[New 70-347 DumpsExam Pass 100%!Braindump2go 70-347 Exam PDF 296Q Instant Download[272-282

2018 July New Microsoft 70-347 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 70-347 Real Exam Questions:1.|2018 Latest 70-347 Exam Dumps (PDF & VCE) 352Q&As Download:https://www.braindump2go.com/70-347.html2.|2018 Latest 70-347 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNflM5NTRpeEU2QjVSTTlFX3M4MEVQZ2NaR3VHZzFLSXZLUDU5N05adDlQckU?usp=sharingQUESTION 272You administer Office 365 tenant for an organization. You assign Enterprise E5 licenses to all users.You need to create a Microsoft Excel workbook and save the file on a local file share.You need to create a Microsoft PowerApp that uses the Excel workbook as its data source.What should you do?A. Convert the Excel workbook to a CSV file.B. Migrate the Excel workbook to an XML file in a cloud storage account.C. Migrate the Excel workbook to a CSV file in a cloud storage account.D. Copy the Excel workbook to a cloud storage account.Answer: DExplanation: **https://docs.microsoft.com/en-us/powerapps/maker/canvas-apps/connections/cloud-storage-blob-connections**QUESTION 273 You are the Office 365 administrator for a company. All accounts include the user's city, office, department, manager, and job title. Users must be able to view all user accounts from a specific department in a single list. The list must not be used to send email to the department.You need to configure Office 365.What should you do?A. In the Microsoft Exchange admin center, create a public Office 365 group.B. In the Microsoft Exchange admin center, create a shared mailbox.C. Connect to Microsoft Exchange Online by using Windows PowerShell and create an address list.D. In the Microsoft Exchange admin center, create a private Office 365 group.Answer: CExplanation:**https://technet.microsoft.com/en-us/library/bb125036(v=exchg.150).aspx**QUESTION 274You are the desktop administrator for a company. All desktops have Office 365 ProPlus installed. You need to ensure that the user can see data in the Telemetry Dashboard.What should you do?A. Add the user to the local Administrators group on the telemetry Dashboard server.B. Instruct the user to authenticate to the Microsoft SQL Server by using SQL Server authentication credentials. C. Instruct the user to authenticate to the Microsoft SQL Server by using Windows authentication.D. Add the user to the Domain Admins group.Answer: AExplanation:**https://docs.microsoft.com/en-us/deployoffice/compat/deploy-telemetry-dashboard** QUESTION 275You administer the Office 365 tenant for an organization. You assign Enterprise E5 licenses to all users.You observe that users share files from Microsoft OneDrive for Business storage in violation of organization policy.You need to ensure that you receive alerts when users share anything from their OneDrive for Business storage.Which two actions should you perform? Each correct answer presents part of the solution.NOTE: Each correct selection is worth one point.A. Create a new alert policy with a custom alert for a Sway activity.B. Create a new alert policy with a custom alert for an access request activity.C. Create a new alert policy with a custom alert for the shared file folder or site activity.D. Create a new alert policy with an elevation of privilege alert.E. Start recording user and admin activities in the Alerts node of the Security&Compliance Center.F. Create as alert in the OneDrive for Business client app.Answer: CEExplanation: **https://www.c-sharpcorner.com/article/alert-policies-in-the-office-365-security-compliance-center/**QUESTION 276 BackgroundContoso Ltd. manufactures and sells computers and related devices. Employees who work in the corporate headquarters use Microsoft Exchange Server, SharePoint Server, and Office 2016 to perform their daily job functions. Mobile and remote employees access resources in the on-premises environment by using VPN connections.The company plans to transition to Office 365. You purchase Office 365 Business Premium Licenses for all users. Contoso, Ltd. uses System Center 2012 R2 Configuration manager to manage desktop software. Office 365 environmentDeployment of all Office 365 applications must be controlled internally by administrators. Users must not have the ability to install Office 365 ProPlus on their own. All user initiated installations of Office 365 applications must be prohibited before administrative deployments are configured. All additional Office 365 licenses must employ the minimum cost to provide the required service. Integration between the on-premises and Office 365 environments must be configured where required.Corporate policiesServices must be configured to enforce the following security policies: All VPN connections must be secured by using a 256-bit, L2TP connection. All users must be use multi-factor authentication (MFA) when connecting over a VPN connection. All content, including emails and documents, must be retained for three years after the last modification. Any access to corporate content must require a user to sign in, even if the user is from an external partner organization and is not yet known to the other Office 365 environment. Sharing of credit card information must not be allowed through email, Microsoft OneDrive or SharePoint. All user passwords must be complex and expire every 30 days. Allow Gmail users from partner organizations to automatically open encrypted emails sent from Contoso, Ltd.Client connections All remote client connections to the on-premises environment must use a VPN connection. Internal and external users from partner organizations must be able to dial in to audio conferences by using their own mobile or landline phones. Users must be able to access content in the on-premises

