[Jan-2019100% Valid AZ-101 VCE and PDF Dumps 70Q Provided by Braindump2go(Q28-Q38)

January/2019 Braindump2go AZ-101 Exam Dumps with PDF and VCE New Updated Today! Following are some new AZ-101 Real Exam Questions:1.|2019 Latest AZ-101 Exam Dumps (PDF & VCE) 70Q&As Download:https://www.braindump2go.com/az-101.html2.|2019 Latest AZ-101 Exam Questions & Answers Download:https://drive.google.com/drive/folders/1KoBQez_BqgPlnBE-cCoz8OkAoozD-2g9?usp=sharingQUESTION 28From the MFA Server blade, you open the Block/unblock users blade as shown in the exhibit. What caused AlexW to be blocked?A. An administrator manually blocked the user.B. The user reported a fraud alert when prompted for additional authentication.C. The user account password expired.D. The user entered an incorrect PIN four times within 10 minutes.**Answer: B**QUESTION 29You are the global administrator for an Azure Active Directory (Azure AD) tenant named adatum.com.From the Azure Active Directory blade, you assign the Conditional Access Administrator role to a user named Admin1.You need to ensure that Admin1 has just-in-time access as a conditional access administrator.What should you do next?A. Enable Azure AD Multi-Factor Authentication (MFA).B. Set Admin1 as Eligible for the Privileged Role Administrator role.C. Set Admin1 as Eligible for the Conditional Access Administrator role.D. Enable Azure AD Identity Protection.Answer: AExplanation:Require MFA for admins is a baseline policy that requires MFA for the following directory roles:Global administratorSharePoint administratorExchange administratorConditional access administratorSecurity administratorReferences: **https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/baseline-protection**QUESTION 30You are the global administrator for an Azure Directory (Azure AD) tenant named adatum.com.You need to enable two-step verification for Azure users.What should you do?A. Create a single sign-in risk policy in Azure AD Identity Protection.B. Enable Azure AD Privileged Identity Management.C. Create and configure the Identity Hub.D. Configure a security policy in Azure Security Center.Answer: AExplanation:With Azure Active Directory Identity Protection, you can:require users to register for multi-factor authenticationhandle risky sign-ins and compromised usersReferences: **https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/flows**QUESTION 31You have an Azure subscription named Subscription1 that contains an Azure virtual machine named VM1.VM1 is in a resource group named RG1.VM1 runs services that will be used to deploy resources to RG1.You need to ensure that a service running on VM1 can manage the resources in RG1 by using the identity of VM1.What should you do first?A. From the Azure portal, modify the Access control (IAM) settings of VM1.B. From the Azure portal, modify the Policies settings of RG1.C. From the Azure portal, modify the value of the Managed Service Identity option for VM1.D. From the Azure portal, modify the Access control (IAM) settings of RG1.Answer: CExplanation:A managed identity from Azure Active Directory allows your app to easily access other AAD-protected resources such as Azure Key Vault. The identity is managed by the Azure platform and does not require you to provision or rotate any secrets.User assigned managed identities can be used on Virtual Machines and Virtual Machine Scale Sets.References: **https://docs.microsoft.com/en-us/azure/app-service/app-service-managed-service-identity**QUESTION 32You are configuring Azure Active Directory (AD) Privileged Identity Management.You need to provide a user named Admin1 with read access to a resource group named RG1 for only one month. The user role must be assigned immediately.What should you do?A. Assign an active role.B. Assign an eligible role.C. Assign a permanently active role.D. Create a custom role and a conditional access policy.Answer: BExplanation:Azure AD Privileged Identity Management introduces the concept of an eligible admin. Eligible admins should be users that need privileged access now and then, but not all-day, every day. The role is inactive until the user needs access, then they complete an activation process and become an active admin for a predetermined amount of time.References: **https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure**QUESTION 33You have an Azure Active Directory (Azure AD) tenant named Tenant1 and an Azure subscription named Subscription1.You enable Azure AD Privileged Identity Management.You need to secure the members of the Lab Creator role. The solution must ensure that the lab creators request access when they create labs.What should you do first?A. From Azure AD Privileged Identity Management, edit the role settings for Lab Creator.B. From Subscription1, edit the members of the Lab Creator role.C. From Azure AD Identity Protection, create a user risk policy.D. From Azure AD Privileged Identity Management, discover the Azure resources of Subscription1.Answer: AExplanation:As a Privileged Role Administrator you can:Enable approval for specific roles Specify approver users and/or groups to approve requestsView request and approval history for all privileged rolesReferences: **https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure**QUESTION 34You create an Azure subscription that is associated to a basic Azure Active Directory (Azure AD) tenant.You need to receive an email notification when any user activates an administrative role.What should you do?A. Purchase Azure AD Premium P2 and configure

