ □□□ □□ □□□ □□□□□.

C. □□ □□□□ Azure AD Connect □□□ □□□ □□□□□.

D. □□□□□ □□□ □□□□ □□□ □□□ □□□□.

E. □□□□□ □□□ □□□□□ □□□ □□□ □□□□□.

Answer: E (LEAVE A REPLY)

Explanation

Azure AD Connect needs to be able to connect to various Microsoft domains such as login.microsoftonline.com. Therefore, you need to modify the list of allowed outbound domains on the firewall.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-ports>

NEW QUESTION: 46

□□□ Microsoft 365 E5 □□□ □□□□.

□□ □□□ □□□□ □□□ □□□□ □□□□□.

□□ □□ □□□ □ □□□ □□□ □□□□□□ □□□□ □□ □□ □□□□ □□□□□ □□

□□ □□ □ □□□□ □□□□□ □□□□ □□ □□□. □□ □□□ □□□□ □□□□□ □□

□□.

□□ □ □□ □□ □□ □□□□ □□□ □□ □□□?

A. □□□ □□ □□□ □□ □□□ □□ □□(DLP) □□□ □□□□.

B. □□□ □□ □□□ □□ DLP(□□□ □□ □□) □□□ □□□□.

C. □□ □□ □□ □□□ □□□□□.

D. □ □□□ □□ □□□ □□□□.

Answer: D (LEAVE A REPLY)

Explanation

ATP Safe Links, a feature of Office 365 Advanced Threat Protection (ATP), can help protect your organization from malicious links used in phishing and other attacks. If you have the necessary permissions for the Office 365 Security & Compliance Center, you can set up ATP Safe Links policies to help ensure that when people click web addresses (URLs), your organization is protected. Your ATP Safe Links policies can be configured to scan URLs in email and URLs in

Microsoft 365 user: admin@LODSe878763.onmicrosoft.com
Microsoft 365 user: m3t^We\$Z7&xy
Microsoft 365 user: CTRL-K
Microsoft 365 user: 11440873



Microsoft 365 user: [redacted]

Answer:

See explanation below.

Explanation

You need to modify the default remote domain. When you add a remote domain, you specify the domain name and the settings apply to that domain. The default remote domain applies to all other domains. Therefore, we need to disable Out of Office replies for external users in the settings of the default remote domain.

1. Go to the Exchange Admin Center.
2. Click Mail Flow in the left navigation pane.
3. Click on Remote Domains.
4. Select the default remote domain and click the Edit icon (pencil icon).
5. In the 'Out of Office automatic reply types' section, select 'None'.
6. Click Save to save to changes to the default remote domain.

NEW QUESTION: 49

[Redacted question text]

Microsoft 365 □□□ □□□□.

□□ □□ □□□□ Microsoft SharePoint □□□□ □□□□ □□□□□□ □□□□□□□□. □□ □□□□ □□□□ □□□□ SharePoint □□ □□□ □□□□□□. □□ SharePoint □□□ □□□□ □□□ □□□ □□□. □□ □□: SharePoint □□ □□□□ □□ □□□ □□□□□□. □□□ □□□ □□□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

Explanation

You need to create a threat management policy in the Security & Compliance admin center.

NEW QUESTION: 50

□□□ □□ □□□□ □□□ □□□ □□□□ □□□□□□ □□□ □□□□ □□□□. □□ □□□□□ □□□ □□ □□□ □□□□.

* □□□□ □□□ □□□□□ □□□□ □□□□□ OneDrive □ □□□□□.

* □□ □□ □□□ □□□□ □□□□.

□□□□□□ □□□ □□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□. □ □□□ □□ □□ □□ □□ □□□□ □□□□ □□□□ □□□□ □□□ □□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Answer Area



Save invoices:

Administrator
Application
Delegated
Super User

Send automated reminders:

Administrator
Application
Delegated
Super User

Answer:



Save invoices:

Administrator
Application
Delegated
Super User

Send automated reminders:

Administrator
Application
Delegated
Super User

Explanation

krdump.com

NEW QUESTION: 51

Microsoft SharePoint Server 2016

Microsoft 365

SharePoint SharePoint Online

Microsoft OneDrive

SharePoint

SharePoint

SharePoint

SharePoint

B2B(Business to Business)

SharePoint

SharePoint

SharePoint

SharePoint

SharePoint

A. SharePoint

B. OneDrive

C. SharePoint

D. SharePoint

Answer: (SHOW ANSWER)

Explanation

Hybrid OneDrive - Choosing this option will redirect on-premises My Sites/OneDrive for Business sites to SharePoint Online OneDrive for Business in Office 365. Once the wizard completes, any click of the OneDrive link from on-premises will redirect to OneDrive for Business in the cloud. This meets the following requirement: OneDrive sites must redirect users to online content.

Cloud hybrid search - Choosing this option creates a cloud Search service application in SharePoint Server and connects the cloud Search service application to your Office 365 tenant. This meets the following requirement: When users search for a document by using keywords, the

results must include online and on-premises results.

Reference:

<https://docs.microsoft.com/en-us/sharepoint/hybrid/hybrid-picker-in-the-sharepoint-online-admin-center>

NEW QUESTION: 52

contoso.onmicrosoft.com Microsoft Azure Active Directory(Azure AD) .
 Windows 10 Pro Azure AD .
 Microsoft 365 E3 .
 Windows 10 Enterprise .

Microsoft 365 .
 ?

- A. .
- B. Windows Autopilot Windows 10 Enterprise .
- C. .
- D. .

Answer: B (LEAVE A REPLY)

Explanation

With Windows Autopilot the user can set up pre-configure devices without the need consult their IT administrator.

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios>
<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot>

NEW QUESTION: 53

Microsoft 365 Enterprise E5 .
 .

- A. .
- B. .
- C. .
- D. .

Answer: (SHOW ANSWER)

Explanation

You can configure a sign-in risk policy that applies to the Finance department users. The policy can be configured to 'Allow access' but with multi-factor authentication as a requirement.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy

NEW QUESTION: 54

□□□□□ SalesApp□ □□ □□□ □□□ □□□□ □□□.
□□□□ □□ □□ □□□ □□□□ □□□.
□□□□ □□□ □□□□ □□□?

- A. □□ □□□ □□
- B. □□□□□□□ □□□
- C. SharePoint Online□ □ □□□□
- D. □□□□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 55

□□□□ Azure AD(Azure Active Directory)□ □□□□□ □□□ □□□□.
Microsoft 365 □□□ □□□□□.
□□□□ Azure AD(Azure Active Directory)□ □□□□□ □□□ □□□□.
Microsoft 365 □□□ □□□□□.
□ □ □□ □ □□□□ □ □□□ Microsoft 365□ □□□□□□□ □□□□□. □ □□□□□□□
Windows 10□ □□□□ □□□ □□□□.
□□□ 5□□ □ □□□ □□□ □□ □□□□□□□□ □□ □□□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□
□ □□ □□□□ □□□□ □□□ □□□ □□□□□□□. □ □□□□□□□ Windows 10□ □□□
□ □□□ □□□□.
□□□ 5□□ □ □□□ □□□ □□ □□□□□□□□ □□ □□□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□
□ □□ □□□□ □□□□ □□□ □□□ □□□□□□□.

Actions

- From SharePoint Online, create 10 libraries.
- From Group Policy Management Editor, configure the OneDrive settings.
- From Group Policy Management Editor, configure the Folder Redirection settings.
- Instruct the users to run gpupdate.exe /force at a command prompt on each device.
- Deploy the Azure File Sync agent to all devices.
- Copy the OneDrive Administrative Templates to your computer.

Answer Area



Answer:



Actions

- From SharePoint Online, create 10 libraries.
- From Group Policy Management Editor, configure the OneDrive settings.
- From Group Policy Management Editor, configure the Folder Redirection settings.
- Instruct the users to run gpupdate.exe /force at a command prompt on each device.
- Deploy the Azure File Sync agent to all devices.
- Copy the OneDrive Administrative Templates to your computer.

Answer Area

- Copy the OneDrive Administrative Templates to your computer.
- From Group Policy Management Editor, configure the OneDrive settings.
- Instruct the users to run gpupdate.exe /force at a command prompt on each device.



Explanation

- Copy the OneDrive Administrative Templates to your computer.
- From Group Policy Management Editor, configure the OneDrive settings.
- Instruct the users to run gpupdate.exe /force at a command prompt on each device.

You need to configure a Group Policy Object (GPO) with the OneDrive settings required to redirect the Home folder of each user to Microsoft 365.

Before you can configure the Group Policy, you need to download the OneDrive Administrative Templates.

These templates add the required OneDrive settings to Group Policy so you can configure the settings as required.

After the OneDrive settings have been configured in Group Policy, you can run the gpupdate /force command on the five computers to apply the new Group Policy settings immediately.

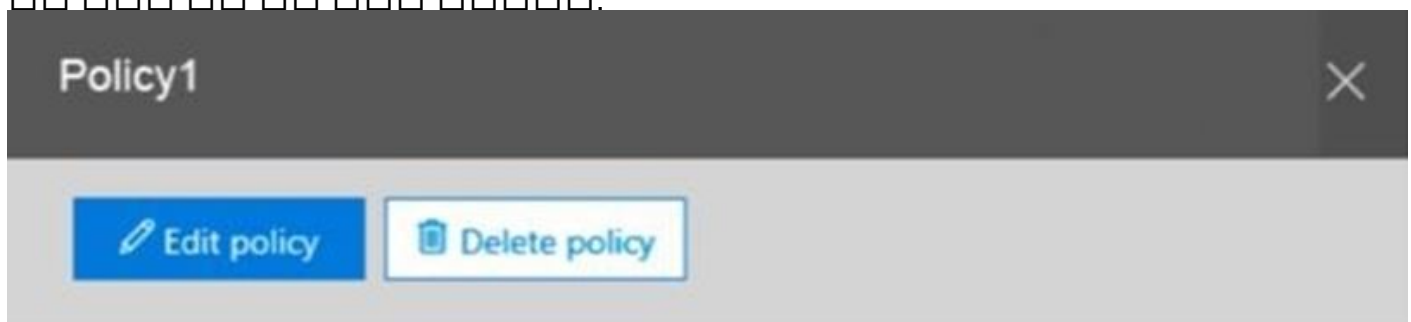
Reference:

<https://practical365.com/clients/onedrive/migrate-home-drives-to-onedrive-for-business/>

NEW QUESTION: 56

Microsoft 365 .

.



Status On

Description Description

Severity Low

[Edit](#)

Category Threat management

Conditions Activity is Detected malware in file

Aggregation Aggregated

Threshold 20 activities

Window 120 minutes

Scope All users

Email recipients User1@sk190107outlook.onmicrosoft.com

Daily No limit

[Edit](#)



Microsoft

Close

□□□□ □□□ □□□□ □□□□ □□□ □□□□ □ □□□ □□□□ □□ □□□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

Microsoft
Policy1 will trigger an alert if malware is detected in [answer choice].

Exchange Online only
SharePoint Online only
SharePoint Online or OneDrive only
Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is [answer choice].

5
12
20
100

Answer:

Microsoft
Policy1 will trigger an alert if malware is detected in [answer choice].

Exchange Online only
SharePoint Online only
SharePoint Online or OneDrive only
Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is [answer choice].

5
12
20
100

Explanation

Answer Area

Microsoft
Policy1 will trigger an alert if malware is detected in [answer choice].

Exchange Online only
SharePoint Online only
SharePoint Online or OneDrive only
Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is [answer choice].

5
12
20
100

The 'Activity is' setting is configured as 'Detected malware in file'. This setting means the policy is applied to files stored in SharePoint or OneDrive. The Aggregation settings has a 120 minute window. This means that if there 20 detections in 120 minutes, an email will be generated. Therefore, the maximum number of emails generated in 24 hours is 12.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies>

NEW QUESTION: 57

Microsoft Azure Active Directory(Azure AD)

Name	Member of
User1	Group1
User2	Group2

Microsoft Intune

Intune

Name	Platform	BitLocker Drive Encryption	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

Intune

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

Microsoft Exchange Online

Microsoft Exchange Online

- Group1

- Exchange Online

- Microsoft Exchange Online, Microsoft Exchange Online

Microsoft Exchange Online

Microsoft Exchange Online

Statements

Yes

No

User1 can access Microsoft Exchange Online from Device1.

User1 can access Microsoft Exchange Online from Device2.

User2 can access Microsoft Exchange Online from Device2.

Answer:

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>

Box 1:

Yes. User1 is in Group1. The Conditional Access Policy applies to Group1. The Conditional Access Policy blocks access unless the device is marked as compliant.

BitLocker is disabled for Device1. Device1 is in Group3 which is assigned device Policy1. The BitLocker policy in Policy1 is 'not configured' so BitLocker is not required.

Therefore, Device1 is compliant so User1 can access Exchange online from Device1.

Box 2:

No. User1 is in Group1. The Conditional Access Policy applies to Group1. The Conditional Access Policy blocks access unless the device is marked as compliant.

BitLocker is disabled for Device2. Device2 is in Group4 which is assigned device Policy2. The BitLocker policy in Policy2 is 'Required so BitLocker is required.

Therefore, Device2 is not compliant so User1 cannot access Exchange online from Device2.

Box3:

Yes. User2 is in Group2. The Conditional Access Policy applies to Group1. The Conditional Access Policy does not apply to Group2. So even though Device2 is non-compliant, User2 can access Exchange Online using Device2 because there is no Conditional Access Policy preventing him/her from doing so.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions>

NEW QUESTION: 58

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □
 □□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□ □□□
 □□□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□.
 □ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□
 □□□ □□□□ □□□□.

□□□ Microsoft Office 365 □□□□ □□□□.
 □□ Office 365 □□□ □□□ □□□□□ □□□ □□□□□.
 □□□□□ □□□ □□□□□ □□ □□□ □□□□ □□□.

□□□: □□ □□ □□ □□□□ Monitoring □ □□□□ □□□□□.
 □□□ □□□ □□□□□?

- A. □
- B. □□□

Answer: B (**LEAVE A REPLY**)

Explanation

Depending on what your organization's Office 365 subscription includes, the Dashboard in Security & Compliance includes several widgets, such as Threat Management Summary, Threat Protection Status, Global Weekly Threat Detections, Malware, etc. The Compliance admin center in Microsoft 365 contains much of the same information but also includes additional entries focusing on alerts, data insights.

The Monitoring and reports section from the Compliance admin center does not display a list of the features that were recently updated in the tenant so this solution does not meet the goal.

To meet the goal, you need to use Message center in the Microsoft 365 admin center.

Reference:

<https://docs.microsoft.com/en-us/office365/admin/manage/message-center?view=o365-worldwide>

NEW QUESTION: 59

contoso.com is a Microsoft Azure Active Directory(Azure AD) tenant.

Server1 is an Azure AD Connect Health sync agent.

Server1 is not listed in the Azure AD Connect Health sync agent list.

Server1 is an Azure Active Directory Connect sync agent.

Server1 is not listed in the Azure AD Connect Health sync agent list.

Server1 is not listed in the Azure AD Connect Health sync agent list.

Server1 is not listed in the Azure AD Connect Health sync agent list.

Server1 is not listed in the Azure AD Connect Health sync agent list.

A. Windows PowerShell `Register-AzureADConnectHealthSyncAgent` cmdlet.

B. Azure Cloud Shell `Connect-AzureAD` cmdlet.

C. Server1 Azure AD Connect Health Services `Register-AzureADConnectHealthSyncAgent` cmdlet.

D. Server1 Azure AD Connect Health Services `Register-AzureADConnectHealthSyncAgent` cmdlet.

E. Server1 Azure AD Connect Health `Register-AzureADConnectHealthSyncAgent` cmdlet.

F. Server1 Azure AD Connect Health `Register-AzureADConnectHealthSyncAgent` cmdlet.

Answer: A,E (LEAVE A REPLY)

Explanation

question states that another administrator removed Server1 from the list. To view the health status of Server1, you need to re-register the AD Connect Health Sync Agent. You can do this manually by running the `Register-AzureADConnectHealthSyncAgent` cmdlet. Alternatively, you can reinstall the Azure AD Connect Health agent. The Azure AD Connect Health agent is registered as part of the installation.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install>

NEW QUESTION: 60

contoso.com is an Azure AD(Azure Active Directory) tenant.

□□□□.

fabnkam.com□□□□ DNS □□□□ □□□□□.

Microsoft Exchange Online □□□□ fabrikam.com □□□□□ □□□ □□ □□□ □□ □ □□ □□□□ □□□.

□□□ □□□□ □□□□?

- A. Microsoft 365 □□ □□
- B. Microsoft Endpoint Manager □□ □□
- C. Exchange □□ □□
- D. Microsoft 365 □□ □□

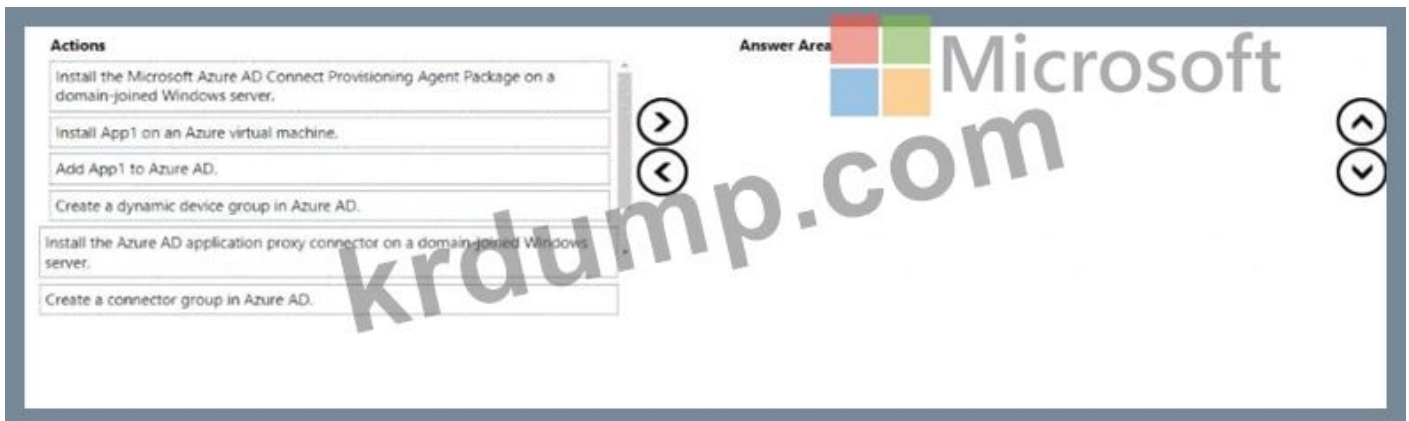
Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 61

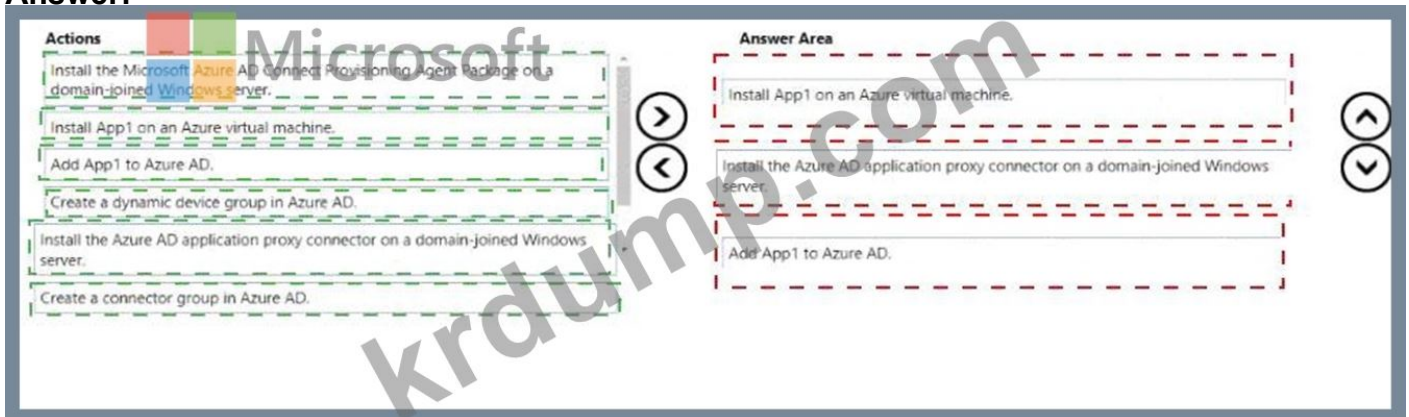
□□□□□ □□□□□ App1□□□ □□ □□□□□□.

100□□ □□□□ □□□ □□□□□ Microsoft 365 □□□ □□□□. □□□□□□ Microsoft 36S E5 □□□□□ □□□□□.

App1□ □□ Azure Active Directory Seamless Single Sign-On(Azure AD Seamless SSO)□ □□ □□□ □□□. □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□□ □ □□□□ □□□□ □□ □□□ □□□□□.



Answer:



Explanation

Graphical user interface, text, application, email Description automatically generated

Answer Area

- 1 Install App1 on an Azure virtual machine.
- 2 Install the Azure AD application proxy connector on a domain-joined Windows server.
- 3 Add App1 to Azure AD.



MS-100-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ MS-100-KR ☐☐!
DumpTop ☐ ☐☐ **MS-100-KR** ☐☐ ☐☐☐ ☐☐☐☐☐, DumpTop MS-100-KR ☐☐ ☐☐☐
☐☐☐☐☐☐☐☐ ☐☐☐ ☐☐☐☐☐☐☐. ☐☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐ DumpTop MS-100-
KR ☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/MS-100-KR-dump.html> (431
Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 62

☐☐☐☐☐☐ contoso.com☐☐☐ ☐☐☐☐☐ Active Directory ☐☐☐☐ ☐☐☐☐ ☐☐☐☐. ☐☐
☐☐☐ ☐☐ ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐.