SharePointServer environment seamlessly when connected to the SharePoint Online environment. When users create objects in Office 365 that require a time zone setting, the time zone must always be set to the Eastern Time (US & Canada) setting.Employees Employees must be able to perform the following actions: Access all resources by using their Contoso Active Directory domain user account. Invite users from business partners to participate in meetings. Coordinate scheduling using Microsoft StaffHub. All team settings should be consistent using a one-month schedule. Add users from external partner organizations to teams.File storageYou identify the following requirements for file storage: All users must store documents in OneDrive storage. All email attachments to on-premises Exchange Server mailboxes and Exchange Online mailboxes must be saved automatically to OneDrive. Users must be able to share documents from their OneDrive storage with other users including those in other organizations. Users must be notified only when someone else changes a document in their OneDrive. Each user may store up to 50 gigabytes (GB) in OneDrive. Users may request an increase to this limit by using a request process. The process is implemented as a SharePoint form in an on-premises SharePoint site.NOTE: This question is part of a series of questions that present the same scenario. Each question in the series holds a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.You need to configure external user sharing for One Drive.Solution: You set the value of the OneDrive default link type option to Internal.Does the solution meet the goal?A. YesB. NoAnswer: BExplanation:
https://support.office.com/en-us/article/manage-sharing-in-onedrive-and-sharepoint-ee8b91c5-05ec-44c2-9796-78fa27ec8425
QUESTION 277BackgroundContoso Ltd. manufactures and sells computers and related devices. Employees who work in the corporate headquarters use Microsoft Exchange Server, SharePoint Server, and Office 2016 to perform their daily job functions. Mobile and remote employees access resources in the on-premises environment by using VPN connections.The company plans to transition to Office 365. You purchase Office 365 Business Premium Licenses for all users. Contoso, Ltd. uses System Center 2012 R2 Configuration manager to manage desktop software. Office 365 environmentDeployment of all Office 365 applications must be controlled internally by administrators. Users must not have the ability to install Office 365 ProPlus on their own. All user initiated installations of Office 365 applications must be prohibited before administrative deployments are configured. All additional Office 365 licenses must employ the minimum cost to provide the required service. Integration between the on-premises and Office 365 environments must be configured where required.Corporate policiesServices must be configured to enforce the following security policies: All VPN connections must be secured by using a 256-bit, L2TP connection. All users must be use multi-factor authentication (MFA) when connecting over a VPN connection. All content, including emails and documents, must be retained for three years after the last modification. Any access to corporate content must require a user to sign in, even if the user is from an external partner organization and is not yet known to the other Office 365 environment. Sharing of credit card information must not be allowed through email, Microsoft OneDrive or SharePoint. All user passwords must be complex and expire every 30 days. Allow Gmail users from partner organizations to automatically open encrypted emails sent from Contoso, Ltd.Client connections All remote client connections to the on-premises environment must use a VPN connection. Internal and external users from partner organizations must be able to dial in to audio conferences by using their own mobile or landline phones. Users must be able to access content in the on-premises SharePointServer environment seamlessly when connected to the SharePoint Online environment. When users create objects in Office 365 that require a time zone setting, the time zone must always be set to the Eastern Time (US & Canada) setting.EmployeesEmployees must be able to perform the following actions: Access all resources by using their Contoso Active Directory domain user account. Invite users from business partners to participate in meetings. Coordinate scheduling using Microsoft StaffHub. All team settings should be consistent using a one-month schedule. Add users