[2019-Aug-NewReal MS-300 Dumps PDF 107Q-Braindump2go[Q1-Q6

August/2019 Braindump2go MS-300 Exam Dumps with PDF and VCE New Updated! Following are some new MS-300 Exam Questions: 1.|2019 Latest Braindump2go MS-300 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/ms-300.html2.|2019 Latest Braindump2go MS-300 Exam Questions & Answers Instant Download:https://drive.google.com/drive/folders/1NAAz3y6CTjZbRBB0_c8l2rpLvhbgKmx1?usp=sharingQUESTION 1Case Study 1 -Litware, IncOverviewLitware, Inc. is a design and manufacturing company that has 4,500 users. The company has sales, marketing, design, research, field test, and human resources (HR) departments.Litware has a main office in California, three branch offices in the United States, and five branch offices in Europe.Existing EnvironmentOn-premises Infrastructure The network contains an Active Directory forest named litwareinc.com that contains a child domain for each region.All domain controllers run Windows Server 2012. The main office syncs identities to Microsoft Azure Active Directory (Azure AD) by using Azure AD Connect. All user accounts are created in the on-premises Active Directory and sync to Azure AD.Each office contains the following servers and client computers:- A domain controller that runs Windows Server 2012 - A file server that runs Windows Server 2012- Client computers that run Windows 10Currently, all content created by users is stored locally on file servers.Cloud Infrastructure Litware is moving the content from the file servers to Microsoft Office 265. The company purchases 4,500 Microsoft 365 E5 licenses.Litware uses Microsoft Exchange Online for email.Problem StatementsLitware identifies the following issues:- Finding content and people within the organization is difficult.- Users cannot access company data outside the corporate network.- Content recovery is slow because all the content is still on-premises.- Data security is compromised because users can copy company content to USB drives.- The locally stored content to USB drives.- Users must frequently contact the HR department to find employees within the organization who have relevant skills.- Users can delete content indiscriminately and without resource as they have full control of the content of the file servers.Business GoalsLitware identifies the following strategic initiatives to remain competitive:- All content must be stored centrally- Access to content must be based on the user's:1.Department2.Security level3.Physical location- Users must be able to work on content offline- Users must be able to share content externally- Content classifications from mobile devices- Content classifications must include a physical location- Content must be retained and protected based on its type- Litware must adhere to highly confidential regulatory standards that include:1.The ability to restrict the copying of all content created internally and externally2.Including accurate time zone reporting in audit trails- Users must be able to search for content and people across the entire organization.- Content classification metadata must adhere to naming conventions specified by the IT department.- Users must be able to access content quickly without having to review many pages of search results to find documents.- Security rules must be implemented so that user access can be revoked if a user shares confidential content with external users.Planned ChangesLitware plans to implement the following changes:- Move all department content to Microsoft SharePoint Online- Move all user content to Microsoft OneDrive for Business- Restrict user access based on location and deviceTechnical Requirements:Litware identifies the following technical requirements:- All on-premises documents (approximately one million documents) must be migrated to the SharePoint document library of their respective department.- Each department must have its own term store group. Stakeholders must be notified when term sets are moved or deleted.- All the OneDrive content of a user must be retained for a minimum of 180 days after the user has left the organization.- All external users must be used as the primary membership service for Microsoft Yammer, Teams, and SharePoint.- A user named Admin1 must be allowed to consume apps in the App Catalog and to add additional app license.- Viewers must be prevented from printing documents that are stored in a modern site named Finance.- Users must be prevented from printing content accessed in OneDrive from iOS and Android devices.- Retention, protection, and security policies must be implemented for all content stored online.- All offices must use the Managed Metadata Service to classify documents uploaded to SharePoint.- The Azure Information Protection client must be deployed to all domain-joined computers.- Searches must show results only when the result set is complete.- OneDrive must be used to work with documents offline.- Solutions must use the principle of least privilege whenever possible.What should you configure to meet the licensing requirements for Admin1?A. Add Admin1 to the App Catalog site owners group of the App Requests list.B. Assign Admin1 the SharePoint administrators of the App Catalog siteC. Add Admin1 to the site collection administrators of the App Catalog siteD. Add Admin1 as a License Manager of the apps.Answer: AExplanation: **https://docs.microsoft.com/en-us/sharepoint/administration/manage-the-app-catalog**QUESTION 2Case Study 1 -Litware, Inc OverviewLitware, Inc. is a design and manufacturing company that has 4,500 users. The company has sales, marketing, design, research, field test, and human resources (HR) departments.Litware has a main office in California, three branch offices in the United States, and five branch offices in Europe.Existing EnvironmentOn-premises Infrastructure The network contains an Active Directory forest named litwareinc.com that contains a child domain for each region.All domain controllers run Windows Server

2012. The main office syncs identities to Microsoft Azure Active Directory (Azure AD) by using Azure AD Connect. All user accounts are created in the on-premises Active Directory and sync to Azure AD.Each office contains the following servers and client computers:- A domain controller that runs Windows Server 2012 - A file server that runs Windows Server 2012- Client computers that run Windows 10Currently, all content created by users is stored locally on file servers.Cloud InfrastructureLitware is moving the content from the file servers to Microsoft Office 265. The company purchases 4,500 Microsoft 365 E5 licenses.Litware uses Microsoft Exchange Online for email.Problem StatementsLitware identifies the following issues:- Finding content and people within the organization is difficult.- Users cannot access company data outside the corporate network.- Content recovery is slow because all the content is still on-premises.- Data security is compromised because users can copy company content to USB drives.- The locally stored content to USB drives.- Users must frequently contact the HR department to find employees within the organization who have relevant skills.- Users can delete content indiscriminately and without resource as they have full control of the content of the file servers.Business GoalsLitware identifies the following strategic initiatives to remain competitive:- All content must be stored centrally- Access to content must be based on the user's:1.Department2.Security level3.Physical location- Users must be able to work on content offline- Users must be able to share content externally- Content classifications from mobile devices- Content classifications must include a physical location- Content must be retained and protected based on its type- Litware must adhere to highly confidential regulatory standards that include:1.The ability to restrict the copying of all content created internally and externally2.Including accurate time zone reporting in audit trails- Users must be able to search for content and people across the entire organization.- Content classification metadata must adhere to naming conventions specified by the IT department.- Users must be able to access content quickly without having to review many pages of search results to find documents.- Security rules must be implemented so that user access can be revoked if a user shares confidential content with external users.Planned ChangesLitware plans to implement the following changes:- Move all department content to Microsoft SharePoint Online- Move all user content to Microsoft OneDrive for Business- Restrict user access based on location and deviceTechnical Requirements:Litware identifies the following technical requirements:- All on-premises documents (approximately one million documents) must be migrated to the SharePoint document library of their respective department.- Each department must have its own term store group. Stakeholders must be notified when term sets are moved or deleted.- All the OneDrive content of a user must be retained for a minimum of 180 days after the user has left the organization.- All external users must be used as the primary membership service for Microsoft Yammer, Teams, and SharePoint.- A user named Admin1 must be allowed to consume apps in the App Catalog and to add additional app license.- Viewers must be prevented from printing documents that are stored in a modern site named Finance.- Users must be prevented from printing content accessed in OneDrive from iOS and Android devices.- Retention, protection, and security policies must be implemented for all content stored online.- All offices must use the Managed Metadata Service to classify documents uploaded to SharePoint.- The Azure Information Protection client must be deployed to all domain-joined computers.- Searches must show results only when the result set is complete.- OneDrive must be used to work with documents offline.- Solutions must use the principle of least privilege whenever possible.You need to recommend a solution for the documents stored in the Finance site.What should you recommend?A. Enable Azure Information policy labelingB. For each library, enable sensitivity labeling that uses protection.C. From Settings in the SharePoint admin center, enable Information Rights Management (IRM) for SharePoint Online.D. Enable an Information Rights Management (IRM) policy for the libraries.Answer: DExplanation: **https://support.office.com/en-us/article/apply-information-rights-management-to-a-list-or-library-3bdb5c4e-94fc-4741-b02f-4e7cc3c54aa1**QUESTION 3Case Study 1 -Litware, IncOverviewLitware, Inc. is a design and manufacturing company that has 4,500 users. The company has sales, marketing, design, research, field test, and human resources (HR) departments.Litware has a main office in California, three branch offices in the United States, and five branch offices in Europe.Existing Environment On-premises Infrastructure The network contains an Active Directory forest named litwareinc.com that contains a child domain for each region.All domain controllers run Windows Server 2012. The main office syncs identities to Microsoft Azure Active Directory (Azure AD) by using Azure AD Connect. All user accounts are created in the on-premises Active Directory and sync to Azure AD. Each office contains the following servers and client computers:- A domain controller that runs Windows Server 2012 - A file server that runs Windows Server 2012- Client computers that run Windows 10Currently, all content created by users is stored locally on file servers.Cloud InfrastructureLitware is moving the content from the file servers to Microsoft Office 265. The company purchases 4,500 Microsoft 365 E5 licenses.Litware uses Microsoft Exchange Online for email.Problem StatementsLitware identifies the following issues:- Finding content and people within the organization is difficult.- Users cannot access company data outside the corporate network.- Content recovery is slow because all the content is still on-premises.- Data security is compromised because users can copy company content to USB drives.- The locally stored content to USB drives.- Users must frequently contact the HR department to find employees within the organization who have relevant skills.- Users can delete content indiscriminately and without resource as they have full control of the content of the file servers.Business GoalsLitware identifies the following strategic initiatives to remain competitive:- All content must be stored centrally- Access to content must be based on the user's:1.Department 2.Security level3.Physical location- Users must be able to work on content offline- Users must be able to share content externally- Content classifications from mobile devices- Content classifications must include a physical location- Content must be retained and protected based on its type- Litware must adhere to highly confidential regulatory standards that include:1.The ability to restrict the copying of all content created internally and externally2.Including accurate time zone reporting in audit trails- Users must be able to search for content and people across the entire organization.- Content classification metadata must adhere to naming conventions specified by the IT department.- Users must be able to access content quickly without having to review many pages of search results to find documents.- Security rules must be implemented so that user access can be revoked if a user shares confidential content with external users.Planned ChangesLitware plans to implement the following changes:- Move all department content to Microsoft SharePoint Online- Move all user content to Microsoft OneDrive for Business- Restrict user access based on location and device Technical Requirements:Litware identifies the following technical requirements:- All on-premises documents (approximately one million documents) must be migrated to the SharePoint document library of their respective department.- Each department must have its own term store group. Stakeholders must be notified when term sets are moved or deleted.- All the OneDrive content of a user must be retained for a minimum of 180 days after the user has left the organization.- All external users must be used as the primary membership service for Microsoft Yammer, Teams, and SharePoint.- A user named Admin1 must be allowed to consume apps in the App Catalog and to add additional app license.- Viewers must be prevented from printing documents that are stored in a modern site named Finance.- Users must be prevented from printing content accessed in OneDrive from iOS and Android devices.- Retention, protection, and security policies must be implemented for all content stored online.- All offices must use the Managed Metadata Service to classify documents uploaded to SharePoint.- The Azure Information Protection client must be deployed to all domain-joined computers.- Searches must show results only when the result set is complete.- OneDrive must be used to work with documents offline.- Solutions must use the principle of least privilege whenever possible.You need to grant an external user guest access to the SharePoint site of the design department.What should you do?A. From the SharePoint team site, modify the Visitors group.B. From the SharePoint team site, modify the Members groupC. From Microsoft Outlook, add a member to a group. **Answer: C**QUESTION 4Case Study 1 -Litware, IncOverviewLitware, Inc. is a design and manufacturing company that has 4,500 users. The company has sales, marketing, design, research, field test, and human resources (HR) departments.Litware has a main office in California, three branch offices in the United States, and five branch offices in Europe.Existing EnvironmentOn-premises Infrastructure The network contains an Active Directory forest named litwareinc.com that contains a child domain for each region. All domain controllers run Windows Server 2012. The main office syncs identities to Microsoft Azure Active Directory (Azure AD) by using Azure AD Connect. All user accounts are created in the on-premises Active Directory and sync to Azure AD.Each office contains the following servers and client computers:- A domain controller that runs Windows Server 2012 - A file server that runs Windows Server 2012- Client computers that run Windows 10Currently, all content created by users is stored locally on file servers. Cloud InfrastructureLitware is moving the content from the file servers to Microsoft Office 265. The company purchases 4,500 Microsoft 365 E5 licenses.Litware uses Microsoft Exchange Online for email.Problem StatementsLitware identifies the following issues:- Finding content and people within the organization is difficult.- Users cannot access company data outside the corporate network.- Content recovery is slow because all the content is still on-premises.- Data security is compromised because users can copy company content to USB drives.- The locally stored content to USB drives.- Users must frequently contact the HR department to find employees within the organization who have relevant skills.- Users can delete content indiscriminately and without resource as they have full control of the content of the file servers.Business GoalsLitware identifies the following strategic initiatives to remain competitive:- All content must be stored centrally- Access to content must be based on the user's:1.Department2.Security level3.Physical location- Users must be able to work on content offline- Users must be able to share content externally- Content classifications from mobile devices- Content classifications must include a physical location- Content must be retained and protected based on its type- Litware must adhere to highly confidential regulatory standards that include:1.The ability to restrict the copying of all content created internally and externally2.Including accurate time zone reporting in audit trails- Users must be able to search for content and people across the entire organization.- Content classification metadata must adhere to naming conventions specified by the IT department.- Users must be able to access content quickly without having to review many pages of search results to find documents.- Security rules must be implemented so that user access can be revoked if a user shares confidential content with external users.Planned ChangesLitware plans to implement the following changes:- Move all department content to Microsoft SharePoint Online- Move all user content to Microsoft OneDrive for Business- Restrict user access based on location and device Technical Requirements:Litware identifies the following technical requirements:- All on-premises documents (approximately one million documents) must be migrated to the SharePoint document library of their respective department.- Each department must have its own term store group. Stakeholders must be notified when term sets are moved or deleted.- All the OneDrive content of a user must be retained for a minimum of 180 days after the user has left the organization.- All external users must be used as the primary membership service for Microsoft Yammer, Teams, and SharePoint.- A user named Admin1 must be allowed to consume apps in the App Catalog and to add additional app license.- Viewers must be prevented from printing documents that are stored in a modern site named Finance.- Users must be prevented from printing content accessed in OneDrive from iOS and Android devices.- Retention, protection, and security policies must be implemented for all content stored online.- All offices must use the Managed Metadata Service to classify documents uploaded to SharePoint.- The Azure Information Protection client must be deployed to all domain-joined computers.- Searches must show results only when the result set is complete.- OneDrive must be used to work with documents offline.- Solutions must use the principle of least privilege whenever possible.You need to minimize the number of documents returned during searches. The solution must meet the technical requirements.What should you configure?A.   Add a result source and prevent partial search results from being returned.B.   Create a managed property for each document type.C.   Create a crawled property for each document type.D.   Add a query transform to restrict results to certain documents types.Answer: AExplanation:**https://docs.microsoft.com/en-us/sharepoint/search/understanding-result-sources-for-search**QUESTION 5Case Study 1 -Litware, IncOverviewLitware, Inc. is a design and manufacturing company that has 4,500 users. The company has sales, marketing, design, research, field test, and human resources (HR) departments.Litware has a main office in California, three branch offices in the United States, and five branch offices in Europe.Existing EnvironmentOn-premises Infrastructure The network contains an Active Directory forest named litwareinc.com that contains a child domain for each region.All domain controllers run Windows Server 2012. The main office syncs identities to Microsoft Azure Active Directory (Azure AD) by using Azure AD Connect. All user accounts are created in the on-premises Active Directory and sync to Azure AD.Each office contains the following servers and client computers:- A domain controller that runs Windows Server 2012 - A file server that runs Windows Server 2012- Client computers that run Windows 10Currently, all content created by users is stored locally on file servers.Cloud Infrastructure Litware is moving the content from the file servers to Microsoft Office 265. The company purchases 4,500 Microsoft 365 E5 licenses.Litware uses Microsoft Exchange Online for email.Problem StatementsLitware identifies the following issues:- Finding content and people within the organization is difficult.- Users cannot access company data outside the corporate network.- Content recovery is slow because all the content is still on-premises.- Data security is compromised because users can copy company content to USB drives.- The locally stored content to USB drives.- Users must frequently contact the HR department to find employees within the organization who have relevant skills.- Users can delete content indiscriminately and without resource as they have full control of the content of the file servers.Business GoalsLitware identifies the following strategic initiatives to remain competitive:- All content must be stored centrally- Access to content must be based on the user's:1.Department2.Security level3.Physical location- Users must be able to work on content offline- Users must be able to share content externally- Content classifications from mobile devices- Content classifications must include a physical location- Content must be retained and protected based on its type- Litware must adhere to highly confidential regulatory standards that include:1.The ability to restrict the copying of all content created internally and externally2.Including accurate time zone reporting in audit trails- Users must be able to search for content and people across the entire organization.- Content classification metadata must adhere to naming conventions specified by the IT department.- Users must be able to access content quickly without having to review many pages of search results to find documents.- Security rules must be implemented so that user access can be revoked if a user shares confidential content with external users.Planned ChangesLitware plans to implement the following changes:- Move all department content to Microsoft SharePoint Online- Move all user content to Microsoft OneDrive for Business- Restrict user access based on location and deviceTechnical Requirements:Litware identifies the following technical requirements:- All on-premises documents (approximately one million documents) must be migrated to the SharePoint document library of their respective department.- Each department must have its own term store group. Stakeholders must be notified when term sets are moved or deleted.- All the OneDrive content of a user must be retained for a minimum of 180 days after the user has left the organization.- All external users must be used as the primary membership service for Microsoft Yammer, Teams, and SharePoint.- A user named Admin1 must be allowed to consume apps in the App Catalog and to add additional app license.- Viewers must be prevented from printing documents that are stored in a modern site named Finance.- Users must be prevented from printing content accessed in OneDrive from iOS and Android devices.- Retention, protection, and security policies must be implemented for all content stored online.- All offices must use the Managed Metadata Service to classify documents uploaded to SharePoint.- The Azure Information Protection client must be deployed to all domain-joined computers.- Searches must show results only when the result set is complete.- OneDrive must be used to work with documents offline.- Solutions must use the principle of least privilege whenever possible.You need to meet the technical requirements for OneDrive mobile users.

