

Exam Questions AZ-400

Microsoft Azure DevOps Solutions (beta)

<https://www.2passeasy.com/dumps/AZ-400/>



NEW QUESTION 1

Note: This question is part of * series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated

goals. Some question sett 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 have an approval process that contains a condition. The condition requires that releases be approved by a team leader before they are deployed.

You have a poky stating that approvals must occur within eight hour.

You discover that deployments fail if the approvals take longer than two hours. You need to ensure that the deployments only fail if the approvals take longer than eight hours.

Solution: From Post-deployment conditions, you modify the Time between reevaluation of gates option.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Use a gate From Pre-deployment conditions instead. References: <https://docs.microsoft.com/enus/ azure/devops/pipelines/release/approvals/gates>

NEW QUESTION 2

You need to recommend a Docker container build strategy that meets the following requirements

¡E Minimizes image sues

¡E Minimizes the security surface area of the final image What should you include m the recommendation?

A. multi-stage builds

B. single-stage builds

C. PowerShell Desired State Configuration (DSC)

D. Docker Swarm

Answer: A

Explanation:

Multi-stage builds are a new feature requiring Docker 17.05 or higher on the daemon and client. Multistage builds are useful to anyone who has struggled to optimize Dockerfiles while keeping them easy to read and maintain. References: <https://docs.docker.com/develop/develop-images/multistage-build/>

NEW QUESTION 3

DRAG DROP

You need to use Azure Automation Sure Configuration to manage the ongoing consistency of virtual machine configurations.

Which five 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.

NOTE: More than one order of answer choices in correct. You writ receive credit for any of the orders you select.

Actions	Answer Area
Onboard the virtual machines to Azure Automation State Configuration.	
Check the compliance status of the node.	
Create a management group.	
Assign the node configuration.	
Compile a configuration into a node configuration.	
Upload a configuration to Azure Automation State Configuration.	
Assign tags to the virtual machines.	

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Step 1: Assign the node configuration.

You create a simple DSC configuration that ensures either the presence or absence of the Web-Server Windows Feature (IIS), depending on how you assign

nodes. Step 2: Upload a configuration to Azure Automation State Configuration.

You import the configuration into the Automation account. Step 3: Compiling a configuration into a node configuration Compiling a configuration in Azure Automation

Before you can apply a desired state to a node, a DSC configuration defining that state must be compiled into one or more node configurations (MOF document), and placed on the Automation DSC Pull Server.

Step 4: Onboard the virtual machines to Azure State Configuration Onboarding an Azure VM for management with Azure Automation State Configuration

Step 5: Check the compliance status of the node.

Viewing reports for managed nodes. Each time Azure Automation State Configuration performs a consistency check on a managed node, the node sends a status report back to the pull server. You can view these reports on the page for that node.

On the blade for an individual report, you can see the following status information for the corresponding consistency check:

The report status is whether the node is "Compliant", the configuration "Failed", or the node is "Not Compliant" (when the node is in ApplyandMonitor mode and the machine is not in the desired state).

References: <https://docs.microsoft.com/en-us/azure/automation/automation-dscgetting-started>

NEW QUESTION 4

You manage build pipelines and deployment pipelines by using Azure DevOps.

Your company has a team of 500 developers. New members are added continually to the team

You need to automate the management of users and licenses whenever possible Which task must you perform manually?

- A. modifying group memberships
- B. procuring licenses
- C. adding users
- D. assigning entitlements

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/migrate-togroup-based-resource-management?view=vsts&tabs=new-nav>

<https://docs.microsoft.com/en-us/rest/api/azure/devops/memberentitlementmanagement/?view=azure-devopsrest-5.0>

NEW QUESTION 5

During a code review, you discover many quality issues. Many modules contain unused variables and empty catch blocks. You need to recommend a solution to improve the quality of the code. What should you recommend?

- A. In a Gradle build task, select Run Checkstyle.
- B. In an Xcode build task, select Use xcpretty from Advanced
- C. In a Grunt build task, select Enabled from Control Options.
- D. In a Maven build task, select Run PM

Answer: D

Explanation:

PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth.