from external partner organizations to teams.File storageYou identify the following requirements for file storage: All users must store documents in OneDrive storage. All email attachments to on-premises Exchange Server mailboxes and Exchange Online mailboxes must be saved automatically to OneDrive. Users must be able to share documents from their OneDrive storage with other users including those in other organizations. Users must be notified only when someone else changes a document in their OneDrive. Each user may store up to 50 gigabytes (GB) in OneDrive. Users may request an increase to this limit by using a request process. The process is implemented as a SharePoint form in an on-premises SharePoint site.NOTE: This question is part of a series of questions that present the same scenario. Each question in the series holds a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.You need to configure external user sharing for One Drive.Solution: You set the value of the OneDrive External sharing option to Anyone.Does the solution meet the goal?A. YesB. NoAnswer: BExplanation:
https://support.office.com/en-us/article/manage-sharing-in-onedrive-and-sharepoint-ee8b91c5-05ec-44c2-9796-78fa27ec8425

QUESTION 278BackgroundContoso Ltd. manufactures and sells computers and related devices. Employees who work in the corporate headquarters use Microsoft Exchange Server, SharePoint Server, and Office 2016 to perform their daily job functions. Mobile and remote employees access resources in the on-premises environment by using VPN connections.The company plans to transition to Office 365. You purchase Office 365 Business Premium Licenses for all users. Contoso, Ltd. uses System Center 2012 R2 Configuration manager to manage desktop software. Office 365 environmentDeployment of all Office 365 applications must be controlled internally by administrators. Users must not have the ability to install Office 365 ProPlus on their own. All user initiated installations of Office 365 applications must be prohibited before administrative deployments are configured. All additional Office 365 licenses must employ the minimum cost to provide the required service. Integration between the on-premises and Office 365 environments must be configured where required.Corporate policiesServices must be configured to enforce the following security policies: All VPN connections must be secured by using a 256-bit, L2TP connection. All users must be use multi-factor authentication (MFA) when connecting over a VPN connection. All content, including emails and documents, must be retained for three years after the last modification. Any access to corporate content must require a user to sign in, even if the user is from an external partner organization and is not yet known to the other Office 365 environment. Sharing of credit card information must not be allowed through email, Microsoft OneDrive or SharePoint. All user passwords must be complex and expire every 30 days. Allow Gmail users from partner organizations to automatically open encrypted emails sent from Contoso, Ltd.Client connections All remote client connections to the on-premises environment must use a VPN connection. Internal and external users from partner organizations must be able to dial in to audio conferences by using their own mobile or landline phones. Users must be able to access content in the on-premises SharePointServer environment seamlessly when connected to the SharePoint Online environment. When users create objects in Office 365 that require a time zone setting, the time zone must always be set to the Eastern Time (US & Canada) setting.EmployeesEmployees must be able to perform the following actions: Access all resources by using their Contoso Active Directory domain user account. Invite users from business partners to participate in meetings. Coordinate scheduling using Microsoft StaffHub. All team settings should be consistent using a one-month schedule. Add users from external partner organizations to teams.File storageYou identify the following requirements for file storage: All users must store documents in OneDrive storage. All email attachments to on-premises Exchange Server mailboxes and Exchange Online mailboxes must be saved automatically to OneDrive. Users must be able to share documents from their OneDrive storage with other users including those in other organizations. Users must be notified only when someone else changes a document in their OneDrive. Each user may store up to 50 gigabytes (GB) in OneDrive. Users may request an increase to this limit by using a request process. The process is implemented as a SharePoint form in an on-premises SharePoint site.NOTE: This question is part of a series of questions that present the same scenario. Each question in the series holds a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.You need to configure external user sharing for One Drive.Solution: You set the value of the OneDrive External sharing option to New and existing external users.Does the solution meet the goal?A. YesB. NoAnswer: AExplanation:
https://support.office.com/en-us/article/manage-sharing-in-onedrive-and-sharepoint-ee8b91c5-05ec-44c2-9796-78fa27ec8425
QUESTION 279BackgroundContoso Ltd. manufactures and sells computers and related devices. Employees who work in the corporate headquarters use Microsoft Exchange Server, SharePoint Server, and Office 2016 to perform their daily job functions. Mobile and remote employees access resources in the on-premises environment by using VPN connections.The company plans to transition to Office 365. You purchase Office 365 Business Premium Licenses for all users. Contoso, Ltd. uses System Center 2012 R2 Configuration manager to manage desktop software. Office 365 environmentDeployment of all Office 365 applications must be controlled internally by administrators. Users must not have the ability to install Office 365 ProPlus on their own. All user initiated installations of Office 365 applications must be prohibited before administrative deployments are configured. All additional Office 365 licenses must employ the minimum cost to provide the required service. Integration between the on-premises and Office 365 environments must be configured where required.Corporate policiesServices must be configured to enforce the following security policies: All VPN connections must be secured by using a 256-bit, L2TP connection. All users must be use multi-factor authentication (MFA) when connecting over a VPN connection. All content, including emails and documents, must be retained for three years after the last modification. Any access to corporate content must require a user to sign in, even if the user is from an external partner organization and is not yet known to the other Office 365 environment. Sharing of credit card information must not be allowed through email, Microsoft OneDrive or SharePoint. All user passwords must be complex and expire every 30 days. Allow Gmail users from partner organizations to automatically open encrypted emails sent from Contoso, Ltd.Client connections All remote client connections to the on-premises environment must use a VPN connection. Internal and external users from partner

organizations must be able to dial in to audio conferences by using their own mobile or landline phones. Users must be able to access content in the on-premises SharePointServer environment seamlessly when connected to the SharePoint Online environment. When users create objects in Office 365 that require a time zone setting, the time zone must always be set to the Eastern Time (US & Canada) setting.EmployeesEmployees must be able to perform the following actions: Access all resources by using their Contoso Active Directory domain user account. Invite users from business partners to participate in meetings. Coordinate scheduling using Microsoft StaffHub. All team settings should be consistent using a one-month schedule. Add users from external partner organizations to teams.File storageYou identify the following requirements for file storage: All users must store documents in OneDrive storage. All email attachments to on-premises Exchange Server mailboxes and Exchange Online mailboxes must be saved automatically to OneDrive. Users must be able to share documents from their OneDrive storage with other users including those in other organizations. Users must be notified only when someone else changes a document in their OneDrive. Each user may store up to 50 gigabytes (GB) in OneDrive. Users may request an increase to this limit by using a request process. The process is implemented as a SharePoint form in an on-premises SharePoint site.You need to configure the Office 365 environment to enforce the information sharing policies.What must you create?A. a data loss prevention policy for financial dataB. a data loss prevention policy for privacy dataC. a device security policy for data encryption on deviceD. a data governance policyAnswer: A Explanation:
https://support.office.com/en-us/article/overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e#howworkQUESTION 280Hotspot QuestionBackgroundContoso Ltd. manufactures and sells computers and related devices. Employees who work in the corporate headquarters use Microsoft Exchange Server, SharePoint Server, and Office 2016 to perform their daily job functions. Mobile and remote employees access resources in the on-premises environment by using VPN connections. The company plans to transition to Office 365. You purchase Office 365 Business Premium Licenses for all users. Contoso, Ltd. uses System Center 2012 R2 Configuration manager to manage desktop software. Office 365 environmentDeployment of all Office 365 applications must be controlled internally by administrators. Users must not have the ability to install Office 365 ProPlus on their own. All user initiated installations of Office 365 applications must be prohibited before administrative deployments are configured. All additional Office 365 licenses must employ the minimum cost to provide the required service. Integration between the on-premises and Office 365 environments must be configured where required.Corporate policiesServices must be configured to enforce the following security policies: All VPN connections must be secured by using a 256-bit, L2TP connection. All users must be use multi-factor authentication (MFA) when connecting over a VPN connection. All content, including emails and documents, must be retained for three years after the last modification. Any access to corporate content must require a user to sign in, even if the user is from an external partner organization and is not yet known to the other Office 365 environment. Sharing of credit card information must not be allowed through email, Microsoft OneDrive or SharePoint. All user passwords must be complex and expire every 30 days. Allow Gmail users from partner organizations to automatically open encrypted emails sent from Contoso, Ltd.Client connections All remote client connections to the on-premises environment must use a VPN connection. Internal and external users from partner organizations must be able to dial in to audio conferences by using their own mobile or landline phones. Users must be able to access content in the on-premises SharePointServer environment seamlessly when connected to the SharePoint Online environment. When users create objects in Office 365 that require a time zone setting, the time zone must always be set to the Eastern Time (US & Canada) setting.EmployeesEmployees must be able to perform the following actions: Access all resources by using their Contoso Active Directory domain user account. Invite users from business partners to participate in meetings. Coordinate scheduling using Microsoft StaffHub. All team settings should be consistent using a one-month schedule. Add users from external partner organizations to teams.File storageYou identify the following requirements for file storage: All users must store documents in OneDrive storage. All email attachments to on-premises Exchange Server mailboxes and Exchange Online mailboxes must be saved automatically to OneDrive. Users must be able to share documents from their OneDrive storage with other users including those in other organizations. Users must be notified only when someone else changes a document in their OneDrive. Each user may store up to 50 gigabytes (GB) in OneDrive. Users may request an increase to this limit by using a request process. The process is implemented as a SharePoint form in an on-premises SharePoint site.You need to implement the email attachment requirements. What should you implement? To answer, select the appropriate option in the answer area.NOTE: Each correct selection is worth one point. Answer: Explanation:**https://flow.microsoft.com/en-us/pricing/**QUESTION 281Drag and Drop QuestionBackground Contoso Ltd. manufactures and sells computers and related devices. Employees who work in the corporate headquarters use Microsoft Exchange Server, SharePoint Server, and Office 2016 to perform their daily job functions. Mobile and remote employees access resources in the on-premises environment by using VPN connections.The company plans to transition to Office 365. You purchase Office 365 Business Premium Licenses for all users. Contoso, Ltd. uses System Center 2012 R2 Configuration manager to

manage desktop software. Office 365 environmentDeployment of all Office 365 applications must be controlled internally by administrators. Users must not have the ability to install Office 365 ProPlus on their own. All user initiated installations of Office 365 applications must be prohibited before administrative deployments are configured. All additional Office 365 licenses must employ the minimum cost to provide the required service. Integration between the on-premises and Office 365 environments must be configured where required.Corporate policiesServices must be configured to enforce the following security policies: All VPN connections must be secured by using a 256-bit, L2TP connection. All users must be use multi-factor authentication (MFA) when connecting over a VPN connection. All content, including emails and documents, must be retained for three years after the last modification. Any access to corporate content must require a user to sign in, even if the user is from an external partner organization and is not yet known to the other Office 365 environment. Sharing of credit card information must not be allowed through email, Microsoft OneDrive or SharePoint. All user passwords must be complex and expire every 30 days. Allow Gmail users from partner organizations to automatically open encrypted emails sent from Contoso, Ltd.Client connections All remote client connections to the on-premises environment must use a VPN connection. Internal and external users from partner organizations must be able to dial in to audio conferences by using their own mobile or landline phones. Users must be able to access content in the on-premises SharePointServer environment seamlessly when connected to the SharePoint Online environment. When users create objects in Office 365 that require a time zone setting, the time zone must always be set to the Eastern Time (US & Canada) setting.Employees Employees must be able to perform the following actions: Access all resources by using their Contoso Active Directory domain user account. Invite users from business