

[June-2019-NewFree Download AZ-400 Exam Questions 81Q from Braindump2go[q34-q44

June/2019 Braindump2go AZ-400 Exam Dumps with PDF and VCE New Updated Today! Following are some new AZ-400 Real Exam Questions:1.**2019 Latest AZ-400 Exam Dumps (PDF & VCE) Instant Download:**

<https://www.braindump2go.com/az-400.html>**2.****2019 Latest AZ-400 Exam Questions & Answers Instant Download:**

https://drive.google.com/drive/folders/1kLhX5N_Pt_noAKZD50xUpnSEA5Tt62TZ?usp=sharing**QUESTION 34**You have an Azure Resource Manager template that deploys a multi-tier application.You need to prevent the user who performs the deployment from viewing the account credentials and connection strings used by the application.What should you use?**A.** an Azure Resource Manager parameter file**B.** an Azure Storage table**C.** an Appsettings.json files**D.** Azure Key Vault**E.** a Web.config file**Answer:** D**Explanation:**When you need to pass a secure value (like a password) as a parameter during deployment, you can retrieve the value from an Azure Key Vault. You retrieve the value by referencing the key vault and secret in your parameter file. The value is never exposed because you only reference its key vault ID. The key vault can exist in a different subscription than the resource group you are deploying to.**References:**

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter>**QUESTION 35**Your company uses a Git repository in Azure Repos to manage the source code of a web application. The master branch is protected from direct updates. Developers work on new features in the topic branches.Because of the high volume of requested features, it is difficult to follow the history of the changes to the master branch.You need to enforce a pull request merge strategy. The strategy must meet the following requirements:- Consolidate commit histories- Merge the changes into a single commitWhich merge strategy should you use in the branch policy?**A.** Git fetch**B.** no-fast-forward merge**C.** squash merge**D.** fast-forward merge**Answer:** C**Explanation:**Squash merging is a merge option that allows you to condense the Git history of topic branches when you complete a pull request. Instead of each commit on the topic branch being added to the history of the default branch, a squash merge takes all the file changes and adds them to a single new commit on the default branch.A simple way to think about this is that squash merge gives you just the file changes, and a regular merge gives you the file changes and the commit history.**Note:** Squash merging keeps your default branch histories clean and easy to follow without demanding any workflow changes on your team. Contributors to the topic branch work how they want in the topic branch, and the default branches keep a linear history through the use of squash merges. The commit history of a master branch updated with squash merges will have one commit for each merged branch. You can step through this history commit by commit to find out exactly when work was done.**References:**

<https://docs.microsoft.com/en-us/azure/devops/repos/git/merging-with-squash>**QUESTION 36**Your company uses cloud-hosted Jenkins for builds.You need to ensure that Jenkins can retrieve source code from Azure Repos.Which three actions should you perform? Each correct answer presents part of the solution**NOTE:** Each correct answer selection is worth one point**A.** Add the Team Foundation Server (TFS) plug-in to Jenkins.**B.** Create a personal access token in your Azure DevOps account.**C.** Create a webhook in Jenkins.**D.** Add a domain to your Jenkins account.**E.** Create a service hook in Azure DevOps.**Answer:** ABE

Explanation:<https://blogs.msdn.microsoft.com/devops/2017/04/25/vsts-visual-studio-team-services-integration-with-jenkins/>
<http://www.aisoftwarellc.com/blog/post/how-to-setup-automated-builds-using-jenkins-and-visual-studio-team-foundation-server/2044>**QUESTION 37**You are developing an open source solution that uses a GitHub repository.You create a new public project in Azure DevOps.You plan to use Azure Pipelines for continuous build. The solution will use the GitHub Checks API.Which authentication type should you use?**A.** a personal access token**B.** SAML**C.** GitHub App**D.** OAuth**Answer:** D**Explanation:**You can authenticate as a GitHub App. **References:**

<https://developer.github.com/apps/building-github-apps/authenticating-with-github-apps/>**QUESTION 38**You plan to share packages that you wrote, tested, validated, and deployed by using Azure Artifacts.You need to release multiple builds of each package by using a single feed. The solution must limit the release of packages that are in development.What should you use?**A.** global symbols**B.** local symbols**C.** upstream sources**D.** views**Answer:** C**Explanation:**Upstream sources enable you to manage all of your product's dependencies in a single feed. We recommend publishing all of the packages for a given product to that product's feed, and managing that product's dependencies from remote feeds in the same feed, via upstream sources. This setup has a few benefits:**Simplicity:** your NuGet.config, .npmrc, or settings.xml contains exactly one feed (your feed). **Determinism:** your feed resolves package requests in order, so rebuilding the same codebase at the same commit or changeset uses the same set of packages **Provenance:** your feed knows the provenance of packages it saved via upstream sources, so you can verify that you're using the original package, not a custom or malicious copy published to your feed**Peace of mind:** packages used via upstream sources are guaranteed to be saved in the feed on first use; if the upstream source is disabled/removed, or the remote feed goes down or deletes a

package you depend on, you can continue to develop and buildReferences:

<https://docs.microsoft.com/en-us/azure/devops/artifacts/concepts/upstream-sources?view=vsts>QUESTION 39You use Azure Artifacts to host NuGet packages that you create.You need to make one of the packages available to anonymous users outside your organization. The solution must minimize the number of publication points.What should you do?A. Create a new feed for the packageB. Publish the package to a public NuGet repository.C. Promote the package to a release view.D. Change the feed URL of the package.Answer: AExplanation:Azure Artifacts introduces the concept of multiple feeds that you can use to organize and control access to your packages.Packages you host in Azure Artifacts are stored in a feed. Setting permissions on the feed allows you to share your packages with as many or as few people as your scenario requires. Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers.References:

<https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feed-permissions?view=vsts&tabs=new-nav>QUESTION 40Your company is concerned that when developers introduce open source Libraries, it creates licensing compliance issues.You need to add an automated process to the build pipeline to detect when common open source libraries are added to the code base.What should you use?A. Code StyleB. Microsoft Visual SourceSafeC. Black DuckD. JenkinsAnswer: CExplanation: Secure and Manage Open Source SoftwareBlack Duck helps organizations identify and mitigate open source security, license compliance and code-quality risks across application and container portfolios.Black Duck Hub and its plugin for Team Foundation Server (TFS) allows you to automatically find and fix open source security vulnerabilities during the build process, so you can proactively manage risk. The integration allows you to receive alerts and fail builds when any Black Duck Hub policy violations are met.Note: WhiteSource would also be a good answer, but it is not an option here.References:

<https://marketplace.visualstudio.com/items?itemName=black-duck-software.hub-tfs>QUESTION 41You have 50 Node.js-based projects that you scan by using WhiteSource. Each project includes Package.json, Package-lock.json, and Npm-shrinkwrap.json files. You need to minimize the number of libraries reports by WhiteSource to only the libraries that you explicitly reference.What should you do?A. Configure the File System Agent plug in.B. Delete Package lock.json.C. Configure the Artifactory plug-in. D. Add a devDependencies section to Package-lock.json.Answer: DExplanation:Separate Your DependenciesWithin your package.json file be sure you split out your npm dependencies between devDependencies and (production) dependencies. The key part is that you must then make use of the --production flag when installing the npm packages. The --production flag will exclude all packages defined in the devDependencies section.References:

<https://blogs.msdn.microsoft.com/visualstudioalmrangers/2017/06/08/manage-your-open-source-usage-and-security-as-reported-by-your-cicd-pipeline/>QUESTION 42You use Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring. You need to write ad-hoc Queries against the monitoring data.Which Query language should you use?A. PL/pgSQLB. Transact-SQLC. Azure Log AnalyticsD. PL/SQLAnswer: CExplanation:Data analysis in Azure SQL Analytics is based on Log Analytics language for your custom querying and reporting.References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-sql>QUESTION 43Your company uses Service Now for incident management.You develop an application that runs on Azure.The company needs to generate a ticket in Service Now when the application fails to authenticate.Which Azure Log Analytics solution should you use?A. Automation & ControlB. IT Service Management Connector (ITSM)C. Application Insights ConnectorD. insight & AnalyticsAnswer: BExplanation:The IT Service Management Connector (ITSMC) allows you to connect Azure and a supported IT Service Management (ITSM) product/service. ITSMC supports connections with the following ITSM tools:ServiceNowSystem Center Service ManagerProvancaCherwellWith ITSMC, you canCreate work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics alerts).Optionally, you can sync your incident and change request data from your ITSM tool to an Azure Log Analytics workspace.References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview>QUESTION 44You have multi-tier application that has an Azure Web Apps front end and an Azure SQL Database back end.You need to recommend a solution to capture and store telemetry data. The solution must meet the following requirements:- Support using ad-hoc queries to identify baselines.- Trigger alerts when metrics in the baseline are exceeded.- Store application and database metrics in a central location.What should you include in the recommendation?A. Azure Application InsightsB. Azure SQL Database Intelligent InsightsC. Azure Event HubsD. Azure Log AnalyticsAnswer: DExplanation:Azure Platform as a Service (PaaS) resources, like Azure SQL and Web Sites (Web Apps), can emit performance metrics data natively to Log Analytics.The Premium plan will retain up to 12 months of data, giving you an excellent baseline ability. There are two options available in the Azure portal for analyzing data stored in Log analytics and for creating queries for ad hoc analysis.References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-azurepass-posh>!!!RECOMMEND!!!1.**2019 Latest AZ-400 Exam Dumps (PDF & VCE) Instant Download:**<https://www.braindump2go.com/az-400.html>2.**2019 Latest AZ-400**

Study Guide Video Instant Download: YouTube Video: [YouTube.com/watch?v=XEIrroW1WvY](https://www.youtube.com/watch?v=XEIrroW1WvY)