# [March-2019-New100% Success-Braindump2go AZ-202 VCE 150Q Instant Download

**2019/March Braindump2go AZ-202 Exam Dumps with PDF and VCE New Updated Today! Following are some new AZ-202 Real Exam Questions:]1.|2019 Latest AZ-202 Exam Dumps (PDF & VCE) Instant Downlopad: https://www.braindump2go.com/az-202.html2.|2019 Latest AZ-202 Exam Questions & Answers Instant Downlopad: https://drive.google.com/drive/folders/1uh5T3u9C6oB2U2tOFeLk0JMzfJD2uu8M?usp=sharing**New QuestionCase Study 3 - Proseware, IncBackgroundYou are a developer for Proseware, Inc. You are developing an application that applies a set of governance policies for Proseware's internal services, external services, and applications. The application will also provide a shared library for common functionality.RequirementsPolicy serviceYou develop and deploy a stateful ASP.NET Core 2.1 web application named Policy service to an Azure App Service Web App. The application reacts to events from Azure Event Grid and performs policy actions based on those events.The application must include the Event Grid Event ID field in all Application Insights telemetry.Policy service must use Application Insights to automatically scale with the number of policy actions that it is performing. PoliciesLog PolicyAll Azure App Service Web Apps must write logs to Azure Blob storage. All log files should be saved to a container named logdrop. Logs must remain in the container for 15 days.Authentication eventsAuthentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible.PolicyLibYou have a shared library named PolicyLib that contains functionality common to all ASP.NET Core web services and applications. The PolicyLib library must:  Exclude non-user actions from Application Insights telemetry.  Provide methods that allow a web service to scale itself  Ensure that scaling actions do not disrupt application usageOtherAnomaly detection serviceYou have an anomaly detection service that analyzes log information for anomalies. It is implemented as an Azure Machine Learning model. The model is deployed as a web service.If an anomaly is detected, an Azure Function that emails administrators is called by using an HTTP WebHook.Health monitoringAll web applications and services have health monitoring at the /health service endpoint.Policy lossWhen you deploy Policy service, policies may not be applied if they were in the process of being applied during the deployment.Performance issueWhen under heavy load, the anomaly detection service undergoes slowdowns and rejects connections.Notification latencyUsers report that anomaly detection emails can sometimes arrive several minutes after an anomaly is detected.Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.    Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.  Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution. Determine whether the solution meets the stated goals.You need to ensure that authentication events are triggered and processed according to the policy.Solution: Create a new Azure Event Grid topic and add a subscription for the events.Does the solution meet the goal?A.    YesB.    NoAnswer: BExplanation:Use a separate Azure Event Grid topics and subscriptions for sign-in and sign-out events.Scenario: Authentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible.New QuestionCase Study 3 - Proseware, IncBackgroundYou are a developer for Proseware, Inc. You are developing an application that applies a set of governance policies for Proseware's internal services, external services, and applications. The application will also provide a shared library for common functionality.RequirementsPolicy serviceYou develop and deploy a stateful ASP.NET Core 2.1 web application named Policy service to an Azure App Service Web App. The application reacts to events from Azure Event Grid and performs policy actions based on those events.The application must include the Event Grid Event ID field in all Application Insights telemetry.Policy service must use Application Insights to automatically scale with the number of policy actions that it is performing.PoliciesLog PolicyAll Azure App Service Web Apps must write logs to Azure Blob storage. All log files should be saved to a container named logdrop. Logs must remain in the container for 15 days.Authentication eventsAuthentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible. PolicyLibYou have a shared library named PolicyLib that contains functionality common to all ASP.NET Core web services and applications. The PolicyLib library must:  Exclude non-user actions from Application Insights telemetry.  Provide methods that allow a web service to scale itself  Ensure that scaling actions do not disrupt application usageOtherAnomaly detection serviceYou have an anomaly detection service that analyzes log information for anomalies. It is implemented as an Azure Machine Learning model. The model is deployed as a web service.If an anomaly is detected, an Azure Function that emails administrators is called by using an HTTP WebHook.Health monitoringAll web applications and services have health monitoring at the /health service endpoint.Policy lossWhen you deploy Policy service, policies may not be applied if they were in the process of being applied during the deployment.Performance issueWhen under heavy load, the anomaly detection service undergoes slowdowns and rejects connections.Notification latencyUsers report that anomaly detection emails can sometimes arrive several minutes after an anomaly is detected.Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.    Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.  Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution. Determine whether the solution meets the stated goals.You need to ensure that authentication events are triggered and processed according to the policy.Solution: Create a new Azure Event Grid subscription for all authentication that delivers messages to an Azure Event Hub. Use the subscription to process signout events.Does the solution meet the goal?A.    YesB.    NoAnswer: B Explanation:Use a separate Azure Event Grid topics and subscriptions for sign-in and sign-out events.Scenario: Authentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible.New QuestionCase Study 3 - Proseware, IncBackgroundYou are a developer for Proseware, Inc. You are developing an application that applies a set of governance policies for Proseware's internal services, external services, and applications. The application will also provide a shared library for common functionality.RequirementsPolicy serviceYou develop and deploy a stateful ASP.NET Core 2.1 web application named Policy service to an Azure App Service Web App. The application reacts to events from Azure Event Grid and performs policy actions based on those events.The application must include the Event Grid Event ID field in all Application Insights telemetry.Policy service must use Application Insights to automatically scale with the number of policy actions that it is performing.PoliciesLog PolicyAll Azure App Service Web Apps must write logs to Azure Blob storage. All log files should be saved to a container named logdrop. Logs must remain in the container for 15 days.Authentication eventsAuthentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible.PolicyLibYou have a shared library named PolicyLib that contains functionality common to all ASP.NET Core web services and applications. The PolicyLib library must:  Exclude non-user actions from Application Insights telemetry.  Provide methods that allow a web service to scale itself  Ensure that scaling actions do not disrupt application usageOtherAnomaly detection serviceYou have an anomaly detection service that analyzes log information for anomalies. It is implemented as an Azure Machine Learning model. The model is deployed as a web service.If an anomaly is detected, an Azure Function that emails administrators is called by using an HTTP WebHook.Health monitoringAll web applications and services have health monitoring at the /health service endpoint.Policy loss When you deploy Policy service, policies may not be applied if they were in the process of being applied during the deployment. Performance issueWhen under heavy load, the anomaly detection service undergoes slowdowns and rejects connections.Notification latencyUsers report that anomaly detection emails can sometimes arrive several minutes after an anomaly is detected.Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.    Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.  Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution. Determine whether the solution meets the stated goals.You need to ensure that authentication events are triggered and processed according to the policy. Solution: Create separate Azure Event Grid topics and subscriptions for sign-in and sign-out events.Does the solution meet the goal?A.    YesB.    NoAnswer: AExplanation:Scenario: Authentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible.