[New Exams!Free Download Updated AZ-500 PDF and AZ-500 VCE 60Q from Braindump2go[Q34-Q44

July/2019 Braindump2go AZ-500 Exam Dumps with PDF and VCE New Updated Today! Following are some new AZ-500 Exam Questions:1.|2019 Latest Braindump2go AZ-500 Exam Dumps (PDF & VCE) Instant Download: **https://www.braindump2go.com/az-500.html**2.|2019 Latest Braindump2go AZ-500Exam Questions & Answers Instant Download:https://drive.google.com/drive/folders/1sQAsVdJ79oBKFiswxjUzGT6Gt6a6PYWl?usp=sharingQUESTION 34You have a hybrid configuration of Azure Active Directory (Azure AD).All users have computers that run Windows 10 and are hybrid Azure AD joined.You have an Azure SQL database that is configured to support Azure AD authentication.Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.Which authentication method should you instruct the developers to use?A. SQL LoginB. Active Directory - Universal with MFA supportC. Active Directory - IntegratedD. Active Directory - PasswordAnswer: CExplanation:Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.Using an Azure AD identity to connect using SSMS or SSDTThe following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.Active Directory integrated authenticationUse this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection. 2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to.(The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.) References: **https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication-configure.md**QUESTION 35You have an Azure SQL Database server named SQL1.You plan to turn on Advanced Threat Protection for SQL1 to detect all threat detection types.Which action will Advanced Threat Protection detect as a threat?A. A user updates more than 50 percent of the records in a table.B. A user attempts to sign as select * from table1.C. A user is added to the db_owner database role.D. A user deletes more than 100 records from the same table.Answer: BExplanation:Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.References:**https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview** QUESTION 36Your company uses Azure DevOps.You need to recommend a method to validate whether the code meets the company's quality standards and code review standards.What should you recommend implementing in Azure DevOps?A. branch foldersB. branch permissionsC. branch policiesD. branch lockingAnswer: CExplanation:Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.References: **https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts** QUESTION 37You have an Azure subscription named Subscription1.You deploy a Linux virtual machine named VM1 to Subscription1.You need to monitor the metrics and the logs of VM1.What should you use?A. the AzurePerformanceDiagnostics extensionB. Azure HDInsightC. Linux Diagnostic Extension (LAD) 3.0D. Azure Analysis Services**Answer: A**QUESTION 38 You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.The User administrator role is assigned to a user named Admin1.An external partner has a Microsoft account that uses the user1@outlook.com sign in.Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: "Unable to invite user user1@outlook.com Generic authorization exception."You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.What should you do?A. From the Roles and administrators blade, assign the Security administrator role to Admin1.B. From the Organizational relationships blade, add an identity provider.C. From the Custom domain names blade, add a custom domain.D. From the Users blade, modify the External collaboration settings.**Answer: D**QUESTION 39Drag and Drop QuestionYou are implementing conditional access policies.You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.You need to identify the risk level of the following risk events:- Users with leaked credentials- Impossible travel to atypical locations- Sign ins from IP addresses with suspicious activityWhich level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used

once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.NOTE: Each correct selection is worth one point. Answer: Explanation:Azure AD Identity protection can detect six types of suspicious sign-in activities:- Users with leaked credentials- Sign-ins from anonymous IP addresses- Impossible travel to atypical locations- Sign-ins from infected devices- Sign-ins from IP addresses with suspicious activity- Sign-ins from unfamiliar locationsThese six types of events are categorized in to 3 levels of risks ?High, Medium&; Low: References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/QUESTION 40 Hotspot QuestionYou have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table. You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:- Assignment: Include Group1, Exclude Group2- Conditions: Sign-in risk of Medium and above- Access: Allow access, Require password changeFor each of the following statements, select Yes if the statement is true. Otherwise, select No.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: YesUser1 is member of Group1. Sign in from unfamiliar location is risk level Medium.Box 2: YesUser2 is member of Group1. Sign in from anonymous IP address is risk level Medium.Box 3: NoSign-ins from IP addresses with suspicious activity is low.Note: Azure AD Identity protection can detect six types of suspicious sign-in activities:Users with leaked credentialsSign-ins from anonymous IP addressesImpossible travel to atypical locationsSign-ins from infected devicesSign-ins from IP addresses with suspicious activitySign-ins from unfamiliar locationsThese six types of events are categorized in to 3 levels of risks ?High, Medium&; Low:References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/QUESTION 41 Drag and Drop QuestionYou need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. Answer: Explanation:Step 1: Create an access review programStep 2: Create an access review controlStep 3: Set Reviewers to Group ownersIn the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review. References:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controlsQUESTION 42Hotspot QuestionYou have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table. You configure an access review named Review1 as shown in the following exhibit. Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 1: User3 onlyUse the Members (self) option to have the users review their own role assignments.Box 2: User3 will receive a confirmation requestUse the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.No change - Leave user's access unchangedRemove access - Remove user's accessApprove access - Approve user's accessTake recommendations - Take the system's recommendation on denying or approving the user's continued access References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-reviewQUESTION 43Drag and Drop QuestionYou create an Azure subscription.You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. Answer: Explanation:Step 1: Consent to PIM Step: 2 Verify your identity by using multi-factor authentication (MFA)Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account.Step 3: Sign up PIM for Azure AD roles Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles.References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-startedQUESTION 44 Hotspot QuestionYour company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table. The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table. The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.) For each of the following statements, select Yes if the statement is true. Otherwise, select No.NOTE: Each correct selection is worth one point. Answer: Explanation:Box 2: NoUse of Microsoft Authenticator is not required.Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.Box 3: NoThe New York IP address subnet is included in the "skip multi-factor authentication for request.References:**https://www.cayosoft.com/difference-enabling-enforcing-mfa/**!!!RECOMMEND!!!1.|2019 Latest

Braindump2go AZ-500 Exam Dumps (PDF & VCE) Instant Download:**https://www.braindump2go.com/az-500.html**2.|2019 Latest Braindump2go AZ-500 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=-d1W44dDS2o