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

contoso.com☐ Azure Active Directory☐ ☐☐☐☐☐☐ Azure AD Connect☐ ☐☐☐☐☐.

☐☐ ☐☐☐ Azure AD☐ ☐☐☐☐☐☐?

- A. ☐☐ 1, ☐☐☐ ☐☐☐☐ 2
- B. ☐☐1 ☐☐☐☐1☐
- C. User1 ☐ User2☐
- D. ☐☐ 1☐

Answer: A (LEAVE A REPLY)

Explanation

Global Security Group is a scope for the group and is set for created groups:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-g>

NEW QUESTION: 63

Group1☐ ☐☐ ☐☐ ☐☐☐☐☐☐☐☐☐.

☐☐☐☐☐☐☐☐?

- A. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐.
- B. Group1☐☐☐☐☐☐☐☐☐.
- C. Group1☐☐☐☐☐☐☐☐☐☐☐☐.
- D. Azure AD ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐.

Answer: D (LEAVE A REPLY)

Explanation

References:

* The members of Group1 must be required to answer a security question before changing their password.

If SSPR (Self Service Password Reset) is enabled, you must select at least one of the following options for the authentication methods. Sometimes you hear these options referred to as "gates." Mobile app notification Mobile app code Email Mobile phone Office phone Security questions You can specify the required authentication methods in the Password reset properties of the Azure AD tenant.

In this case, you should set the required authentication method to be 'Security questions'.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

NEW QUESTION: 64

Microsoft SharePoint Online □□□□ □-□□□□ □□ □□□ □□□□.

□□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	In SharePoint library	Last modified
File1.docx	Documents	1/11/2019
File2.docx	Documents	1/12/2019

□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	In folder	Last modified
File1.docx	D:\Folder1	1/1/2020
File2.xlsx	D:\Folder1	1/13/2020
File2.xlsx	D:\Folder2	1/7/2020
File3.pptx	D:\Folder2	1/20/2020

□□ □□□ □□ SharePoint □□□□□□ □□□ □□□□ D:\Folder1 □ D:\Folder2□ □□ □
□□□□□ □□□□□□□□□□.

All migration settings

General

Only perform scanning ⓘ

Off

Preserve file share permissions ⓘ

On

Users

Azure Active Directory Lookup ⓘ

On

User mapping file ⓘ

Choose file

Filters

Keep all versions ⓘ

On

Migrate hidden files ⓘ

On

Migrate files created after ⓘ

Select a date...



Migrate files modified after ⓘ

Select a date...



Save

Cancel

□□ □ □□□ □□ □□□ □□ □□ □□□□□□. □□□ □□□ □□□□ □□□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements

Yes

No

There will be two versions of File1.docx in the Documents library.

There will be two copies of File2.xlsx in the Documents library.

There will be a single copy of File3.pptx in the Documents library.

Answer:

Microsoft Outlook □ □□□ □□□ □□□ □□ □□ □□□□ □□□. □□□ □□ □□□ □□□ □□□□□ □□ □□□ □□□□ □□□□□. □□□ □ □ □□ □□ □□□ □□□□ □ □□□ □□□□ □□ □□□□ □□□□□ □□□□ □□□ □□□ □ □ □□□ □ □□.

□□□ □□ JSON□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□ □□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Answer Area

```
{
  "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
  "type": "AdaptiveCard",
  "version": "1.0",
  ...
  "actions": [
    {
      "type": "Action.Http",
      "url": "https://actionablemessages.contoso.com/api/getupdatedcard",
      "body": "",
      "method": "POST",
      "contentType": "application/json"
    }
  ]
}
```

Microsoft

Answer:

```
{
  "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
  "type": "AdaptiveCard",
  "version": "1.0",
  ...
}
```

```
&quot;actions&quot;: [
  &quot;autoInvokeAction&quot;: {
  &quot;expectedActors&quot;: {
```

```
&quot;method&quot;: &quot;MERGE&quot;,
&quot;method&quot;: &quot;POST&quot;,
&quot;method&quot;: &quot;PUT&quot;,
```

```
"url": "https://actionablemessages.contoso.com/api/getupdatedcard",
"body": "",
"type": "Action.Http"
}
}
```



Explanation

Graphical user interface, text, application, email Description automatically generated

```
{
  "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
  "type": "AdaptiveCard",
  "version": "1.0",
  . . .
  &quot;actions&quot;: {
  &quot;autoInvokeAction&quot;: {
  &quot;expectedActors&quot;: {
  &quot;method&quot;: &quot;MERGE&quot;,
  &quot;method&quot;: &quot;POST&quot;,
  &quot;method&quot;: &quot;PUT&quot;,
  "url": "https://actionablemessages.contoso.com/api/getupdatecard"
  "body": "",
  "type": "Action.Http"
}
}
```



Box 1: "autoInvokeaction":{

With the autoInvokeAction property on actionable messages, you can provide an HTTP endpoint to retrieve an up-to-date Adaptive Card payload with the latest information when the user opens the email in Outlook.

Box 2: "method": ";POST";

With the autoInvokeAction property on actionable messages, you can provide an HTTP endpoint

□□□ □□□□□□ □□□ □□□□ □□□.

□□□ □□□□ □□□□□□ □□□.

Answer:

See explanation below.

Explanation

You need to modify the default mobile device mailbox policy.

1. Go to the Exchange Admin Center.
2. Select 'mobile' then select 'mobile device mailbox policies'.
3. Click the 'Create a policy' button.
4. Select the Default policy and click the edit icon (pencil icon).
5. Select the 'Security' link to open the security settings.
6. Tick the 'Require a password' checkbox.
7. Tick the 'Require encryption on device' checkbox.
8. Click the Save button to save the changes.

References:

<https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-d>

NEW QUESTION: 69

□□□□ □□ □□ □□□ □□□□ □□□□ contoso.onmicrosoft.com□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.

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

□□ □□ □□□ □□□ □ □□ □□□□ □□□□ □□□.

User4□ □□□ □□□□□□.

User4□ □□□ □□ □□ □□□□□.

□ □□□ □□ □□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Answer Area

Reset the password of User4:

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

Modify the value for the manager attribute of User4:

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



Answer:

Answer Area

Reset the password of User4:

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

Modify the value for the manager attribute of User4:

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

Explanation

Answer Area

Reset the password of User4:

- User1 only
- User2 only
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3

Modify the value for the manager attribute of User4:

- User1 only
- User2 only
- User3 only
- User1 and User3 only
- User1, User2, and User3

Box 1:

A Password Administrator or a User Administrator can reset the password non-administrative users.

Box 2: A User Administrator can configure other attributes such as the Manager attribute of non-administrative users.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles>

NEW QUESTION: 70

Microsoft 365 ☐☐☐ ☐☐☐☐.

☐☐ ☐☐☐☐ ☐☐ ☐☐☐ Microsoft Exchange Online☐ ☐☐☐☐☐.

User☐☐ ☐☐☐☐ ☐☐☐☐☐ ProjectX☐☐ ☐☐☐ ☐☐☐ ☐☐ ☐☐☐☐☐ ☐☐☐☐☐ ☐☐☐☐☐☐.

☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐?

- A. Exchange ☐☐ ☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐.
- B. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐.
- C. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐.
- D. Exchange ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐.

Answer: C (LEAVE A REPLY)

Explanation

When you configure conditions for a label, you can automatically assign a label to a document or email. In this case, we would create a label to label all email messages that contain the word ProjectX. We would then create a label policy to preserve a copy of all message that have the label assigned.

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION: 71

Environment1(□□□)□□□ Microsoft Power Platform □□□ □□□□ Microsoft 365 □□□□ □□□□. Environment1□□ Microsoft Dataverse □□□□□□□□ □□□□ □□□□. □□□□□ User1□□□□ □□□□ □□□□. User1□□ Microsoft Power Apps □□□□□ □□ □□□.

User1□□ □□□□ □□□□ Environment1□ □□ □□□ □□□□□?

- A. □□ □□□
- B. □□□ □□□□□□
- C. □□
- D. □□□ □□□□□□

Answer: (SHOW ANSWER)

Reference:

<https://docs.microsoft.com/en-us/power-platform/admin/database-security#predefined-security-roles>

NEW QUESTION: 72

□□□□□□ □□□□□ Active Directory □□□□*□ □□□□ □□□□.

Microsoft 365 □□ □ □□ □□ □□□ □□□□ □□□□.

□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□.

* □□□□ □□□ □□ □□ □□□□ □□□□ □□□□ □ □□□□.

* □□□□ SSO□ □□□□ □□□□□ □ Microsoft 365 □□□□ □□□ □ □□□□. □□ □□ □□□ □□□□ □□□?

- A. □□ □□ □□□ □ □□□ SSO
- B. AD FS(Active Directory Federation Services)□□ □□□□□
- C. □□ □□ □ □□□ SSO

Answer: B (LEAVE A REPLY)

Explanation

References:

Federation with Active Directory Federation Services (AD FS) is required to allow users to sign in by using smart card-based certificates.

Federated authentication

When you choose this authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password.

The authentication system can provide additional advanced authentication requirements. Examples are smartcard-based authentication or third-party multifactor authentication.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn>

NEW QUESTION: 73

□□□ Microsoft 365 □□□□ □□□□.

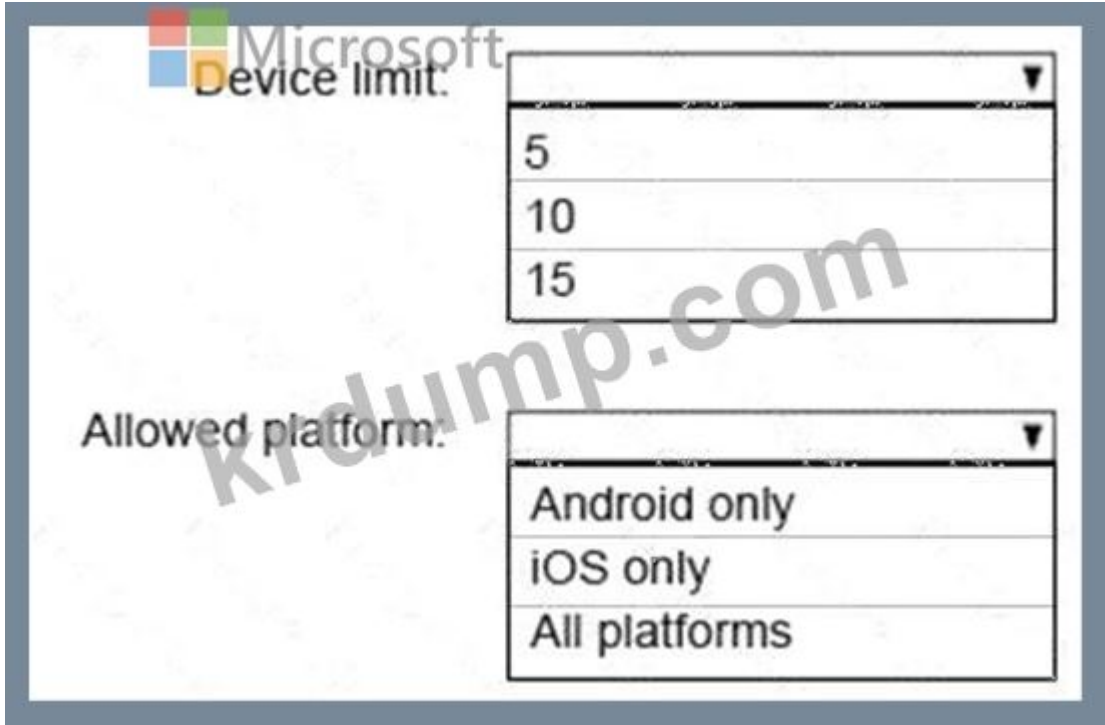
MDM() .
 .

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

.

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

? .
 .
 : 1 .



Answer:



Explanation



When multiple policies are applied to groups that users are a member of, only the highest priority (lowest number) policy applies.

In this case, the Engineering users are assigned two device type policies (the default policy and the priority 2 policy). The priority 2 policy has a higher priority than the default policy so the Engineers' allowed platform is Android only.

The engineers have two device limit restrictions policies applied them. The priority1 policy is a higher priority than the priority2 policy so the priority1 policy device limit (15) applies.

Reference:

<https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set>

NEW QUESTION: 74

SalesApp Office .

?

A.

B. □□ □

C. □□□ □□ □□

D. □□

Answer: B (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/office/dev/add-ins/word/word-add-ins-programming-overview>

NEW QUESTION: 75

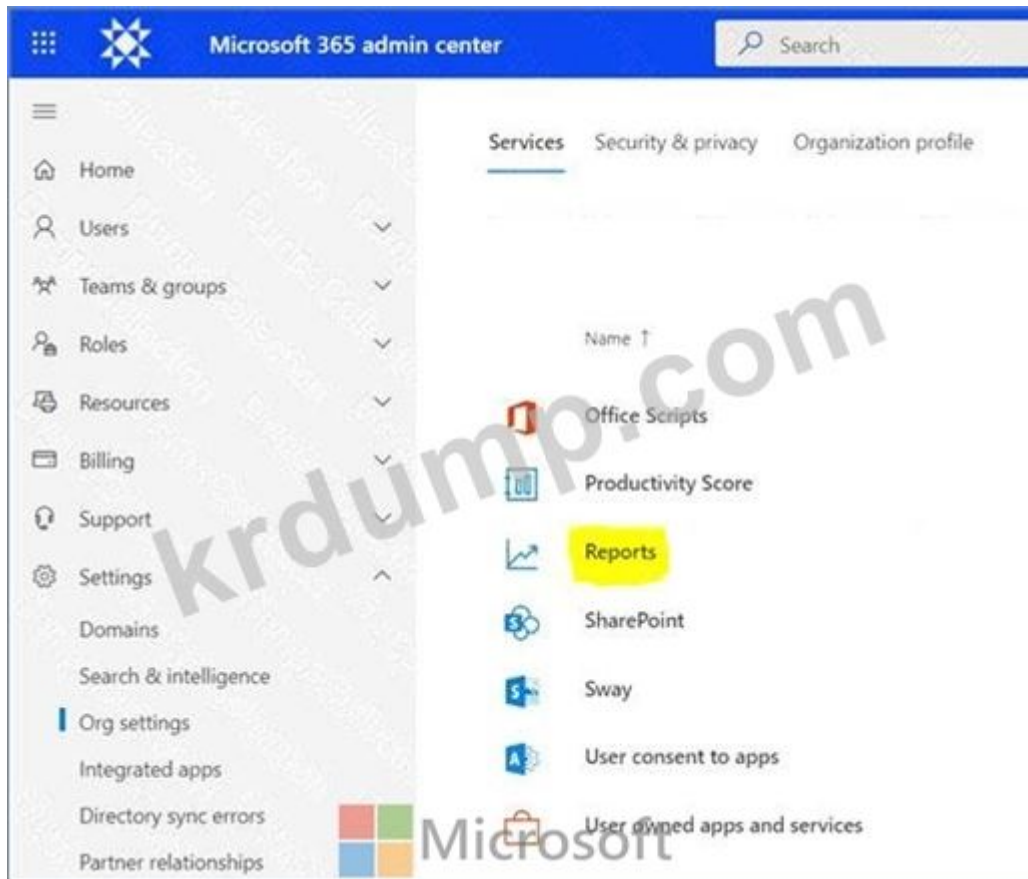
Microsoft 365 E5 □□□ □□□□.

□□ □□□□ Microsoft Office □□□□ □□□□□□□□ Microsoft 365 □□ □□□ □ □□□□.
□□ □□ □□□□ □□□.

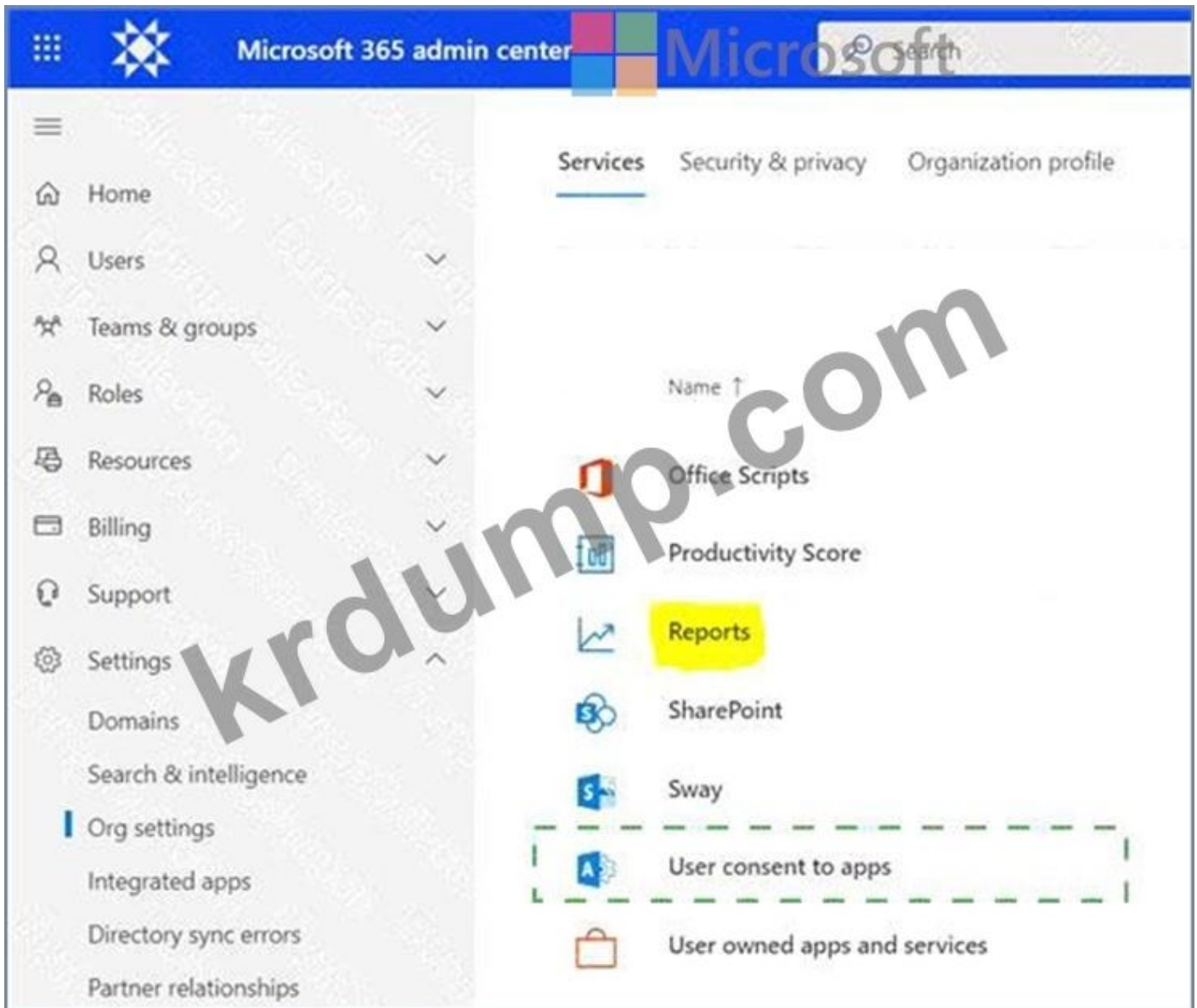
* Office □□□□ □□□□□□□□ Microsoft 365 □ □□ □□□

* □□□□ Microsoft Teams □□□□□ □□ □□□ □ □□□ □□□□□.

Microsoft 365 □□ □□□□ □□□□ □□ □ □□ □□ □□□ □□□□□? □□□□□ □□ □
□□□ □□□ □□□ □□□□□□.



Answer:



Explanation

Answer Area



NEW QUESTION: 76

Microsoft 365 E5 □□□ □□□□.

ID □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

* □□ □□□ □□□□ □□ □□□ □□□□ □□□□ □□□□□.

* □□□ □□ □□□ □□ □□□□□ □□ □□ □□□ □□□□□.

□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□□□. □□: □ □□□ □
□□ 1□□ □□□ □□□□.

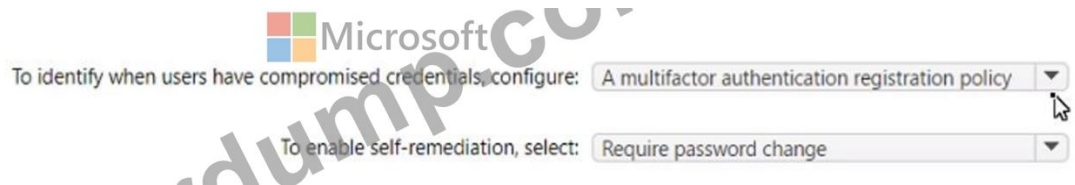


Answer:
answer Area



Explanation

Answer Area



MS-100-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-100-KR □□!
 DumpTop □ □□ **MS-100-KR** □□ □□□ □□□□□□, DumpTop MS-100-KR □□ □□□
 □□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-100-
 KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/MS-100-KR-dump.html> (431
 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 77

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □
 □□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□ □□□
 □□□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□.
 □ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□

□□□ □□□□ □□□□.

□□□□□□ contoso.com□□□ □-□□□□ Active Directory □□□□□ □□□□ □□□□. □□□□□□ □□ □□□□ □□□□□□.