partners to participate in meetings. Coordinate scheduling using Microsoft StaffHub. All team settings should be consistent using a one-month schedule. Add users from external partner organizations to teams.File storageYou identify the following requirements for file storage: All users must store documents in OneDrive storage. All email attachments to on-premises Exchange Server mailboxes and Exchange Online mailboxes must be saved automatically to OneDrive. Users must be able to share documents from their OneDrive storage with other users including those in other organizations. Users must be notified only when someone else changes a document in their OneDrive. Each user may store up to 50 gigabytes (GB) in OneDrive. Users may request an increase to this limit by using a request process. The process is implemented as a SharePoint form in an on-premises SharePoint site.You need to define the steps required for a partner user to read encrypted email.Which three steps must they perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. Answer: Explanation:

https://support.office.com/en-us/article/how-do-i-open-a-protected-message-1157a286-8ecc-4b1e-ac43-2a608fbf3098

QUESTION 282Drag and Drop QuestionBackgroundContoso Ltd. manufactures and sells computers and related devices. Employees who work in the corporate headquarters use Microsoft Exchange Server, SharePoint Server, and Office 2016 to perform their daily job functions. Mobile and remote employees access resources in the on-premises environment by using VPN connections. The company plans to transition to Office 365. You purchase Office 365 Business Premium Licenses for all users. Contoso, Ltd. uses System Center 2012 R2 Configuration manager to manage desktop software. Office 365 environmentDeployment of all Office 365 applications must be controlled internally by administrators. Users must not have the ability to install Office 365 ProPlus on their own. All user initiated installations of Office 365 applications must be prohibited before administrative deployments are configured. All additional Office 365 licenses must employ the minimum cost to provide the required service. Integration between the on-premises and Office 365 environments must be configured where required.Corporate policiesServices must be configured to enforce the following security policies: All VPN connections must be secured by using a 256-bit, L2TP connection. All users must be use multi-factor authentication (MFA) when connecting over a VPN connection. All content, including emails and documents, must be retained for three years after the last modification. Any access to corporate content must require a user to sign in, even if the user is from an external partner organization and is not yet known to the other Office 365 environment. Sharing of credit card information must not be allowed through email, Microsoft OneDrive or SharePoint. All user passwords must be complex and expire every 30 days. Allow Gmail users from partner organizations to automatically open encrypted emails sent from Contoso, Ltd.Client connections All remote client connections to the on-premises environment must use a VPN connection. Internal and external users from partner organizations must be able to dial in to audio conferences by using their own mobile or landline phones. Users must be able to access content in the on-premises SharePointServer environment seamlessly when connected to the SharePoint Online environment. When users create objects in Office 365 that require a time zone setting, the time zone must always be set to the Eastern Time (US & Canada) setting.EmployeesEmployees must be able to perform the following actions: Access all resources by using their Contoso Active Directory domain user account. Invite users from business partners to participate in meetings. Coordinate scheduling using Microsoft StaffHub. All team settings should be consistent using a one-month schedule. Add users from external partner organizations to teams.File storageYou identify the following requirements for file storage: All users must store documents

in OneDrive storage. All email attachments to on-premises Exchange Server mailboxes and Exchange Online mailboxes must be saved automatically to OneDrive. Users must be able to share documents from their OneDrive storage with other users including those in other organizations. Users must be notified only when someone else changes a document in their OneDrive. Each user may store up to 50 gigabytes (GB) in OneDrive. Users may request an increase to this limit by using a request process. The process is implemented as a SharePoint form in an on-premises SharePoint site.You need to configure Office 365 to comply with the corporate policies.Which three steps should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. Answer: Explanation:
https://support.office.com/en-us/article/overview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423
!!!RECOMMEND!!!1.|2018 Latest 70-347 Exam Dumps (PDF & VCE) 352Q&As Download:https://www.braindump2go.com/70-347.html2.|2018 Latest 70-347 Study Guide Video: YouTube Video: YouTube.com/watch?v=XzbCjLY3Pq0