Which settings should you configure from the OneDrive admin center?A. Device accessB. StorageC. SharingD. ComplianceAnswer: AExplanation:**https://docs.microsoft.com/en-us/onedrive/control-access-to-mobile-app-features** QUESTION 6Case Study 2 - Contoso, LtdOverviewContoso, Ltd. is a pharmaceutical company that has 750 users. Contoso has departmental teams spread across offices in North America.The company has a main office in Seattle and four branch offices in New York, New jersey, Boston, and Florida.Existing EnvironmentActive Directory EnvironmentThe network contains an on-premises Active Directory domain. All the users use their domain credentials to sign in to their computer.Microsoft Office 365 Environment Contoso has a Microsoft Office 365 subscription and uses the following services:- OneDrive for Business- SharePoint Online- Exchange Online- Yammer- TeamsCurrently, the identity of each user is maintained in both on-premises Active Directory and Office 365.Contoso implements SharePoint site collections for the following departments:- Research & development- Human resources (HR)- Marketing- Finance- ITEach department assigns a site owner to manage its site collection and to manage access. The site collection of each department contains multiple subsites. Sharing is allowed across different site collections by default. External sharing is enabled for the organization.Current Business ModelContoso has the following business model:- The HR department has a branded site collection- Currently, the default storage limit is set for all the site collections- The marketing department uses multiple site collections created by an administrator named Admin1.- Contoso has a strategic partnership with a company name Litware, Inc. Litware has an Office 365 subscription. All users at Litware have a user account in the litwareinc.com domain.Problem StatementsContoso identifies the following issues:- Non-site owners invite external users to access the content in SharePoint Online.- Users upload audio, video, and executable program files to OneDrive for Business.- The company manages two separate identities for each user, which creates more administrative work.- Users in the HR department report performance issues affecting their site collection. You suspect that the issues are due to large images on the home page.Technical RequirementsContoso has the following technical requirements for the Office 365 environment:- Add a Yammer feed to new communication sites.- Prevent non-site owners from inviting external users.- Troubleshoot the performance issues of the HR department site collection.- Increase a 100-GB storage limit for the site collection of the marketing department.- Prevent users from syncing media files, such as MP3 and MP4 files, from OneDrive.- Restrict users from sharing content from the finance department site collection to the Litware users.- Ensure that SharePoint administrators do not have administrative permissions to the site collections.- Ensure that the managers in the marketing department can view the storage metrics of the marketing department sites.- Maintain all user identities in on-premises Active Directory. Sync passwords to Microsoft Azure Active Directory (Azure AD).- Ensure that when users are deleted from Microsoft 365 their associated OneDrive content is retained for 90 days. After 90 days, the content must be deleted permanently.You need to meet the technical requirements for the finance department site collection.What should you do?A. From the SharePoint admin center, select the finance department site collection, and then configure the Sharing settings.B. From the Security & Compliance admin center, create a classification label policy.C. From the Security & Compliance admin center, create a permission policy.D. From the SharePoint Admin center, select Sharing, and then select Limit external sharing using domains.Answer: AExplanation:
https://docs.microsoft.com/en-us/sharepoint/restricted-domains-sharing?redirectSourcePath=%252fen-us%252farticle%252fRestricted-Domains-Sharing-in-O365-SharePoint-Online-and-OneDrive-for-Business-5d7589cd-0997-4a00-a2ba-2320ec49c4e9!!!RECOMMEND!!!1.|2019 Latest Braindump2go MS-300 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/ms-300.html2.|2019 Latest Braindump2go MS-300 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=PueQURvxAGU