Contoso.com

East.contoso.com

Azure AD Connect □□□ contoso.com□ □□□□□. Azure AD Connect□ Azure AD(Azure Active Directory) □□□□ □□□□□□.

west.contoso.com□□□□ □ □□□□□ □□□□□□ □□□□□□.

west.contoso.com□ Azure AD □□□□□ □□□□□□□ □□□□□ □□□□.

□□ □□: west.contoso.com□ □ Azure AD Connect □□□ □□□□□ AD Connect□ □□ □□□ □□□□□□.

□□□ □□□ □□□□□□?

A. □

B. □□□

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 78

Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□□□.

□□□□□ □□□ □□ □□□ □□□□□□ □□□□. □□□□ □□□□□ □□□□?

A. Microsoft 365 □□ □□□ □

B. Microsoft Authenticator □

C. Intune □□ □□

D. Intune □

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 79

□□□ □□ Microsoft Teams □ □□□ □□ □□□□□ □□□□□ □□ □□□□□ □□□□□. □□ □□□□ □□□□□□□? □□□□□ □□ □□ □□□□ □□□□ □□□□.

A. □□. □□. □□

B. Channel.ReadBasic.All

C. TeamSettings.Read.All

D. □□□□.□□.□□

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 80

Microsoft Teams □□ □□ webhook1□□□□ □□ □□□□□ □□□□□□.

webhook1□ □□□□□□ □□□□. □□□□ □□ □□□□?

A. □□□□ @mention webhookl.

B. □□ □□□□□ @□□□□ webhookl.

C. @webhook1□ □□ □□□□ URL□ □□ http get □□□□ □□□□□□.

D. @webhook1□ □□ □□□□ URL□ □□ http □□ □□□□ □□□□□□.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 81

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □ □□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□ □□□ □□□ □□□□ □□ □ □□□ □□ □ □□□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□ □□□□ □□□□.

A. □

B. □□□

Answer: B ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide>

NEW QUESTION: 82

□□□ □-□□□□ □□ □□ □□□□ Microsoft Exchange Online□□ □□□□□□□□□ □□ □ □□□□□ □□□□ □□□□.

IT □ Managers□□ □ □□□ □□□□ □□ □□ □□□ □□□ □□□ □ □□□ □□□□.

Feature	Available to
Microsoft Azure Active Directory (Azure AD) conditional access	IT group, Managers group
Microsoft Azure Active Directory (Azure AD) Privileged Identity Management	IT group

IT □□□□ 50□□ □□□□ □□□□ □□□□. □□□ □□□□ 200□□ □□□□ □□□□□. □□□ □□□□ □□ □□□□ □□ □□□□□ □□□□ □□□. □□□□ □□□□ □□□ □ □□□□ □□□.

□□ □□□□□ □□□□ □□□□?

- A. Microsoft 365 E3 □□ 250□
- B. Microsoft 365 E 3 50□ □ Microsoft 365 E5 200□
- C. Microsoft 365 E5 □□ 250□
- D. Microsoft 365 E3 200□ □ Microsoft 365 E5 50□

Answer: D ([LEAVE A REPLY](#))

Explanation

Microsoft Azure Active Directory Privileged Identity Management requires an Azure AD Premium P2 license.

This license comes as part of the Microsoft 365 E5 license. Therefore, we need 50 Microsoft 365 E5 licenses for the IT group.

Conditional Access requires the Azure AD Premium P1 license. This comes as part of the Microsoft E3 license. Therefore, we need 200 Microsoft 365 E3 licenses for the Managers group.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requiremen>

NEW QUESTION: 83

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□□ □□□□□. □□□□ □□□ □□□ □ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□ □ □□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□. □ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□ □□□□ □□□□.

□□□ Microsoft Office 36S □□□□ □□□□.

□□ Office 365 □□□ □□□ □□□□□ □□□ □□□□□.

□□□□□ □□□ □□□□□ □□□ □□□ □□□□ □□□.

□□ □□: □□ □ □□ □□□□ □□□□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

Explanation

Depending on what your organization's Office 365 subscription includes, the Dashboard in Security & Compliance includes several widgets, such as Threat Management Summary, Threat Protection Status, Global Weekly Threat Detections, Malware, etc. It does not display a list of the features that were recently updated in the tenant so this solution does not meet the goal.

To meet the goal, you need to use Message center in the Microsoft 365 admin center.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/security-dashboard>

<https://docs.microsoft.com/en-us/office365/admin/manage/message-center?view=o365-worldwide>

NEW QUESTION: 84

Microsoft 365 Enterprise □□□ □□□□.

□□□ □□□□ Microsoft SharePoint□ □□□□ □ □□□ □□□ □□□□ □□□ □□□ □□ □□□□. □□□ □□□ □□□□ □□□ □□□□ □□□□ □□□.

□□□ □□ □□□?

A. Microsoft 36S □□ □□□□ □□ □□ □□ □□□□ □□□.

B. Azure Active Directory □□ □□□□ □□□ □□□□ □□□.

C. Microsoft 365 □□ □□□□ □□□ □□□□ □□□.

D. Azure Active Directory □□ □□□□ □□ □□□ □□□.

Answer: B (LEAVE A REPLY)

Explanation

With the sign-ins activity report in the Azure portal, you can get the information you need to determine how your environment is doing.

The sign-ins report can provide you with information about the usage of managed applications and user sign-in activities, which includes information about multi-factor authentication (MFA) usage. The MFA data gives you insights into how MFA is working in your organization

References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-reporting>

NEW QUESTION: 85

Microsoft Azure Active Directory(Azure AD) adatum.com Active Directory

1000 000 0000 0000.

00 0000 00 0000 0000 0000 0000 000000.

00 00 00 0 0000 300 00 0000 0000 0000.

000 00 0000?

A. Active Directory 00 0000 Active Directory 0000 0000 00 00 0000 000000.

B. Microsoft 365 00 0000 0000 0000 00 00 00 0000 000000.

C. Azure Cloud Shell 00 Get-MsolUser 0 Set-MSOLuser cmdlet 0 000000.

D. 000 000000 Windows PowerShell 00 Get-AzureADUser 0 Set-AzureADUser cmdlet 0 000000.

Answer: A (LEAVE A REPLY)

Explanation

The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on-premise Active Directory.

You can modify certain attributes of multiple user accounts simultaneously by selecting them in Active Directory Administrative Center or Active Directory Users and Computers, right clicking then selecting Properties.

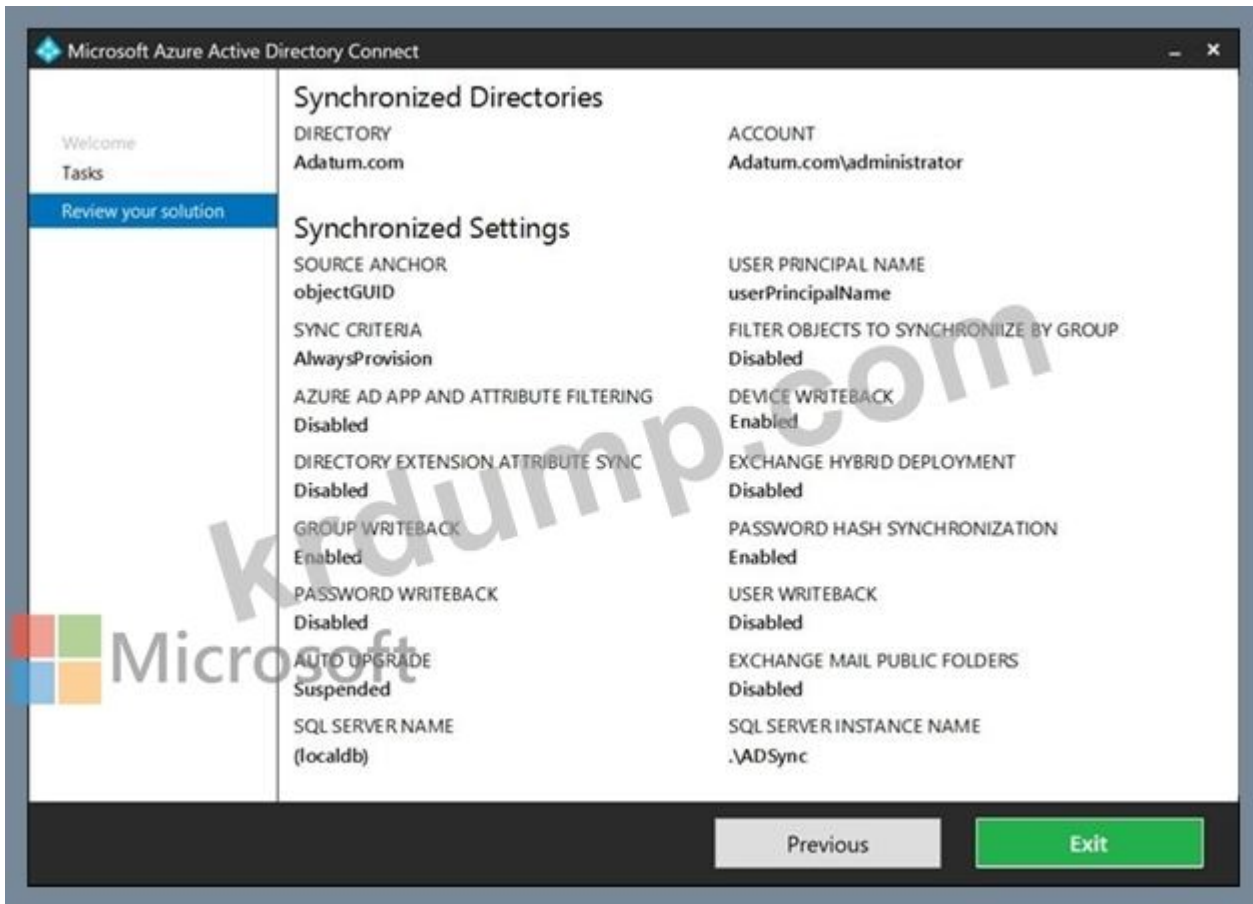
The other three options all suggest modifying the city attribute of the users in the Azure Active Directory which is incorrect.

Reference:

<https://blogs.technet.microsoft.com/canitpro/2015/11/25/step-by-step-managing-multiple-user-accounts-via-activ>

NEW QUESTION: 86

0000 000 00 Azure Active Directory 0 0000 Adatum.com 000 Active Directory 0 000 00000.



□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□ □□□□□□
 □.
 □□: □ □□□ □□□ 1□□ □□□ □□□□.

If you create a security group in Azure AD, the group will [answer choice].

- not sync to adatum.com
- sync to adatum.com as a security group
- sync to adatum.com as a distribution group

If you join a computer to Azure AD, the object will [answer choice].

- not sync to adatum.com
- sync to the Computers container in adatum.com
- sync to the LostAndFound container in adatum.com
- sync to the RegisteredDevices container in adatum.com

Answer:

If you create a security group in Azure AD, the group will [answer choice].

- not sync to adatum.com
- sync to adatum.com as a security group
- sync to adatum.com as a distribution group

If you join a computer to Azure AD, the object will [answer choice].

- not sync to adatum.com
- sync to the Computers container in adatum.com
- sync to the LostAndFound container in adatum.com
- sync to the RegisteredDevices container in adatum.com

Explanation

If you create a security group in Azure AD, the group will [answer choice].

If you join a computer to Azure AD, the object will [answer choice].

Group Writeback is enabled in the Azure AD Connect configuration so groups created in Azure Active Directory will be synchronized to the on-premise Active Directory. A security group created in Azure Active Directory will be synchronized to the on-premise Active Directory as a security group.

Device Writeback is enabled in the Azure AD Connect configuration so computers joined to the Azure Active Directory will be synchronized to the on-premise Active Directory. They will sync to the RegisteredDevices container in the on-premise Active Directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

NEW QUESTION: 87

Microsoft 365 □□□ □□□□.
 □□ □□□ □□ □□□ □□ □□□ □ □ □□□□.

Service health

October 18, 2022 4:20 PM

Overview Issue history Reported issues

View the issues and health status of all services that are available with your current subscriptions. [Learn more about Service Health](#)

Report an issue Customize

Active issues

Issue title Affected service Issue type

Microsoft service health (6)

Issues in your environment that require action (0)

Microsoft service health

Shows the current health status of your Microsoft services, and updates when we fix issues.

Service	Status
Exchange Online	3 advisories
Microsoft 365 suite	2 advisories
Microsoft Teams	1 advisory
OneDrive for Business	1 advisory
SharePoint Online	2 advisories



User1□□□ □□□□ □□□ □□ □□□ □□□□ □□ □□□ □ □□□ □□□□ □□□.

User1□□ □□ □□□ □□□□ □□□□?

- A. □□□ □□ □□
- B. □□□ □□
- C. □□ □□ □□□
- D. □□□ □□ □□□

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 88

ToDoListSPA□□ □□ □□□ □□□□□□(SPA)□ ToDoUstServKe□□ □□ □□ □□□ □□ □□.

TodoListSPA API □□ □□□ TodoUstSPA □□□(TodoUstSPA □ □□)□ □□□ □□ □□ □□□. TodoUstService API□ □□ □□□ TodoListService □□□(TodoUstService □ □□)□ □□□ □□ □□□□□. TodoUstService□ a□ □□□□ □ □□□ □□□□ □□□. □□□□ □□□□ Microsoft OneDnve □□. □□□□ □□ □□ □□□ □□□□ □□□. □□ □□ □□□ □□□□ □□□?

- A. TodoUstSPA□ □□ sites.Read.All □□□□□□ □□
- B. TodoUstService□ □□ sites.Read.All □□ □□
- C. TodoUstService□ □□ sites.Read.All □□□□□□ □□
- D. thesites.Read.All TodoListSPA□ □□ □□□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 89

□□□□□□ Microsoft Azure Active Directory(Azure AD)□ □□□□□ .Ki.ituin.com□□□ Active Directory □□□□ □□□□ □□□□. □□□□□ 100□□ □□□ □□□ □□□□. □□ □□□□ □□ □□□ □□□□ □□□□ □□□ □□□□□. □□ □□ □□ □ □□□ □ □□ □□ □□□ □□□□ □□□. □□□ □□ □□□?

- A. Active Directory □□ □□□□ Active Directory □□□□ □□□ □□ □□ □□□ □□□□□.
- B Microsoft 365 □□ □□□□ □□□□ □□□ □□ □□ □□ □□□ □□□□□.
- B. Azure Cloud Shell□□ Get-AzureADUsers□ □□□ □□ □□ □□ □□□ □□□□□.
- C. Azure Cloud Shell□□ Get-AzureADUser □ set-AzureADUser cmdlet□ □□□□□.
- D. □□□ □□□□□ Windows PowerShell□□ Get-AzureADUser □ Set-AzureADUser cmdlet □ □□□□□.

Answer: (SHOW ANSWER)

Explanation

The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on-premise Active Directory.

You can use Windows PowerShell on a domain controller and run the Get-ADUser cmdlet to get the required users and pipe the results into Set-ADUser cmdlet to modify the city attribute.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser?view=win10-ps>

NEW QUESTION: 90

Microsoft 365 □□□□ □□□□. □□ □□□ □□ Azure AD Connect□ □□□□□.

Azure Active Directory admin center

Home > Azure AD Connect

Azure AD Connect

Azure Active Directory

 Troubleshoot  Refresh

SYNC STATUS



Sync Status

Enabled

Last Sync

Less than 1 hour ago

Password Sync

Enabled

USER SIGN-IN



Federation

Disabled

0 domains

Seamless single sign-on

Disabled

0 domain

Pass-through authentication

Disabled

0 agents

□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□ □□□□□
□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

Answer Area

Sales department users can access [answer choice] applications by using SSO.

▼
both on-premises and cloud-based
only cloud-based
only on-premises

If Active Directory becomes unavailable, users can access the resource [answer choice].

▼
both on-premises and in the cloud
in the cloud only
on-premises only

Answer:

MS-100-KR <https://www.dumpst.com> DumpTop <https://www.dumpst.com> MS-100-KR <https://www.dumpst.com>!
DumpTop <https://www.dumpst.com> **MS-100-KR** <https://www.dumpst.com>, DumpTop MS-100-KR <https://www.dumpst.com>
<https://www.dumpst.com> <https://www.dumpst.com>. <https://www.dumpst.com> DumpTop MS-100-
KR <https://www.dumpst.com>. <https://www.dumpst.com/Microsoft/MS-100-KR-dump.html> (431
Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 92

Microsoft 365 Admin Center: <https://admin.microsoft.com>.
Admin Center > Users > External Users > External Collaboration Settings.
Under External Users, select the 'Manage external collaboration settings'.
In the 'External collaboration settings' pane, under 'External collaboration settings',
click 'Add external domain'.
In the 'Add external domain' dialog box, under 'Domain', enter the domain name
(e.g., gmail.com, yahoo.com) and click 'Add'.
The domain is added to the list of external domains. To deny access to the
domain, click the domain name and click 'Deny'.
The domain is moved to the 'Denied domains' list.
Repeat the steps for each domain you want to deny access to.
Click 'Save' to save the changes.

Microsoft 365 Admin Center:

admin@LODSe426243.onmicrosoft.com

Microsoft 365 Admin Center: 3&YWyjse-6-d

Microsoft 365 Admin Center > External Users > External Collaboration Settings
CTRL-K

Microsoft 365 Admin Center > External Users > External Collaboration Settings

Microsoft 365 Admin Center: 10887751

Microsoft 365 Admin Center > External Users > External Collaboration Settings

Microsoft 365 Admin Center > External Users > External Collaboration Settings
@gmail.com

Answer:

See explanation below.

Explanation

You need to add gmail.com as a denied domain in the 'External collaboration settings'.

1. Go to the Azure Active Directory admin center.
2. Select Users then select 'User settings'.
3. Under External Users, select the 'Manage external collaboration settings'.

- 4. Click the 'Add' button.
- 5. Start typing the name Christie then select her account when it appears.
- 6. Click Save.

References:

<https://docs.microsoft.com/en-US/azure/active-directory/users-groups-roles/directory-assign-admin-roles>

NEW QUESTION: 94

Microsoft 365 [redacted] User1 [redacted].
 User1 [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].
 User1 [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]?

- A. Microsoft 365 [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]
- B. [redacted] [redacted] [redacted] [redacted] [redacted] eDiscovery [redacted] [redacted]
- C. Azure Active Directory [redacted] [redacted] Information Protection [redacted] [redacted]
- D. Exchange [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

Answer: (SHOW ANSWER)

Explanation

To create a query-based In-Place Hold, a user requires both the Mailbox Search and Legal Hold roles to be assigned directly or via membership in a role group that has both roles assigned. To create an In-Place Hold without using a query, which places all mailbox items on hold, you must have the Legal Hold role assigned.

The Discovery Management role group is assigned both roles.

Reference:

<https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions>

NEW QUESTION: 95

[redacted] adatum.com [redacted] contoso.com [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] Active Directory [redacted] [redacted] [redacted].
 nwtraders.com [redacted] Azure AD [redacted] [redacted].
 [redacted] [redacted] nwtraders.com [redacted] [redacted] [redacted]. [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].
 * adatum.com [redacted] contoso.com [redacted] [redacted] [redacted] [redacted] [redacted].
 * Microsoft Exchange [redacted] [redacted] [redacted] [redacted].
 * [redacted] [redacted] [redacted] [redacted] [redacted].
 * [redacted] [redacted] [redacted] [redacted].

Answer:

Tools

- Azure AD Connect
- Azure AD Connect Cloud Sync
- Active Directory Migration Tool

Answer Area

Provide the ability to sync device objects: Azure AD Connect

Provide support for Microsoft Exchange hybrid: Azure AD Connect Cloud Sync

Provide the ability to connect to adatum.com and contoso.com: Active Directory Migration Tool

Explanation

Answer Area

Provide the ability to sync device objects: Azure AD Connect

Provide support for Microsoft Exchange hybrid: Azure AD Connect Cloud Sync

Provide the ability to connect to adatum.com and contoso.com: Active Directory Migration Tool

NEW QUESTION: 96

████████████████████ Microsoft Exchange Server 2019 ████████████████████. Microsoft 365 E5 ████████████████████. ████████████████████ Exchange Online ████████████████████. ████████████████████?

- A. Azure AD Connect ████████████████████.
- B. Azure AD(Azure Active Directory) ████████████████████ ████████████████████ ████████████████████.
- C. ████████████████████ ████████████████████ ████████████████████.
- D. Exchange Online ████████████████████ ████████████████████.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 97

██████████ ████████████████████ Microsoft 365 ████████████████████ ████████████████████.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

Policy1 ████████████████████ ████████████████████ Policy1 ████████████████████. (Policy1 ████████████████████) ████████████████████

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... 4 years

Retain the content based on when it was created ⓘ

Do you want us to delete it after this time? ⓘ

Yes No

No, just delete content that's older than ⓘ

2 years

Need more options?

Use advanced retention settings ⓘ

Back Next Cancel

□□ □ □□□ □□ □□□ □□□ □□ □□□□□□. □□□ □□□ □□□□ □□□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, and administrator will be able to recover the file on April 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020	<input type="radio"/>	<input checked="" type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, and administrator will be able to recover the file on April 15, 2020.	<input checked="" type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020	<input type="radio"/>	<input checked="" type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, and administrator will be able to recover the file on April 15, 2020.	<input checked="" type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	<input checked="" type="radio"/>	<input type="radio"/>

* Retention wins over deletion. Suppose that one retention policy says to delete Exchange email after three years, but another retention policy says to retain Exchange email for five years and then delete it.

Any content that reaches three years old will be deleted and hidden from the users' view, but still retained in the Recoverable Items folder until the content reaches five years old, when it is permanently deleted.

* The longest retention period wins. If content is subject to multiple policies that retain content, it will be retained until the end of the longest retention period.

Box 1: No.

The file will be deleted and hidden from the users' view, but still retained in the Recoverable Items folder. An administrator would need to recover the file.

Box 2: Yes.

The file will be deleted and hidden from the users' view, but still retained in the Recoverable Items folder. An administrator will be able to recover the file.

Box 3: Yes.

2018 to 2023 is five years. Policy2 has a retention period of four years. However, Policy2 is configured to not delete the files after the four-year retention period.

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or->

NEW QUESTION: 98

Office 365 is a cloud-based productivity suite that includes various applications such as Word, Excel, PowerPoint, Outlook, and Teams. Microsoft 365 is a subscription-based service that provides access to Office 365 applications along with other services like OneDrive and Microsoft Edge. The pricing for Microsoft 365 varies depending on the number of users and the features included.

To configure the notifications:

▼
Briefing email
Help desk information
Organization information

To limit access:

▼
Privileged Access
Release preferences
Office installation options



Answer:

To configure the notifications:

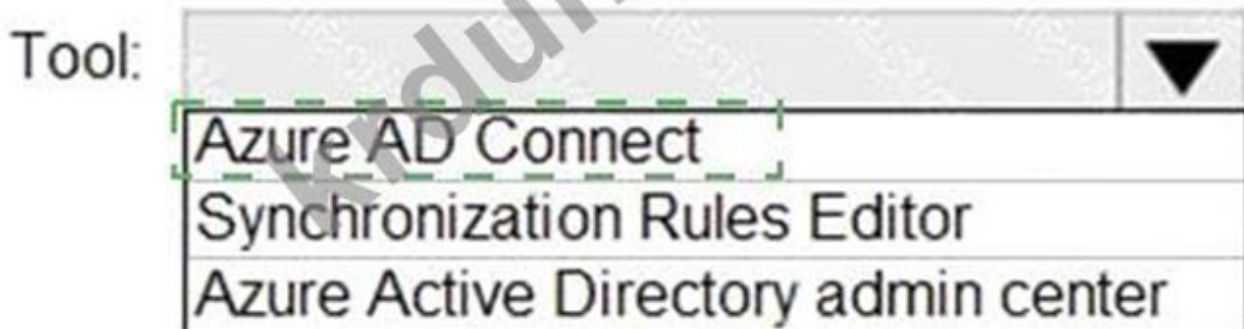
▼
Briefing email
Help desk information
Organization information

To limit access:

▼
Privileged Access
Release preferences
Office installation options

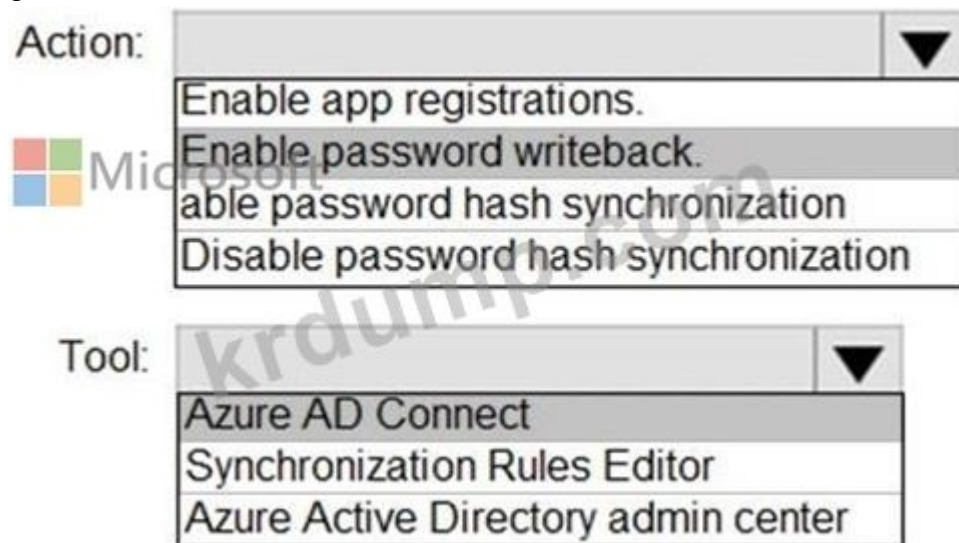
Explanation

Graphical user interface, text, table Description automatically generated



Explanation

Graphical user interface, text, application, chat or text message Description automatically generated



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

Topic 4, NEW Case Study

Case Study

Overview

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is

provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the question. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, n..... that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to ret..... to the question.

Existing Environment

Microsoft 365

Contoso identifies the following business goals:

- * Utilize core functionality of apps whenever possible.
- * Reduce app development costs.
- * Minimize training costs for end users.

Microsoft SharePoint/Microsoft Exchange

Contoso has a Microsoft 365 subscription that uses a domain named contoso.com. Each user is assigned a Microsoft 365 Enterprise E5 licence.

Problem Statement

Contoso moves all email accounts to Microsoft 365.

Contoso migrates the SharePoint Server 2013 intranet sites of the research department to SharePoint Online.

Requirements

Business Goals

Contoso identifies the following issues:

- * Users in the sales department report that preparing quotations is time-consuming as it requires manually copying and pasting data from multiple sources.
- * Users in the HR department must use multiple apps to manage the hiring process.
- * The solution to claim expenses requires multiple manual steps.

Planned Changes

Contoso identifies the following business goals:

- * Utilize core functionality of apps whenever possible.
- * Reduce app development costs.
- * Minimize training costs for end users.

Technical Requirements

Contoso plans to implement the following changes;

- * Redesign the SharePoint Online sites of the research department to provide users with an

experience that is consistent with the Microsoft 365 portal. The research department has a third-party project management solution that uses the Microsoft identity platform in Azure AD.

* Create an email workflow solution for expense claims. Users will submit their expense claims and the system will email an approval request to their manager.

* Implement a bring your own device (BYOD) model that supports Windows 10, macOS, and Android devices.

* Develop a custom Microsoft 365 app named SalesApp for the sales department.

* Develop a custom Microsoft 365 app named HRApp for the HR department

Security Requirement

Contoso identifies the following technical requirements for app development:

* The expense claims solution must provide managers with claim information and the ability to manage the claim by using Microsoft Outlook. Outlook on the web, or Outlook for iOS and Android.

* HRApp must include a bot named HRBot that will answer HR questions. Users must be able to access the bot by mentioning HRBot in a Microsoft Teams channel or private chat.

* HRApp must enable users to query a third-party HR system by using a tab from within a Microsoft Teams channel.

* HRApp must include a messaging extension that enables users to search jobs by job title or job ID.

* SalesApp must be integrated with Microsoft Word and must combine images and text from multiple sources to create a quotation as a DOCX file.

* The distribution of SalesApp must be automatic and require minimal user interaction.

* Solutions for SharePoint Online and Microsoft Office must follow the current Office user interface (UI) design.

* Development tools and solutions must support Windows and non-Windows devices.

* Development effort must be minimized.

HRApp Manifest

All solutions must support the Microsoft identity platform in Azure AD.

Intranet components must not share access tokens.

NEW QUESTION: 100

contoso.com is an Azure AD(Azure Active Directory) tenant. Microsoft 365 is deployed to contoso.com.

Contoso is planning to develop a new application that will be used by all employees.

Which of the following is the best solution for this scenario?

A. Azure Active Directory ID application extension.

B. Microsoft 365 app extension.

C. Azure AD ID application extension.

D. Azure Active Directory ID application extension.

Answer: A (LEAVE A REPLY)

Explanation

The Password protection settings allows you to specify a banned password list of phrases that users cannot use as part of their passwords.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premisesope>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-configure>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#custombanned>

NEW QUESTION: 101

Which of the following file types is supported by the Password Protection settings in Microsoft 365?

A. Microsoft 365 CSV

B. Microsoft 365 JSON

C. Microsoft 365 PST

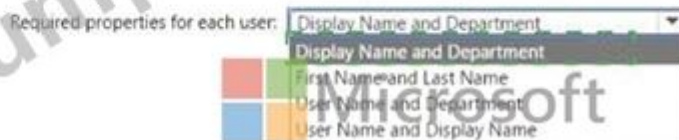
D. Microsoft 365 XML

ANSWER AREA



Answer:

Answer Area



Explanation



NEW QUESTION: 102

Which of the following file types is supported by the Password Protection settings in Microsoft 365?

A. Microsoft Office 365 CSV

□. □□□□□ □□□□□ □□□□ □ □□□□ □□□ □□□ □□□□□ □□□.
□□□ □□□□ □□□?

- A. Azure Portal □ □□□□ □□□□
- B. Microsoft 365 □□ □□□ □□□
- C. Microsoft 365 □□ □□□ □□ □□□
- D. □□ □ □□ □□ □□□

Answer: A (LEAVE A REPLY)

Explanation

In the Azure AD Admin Center, select Azure Active Directory then select Licenses to open the Licenses blade.

From there you need to click on the 'Managed your purchased licenses link'. Select a license you want to view, for example Office 365 E3. This will then display a list of all users with that license. In the 'Assignment Paths' column, it will say 'Direct' for a license that has been assigned directly to a user or 'Inherited (Group Name)' for a license that has been assigned through a group.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign>

NEW QUESTION: 103

□□□□ □□ □□ □□□ □□□□ □□□□ contoso.com □□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Usage location	Membership
User1	United States	Group1, Group2
User2	Not applicable	Group2
User3	Not applicable	Group1
User4	Canada	Group1

Group2 □ Group1 □ □□□□□□.

Microsoft Office 365 Enterprise E3 □□□□□ Group1 □ □□□□□.

□□□ Office 365 E3 □□□□ □□ □□□□ □□□.

□□□ □□□□ □□□?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: C (LEAVE A REPLY)

Explanation

Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied. Therefore, User2 will not be assigned a license.

When Azure AD assigns group licenses, any users without a specified usage location inherit the location of the directory. Therefore, User3 will be assigned a license and his usage location will be set to the location of the directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign>

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-group-advanced>

NEW QUESTION: 104

□□ □□□ □□□ □□□□ □□□ Microsoft 365 □□□ □□□□.



□□□□ □□□ □ □□ □□□ □□ □□□□ □□□ □ □□□□?

- A. Contoso1919.onmicrosoft.com □ Sub2.Contoso1919.onmicrosoft.com □ □□
- B. Sub1.Contoso1919.onmicrosoft.com □ □□
- C. □□□ □□ □□□
- D. Contoso1919.onmicrosoft.com, Sub1.Contoso1919.onmicrosoft.com □
Sub2.Contoso1919.onmicrosoft.com □ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 105

Project1 □ □□ □□□□□□ □□□□ □□□□ □□□?

- A. Exchange Online PowerShell □□ New-MailboxImportRequest cmdlet □ □□□□□.
- B. Exchange Online PowerShell □□ New-MailboxExportRequest cmdlet □ □□□□□.
- C. Microsoft 365 □□ □□□□ □□□ □□□□□□□ □□□□ □□□ □□□□ PSST □□□ □ □□□□□.
- D. Exchange □□ □□□□ □□□□□□□ □□□□ □□ □□ □□□□□□□ □□□□□.

Answer: D (LEAVE A REPLY)

Explanation

During Project1, some users will have mailboxes in Microsoft 365 and some users will have mailboxes in Exchange on-premises. To enable users be able to exchange email messages successfully during Project1 by using their current email address, we'll need to configure hybrid Exchange.

To migrate mailboxes in a hybrid Exchange configuration, you use Exchange admin center

perform Remote move migrations.

Reference:

<https://docs.microsoft.com/en-us/exchange/hybrid-deployment/move-mailboxes>

NEW QUESTION: 106

Group1 is a Microsoft 365 E5 group. contoso.com is an Azure AD tenant. contoso.com ID is 12345678-9012-3456-7890-123456789012.

Setting	Value
Block external user from signing in to this directory	Yes
Remove external user	Yes
Number of days before removing external user from this directory	30

2022-03-01, Guest1 is added to Group1.

Name	Email address
Guest1	Guest1@outlook.com
Guest2	Guest2@outlook.com

2022-03-02, Guest1 is removed from Group1.

2022-03-05, Package1 is added to Group1.

* Resource roles

- o Name: Group1
- o Type: Group and Team
- o Role: Member

* Lifecycle

- o Start date: 2022-03-20, End date: 2022-03-30, Package1 is added to Group1.

Name	Email address
Guest3	Guest3@outlook.com
Guest4	Guest4@outlook.com

2022-03-06, Guest3 is added to Group1.

2022-03-10, Guest2 is added to Group1.

Answer Area

Statements	Yes	No
On April 10, 2022, Guest2 will be able to sign in to contoso.com.	<input type="radio"/>	<input type="radio"/>
On April 25, 2022, Guest3 will be able to sign in to contoso.com.	<input type="radio"/>	<input type="radio"/>
On May 1, 2022, Guest1 will be able to sign in to contoso.com.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation

In the Licenses blade, click All Products then select the E3 License. This will display a list of all users assigned an E3 license. Select User1. You'll see how many services are assigned in the Enabled Services column. Click on the number in the Enabled Services column for User1 and you'll be taken to the licenses page for that user. Click on the number in the Enabled Services column for User1 again and a page will open which shows you exactly which services are enabled or disabled.

Alternatively, you can go into the user account properties directly then select Licenses. This will display the licenses blade for that user. You can then click on the number in the Enabled Services column for the user and a page will open which shows you exactly which services are enabled or disabled.

NEW QUESTION: 108

□□ □□□ □□□□ □□ □□ □□□ □□□□. □□□□ □ □□□□ □□□ □ □□□□. □ □□□ □ □ □□ □□□ □ □□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□. □□ □□□ □□□ □ □□□ □□□□ □□ □□□ □□□□□□□. □ □□□□□ □□□ □□□ □ □□□ □□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□□ □□□ □ □□□ □□ □□(□: □□ □ □□□□, □□ □ □□□ □□ □□)□ □□□ □□□□□□□. □□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□. □, □□□ □□□ □□□□□□ □ □□□ □□□ □□□□□ □□□□ □□ □□□ □□ □□□□ □□ □□□. □□ □□□ □□□ □□□□ □□□ □ □□□□ □□□□ □□ □□□ □ □ □□ □□ □ □□□ □. □ □□□ □□□□ □ □□□ □□ □□□ □□□ □ □□□□. □□□ □□□ □□ □□ □□ □□□ □□ □□ □□□ □□□ □ □□□ □□□ □□□ □□□□ □□□□ □□□. □ □□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □ □□□□. □□ □□□ □□□□ □□□ □□□ □ □□□□. □□□ □□ □□ □□□ □□□ □□□ □□□ □□□□ □□□□□□□. □□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□□□.

Microsoft 365 □□□ □□:

admin@M365x981607.onmicrosoft.com

Microsoft 365 □□: *yfLo7lr2&y-

Microsoft 365 □□□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□ □ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

□ □□□□: 10811525

□□□ □□□□ □□□□□ Microsoft Skype□□ □□ Skype □□□□□ □□ □□□ □□□□ □□□□ □□ □□□.

Answer:

See explanation below.

Explanation

You need to configure the External Communications settings in the Skype for Business admin center.

1. You need to go to the Skype for Business admin center. If you see a Skype for Business admin center in the admin center list in the Microsoft portal, open it and skip to step 4.
2. If you don't see a Skype for Business admin center in the admin center list in the Microsoft portal, open the Teams admin center.
3. In the Teams admin center, choose Skype > Legacy Portal.
4. In the Skype for Business admin center, select Organization.
5. Select External communications.
6. Untick the 'Let people use Skype for Business to communicate with Skype users outside your organization' checkbox.
7. Click Save to save the changes.

NEW QUESTION: 109

□□ □□□ □□□□ □□ □□ □□□ □□□□. □□□□ □ □□□□ □□□ □ □□□□. □ □□□ □ □ □□ □□□ □ □□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□. □□ □□□ □□□ □ □□□ □□□□ □□ □□□ □□□□□□. □ □□□□□ □□□ □□□ □ □□□ □□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□□ □□□ □ □□□ □□ □□(□: □□ □ □□□□, □□ □ □□□ □□ □□)□ □□□ □□□□□□. □□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□. □, □□□ □□□ □□□□□□ □ □□□ □□□ □□□□□ □□□□ □□ □□□ □□ □□□□ □□ □□□. □□ □□□ □□□ □□□□ □□□ □ □□□□ □□□□ □□ □□□ □ □ □□ □□ □ □□□ □. □ □□□ □□□□ □ □□□ □□ □□□ □□□ □ □□□□. □□□ □□□ □□ □□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□. □ □□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □ □□□□. □□ □□□ □□□□ □□□ □□□ □ □□□□.

□□□ □□ □□□ □□ □□ □□□ □□□□□□. □□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□ □□□ □□□ □□□□□□. □□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□□.

Microsoft 365 □□□ □□:
admin@LODSe426243.onmicrosoft.com
□□□□□□□ 365 □□: 3&YWyjse-6-d
Microsoft 365 □□□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□ □ □□□ □□ □□□□□. □□ □□□ □□ □□ □□□□□ □□□□□. □ □□□□: 10887751
Johanna Lorenz□□ □□□□ □□ □□□ □□□□□. Ben Smith□□ □ □□□ Johanna Lorenz□ □□□ □□□□□. Ben Smith□□ □□□□ □□□□ □□□. Ben Smith□ http://myapps.microsoft.com□ □□□□ □ □□□□ □□ □ □□ □□□ □□□.

Answer:

See explanation below.

Explanation

You need to create a user account and assign a license to the account. You then To create the user account and mailbox:

- * In the Microsoft 365 admin center, go to User management, and select Add user.
- * Enter the name Ben Smith in the First Name and Last Name fields.
- * Enter Ben.Smith in the username field and click Next.
- * Assign a Microsoft 365 license to the account.
- * Click Next.
- * Click Next again.
- * Click 'Finish adding'.

NEW QUESTION: 110

□□ □□ □□□ □□□□ □□□□ Microsoft 365 E5 □□□ □□□□.

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1, Group2	Enabled
User3	Group2	Disabled

□□ □□□ □□ MFA(Multi-Factor Authentication) □□ □□□ □□□□□.

□□:

- □□: □□ 1

- □□: □□ 2

□□□ □□: Azure MFA □□ □□

□□ □□: □□

□□ □□□ □□ □□□ □□□ □□□ □□□□.

□□: □□1

□□:

- □□: □□ 2

- □□: □□ 1

□□□ □□:

- □□, □□□ □□ □□

□□ □□□: □□

□□ □ □□□ □□ □□□ □□□ □□ □□□□□□. □□□ □□□ □□□□ □□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements	Yes	No
User1 will be required to use MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User2 will be required to use MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User3 will be required to use MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 will be required to use MFA on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 will be required to use MFA on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be required to use MFA on the next sign-in.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation

Graphical user interface, text, application Description automatically generated

Statements	Yes	No
User1 will be required to use MFA on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 will be required to use MFA on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be required to use MFA on the next sign-in.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: No

The MFA policy applies to User1 so he will be prompted to register for MFA. He has 14 days to complete the registration. During this 14-day period, he can bypass registration but at the end of the period he will be required to register before he can complete the sign-in process. The Conditional Access Policy does not apply to User1 so MFA is not required.

Box 2: No

User2's MFA status is Enabled which means he has been enrolled in MFA but has not yet

completed the registration.

The Conditional Access Policy does not apply to User2 because Group1 is excluded so MFA is not required.

Box 3: Yes

The Conditional Access Policy does apply to User3 so MFA will be required. He will need to be enrolled for MFA first.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-m>

<https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authenticatio>

NEW QUESTION: 111

□□ □□□ □□□□ □□ □□ □□□ □□□□. □□□□ □ □□□□ □□□ □ □□□□. □ □□□ □ □ □□ □□□ □ □□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□. □□ □□□ □□□ □ □□□ □□□□ □□ □□□ □□□□□□□. □ □□□□□ □□□ □□□ □ □□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□□ □□□ □ □□□ □□ □□(□: □□ □ □□□□, □□ □ □□□ □□ □□)□ □□□ □□□□□□□. □□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□. □, □□□ □□□ □□□□□□ □ □□□ □□□ □□□□□ □□□□ □□ □□□ □□ □□□□ □□ □□□. □□ □□□ □□□ □□□□ □□□ □ □□□□ □□□□ □□ □□□ □ □ □□ □□ □ □□□ □. □ □□□ □□□□ □ □□□ □□ □□□ □□□ □ □□□□. □□□ □□□ □□ □□ □□ □□□ □□ □□□ □□□ □ □□□ □□□□ □□□□ □□□□ □□□. □ □□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □ □□□□. □□ □□□ □□□□ □□□ □□□ □ □□□□. □□□ □□ □□ □□□ □□□ □□□ □ □□□□.

Microsoft 365 □□□ □□:

admin@LODSe426243.onmicrosoft.com

□□□□□□□ 365 □□: 3&YWyjse-6-d

Microsoft 365 □□□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□ □ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

□ □□□□: 10887751

Microsoft 365 □□□□ □□□□ □□ Irvin Sayers□□ □ □□ □□□□ □□□□□.

□□ □□ □□□ □□□□□ Irvin Sayers□ □□□□ □□□.

□ □□ □□□ □□□ □□ □□□ □□□□□.

□□ □□ Microsoft Office 365 □□ □□□ □□□□.

Answer:

Condition: Condition1

Default Directory - Azure Information Protection



Save



Discard



Delete

Choose the type of condition

Information Types

Custom

* Name

Condition1

* Match exact phrase or pattern

im

Match as a regular expression

Off

On

Match with case sensitivity

Off

On

* Maximum number of occurrences

2

Count occurrences with unique value only

Off

On

□□ □ □□□ □□ □□□ □□□ □□ □□□□□□. □□□ □□□ □□□□ □□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements	Yes	No
Label1 applies to File1.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File2.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File3.docx.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Label1 applies to File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
Label1 applies to File2.docx.	<input checked="" type="radio"/>	<input type="radio"/>
Label1 applies to File3.docx.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation

Statements	Yes	No
Label1 applies to File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
Label1 applies to File2.docx.	<input checked="" type="radio"/>	<input type="radio"/>
Label1 applies to File3.docx.	<input type="radio"/>	<input checked="" type="radio"/>

The phrase to match is "im" and it is case sensitive. The phrase must also appear at least twice.

Box 1: No

File1.docx contain the word "import" once only

Box 2: Yes

File2.docx contains two occurrences of the word "import" as well as the word "imported" Box 3:

No File3.docx contains "IM" but his is not the correct letter case.

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION: 113

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □
 □□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□ □□□
 □□□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□.
 □ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□
 □□□ □□□□ □□□□.
 □□□□□□ Active Directory □□□□□ □□□□□ □□□□□.

Microsoft 365.

 ID.
 Active Directory Microsoft 365

 10.
 : Azure AD
 ?

- A.
 B.

Answer: (SHOW ANSWER)

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization>

NEW QUESTION: 114

contoso.com Azure AD(Azure Active Directory) Microsoft 365

 user1@outlook.com
 user1@outlook.com contoso.com
 ?

- A. Azure Active Directory
 B. Microsoft 365
 C. Azure Active Directory
 D. Microsoft 365

Answer: C (LEAVE A REPLY)

Explanation

You can invite guest users to the directory, to a group, or to an application. After you invite a user through any of these methods, the invited user's account is added to Azure Active Directory (Azure AD), with a user type of Guest. The guest user must then redeem their invitation to access resources. An invitation of a user does not expire.

The invitation will include a link to create a Microsoft account. The user can then authenticate using their Microsoft account. In this question, the external vendor already has a Microsoft account (user1@outlook.com) so he can authenticate using that.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator>

NEW QUESTION: 115

?

- A.

- B. □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□
- C. □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□
- D. □□ □□□ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□

Answer: D (LEAVE A REPLY)

Explanation

Sending actionable messages via email is supported. You use actionable message cards.

Scenario:

Create an email workflow solution for expense claims. Users will submit their expense claims and the system will email an approval request to their manager.

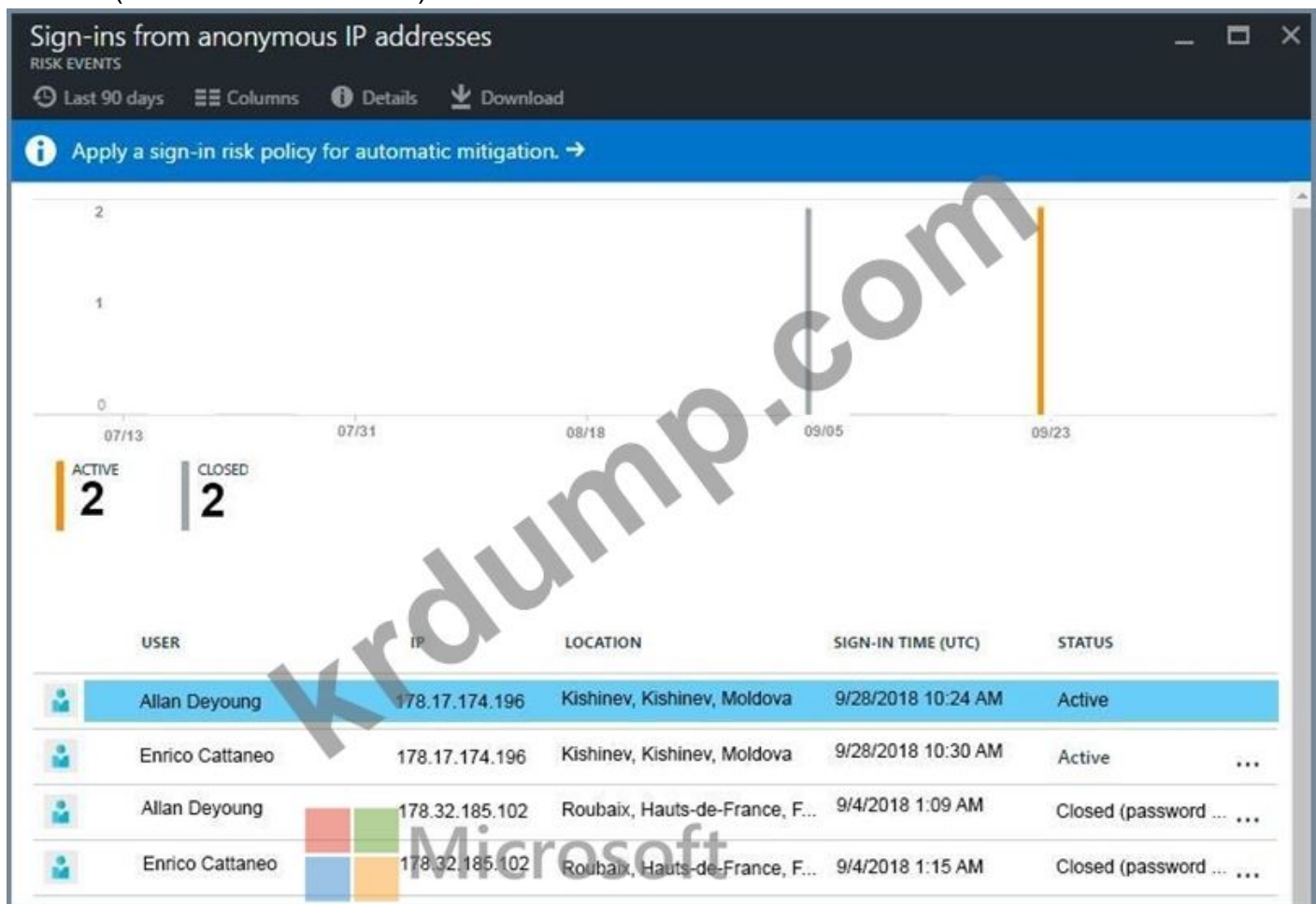
The expense claims solution must provide managers with claim information and the ability to manage the claim by using Microsoft Outlook, Outlook on the web, or Outlook for iOS and Android.

Reference:

<https://docs.microsoft.com/en-us/outlook/actionable-messages/send-via-email>

NEW QUESTION: 116

Microsoft Azure Active Directory(Azure AD) ID □□ □□□□□□ □□□□ □□□ □□ □□□□ □□□. (□□ □□ □□□□□.)



□□□□ □□□ □□□ □□□ □□□□ □□□ □□□.

□□□ □□ □□□?

A. Security & Compliance □□ □□□□ Security Readers □□ □□□ □□□□ □□□□□.

- B. Azure Active Directory □□ □□□ □□□ □□□ □□□□□□ □□□ □□□ □□□□.
- C. Azure Active Directory □□ □□□□ □□□ □□□ □□ □□□ □ □□ IP□ □□□□□□.
- D. □□ □ □□ □□ □□ □□□□ □□ □□□□ □□□□.

Answer: B (LEAVE A REPLY)

Explanation

A named location can be configured as a trusted location. Typically, trusted locations are network areas that are controlled by your IT department. In addition to Conditional Access, trusted named locations are also used by Azure Identity Protection and Azure AD security reports to reduce false positives for risky sign-ins.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

NEW QUESTION: 117

Office 365 ProPlus □□ □□□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□.

□□ □□□ □□□ XML □□□ □□□□.

```
<Add SourcePath="Server1\OfficeSoftware"
OfficeClientEdition="32"
Channel="Targeted"
AllowCdnFallback="True">
<Product ID="O365ProPlusRetail">
<Language ID="MatchOS" Fallback="en-us" />
</Product>
</Add> |
```

□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□ □□□□ □□ □□□ □□ □□□ □□ □□□.

□□□.

□□: □ □□□ □□□ □□□ 1□□ □□□ □□□□.

Answer Area

Office 365 ProPlus feature updates will be installed. **[answer choice]**.

To meet the technical requirement for Office 365 ProPlus. **[answer choice]**.

Change SourcePath to DownloadPath. Set the value for AllowCdnFallback to False. Add SCLCacheOverride=1 to the Product section.

Microsoft

automatically once a year
 automatically twice a year
 manually

Answer:

Answer Area

Office 365 ProPlus feature updates will be installed. **[answer choice]**.

To meet the technical requirement for Office 365 ProPlus. **[answer choice]**.

Microsoft

automatically once a year
 automatically twice a year
 manually

Change SourcePath to DownloadPath. Set the value for AllowCdnFallback to False. Add SCLCacheOverride=1 to the Product section.

NEW QUESTION: 118

□□□□ □□ □□ □□□ □□□ □□□ Microsoft Office 365 □□□ □□□□.

Name	Members
Group1	User1, User2
Group2	User3

□□ □□ □□□ □□□□□ □□□□□.

License	Included service	Assigned to
Microsoft 365	Microsoft Exchange Online	Group1
Microsoft 365	Microsoft SharePoint Online	User1, User2, User3

□□ □□□□ Group1 □□ User1 □ □□□□ Group2 □ Group1 □ □□□□□.

□□ □ □□□ □□ □□□ □□□ □□ □□□□□□□□. □□□ □□□ □□□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□□.

Statements	Yes	No
User1 is licensed for SharePoint Online.	<input type="radio"/>	<input type="radio"/>
User2 is licensed for SharePoint Online.	<input type="radio"/>	<input type="radio"/>
User3 is licensed for SharePoint Online.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 is licensed for SharePoint Online.	<input checked="" type="radio"/>	<input type="radio"/>
User2 is licensed for SharePoint Online.	<input checked="" type="radio"/>	<input type="radio"/>
User3 is licensed for SharePoint Online.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation

Statements	Yes	No
User1 is licensed for SharePoint Online.	<input checked="" type="radio"/>	<input type="radio"/>
User2 is licensed for SharePoint Online.	<input checked="" type="radio"/>	<input type="radio"/>
User3 is licensed for SharePoint Online.	<input checked="" type="radio"/>	<input type="radio"/>

User1, User2 and User3 have each been assigned a SharePoint license directly. Therefore, they are all licensed for SharePoint Online.

Changing the group memberships will only affect whether or not they are licensed for Exchange Online because the Exchange Online licenses are assigned to Group1.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-licensing-whatis-azure-po>

NEW QUESTION: 119

□□□ □□ □□ □□ Microsoft Power Apps □□ □□□ Microsoft Power Platform □□□□ □ □□ □□□□.

□□□ □□□ □□□ □□ □□ □□ □□□□□?

- A. 7
- B. 14
- C. 28
- D. 90

Answer: C (LEAVE A REPLY)

Explanation

All your environments, except Trial environments (standard and subscription-based), are backed up. System backups for production environments that have been created with a database and have one or more Dynamics

365 applications installed are retained up to 28 days. System backups for production environments which do not have Dynamics 365 applications deployed in them will be retained for 7 days. System backups for sandbox environments will be retained for 7 days.

Reference:

<https://docs.microsoft.com/en-us/power-platform/admin/backup-restore-environments>

NEW QUESTION: 120

□□□□□□ Active Directory □□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.

□□□ □□ □□□ 10,000□□ □□ □□□□ □□□□ □□□□□.

100□□ □ □□□ □□ □□□ □□□□□□.

□ □□□ □□□ □□□ □ □□ Azure AD□ □□□□□□□ □□ □□□. □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □ □□□ □□ □□□ 1□□ □□□ □□□□.

Answer Area

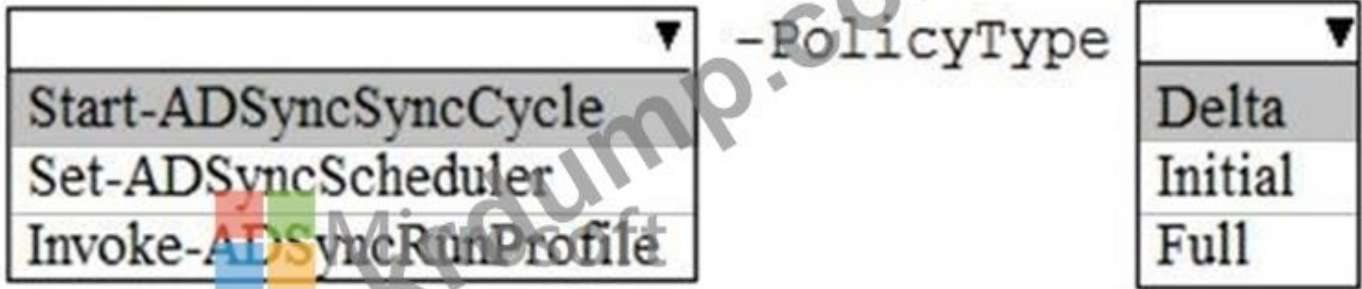
Start-ADSyncSyncCycle	-PolicyType	Delta
Set-ADSyncScheduler		Initial
Invoke-ADSyncRunProfile		Full

Answer Area

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

Explanation

Answer Area



Azure AD Connect synchronizes Active Directory to Azure Active Directory on a schedule. The minimum time between synchronizations is 30 minutes.

If you want to synchronize changes to Active Directory without waiting for the next sync cycle, you can initiate a sync by using the Start-AdSyncSyncCycle. The Delta option synchronizes changes to Active Directory made since the last sync. The Full option synchronizes all Active Directory objects including those that have not changed.

Reference:

<https://blogs.technet.microsoft.com/rmilne/2014/10/01/how-to-run-manual-dirsync-azure-active-directory-sync-u>

NEW QUESTION: 121

contoso.com Active Directory .

.

Microsoft 365 Microsoft 365 .

ID .

SSO

. Microsoft

Azure Active Directory(Azure AD) . .

Microsoft 365 . . .

.

: 1 .

A. .

B. SSO

C. Azure AD . . .

D. . Microsoft 365 . . .

Answer: B,D (LEAVE A REPLY)

Explanation

When you choose this federation as the authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password. AD FS can use on-premise Active Directory as an authentication provider. AD FS can also provide SSO when using Active Directory as an authentication provider.

From: <https://docs.microsoft.com/en-us/microsoftteams/network-planner>

Network Planner is a new tool that is available in the Teams admin center. It can be found by going to Planning > Network planner. In just a few steps, the Network Planner can help you determine and organize network requirements for connecting Microsoft Teams users across your organization. When you provide your network details and Teams usage, the Network Planner calculates your network requirements for deploying Teams and cloud voice across your organization's physical locations.

NEW QUESTION: 124

contoso.com Azure AD(Azure Active Directory) Microsoft 365 E5

100 Microsoft 365 Business Voice

Voice Microsoft 365 Business Voice

?

A. Azure Active Directory

B. Microsoft 365

C. Microsoft 365

Answer: A (LEAVE A REPLY)

Explanation

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-assign>

NEW QUESTION: 125

Microsoft 365 Azure AD(Azure Active Directory)

Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account

Azure AD

CUSTOM SMART LOCKOUT

Lockout threshold ✓

Lockout duration in seconds ✓

Custom banned passwords

Enforce custom list Yes No

Custom banned password list ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory Yes No

Mode Enforced Audit

Which of the following is a valid password for a user in the Contoso domain?

- A. User1
- B. User1 User2
- C. User1 User3
- D. User1, User2, User3

Answer: D (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>

NEW QUESTION: 126

You are configuring a Microsoft SharePoint Online site for a Microsoft 365 tenant. You want to ensure that the site is accessible only to users who are already in your directory. Which setting should you configure?

- A. Microsoft 365 Settings > Security & Compliance > Sharing > Sharing settings
- B. SharePoint Admin Center > Site Settings > Site Permissions > Site Permissions
- C. Azure Active Directory > Users & Groups > Users & Groups > Users & Groups
- D. SharePoint Admin Center > Site Settings > Site Permissions > Site Permissions

Answer: D (LEAVE A REPLY)

Explanation

You need to set the Sharing settings to 'Existing Guests'. This setting allows sharing only with guests who are already in your directory. These guests may exist in your directory because they

previously accepted sharing invitations or because they were manually added.

Reference:

<https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>

NEW QUESTION: 127

Contoso is migrating its Microsoft Exchange Server 2016 mailboxes to Microsoft 365 Enterprise Exchange Online. The migration is causing the slow performance of the Exchange Server.

The migration is causing the slow performance of the Exchange Server.

The migration is causing the slow performance of the Exchange Server.

The migration is causing the slow performance of the Exchange Server.

The migration is causing the slow performance of the Exchange Server.

The migration is causing the slow performance of the Exchange Server.

A. The migration is causing the slow performance of the Exchange Server.

B. The migration is causing the slow performance of the Exchange Server.

C. The migration is causing the slow performance of the Exchange Server.

D. The migration is causing the slow performance of the Exchange Server.

Answer: C (LEAVE A REPLY)

Explanation

The migration is causing the slow performance. This suggests that the on-premise Exchange server is struggling under the load of copying the mailboxes to Exchange Online. You can reduce the load on the on-premise server by reducing the maximum number of concurrent mailbox migrations. Migrating just a few mailboxes at a time will have less of a performance impact than migrating many mailboxes concurrently.

Reference:

<https://support.microsoft.com/en-gb/help/2797784/how-to-manage-the-maximum-concurrent-migration-batches->

NEW QUESTION: 128

Contoso is migrating its Microsoft 365 mailboxes to Exchange Online.

Contoso.onmicrosoft.com

Contoso.com

Contoso is migrating its Microsoft 365 mailboxes to Exchange Online.

Sub1.contoso.onmicrosoft.com

Sub2.contoso.com

Fabrikam.com

Contoso is migrating its Microsoft 365 mailboxes to Exchange Online.

Contoso is migrating its Microsoft 365 mailboxes to Exchange Online.

Contoso is migrating its Microsoft 365 mailboxes to Exchange Online.

Contoso is migrating its Microsoft 365 mailboxes to Exchange Online.

MX records:

CNAME records:

Answer:

MX records:

CNAME records:

Explanation

MX records:

CNAME records:

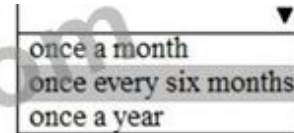
Box 1: 2

You don't need to verify Sub1.contoso.onmicrosoft.com because the onmicrosoft.com domain

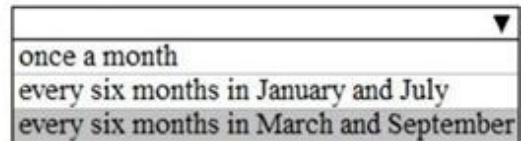


Explanation

Office 365 ProPlus feature updates will be installed [answer choice].



Office 365 ProPlus security updates will be installed [answer choice].



References:

<https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool#updat>

<https://docs.microsoft.com/en-us/deployoffice/overview-of-update-channels-for-office-365-proplus>

NEW QUESTION: 130

□□□ □-□□□□ Microsoft Exchange Server 2016 □□□ □□□□. □□□ □□□□ □□ □□ □□□ □□□□. □□□ □□□□ □□ □□□□□ □□□□ □□□□. □□□□ 250□□ □□□□ □□□□.

Microsoft 365 □□□ □□□□ □□ □□ Exchange Online□□ □□□□□□□ □□□□□□. 12□□ □□ □□□ □□□ □□□ □ □□ □□□□ □□ □□□□□□.

□□□ □□ □□□ □□□□□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.

□□□ □□□□ □□ □□□ □□ □□□ □□□□□? □□ □□□ □□ □□□ □□□ □□□ □□□□□. □□ □□ □□ □□□□□□.

- A. □□□□ □□□
- B. □□□ □□□□□□
- C. □□□□□ □□□□□□
- D. □□□ □□□□□□

Answer: (SHOW ANSWER)

Explanation

With a hybrid migration, you can migrate the mailboxes in small batches over a period of time which will help to avoid saturating the bandwidth. With the migration wizard, you can configure a migration batch to start outside office hours which would minimize bandwidth usage during office hours.

With a hybrid migration, you do not need to reconfigure Outlook to connect to the migrated mailbox. Outlook will automatically detect the new mailbox location. This reduces administrative effort.

Reference:

<https://docs.microsoft.com/en-us/exchange/mailbox-migration/mailbox-migration>

NEW QUESTION: 131

Microsoft Azure Active Directory(Azure AD) is configured for contoso.com. An Active Directory forest is configured for contoso.com. Windows Server 2016 Server1 is configured for Windows 10. The forest functional level is 2008 R2.

Microsoft 365 is installed on Server1.

Server1 has a Share1 folder. Microsoft Office Word (ODT) is installed on Share1.

Office 365 ProPlus is installed on Share1. Windows 10 is installed on all client computers.

What is the correct sequence of actions to migrate the Word documents from Share1 to the Office 365 ProPlus installation on the client computers?

Actions

Answer Area

- Create an XML configuration file.
- On Server1, run `setup.exe` and specify the `/configure` parameter.
- On every client computer, run `setup.exe` and specify the `/configure` parameter.
- On Server1, run `setup.exe` and specify the `/package` parameter.
- On every client computer, run `setup.exe` and specify the `/download` parameter.
- On Server1, run `setup.exe` and specify the `/download` parameter.

Answer:

- Create an XML configuration file.
- On Server1, run `setup.exe` and specify the `/configure` parameter.
- On every client computer, run `setup.exe` and specify the `/configure` parameter.
- On Server1, run `setup.exe` and specify the `/package` parameter.
- On every client computer, run `setup.exe` and specify the `/download` parameter.
- On Server1, run `setup.exe` and specify the `/download` parameter.

Answer Area

- On Server1, run `setup.exe` and specify the `/download` parameter.
- Create an XML configuration file.
- On every client computer, run `setup.exe` and specify the `/configure` parameter.

Explanation

Note:

Step 1: Create an XML configuration file with the source path and download path for the installation files.

Step 2: On the deployment server, run the ODT executable in download mode and with a reference to the XML configuration file.

Step 3: Create another XML configuration file with the source path to the installation files.

Step 4: On the client computer, run the ODT executable in configure mode and with a reference to the XML configuration file.

Reference:

<https://docs.microsoft.com/en-us/DeployOffice/overview-of-the-office-2016-deployment-tool>

NEW QUESTION: 132

□□ □□□ □□□□ □□ □□ □□□ □□□□. □□□□ □ □□□□ □□□ □ □□□□. □
 □□□ □ □ □□ □□□ □ □□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□.
 □□ □□□ □□□ □ □□□ □□□□ □□ □□□ □□□□□□. □ □□□□□ □□□ □□□
 □ □□□ □□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□□ □□□ □ □□□
 □□ □□(□: □□ □ □□□□, □□ □ □□□ □□ □□)□ □□□ □□□□□□.
 □□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□. □, □□□ □□□ □□□□□□ □
 □□□ □□□ □□□□□ □□□□ □□ □□□ □□ □□□□ □□ □□□.

Microsoft 365 license assignment question. The question asks how to assign a license to a group. The correct answer is to create the group and assign the license to the group. The explanation states that anyone added to the group will automatically be assigned the license assigned to the group. The steps provided are: 1. Go to the Azure Active Directory admin center. 2. Select the Azure Active Directory link then select Groups. 3. Click the New Group link. 4. Select 'Security' as the group type and enter 'Group2' for the group name. 5. Click the Create button to create the group. 6. Back in the Groups list, select Group2 to open the properties page for the group. 7. Select 'Licenses'. 8. Select the '+ Assignments' link. 9. Tick the box to select the license. 10. Click the Save button to save the changes.

Microsoft 365 license assignment question:

admin@LODSe426243.onmicrosoft.com

Microsoft 365 license: 3&YWyjse-6-d

Microsoft 365 license assignment question. The question asks how to assign a license to a group. The correct answer is to create the group and assign the license to the group. The explanation states that anyone added to the group will automatically be assigned the license assigned to the group.

The steps provided are:

1. Go to the Azure Active Directory admin center.

2. Select the Azure Active Directory link then select Groups.

Answer:

See explanation below.

Explanation

You need to create the group and assign a license to the group. Anyone who is added to the group will automatically be assigned the license that is assigned to the group.

1. Go to the Azure Active Directory admin center.
2. Select the Azure Active Directory link then select Groups.
3. Click the New Group link.
4. Select 'Security' as the group type and enter 'Group2' for the group name.
5. Click the Create button to create the group.
6. Back in the Groups list, select Group2 to open the properties page for the group.
7. Select 'Licenses'.
8. Select the '+ Assignments' link.
9. Tick the box to select the license.
10. Click the Save button to save the changes.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign>

NEW QUESTION: 133

Microsoft 365 license assignment question.

Admin1 license assignment question. The question asks how to assign a license to a group. The correct answer is to create the group and assign the license to the group. The explanation states that anyone added to the group will automatically be assigned the license assigned to the group.

contoso.com? Microsoft Azure Active Directory(Azure AD) Microsoft 365 User1 Azure AD ID
 User1 Azure AD ID

Answer Area

Admin center to use: Azure Active Directory
 Exchange
 Microsoft 365
 Security & Compliance

Role to assign: eDiscovery Manager
 Information Protection Administrator
 User management administrator

Answer:

Answer Area

Admin center to use: Azure Active Directory
 Exchange
 Microsoft 365
 Security & Compliance

Role to assign: eDiscovery Manager
 Information Protection Administrator
 User management administrator

Explanation

Admin center to use: Azure Active Directory
 Exchange
 Microsoft 365
 Security & Compliance

Role to assign: eDiscovery Manager
 Information Protection Administrator
 User management administrator

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-cent>

NEW QUESTION: 134

contoso.com Microsoft Azure Active Directory(Azure AD) Microsoft 365 User1 Azure AD ID
 User1 Azure AD ID

- A. [] [] [] []
- B. [] [] [] []

The [answer choice] will be **uninstalled** from the computers.

If the Office share on Server1 is missing the Japanese language pack, Office 365 ProPlus will [answer choice].

MSI version of Microsoft Visio only
C2R version of Microsoft Visio only
MSI and C2R versions of Microsoft Visio

be installed in English only
be installed in a randomly selected language
NOT be installed

Answer:

The [answer choice] will be uninstalled from the computers.

MSI version of Microsoft Visio only
C2R version of Microsoft Visio only
MSI and C2R versions of Microsoft Visio

If the Office share on Server1 is missing the Japanese language pack, Office 365 ProPlus will [answer choice].

be installed in English only
be installed in a randomly selected language
NOT be installed

Explanation

The [answer choice] will be uninstalled from the computers.

MSI version of Microsoft Visio only
C2R version of Microsoft Visio only
MSI and C2R versions of Microsoft Visio

If the Office share on Server1 is missing the Japanese language pack, Office 365 ProPlus will [answer choice].

be installed in English only
be installed in a randomly selected language
NOT be installed

Box 1:

The C2R (click-to-run) version of Microsoft Visio only will be uninstalled from the computers. To remove the MSI version of Microsoft Visio, you would need to specify the RemoveMSI parameter. The RemoveMSI parameter is not configured in the configuration file in this question. Therefore, only the C2R version will be installed.

Box 2:

If the Office share on Server1 is missing the Japanese language pack, Office 365 ProPlus will be installed in English only.

In the configuration file, English is the first in the list above Japanese. Therefore, English is the primary language and the installation will continue in English only.

Reference:

<https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool>

NEW QUESTION: 136

□□ □□ □□□ □□□□ □□□□ contoso.com□□□ Azure AD(Azure Active Directory) □□ □□ □□□□.

Name	Type	Member of
User1	User	Group1
User2	User	Group1, Group2
User3	User	Group1, Group2
User4	Guest User	Group2

User1 is a member of Group1. User2 is a member of Group2.

User1 is the owner of Group1.

* User1 can review access for User2.

* User1 can review access for User3.

* User3 can review access for User4.

* User3 cannot review access for User4.

Group owners can review access for members of their group.

Group members can review access for other members of their group.

Answer:

Explanation

Box 1: Yes

User1 is the owner of Group1. User2 is in Group1 and Group2. Group owners can review access. Therefore, User1 can review User2's membership of Group1.

Box 2: Yes

User1 is the owner of Group1. User3 is in Group1 and Group2. Group owners can review access. Therefore, User1 can review User3's membership of Group1.

Box 3: No

Only group owners can review access. User3 is not a group owner. Therefore, User3 cannot



Sign in

Email, phone, or Skype

No account? [Create one!](#)



Sign-in options

Next

Project1 □□□ SharePoint □□□□ □□□□ □□□. □□□ □□□□ □□□□ □□□□ □□
 □□□□ □□□ □ □□□ □□□.
 □□□□□ Microsoft 365 □□□ □□□□□□.

Answer:

See explanation below.

Explanation

You need to create a SharePoint site and configure the sharing settings.

1. Go to the SharePoint Admin Center.
2. In the left navigation pane, expand Sites then select 'Active Sites'.
3. Click on the '+ Create' link to add a new site.
4. Select 'Other Options' then 'Team Site' for the template.
5. Give the site the name 'Project1'.
6. In the 'Primary Administrator' field, start typing 'admin' then select the admin@LODSe878763.onmicrosoft.com account when it appears.
7. Click Finish to create the site.
8. In the Active Sites list, select the Project1 site.
9. Click the Sharing link at the top of the sites list.
10. Under 'External Sharing', select 'Anyone'.
11. Click Save to save the changes.

NEW QUESTION: 138

□□ □□□ □□□□ □□ □□ □□□ □□□□. □□□□ □ □□□□ □□□ □ □□□□. □
 □□□ □ □ □□ □□□ □ □□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□.
 □□ □□□ □□□ □ □□□ □□□□ □□ □□□ □□□□□□. □ □□□□□ □□□ □□□
 □ □□□ □□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□□ □□□ □ □□□
 □□ □□(□: □□ □ □□□□, □□ □ □□□ □□ □□)□ □□□ □□□□□□.
 □□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□. □, □□□ □□□ □□□□□□□ □
 □□□ □□□ □□□□□ □□□□ □□ □□□ □□ □□□□ □□ □□□.
 □□ □□□ □□□ □□□□ □□□ □ □□□□ □□□□ □□ □□□ □ □ □□ □□ □ □□□
 □. □ □□□ □□□□ □ □□□ □□ □□□ □□□ □ □□□□. □□□ □□□ □□ □□ □□

Microsoft 365 Admin Center: admin@LODSe878763.onmicrosoft.com
Microsoft 365 ID: m3t^We\$Z7&xy
Microsoft 365 ID: CTRL-K
Microsoft 365 ID: 11440873

Microsoft 365 ID: admin@LODSe878763.onmicrosoft.com

Microsoft 365 ID: m3t^We\$Z7&xy

Microsoft 365 ID: CTRL-K

Microsoft 365 ID: 11440873

Microsoft 365 ID: 11440873



Sign in

Email, phone, or Skype

No account? [Create one!](#)



Sign-in options

Next

Managers group: Adele Vance
Microsoft 365 ID: 11440873

Answer:

See explanation below.

Explanation

You need to create a group named Managers and add Adele Vance to the group. To ensure that you can grant permissions to the Managers group, the group needs to be a Security Group.

1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Groups section then select Groups.
3. Click the 'Add a group' link.
4. For the group type, select Security and click Next.
5. Enter 'Managers' in the Name field and click Next.
6. Click the 'Create Group' button to create the Managers group.
7. In the list of groups, select the Managers group.
8. Click the Members link.
9. Click the 'View all and manage members link'.

10. Click the 'Add Members' button.
11. Select Adele Vance and click the Save button.
12. Click the Close button to close the group page.

NEW QUESTION: 139

contoso.com is a Microsoft Azure Active Directory (Azure AD) tenant. Microsoft 365 is deployed to contoso.com. The Microsoft 365 administrator wants to ensure that users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically. The administrator also wants to ensure that users must be able to authenticate during business hours only. Authentication requests must be processed successfully if a single server fails. When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in.

Which configuration option should be used to meet these requirements?

- * Synchronization of passwords between on-premises and cloud user accounts.
- * Password synchronization.
- * Password synchronization with a password synchronization proxy.
- * Password synchronization with a password synchronization proxy and password synchronization with a password synchronization proxy.

- A. Password synchronization
- B. Password synchronization with a password synchronization proxy

Answer: B (LEAVE A REPLY)

Explanation

This solution meets the following goals:

- * Users must be able to authenticate during business hours only.
- * Authentication requests must be processed successfully if a single server fails.
- * When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in.

However, the following goal is not met:

- * Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.

You would need to configure Single-sign on (SSO) to meet the last requirement.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn>

NEW QUESTION: 140

contoso.com is a Microsoft Azure Active Directory (Azure AD) tenant. Microsoft 365 is deployed to contoso.com. The Microsoft 365 administrator wants to ensure that users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.

□□□□.

User1□ Azure AD ID □□□□ □□□ □ □□□□□ □□□ □□□ □□□ □ □□□ □□□ □ □□□.

User1□ □□ □□□ □□□□ □□□?

- A. □□ □□□
- B. □□ □□ □□□
- C. □□□ □□
- D. □□ □□□

Answer: ([SHOW ANSWER](#))

Explanation

The risky sign-ins reports are available to users in the following roles:

- * Security Administrator
- * Global Administrator
- * Security Reader

Of the three roles listed above, the Security Reader role has the least privilege.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risky-sign-ins>

NEW QUESTION: 141

□□□ □□□ Microsoft 365 □□□ □□□□□□.

Azure AD(Azure Active Directory) □□□□ □□ 500□□ □□□□ □□ Microsoft Azure MI A(Multi-Factor Authentication)□ □□□□□ □□□□□.

Azure MFA □□ □□□□□ □□□ □□ □□□□ □□□□ □□□□ □□□□ □□□.

□□□ □□□□ □□ □□□ □□ □□□ □□□□□? □□ □□□ □□ □□□ □□□ □□□ □ □□□□. □□ □□ □□ □□□□□.

- A. Azure Cloud Shell□□ Get-AzureADUser cmdlet□ □□□□□.
- B. Azure Cloud Shell□□ Get-MsolUser cmdlet□ □□□□□.
- C. Azure Active Directory □□ □□□□ MFA □□ □□□□□ □□□□□.
- D. Azure Active Directory □□ □□□□ □□□ □□□ □□□□□ □□□□□.

Answer: B ([LEAVE A REPLY](#))

Explanation

You can use the Get-MsolUser cmdlet to generate a report that lists all the users who completed the Azure MFA registration process. The full command would look like this:

```
Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0} | Select-Object -Property UserPrincipalName
```

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-reporting>

NEW QUESTION: 142

□□ □□□ □□□□ □□ □□ □□□ □□□□. □□□□ □ □□□□ □□□ □ □□□□. □ □□□ □ □ □□ □□□ □ □□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□. □□ □□□ □□□ □ □□□ □□□□ □□ □□□ □□□□□□. □ □□□□□ □□□ □□□

Microsoft 365 Admin Center: Add Domain. You need to add the contoso.com domain to Microsoft 365 then set the domain as the default. In the Admin Center, click Setup then click Domains. Click the 'Add Domain' button. Type in the domain name (contoso.com) and click the 'Use this domain' button. The question states that another administrator will perform the required information to your DNS zone. Therefore, you just need to click the 'Verify' button to verify domain ownership. Click Finish. In the domains list, select the contoso.com domain. Select 'Set as default'.

Microsoft 365 Admin Center:

admin@LODSe426243.onmicrosoft.com

Microsoft 365 Admin Center: 3&YWyjse-6-d

Microsoft 365 Admin Center: CTRL-K

Microsoft 365 Admin Center:

Microsoft 365 Admin Center:

Microsoft 365 Admin Center: 10887751

Microsoft 365 Admin Center: 1,000

Microsoft 365 Admin Center: @contoso.com

Microsoft 365 Admin Center: DNS

Answer:

See explanation below.

Explanation

You need to add the contoso.com domain to Microsoft 365 then set the domain as the default.

1. In the Admin Center, click Setup then click Domains.
2. Click the 'Add Domain' button.
3. Type in the domain name (contoso.com) and click the 'Use this domain' button.
4. The question states that another administrator will perform the required information to your DNS zone.

Therefore, you just need to click the 'Verify' button to verify domain ownership.

5. Click Finish.
6. In the domains list, select the contoso.com domain.
7. Select 'Set as default'.

References:

<https://docs.microsoft.com/en-us/office365/admin/setup/add-domain?view=o365-worldwide>

NEW QUESTION: 143

Microsoft 365 Admin Center: Add Domain. You need to add the contoso.com domain to Microsoft 365 then set the domain as the default. In the Admin Center, click Setup then click Domains. Click the 'Add Domain' button. Type in the domain name (contoso.com) and click the 'Use this domain' button. The question states that another administrator will perform the required information to your DNS zone. Therefore, you just need to click the 'Verify' button to verify domain ownership. Click Finish. In the domains list, select the contoso.com domain. Select 'Set as default'.

Microsoft 365 Admin Center: admin@LODSe878763.onmicrosoft.com
Microsoft 365 Admin Center: m3t^We\$Z7&xy
Microsoft 365 Admin Center: CTRL-K
Microsoft 365 Admin Center: 11440873

Microsoft 365 Admin Center: admin@LODSe878763.onmicrosoft.com
Microsoft 365 Admin Center: m3t^We\$Z7&xy
Microsoft 365 Admin Center: CTRL-K
Microsoft 365 Admin Center: 11440873



Microsoft 365 Admin Center: admin@LODSe878763.onmicrosoft.com
Microsoft 365 Admin Center: m3t^We\$Z7&xy
Microsoft 365 Admin Center: CTRL-K
Microsoft 365 Admin Center: 11440873

Answer:

See explanation below.
You need to configure the Password Expiration Policy.

- Explanation
1. Sign in to the Microsoft 365 Admin Center.
 2. In the left navigation pane, expand the Settings section then select the Settings option.
 3. Click on Security and Privacy.

4. Select the Password Expiration Policy.
5. Ensure that the checkbox labelled "Set user passwords to expire after a number of days" is ticked.
6. Enter 60 in the "Days before passwords expire" field.
7. Enter 10 in the "Days before a user is notified about expiration" field.
8. Click the 'Save changes' button.

NEW QUESTION: 144

Configure an Azure AD (Azure Active Directory) password policy for the contoso.com domain. The policy should be applied to all users in the Active Directory. The policy should require passwords to be at least 12 characters long, contain at least one uppercase letter, one lowercase letter, one digit, and one special character. The password should not be reused for 30 days. The password should expire every 60 days. The password should be notified 10 days before expiration.

Name	Source
User1	Azure Active Directory
User2	Azure Active Directory
User3	Windows Active Directory

The password policy should be applied to all users in the Active Directory.

Name	Password
User1	Contoso123
User2	N3w3rT0Gue33
User3	ComplexPassword33

The password policy should be applied to all users in the Active Directory.

Custom smart lockout

Lockout threshold:

Lockout duration in seconds:

Custom banned passwords

Enforce custom list: Yes No

Custom banned password list:

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes No

Mode: Enforced Audit

The password policy should be applied to all users in the Active Directory. The password should be notified 10 days before expiration.

Statements	Yes	No
User1 must change his password at the next sign in.	<input type="radio"/>	<input type="radio"/>
User2 can change his password to C0nt0s0_C0mplex123.	<input type="radio"/>	<input type="radio"/>
User3 can change his password to MyPasswordContoso123.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 must change his password at the next sign in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can change his password to C0nt0s0_C0mplex123.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can change his password to MyPasswordContoso123.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation

Statements	Yes	No
User1 must change his password at the next sign in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can change his password to C0nt0s0_C0mplex123.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can change his password to MyPasswordContoso123.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: No

User1's password contains the banned password 'Contoso'. However, User1 will not be required to change his password at next sign in. When the password expires or when User1 (or an administrator) changes the password, the password will be evaluated and will have to meet the password requirements.

Box 2: Yes

Password evaluation goes through several steps including normalization and Substring matching which is used on the normalized password to check for the user's first and last name as well as the tenant name.

Normalization is the process of converting common letter substitutes into letters. For example, 0 converts to o.

\$ converts to s. etc.

The next step is to identify all instances of banned passwords in the user's normalized new password. Then:

* Each banned password that is found in a user's password is given one point.

* Each remaining unique character is given one point.

* A password must be at least five (5) points for it to be accepted.

'C0nt0s0' becomes 'contoso' after normalization. Therefore, C0nt0s0_C0mplex123 contains one instance of the banned password (contoso) so that equals 1 point. After 'contoso', there are 11 unique characters.

Therefore, the score for 'C0nt0s0_C0mplex123' is 12. This is more than the required 5 points so the password is acceptable.

Box 3:

The 'Password protection for Windows Server Active Directory' is in 'Audit' mode. This means that the password protection rules are not applied. Audit mode is for logging policy violations before putting the password protection 'live' by changing the mode to 'enforced'.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>

NEW QUESTION: 145

00: 0 000 000 00000 0000 000 00 0 00000. 0000 0 0000 0
00 000 000 0 00 000 0000 0000 0000. 00 00 0000 00 000
000 0000 00 0 000 00 00 0000 000 0000 00 0 0000.
0 000 000 00 000 00 0000 000 0 0000. 00000 000 000 00
000 0000 0000.

000 Microsoft Office 365 0000 0000.

00 Office 365 000 000 00000 000 00000.

00000 000 00000 00 000 0000 000.

00 00: Microsoft 365 00 00 000 0000 00000.

000 000 00000?

A. 000

B. 0

Answer: A (LEAVE A REPLY)

NEW QUESTION: 146

00 000 0000 00 00 000 0000. 0000 0 0000 000 0 0000. 0
000 0 0 00 000 0 000 00 000 00 000 0000 0000 0000.
00 000 000 0 000 0000 00 000 000000. 0 00000 000 000
0 000 000 00000. 0000 000 000 00000 00000 000 0 000
00 00(0: 00 0 0000, 00 0 000 00 00)0 000 000000.

000 000 000 000 000 000 0000 000. 0, 000 000 000000 0
000 000 00000 0000 00 000 00 0000 00 000.

00 000 000 0000 000 0 0000 0000 00 000 0 0 00 00 0 000
0. 0 000 0000 0 000 00 000 000 0 0000. 000 000 00 00 00
000 00 00 000 000 0 000 000 0000 0000 000.
0 000 00 000 0000 000 0000 000 000 0 0000.

□□ □□□ □□□□ □□□ □□□ □ □□□□.
□□□ □□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□ □□□ □□□ □□□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□□.

Microsoft 365 □□□ □□:

admin@M365x981607.onmicrosoft.com

Microsoft 365 □□: *yfLo7lr2&y-

Microsoft 365 □□□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□
□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

□ □□□□: 10811525

□□□ □□□ □□□ Fabrikam, Inc.□□ □□ □□□ □□□ □□□ □□□□□.

user1@fabrikam.com□□□ □□ □□□□□ Microsoft 365 □□□□□ □□□ □□ □□ □□□
□ □□□ □□□ □□□□□.

□□□ □□□□□□ user1@fabrikam.com□ □□□□ □□□.

Answer:

See explanation below.

Explanation

You need to create a guest account for user1.

1. Go to the Azure Active Directory admin center.
2. Select Users.
3. Click the 'New guest user' link.
4. Select the 'Invite user' option.
5. Give the account a name (User1) and enter user1@fabrikam.com in the email address field.
6. Click the 'Invite' button.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/b2b/b2b-quickstart-add-guest-users-portal>

NEW QUESTION: 147

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □
□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□ □□□
□□□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□.

□ □□□ □□□ □□ □□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□
□□□ □□□□ □□□□.

□□□□ 3,000□□ □□□□ □□□□. □□ □□□□□ Microsoft 365 E3 □□□□□ □□□□
□.

□□ □□□□□□ □□ Microsoft 365 □□□□ □□ □□□□□ □□□□□. □□ □□□□□□
□□ Microsoft 365 □□□□ □□ □□□□□ □□□□□.

User1□□□ □□□□ Exchange Online□ □□□□ □□□ □□□□□□ □□□ □□□□ □□
□.

□□ □□: Get-MsolUser cmdlet □ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

Explanation

The Get-MsolUser cmdlet will tell you if a user is licensed for Microsoft 365 but it does not tell you which licenses are assigned.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/msonline/get-msoluser?view=azureadps-1.0>

NEW QUESTION: 148

User1□□□ □□□□ □□□ Microsoft 365 □□□ □□□□.

□□□□□ □□ □□□□□ □□□□□ □□ User1□ Microsoft 365 □□ □ □□□ □□□□□ □□□ □□ □□□.

Microsoft 365 □□ □□□□ □□□ □□ □□□?

A. □□ □□□□□ □□ □□□ □□□□□.

B. Office □□□□□ □□□□ □□□ □□□□□.

C. □□□ □□ □□□ □□□□□.

D. □ □□□ □□□ □□□□□.

Answer: (SHOW ANSWER)

Reference:

<https://practical365.com/blog/first-steps-configure-office-365-first-release-settings/>

NEW QUESTION: 149

□□ □□ □□□ □□□□ □□□□ Microsoft 365 □□□□ □□□□.

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com
User3	User3@contoso.com

Microsoft Exchange Online□□ □□ □□ □□□ □□ □□ □□□ □□□□.

Name	Priority
Rule1	0
Rule2	1
Rule3	2

Rule1□□ □□□ □□ □□□ □□□□.

Statements	Yes	No
If User1 sends an email to User3, User3 receives the email.	<input type="radio"/>	<input type="radio"/>
If User1 sends an email, a disclaimer is added to the email.	<input type="radio"/>	<input type="radio"/>
If an email is sent to User2, two disclaimers are added to the email.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If User1 sends an email to User3, User3 receives the email.	<input type="radio"/>	<input checked="" type="radio"/>
If User1 sends an email, a disclaimer is added to the email.	<input checked="" type="radio"/>	<input type="radio"/>
If an email is sent to User2, two disclaimers are added to the email.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation

Answer Area

Statements	Yes	No
If User1 sends an email to User3, User3 receives the email.	<input type="radio"/>	<input checked="" type="radio"/>
If User1 sends an email, a disclaimer is added to the email.	<input checked="" type="radio"/>	<input type="radio"/>
If an email is sent to User2, two disclaimers are added to the email.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 150

Microsoft 365 E5 □□□ □□□□.

□□□□ Microsoft SharePoint Online □□□□ □□□□□□ □ □ MFA(Multi-Factor Authentication)□ □□ □□□□ □□□□□ □□□□ □□□. □□□□ □□ Microsoft 365 □□ □□ □□□□□□ □ □ MFA□ □□ □□□□ □□□□ □ □□□. □□□ □□ □□□?

- A. Microsoft Endpoint Manager □□ □□□□ □ □□ □□□ □□□□.
- B. □□□ □□ □□□□□ □□□ □□□ □□□□□.
- C. Azure Active Directory □□ □□□□ □□□ □□□ □□□ □□□□.
- D. Cloud App Security □□ □□□□ □ □□□ □□□ □□□□.

Answer: C (LEAVE A REPLY)

Explanation

Multi-factor authentication (MFA) is configured through conditional access policies.

Reference:

<https://docs.microsoft.com/en-us/appcenter/general/configuring-aad-conditional-access>

NEW QUESTION: 151

□□ □□ □□□ □□□□ □□□□ Microsoft 365 □□□ □□□□.

Name	Group
User1	Group1
User2	Group1, Group2

□□ □□ □□□ □□□ □□□ □□□□.

Named location	IP range
Montreal	133.107.0.0/16
Toronto	193.77.10.0/24

□□ □□□ □□ □□□ □□□ □□□ □□□□.

□□□ □ □□:

□□: □□ 1

□□: □□ 2

□□□□ □: □□ □□□□ □ □□

□□:

□□: □□ □□

□□: □□□□

□□□ □□: □□□ □□ □□, □□□ □□ □□

User1 □ □□ □□ □□(MFA) □□ □□□ □□□ □□□□.

□□ □ □□□ □□ □□□ □□□ □□ □□□□□□. □□□ □□□ □□□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements

Yes

No

User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.

User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.

User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.

Answer:

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	<input type="radio"/>	<input type="radio"/>

Explanation

Microsoft Graph permissions?

- A. Calendars.Readwrite Mail.Read
- B. Calendars.Readwrite.Shared Mail.Read
- C. Calendars.Readwrite Mail.ReadWrite
- D. Mail.ReadWrite Mail.Readwrite

Answer: D (LEAVE A REPLY)

NEW QUESTION: 153

Microsoft 365 App1 score.

App1 score in Cloud Discovery.

Microsoft Cloud App Security Cloud Discovery score categories.

Cloud Discover score categories?

- A. General
- B. Security
- C. Compliance
- D. Legal

Answer: B (LEAVE A REPLY)

Explanation

An app's score in Cloud Discovery is based on categories such as General, Security, Compliance and Legal.

Each category has several parameters. For example, the domain registration and consumer popularity parameters are part of the General category. These parameters are known as Score Metrics.

You can modify the default weights given to the Cloud Discovery score configuration. By default, all the various parameters evaluated are given an equal weight. If there are certain parameters that are more or less important to your organization, you can adjust the weight of each score metric.

References:

https://docs.microsoft.com/en-us/cloud-app-security/discovered-app-queries

NEW QUESTION: 154

contoso.com Azure AD Microsoft 365 E5 User1 Team 1 Microsoft Teams collaboration restrictions.

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

Statements	Yes	No
User1 can share his screen with guest users during meetings.	<input type="radio"/>	<input type="radio"/>
User1 can add user1@europe.adatum.com to Team1.	<input type="radio"/>	<input type="radio"/>
User1 can add user1@litware.com to Team1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can share his screen with guest users during meetings.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can add user1@europe.adatum.com to Team1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can add user1@litware.com to Team1.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation


NO, NO Yes

NEW QUESTION: 155


contoso.onmicrosoft.com Azure AD(Azure Active Directory) Microsoft 365
 sub1.contoso.onmicrosoft.com sub2.contoso.onmicrosoft.com
 Contact2

Name	Type	Attribute
Group1	Distribution group	Group email: group1@sub1.contoso.onmicrosoft.com
Group2	Mail-enabled security group	Group email: group2@sub2.contoso.onmicrosoft.com
Group3	Office 365 group	Group email: group3@contoso.onmicrosoft.com
User1	User	Username: user1@sub1.contoso.onmicrosoft.com
Contact2	Contact	Email: contact2@sub2.contoso.onmicrosoft.com

sub1.contoso.onmicrosoft.com sub2.contoso.onmicrosoft.com
 Contact2

sub1.contoso.onmicrosoft.com:  Microsoft

- User1 only
- Group1 only
- User1 and Group1 only
- User1, Group1, and Group3
- No resources must be deleted or modified


sub2.contoso.onmicrosoft.com:  Microsoft

- Contact2 only
- Group2 only
- Contact2 and Group2 only
- Contact2, Group2, and Group3
- No resources must be deleted or modified

Answer:

ub1.contoso.onmicrosoft.com:  Microsoft

- User1 only
- Group1 only
- User1 and Group1 only
- User1, Group1, and Group3
- No resources must be deleted or modified

ub2.contoso.onmicrosoft.com:  Microsoft

- Contact2 only
- Group2 only
- Contact2 and Group2 only
- Contact2, Group2, and Group3
- No resources must be deleted or modified

Explanation



Anything with an email address in the subdomain needs to be removed or moved to another domain. This includes users, mail-enabled security groups, distribution groups and contacts. Office 365 groups will also need to be removed from the subdomains (they cannot be moved to another domain). However, the only Office 365 group in this question is in the parent domain, not the subdomains.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/remove-a-domain?view=o365-wo>

NEW QUESTION: 156

contoso.com is a Microsoft 365 tenant. The tenant contains the following resources:

Name	Member of
User1	Compliant
User2	Group1, Group2

The domain contains the devices shown in the following table.

Name	Compliance status
Device1	Compliant
Device2	Noncompliant

App1 is a Microsoft 365 application. The application is installed on Device1 and Device2. App1 is not installed on Device2.

Name	Includes	Excludes	Device state includes	Device state excludes	Grant
Policy1	Group1	None	All device states	Devices marked as compliant	Block access
Policy2	Group1	Group2	None	None	Block Access
Policy3	Group1	None	All device states	None	Grant access

□□ □ □□□ □□ □□□ □□□ □□ □□□□□□. □□□ □□□ □□□□ □□□□□.
 □□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements	Yes	No
User1 can access App1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from Device2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can access App1 from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation

Statements	Yes	No
User1 can access App1 from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes.

User1 is in a group named Compliant. All the conditional access policies apply to Group1 so they

don't apply to User1.

As there is no conditional access policy blocking access for the group named Compliant, User1 is able to access App1 using any device.

Box 2: Yes.

User2 is in Group1 so Policy1 applies first. Policy1 excludes compliant devices and Device1 is compliant.

Therefore, Policy1 does not apply so we move on to Policy2.

User2 is also in Group2. Policy2 excludes Group2. Therefore, Policy2 does not apply so we move on to Policy3.

Policy3 applies to Group1 so Policy3 applies to User2. Policy3 applies to 'All device states' so Policy3 applies to Device1. Policy3 grants access. Therefore, User2 can access App1 using Device1.

Box 3: No.

User2 is in Group1 so Policy1 applies. Policy1 excludes compliant devices but Devices is non-compliant.

Therefore, User2 cannot access App1 from Device2.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access>

NEW QUESTION: 157

contoso.com is an Active Directory forest.

Microsoft Teams is used to connect to Microsoft 365.

Users are using Teams to connect to Microsoft 365. The network is a hybrid cloud environment.

Users are reporting slow performance when using Teams.

What should you do to improve performance?

A. Microsoft Teams is configured to use BITS (Background Intelligent Transfer Service).

B. Microsoft Teams is configured to use QoS.

C. Microsoft Teams is configured to use QoS.

D. Microsoft Teams is configured to use QoS (QoS) on the network.

E. Microsoft Teams is configured to use QoS.

Answer: D,E ([LEAVE A REPLY](#))

NEW QUESTION: 158

contoso.com is an Active Directory forest.

Users are reporting slow performance when using Teams.

What should you do to improve performance?

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [answer choice].

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [answer choice].

- allowed
- blocked without warning
- blocked, but the user can override the policy

- allowed
- blocked without warning
- blocked, but the user can override the policy

The text in the Policy Settings section of the exhibit explains what will happen. If a user sends between 1 and 10 instances of the sensitive info (passport number), then a notification email will be sent to the user and a policy tip will be displayed. The email will not be blocked though. Therefore, it will be allowed. If a user sends more than 10 instances of the sensitive info (passport number), the email will be blocked and a high-severity alert generated. However, the user can override the block. Reference: <https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

NEW QUESTION: 159

contoso.com Azure AD(Azure Active Directory) Microsoft 365. User1, User2, and User3 are located in the contoso.com Azure AD Connect.

Name	Country	Organizational unit (OU)
User1	United States	OU1
User2	Canada	OU1
User3	United States	OU2

contoso.com Azure AD(Azure Active Directory) Microsoft 365. User1, User2, and User3 are located in the contoso.com Azure AD Connect.

Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
User3 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	<input type="checkbox"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input type="checkbox"/>	<input type="radio"/>
User3 syncs to Azure AD.	<input type="checkbox"/>	<input type="radio"/>

Explanation

Statements	Yes	No
User1 syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User3 syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 160

Microsoft 365 □□□ □□□□.

MDM(□□□ □□ □□)□ □□□ □□□ □□□ □□ □□ □□□ □□ Windows Defender

ATP(Advanced Threat Protection)□ □□□□ □□□.

□□ □□ □□□□ □□□ □□□□ □□□? □□□□□□ □□ □□□□ □□□ □□□ □□□□ □□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Platform:

- Android
- iOS
- Windows 10 and later
- Windows 8.1 and later

Settings:

- Offboard package
- Onboard package
- Windows Defender Application Guard
- Windows Defender Firewall

Answer:

Platform:

- Android
- iOS
- Windows 10 and later
- Windows 8.1 and later

Settings:

- Offboard package
- Onboard package
- Windows Defender Application Guard
- Windows Defender Firewall

Explanation

Platform:

- Android
- iOS
- Windows 10 and later
- Windows 8.1 and later

Settings:

- Offboard package
- Onboard package
- Windows Defender Application Guard
- Windows Defender Firewall

You can integrate Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization. Microsoft Defender ATP works with devices that run Windows 10 or later.

When you establish a connection from Intune to Microsoft Defender ATP, Intune receives a Microsoft Defender ATP onboarding configuration package from Microsoft Defender ATP. This package is deployed to devices by using a device configuration profile.

Reference:

<https://docs.microsoft.com/en-us/intune/advanced-threat-protection>

NEW QUESTION: 161

□□ □□□ □□□□ □□ □□ □□□ □□□□. □□□□ □ □□□□ □□□ □ □□□□. □
 □□□ □ □ □□ □□□ □ □□□ □□ □□□ □□□□ □□□□ □□□□.
 □□ □□□ □□□ □ □□□ □□□□ □□ □□□ □□□□□□□. □ □□□□□ □□□ □□□
 □ □□□ □□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□□ □□□ □ □□□

00 00(0: 00 0 0000, 00 0 000 00 00)0 000 000000.
000 000 000 000 000 000 000 0000 000. 0, 000 000 0000000 0
000 000 000000 0000 00 000 00 0000 00 000.
00 000 000 0000 000 0 00000 00000 00 000 0 0 00 00 0 0000
0. 0 000 00000 0 0000 00 0000 0000 0 00000. 000 0000 00 00 00
0000 00 00 0000 0000 0 0000 0000 00000 00000 0000.
0 000 00 0000 00000 0000 00000 0000 0000 0 00000.
00 0000 00000 0000 0000 0 00000.
0000 00
0000 00 00 0000 00 0000 0000000.
0000 0000 000000 0000 0000 0000 00 00 0000 0000 0000000.
000000 000000 000000 00 0000 0000 00 0000 0000000 0000000.
Microsoft 365 000 00:
admin@LODSe1211885.onmicrosoft.com
Microsoft 365 00: oL9z0=?Nq@ox
Microsoft 365 000 000000 000000 00000 0000 CTRL-K0 00 0 00000 00
0 000 00 000000.
00 0000 00 00 000000 000000.
0 00000: 11098651



0000 00 000000 1800000 0000 0000000 000000 000000 00000 0000.
0000 00000 Microsoft 365 0000 00000000.

Answer:

See explanation below.

Explanation

You need to configure the Password Expiration Policy.

1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Settings section then select the Settings option.
3. Click on Security and Privacy.
4. Select the Password Expiration Policy.
5. Ensure that the checkbox labelled "Set user passwords to expire after a number of days" is ticked.
6. Enter 180 in the "Days before passwords expire" field.
7. Click the 'Save changes' button.

NEW QUESTION: 162

□□□□ 20□□ □□□ □□ □ □□□ Outlook.com□□ □□□□□ □□□□ □□□ □□□□.

□□□ Microsoft 365 □□□ □□□□□.

□□ □□□□ Microsoft 365□ □□□□□□□□ □□□□□.

□□□□ □□□ □□□□□□□ □□□ □□□□ □□□.

□□□ □□□□ □□□?

- A. □□□ □□□□□□
- B. □□□ □□□□□□
- C. IMAP □□□□□□
- D. □□ □□□□□ □□□□□□

Answer: (SHOW ANSWER)

Explanation

To migrate mailboxes from Outlook.com to Office 365, you need to use the IMAP migration method.

After you've added your users to Office 365, you can use Internet Message Access Protocol (IMAP) to migrate email for those users from their IMAP-enabled email servers.

In the Microsoft 365 admin center, go to Setup > Data migration to start migrating IMAP enabled emails.

The email migrations page is pre-configured for migrations from Gmail, Outlook, Hotmail and Yahoo. You can also enter your own IMAP server name and connection parameters to migrate from an email service that is not listed.

References:

<https://docs.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/imap-migration-in-the>

NEW QUESTION: 163

□□ □□ □□ □□□□ Project1 □ Project2 □□ □□□□□ □□□ □ □□□ □□□□ □□□.

□□□ □□□□□ □□ □□ □□ □□□ □□□□ □□□?

contoso.com Active Directory .
 .

Name	Domain	User UPN suffix
User1	Contoso.com	Fabrikam.com
User2	East.contoso.com	Contoso.com

fabrikam.onmicrosoft.com Azure AD(Azure Active Directory) .

Azure AD Connect . fabrikam.onmicrosoft.com .

Azure AD User1 User2 .? .

: 1 .

User1:

User1@contoso.com

User1@east.contoso.com

User1@fabrikam.com

User1@fabrikam.onmicrosoft.com

User2:

User2@contoso.com

User2@east.contoso.com

User2@fabrikam.com

User2@fabrikam.onmicrosoft.com

Answer:

User1:

- User1@contoso.com
- User1@east.contoso.com
- User1@fabrikam.com
- User1@fabrikam.onmicrosoft.com

User2:

- User2@contoso.com
- User2@east.contoso.com
- User2@fabrikam.com
- User2@fabrikam.onmicrosoft.com

Explanation

User1:

- User1@contoso.com
- User1@east.contoso.com
- User1@fabrikam.com
- User1@fabrikam.onmicrosoft.com

User2:

- User2@contoso.com
- User2@east.contoso.com
- User2@fabrikam.com
- User2@fabrikam.onmicrosoft.com

If you added the contoso.com and east.contoso.com domains as custom domains in Microsoft 365, then the users would be assigned their user principle names as Microsoft 365 usernames. However, the question does not state that you have added the domains as custom domains.

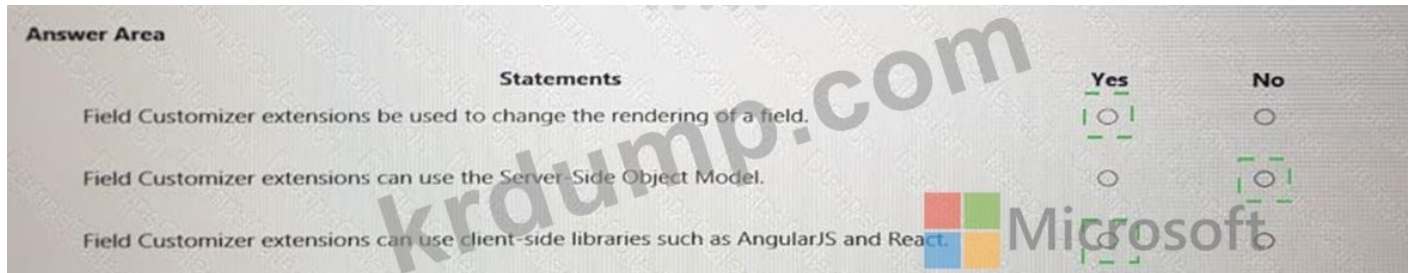
SPFx(SharePoint Framework) □□□□ □□□□ □□□□.

□□ □ □□□ □□ □□□□ □□□□ □□ □□□□□□. □□□□ □□□□ □□□□□□□□.

□□: □ □□□ □□□□ 1□□ □□□□ □□□□.



Answer:



Explanation

Graphical user interface, text, application, chat or text message Description automatically generated

Statements	Yes	No
Field Customizer extensions can be used to change the rendering of a field.	<input checked="" type="radio"/>	<input type="radio"/>
Field Customizer extensions can use the Server-Side Object Model.	<input type="radio"/>	<input checked="" type="radio"/>
Field Customizer extensions can use client-side libraries such as AngularJS and React.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/sharepoint/dev/spfx/extensions/get-started/building-simple-field-customizer#en>

<https://www.spguides.com/spfx-application-customizer/>

NEW QUESTION: 168

□□ □□ □□□□ □□□□ □□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Windows Defender ATP(Advanced Threat Protection) Windows Defender ATP

Name	Permission	Assigner user group
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Windows Defender ATP

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

Statements

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>
User2 can sign in to Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>
User3 can view Device1 in Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in to Windows Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can view Device1 in Windows Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation

The Get-MsolAccountSku cmdlet returns all the SKUs that the company owns. It does not tell you which licenses are assigned to users.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolaccountsku?view=azureadps-1.0>

NEW QUESTION: 170

□□□□□ Azure AD(Azure Active Directory) □ □□□□ □ □□□□ Active Directory □□ □□ □□□□ □□□□.

□□□□□ □□□□□□ Microsoft SharePoint Server 2019 □□ □□□□ □□□□.

□□□ Microsoft 365 □□□ □□□□□.

□□ □□ □□□ □□□□ □□□□.

Name	Source
User1	Windows Active Directory
User2	Azure Active Directory

SharePoint □□□□□ □□ □□□□ □□□□ □ □□□ □□□ User1 □ User2□ □□□ □□ □□□.

User1□ □□□□□ □□ □□□ □□□□ User2□ □□□□ □□ □□□ □□□□□.