Azure AD Privileged Identity Management.B. Purchase Enterprise Mobility + Security E3 and configure conditional access policies.C. Purchase Enterprise Mobility + Security E5 and create a custom alert rule in Azure Security Center.D. Purchase Azure AD Premium P1 and enable Azure AD Identity Protection.Answer: AExplanation:When key events occur in Azure AD Privileged Identity Management (PIM), email notifications are sent.For example, PIM sends emails for the following events:When a privileged role activation is pending approvalWhen a privileged role activation request is completedWhen a privileged role is activatedWhen a privileged role is assignedWhen Azure AD PIM is enabledReferences: **https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications**QUESTION 35You have an Azure Active Directory (Azure AD) tenant.You have an existing Azure AD conditional access policy named Policy1. Policy1 enforces the use of Azure AD-joined devices when members of the Global Administrators group authenticate to Azure AD from untrusted locations.You need to ensure that members of the Global Administrators group will also be forced to use multi-factor authentication when authenticating from untrusted locations.What should you do?A. From the multi-factor authentication page, modify the service settings.B. From the multi-factor authentication page, modify the user settings.C. From the Azure portal, modify grant control of Policy1.D. From the Azure portal, modify session control of Policy1.Answer: C Explanation:There are two types of controls:Grant controls - To gate accessSession controls - To restrict access to a sessionGrant controls oversee whether a user can complete authentication and reach the resource that they're attempting to sign-in to. If you have multiple controls selected, you can configure whether all of them are required when your policy is processed. The current implementation of Azure Active Directory enables you to set the following grant control requirements: References: **https://blog.lumen21.com/2017/12/15/conditional-access-in-azure-active-directory/**QUESTION 36You have an Azure subscription.You enable multi-factor authentication for all users.Some users report that the email applications on their mobile device cannot connect to their Microsoft Exchange Online mailbox. The users can access Exchange Online by using a web browser and from Microsoft Outlook 2016 on their computer.You need to ensure that the users can use the email applications on their mobile device.What should you instruct the users to do?A. Enable self-service password reset.B. Create an app password.C. Reset the Azure Active Directory (Azure AD) password.D. Reinstall the Microsoft Authenticator app.Answer: AExplanation: **https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks**QUESTION 37You have an Azure subscription named Subscription1 and two Azure Active Directory (Azure AD) tenants named Tenant1 and Tenant2. Subscription1 is associated to Tenant1. Multi-factor authentication (MFA) is enabled for all the users in Tenant1.You need to enable MFA for the users in Tenant2. The solution must maintain MFA for Tenant1.What should you do first?A. Transfer the administration of Subscription1 to a global administrator of Tenant2B. Configure the MFA Server setting in Tenant1.C. Create and link a subscription to Tenant2.D. Change the directory for Subscription1.**Answer: C**QUESTION 38SIMULATIONThis is a lab or performance-based testing (PBT) section.The following section of the exam is a lab. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.Please, note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.To start the labYou may start lab by clicking the Next buttonTasksClick to expand each objectiveasTo connect to the Azure portal, type https:/portal.azure.com in the browser address bar.You need to create a function app named corp7509086n1 that supports sticky sessions. The solution must minimize the Azure-related costs of the App Service plan.What should you do from the Azure portal?**A. See below explanation** Answer: AExplanation:Step 1:Select the New button found on the upper left-hand corner of the Azure portal, then select Compute > Function App.Step 2:Use the function app settings as listed below.App name: corp7509086n1Hosting plan: Azure App Service plan (need this for the sticky sessions)Pricing tier of the the App Service plan: Shared compute: FreeStep 3:Select Create to provision and deploy the function app.References: **https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-function-app-portal**!!!RECOMMEND**!!!**]1.|2019 Latest AZ-101 Exam Dumps (PDF & VCE) 70Q&As Download:https://www.braindump2go.com/az-101.html2.|2019 Latest AZ-101 Study Guide Video: YouTube Video: YouTube.com/watch?v=4qoOHoNxDFU