User2□□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

User2□□ □□ □□□ □□□□ □□□?

- A. □□□□□□ □□□
- B. SharePoint □ □□□
- C. □□□ □□□
- D. SharePoint □□□

Answer: C (LEAVE A REPLY)

Explanation

To run the SharePoint Hybrid Configuration Wizard, you need to provide credentials of a user (in this case User2) of a Global Administrator account in Azure Active Directory.

Reference:

<https://www.c-sharpcorner.com/article/sharepoint-2019-enable-hybrid-experience/>
<https://docs.microsoft.com/en-us/sharepoint/hybrid/accounts-needed-for-hybrid-configuration-and-testing>

NEW QUESTION: 171

□□□□ □□ □□ □□□ □□□□ □□□□ Microsoft Azure Active Directory(Azure AD) □□□ □ □□□□.

Name	Role
User1	Privileged role administrator
User2	User administrator
User3	Security administrator
User4	Billing administrator

Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group.

Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group.

Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group.

User3 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group.

Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group.

Admin1 is a group. Admin1 is a group. Admin1 is a group. Admin1 is a group.

Create guest user accounts

- Microsoft
- User4 only
- User2 only
- User3 only
- User2 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Add User3 to Admin1:

- User4 only
- User2 only
- User3 only
- User2 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Answer:

Microsoft

Create guest user accounts: ▼

- User4 only
- User2 only
- User3 only
- User2 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Add User3 to Admin1: ▼

- User4 only
- User2 only
- User3 only
- User2 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Explanation

Microsoft

Create guest user accounts: ▼

- User4 only
- User2 only
- User3 only
- User2 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Add User3 to Admin1: ▼

- User4 only
- User2 only
- User3 only
- User2 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

References:

A User Administrator is the only role listed that can create user accounts included Guest user accounts. A Global Administrator can also create user accounts.

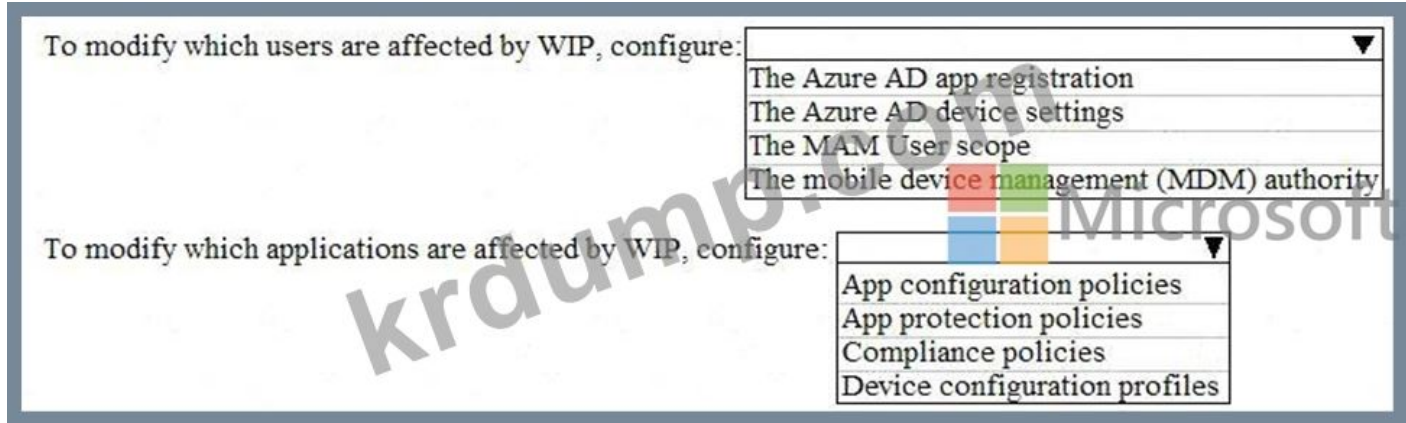
A User Administrator is also the only role listed that can modify the group membership of users.

Reference:

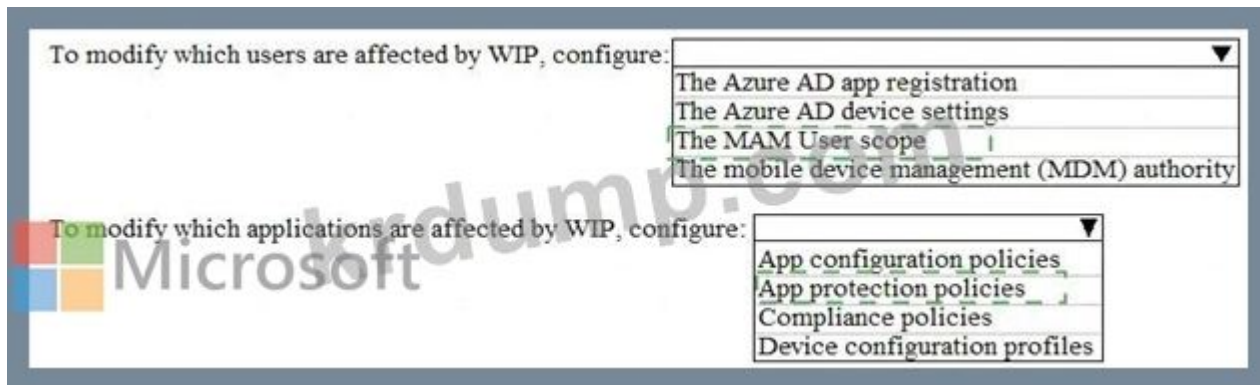
<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles>

NEW QUESTION: 172

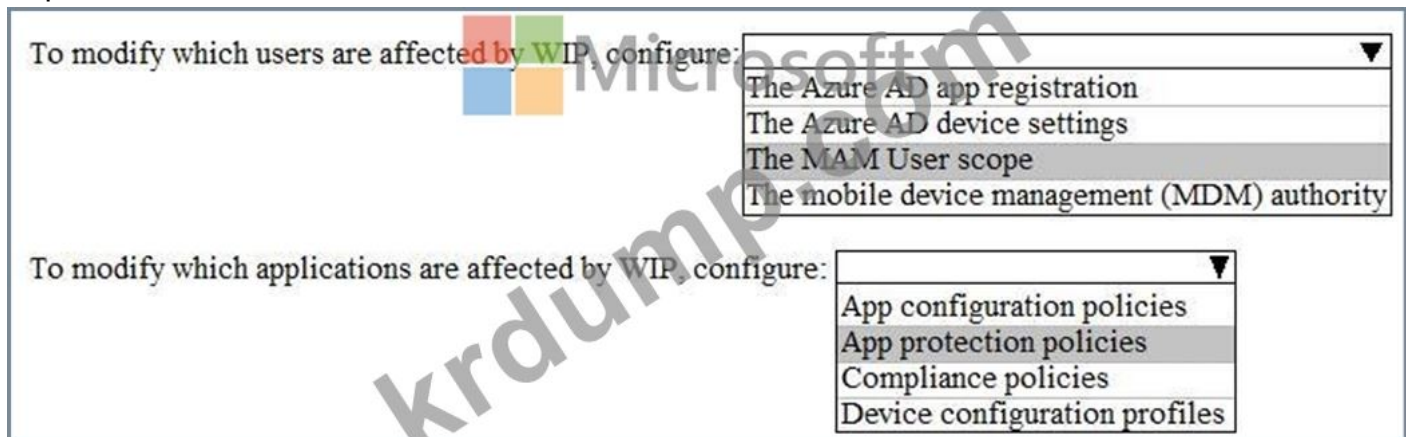
Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.
□□□□ WIP(Windows Information Protection)□ □□□□□.
WIP□ □□□ □□ □□□ □ □□ □□□□□□ □□□□ □□□□.
□□□□ □□ □□□□? □□□□□□ □□ □□□□□ □□□ □□□ □□□□□□□□.
□□: □ □□□ □□□□ 1□□ □□□ □□□□□.



Answer:



Explanation



Microsoft Intune has an easy way to create and deploy a Windows Information Protection (WIP) policy. You can choose which apps to protect, the level of protection, and how to find enterprise data on the network. The devices can be fully managed by Mobile Device Management (MDM),

Microsoft 365 admin center: [admin@LODSe426243.onmicrosoft.com](https://admin.microsoft.com)
Microsoft 365 tenant ID: 3&YWyjse-6-d
Microsoft 365 tenant ID: 10887751
Nestor Wilke is a Microsoft 365 tenant. Nestor Wilke is a Microsoft 365 tenant.
Nestor Wilke is a Microsoft 365 tenant. Nestor Wilke is a Microsoft 365 tenant.

Microsoft 365 admin center:

admin@LODSe426243.onmicrosoft.com

Microsoft 365 tenant ID: 3&YWyjse-6-d

Microsoft 365 tenant ID: 10887751
Microsoft 365 tenant ID: 10887751

Microsoft 365 tenant ID: 10887751

Microsoft 365 tenant ID: 10887751

Nestor Wilke is a Microsoft 365 tenant. Nestor Wilke is a Microsoft 365 tenant.
Nestor Wilke is a Microsoft 365 tenant. Nestor Wilke is a Microsoft 365 tenant.

Nestor Wilke is a Microsoft 365 tenant. Nestor Wilke is a Microsoft 365 tenant.

Answer:

See explanation below.

Explanation

You need to sign-in status for the account to 'Blocked'. Blocking doesn't stop the account from receiving email and it doesn't delete any data.

1. On the home page of the Microsoft 365 admin center, type the user's name into the Search box.
2. Select the Nestor Wilke account in the search results.
3. In the 'Sign-in status' section of the account properties, click the Edit link.
4. Select 'Block the user from signing in' and click the Save button.

NEW QUESTION: 175

Microsoft 365 admin center: [admin@LODSe426243.onmicrosoft.com](https://admin.microsoft.com)
Microsoft 365 tenant ID: 3&YWyjse-6-d
Microsoft 365 tenant ID: 10887751
Nestor Wilke is a Microsoft 365 tenant. Nestor Wilke is a Microsoft 365 tenant.
Nestor Wilke is a Microsoft 365 tenant. Nestor Wilke is a Microsoft 365 tenant.

Microsoft 365 user: admin@LODSe503797.onmicrosoft.com
Microsoft 365 user: x?-ofP?fG70o
Microsoft 365 user: CTRL-K
Microsoft 365 user: 11325860



Microsoft 365 user: dev@fabrikam.com
Microsoft 365 user: [unclear]
Microsoft 365 user: [unclear]

Answer:

See explanation below.

Explanation

You need to create a guest account for the external user and assign the Application Developer role. As the user's domain is an external domain, you will need to 'invite' the user. The external user will need to accept the invitation to create the account.

1. Go to the Azure Active Directory Admin Center.
2. In the left navigation pane, select Users.
3. Click on the '+ New Guest User' link.
4. Ensure that the 'Invite user' option is selected.
5. Enter dev@fabrikam.com in the email address field.
6. In the Roles section, 'user' will be selected by default. Click on 'user' to open a list of roles.
7. Select Application Developer in the list and click the 'Select' button to assign the role.

□ □□□ □□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□□ □□□ □ □□□
□□ □□(□: □□ □ □□□□, □□ □ □□□ □□ □□)□ □□□ □□□□□□□.
□□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□. □, □□□ □□□ □□□□□□ □
□□□ □□□ □□□□□ □□□□ □□ □□□ □□ □□□□ □□ □□□.
□□ □□□ □□□ □□□□ □□□ □ □□□□ □□□□ □□ □□□ □ □ □□ □□ □ □□□□
□. □ □□□ □□□□ □ □□□ □□ □□□ □□□ □ □□□□. □□□ □□□ □□ □□ □□
□□□ □□ □□ □□□ □□□ □ □□□ □□□ □□□□ □□□□ □□□□ □□□.
□ □□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □ □□□□.
□□ □□□ □□□□ □□□ □□□ □ □□□□.
□□□ □□
□□□ □□ □□ □□□ □□ □□□ □□□□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□ □□□ □□□ □□□□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□□□.

Microsoft 365 □□□ □□:

admin@M365x981607.onmicrosoft.com

Microsoft 365 □□: *yfLo7lr2&y-

Microsoft 365 □□□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□
□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

□ □□□□: 10811525

□□□ □□ □□□□□ Windows 10 □□□ Microsoft Azure Active Directory(Azure AD)□ □□
□□ □ □□ □□□ □□□ □□□□□.

□□□□□ □□□□ □□ □□□□ □□□ □□□ □□□□□ □□□□ □□□.

Answer:

See explanation below.

Explanation

You need to configure the device settings in Azure Active Directory.

1. Go to the Azure Active Directory admin center.
2. Select Azure Active Directory.
3. Select Devices.
4. Select Device Settings.
5. Toggle the 'Require Multi-Factor Auth to join devices' setting to Yes.
6. Click Save to save the changes.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

NEW QUESTION: 179

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □
□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□ □□□
□□□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□

□□□ □□□□ □□□□.

□□□□□□ Microsoft Azure Active Directory(Azure AD)□ □□□□□ contoso.com□□□
Active Directory □□□□ □□□□ □□□□.

Microsoft System Center Configuration Manager(□□ □□)□ □□□□ Windows 10 □□□□□
□□□□□.

□□ □□□ □□ □□□□ □□□□□.

Device1□□□ □ □□□ □□□□ □□□□□. Device1□ Configuration Manager □□□□□□
□□□□□.

Microsoft Intune □ Configuration Manager□ □□□□ Device1□ □□□ □ □□□ □□□□ □
□□.

□□□: Device1□ Active Directory □□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

Explanation

Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.

To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection, not an Active Directory Group. Therefore, this solution does not meet the requirements.

Reference:

<https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable>

NEW QUESTION: 180

User1□□□ □□□□ □□□□ contoso.com□□□ Microsoft Azure Active Directory(Azure AD)
□□□□ □□□□.

contoso.com□ □□ □□□ □□□ □□□□□ □□□□ □□ □ □□ □□ □□ □□□ □□□□
□.

□□□□ □□ □□□ □□□□□ □□ □□: □□

□□ □□ □□□ □□ □□: □□

□□□ □□□□□ □□ □□ □□□ □□□□ □□□□□ □□□□ □□□.

□□□□□ □□□ □□□ □□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□
□.


□□: □ □□□ □□□ 1□□ □□□ □□□□□.

A user can report fraud on her account by:

- Typing a special code after receiving an alert call
- Sending an email message to an administrator
- Using the Microsoft Authenticator app

If User1 reports fraud on his account, the account will be blocked automatically for:

- 6 hours
- 1 day
- 7 days
- 90 days



Answer:

A user can report fraud on her account by:

- Typing a special code after receiving an alert call
- Sending an email message to an administrator
- Using the Microsoft Authenticator app

If User1 reports fraud on his account, the account will be blocked automatically for:

- 6 hours
- 1 day
- 7 days
- 90 days


Explanation

A user can report fraud on her account by:

- Typing a special code after receiving an alert call
- Sending an email message to an administrator
- Using the Microsoft Authenticator app

If User1 reports fraud on his account, the account will be blocked automatically for:

- 6 hours
- 1 day
- 7 days
- 90 days



Code to report fraud during initial greeting: When users receive a phone call to perform two-step verification, they normally press # to confirm their sign-in. To report fraud, the user enters a code before pressing #. This code is 0 by default, but you can customize it.

Block user when fraud is reported: If a user reports fraud, their account is blocked for 90 days or until an administrator unblocks their account. An administrator can review sign-ins by using the sign-in report, and take appropriate action to prevent future fraud. An administrator can then unblock the user's account.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert>

NEW QUESTION: 181

litwareinc.com Microsoft 365

Microsoft Teams

External access

External access lets your Teams and Skype for Business users communicate with other users that are outside of your organization. By default, your organization can communicate with all external domains. If you add blocked domains, all other domains will be allowed but if you add allowed domains, all other domains will be blocked. [Learn more](#)

Users can communicate with other Skype for Business and Teams users

Off

Users can communicate with Skype users

Off

+ Add a domain



Name

Status

contoso.com

Allowed



Microsoft

Save

Discard

adventureworks.com 3 litwareinc.com
Microsoft Teams

User1@contoso.com

User2@adventureworks.com

litwareinc.com
1

Statements	Yes	No
User2@adventureworks.com can share files by using a Microsoft Teams channel of litwareinc.com.	<input type="radio"/>	<input type="radio"/>
User1@contoso.com can use Meet now in Microsoft Teams.	<input type="radio"/>	<input type="radio"/>
Litwareinc.com users can block user1@contoso.com in Microsoft Teams.	<input type="radio"/>	<input type="radio"/>

Answer:



Statements

Yes

No

User2@adventureworks.com can share files by using a Microsoft Teams channel of litwareinc.com.



User1@contoso.com can use Meet now in Microsoft Teams.



Litwareinc.com users can block user1@contoso.com in Microsoft Teams.



Explanation

Graphical user interface, text, application Description automatically generated

Statements	Yes	No
User2@adventureworks.com can share files by using a Microsoft Teams channel of litwareinc.com.	<input type="radio"/>	<input type="radio"/>
User1@contoso.com can use Meet now in Microsoft Teams.	<input type="radio"/>	<input type="radio"/>
Litwareinc.com users can block user1@contoso.com in Microsoft Teams.	<input type="radio"/>	<input type="radio"/>

The answer to this question depends on whether User1 and User2 have been added as guests. The question does not say that they are guests so we would have to assume they're not. External Access is turned off. Even with the Contoso.com domain added as an allowed domain, the Off settings override this. If the external access settings were 'On', they would be on for only the Contoso.com domain.

Box 1: No

If External Access was On, the answer to this would still be No. If User2 was a guest, the answer to this would be Yes.

Box 2: No

If External Access was On, the answer to this would still be No. External Access does not enable Meet Now for the external user. If User1 was a guest, the answer to this would be Yes.

Box 3: No

If External Access was On, the answer to this would still be No. External Access does not allow blocking. If User1 was a guest, the answer to this would be Yes.

Reference:

<https://docs.microsoft.com/en-us/microsoftteams/set-up-guests>

<https://docs.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organizations>



App1 Group1

On Device1, Office 365 ProPlus will be installed and the display language will be German.
 On Device2, Office 365 ProPlus will be installed and both the German and English display languages will be installed.
 On Device3, Office 365 ProPlus will be installed and both the German and French display languages will be installed.

Statements

	Yes	No
On Device1, Office 365 ProPlus will be installed and the display language will be German.	<input type="radio"/>	<input type="radio"/>
On Device2, Office 365 ProPlus will be installed and both the German and English display languages will be installed.	<input type="radio"/>	<input type="radio"/>
On Device3, Office 365 ProPlus will be installed and both the German and French display languages will be installed.	<input type="radio"/>	<input type="radio"/>

Answer:



Statements

Yes

No

On Device1, Office 365 ProPlus will be installed and the display language will be German.

On Device2, Office 365 ProPlus will be installed and both the German and English display languages will be installed.

On Device3, Office 365 ProPlus will be installed and both the German and French display languages will be installed.

Explanation



Statements

Yes

No

On Device1, Office 365 ProPlus will be installed and the display language will be German.

On Device2, Office 365 ProPlus will be installed and both the German and English display languages will be installed.

On Device3, Office 365 ProPlus will be installed and both the German and French display languages will be installed.

Box 1: No

Device1 is x86 (32-bit) so Office 365 will not be installed.

Box 2: Yes

Device2 is x64 (64-bit) so Office 365 will be installed. The German language pack will be installed and the OS language pack (English) will be installed.

Box 3: Yes

Device2 is x64 (64-bit) so Office 365 will be installed. The German language pack will be installed and the OS language pack (French) will be installed.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365>

NEW QUESTION: 184

Microsoft 565 □□□ □□□□.

□□□ □□□ □□□ □□□□ □□ □ □□□□□ □□□□ □□ □ □□□ □□□□ □□□.

□□□ □□ □□□?

A. □□ □□ □□□□ □□□□□□.

B. □□ □□ □□

C. □ □□□□ Microsoft 365 □□□□ □□ □□□□ □□□□□.

D. □□□□□ □□□ □□□□□□.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 185

MSALjs□ □□□□ □□□□ □□□□ SPA(□□ □□□ □□□□□□□)□ □□□□ □□□□□. SPA□ □□ □□ □□□ □□□□□ □□□.

* contoso.onmicrosoft.com□□□□ □□□□ □□□□□□□ □□□□□ □□□□□□.

* □□ □□□□ □□□□□ SSO(Single Sign-On)□ □□□□□□.

SPA□ □□□□ □□□□ □□□□ □□□□? □□□□□□ □□□□□ □□□ □□□ □□□□□□□□. □□: □ □□□ □□□□ 1□□ □□□□ □□□□□.



Answer:



Explanation



NEW QUESTION: 186

contoso.com□□□□ Microsoft Azure Active Directory(Azure AD) □□□□□ □□□□□.

contoso.com□ □□□□□□□□□□ □□□□□□□□ App1□□□□ □□ □□□□□□. App1□ □□□ □□ □□□□□□□□□□□ □□□□.

□□ □□□ □□ □□□?

- A. □□□ □ □□□ App1□ □□□□□.
- B. App1□ □□□□ □□□□□.
- C. App1□ □□ □□□□□ □□□ □□□□□.
- D. App1□ □□ SSO □□□ □□□□□.

Answer: C (LEAVE A REPLY)

Explanation

The provisioning mode (manual or automatic) needs to be configured for an app before you can enable self-service application access.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

MS-100-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-100-KR □□!
DumpTop □ □□ **MS-100-KR** □□ □□□ □□□□□□, DumpTop MS-100-KR □□ □□□
□□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-100-
KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/MS-100-KR-dump.html> (431
Q&As Dumps, **30%OFF Special Discount: KrDump**)