There is an Apache Maven PMD Plugin which allows you to automatically run the PMD code analysis tool on your project's source code and generate a site report with its results.

References: <https://pmd.github.io/>

NEW QUESTION 6

DRAG DROP

You need to increase the security of your team's development process.

Which type of security tool should you recommend for each stage of the development process? To answer, drag the appropriate security tools to the correct stages. Each security tool 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.

Security Tools	Answer Area
Penetration testing	Pull request: <input type="text"/>
Static code analysis	Continuous integration: <input type="text"/>
Threat modeling	Continuous delivery: <input type="text"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Threat modeling

Threat modeling's motto should be, "The earlier the better, but not too late and never ignore."

Box 2: Static code analysis

Validation in the CI/CD begins before the developer commits his or her code. Static code analysis tools in the IDE provide the first line of defense to help ensure that security vulnerabilities are not introduced into the CI/CD process.

Box 3: Penetration testing

Once your code quality is verified, and the application is deployed to a lower environment like development or QA, the process should verify that there are not any security vulnerabilities in the running application. This can be accomplished by executing automated penetration test against the running application to scan it for vulnerabilities.

References: <https://docs.microsoft.com/en-us/azure/devops/articles/securityvalidation- cicd-pipeline?view=vsts>

NEW QUESTION 7

DRAG DROP

You need to recommend project metrics for dashboards in Azure DevOps. Which chart widgets should you recommend for each metric? To answer, drag the appropriate chart widgets to the correct metrics. Each chart widget 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.

Chart Widgets	Answer Area
Burndown	The elapsed time from the creation of work items to their completion: <input type="text"/>
Cycle Time	
Lead Time	The elapsed time to complete work items once they are active: <input type="text"/>
Velocity	The remaining work: <input type="text"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Lead time

Lead time measures the total time elapsed from the creation of work items to their completion.

Box 2: Cycle time

Cycle time measures the time it takes for your team to complete work items once they begin actively working on them.

Box 3: Burndown

Burndown charts focus on remaining work within a specific time period. Incorrect Answers:

Velocity provides a useful metric for these activities: Support sprint planning

Forecast future sprints and the backlog items that can be completed

A guide for determining how well the team estimates and meets their planned

commitments References:

<https://docs.microsoft.com/en-us/azure/devops/report/dashboards/velocityguidance? view=vsts>

<https://docs.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-andlead- time?view=vsts>

<https://docs.microsoft.com/en-us/azure/devops/report/dashboards/configureburndown- burnup-widgets?view=vsts>

NEW QUESTION 8

Your company deploys applications m Docket containers.

You want to detect known explogts in the Docket images used to provision the Docker containers.

You need to integrate image scanning into the application lifecycle. The solution must expose the explogts as early as possible during the application lifecycle.

What should you configure?

- A. a task executed in the continuous deployment pipeline and a scheduled task against a running production container.
- B. a task executed in the continuous integration pipeline and a scheduled task that analyzes the production container.
- C. a task executed in the continuous integration pipeline and a scheduled task that analyzes the image registry
- D. manual tasks performed during the planning phase and the deployment phase

Answer: C

Explanation:

You can use the Docker task to sign into ACR and then use a subsequent script to pull an image and scan the container image for vulnerabilities.

Use the docker task in a build or release pipeline. This task can be used with Docker

or Azure Container registry.

References: <https://docs.microsoft.com/en-us/azure/devops/articles/securityvalidation- cicd-pipeline?view=vsts>

NEW QUESTION 9

DRAG DROP

Your company has four projects. The version control requirements for each project are shown in the following table.

Project	Requirement
Project 1	Project leads must be able to restrict access to individual files and folders in the repository.
Project 2	The version control system must enforce the following rules before merging any changes to the main branch. <ul style="list-style-type: none"> Changes must be reviewed by at least two project members. Changes must be associated to at least one work team.
Project 3	The project members must be able to work in Azure Repos directly from Xcode.
Project 4	The release branch must only be viewable or editable by the project leads.

You plan to use Azure Repos for all the projects.

Which version control system should you use for each project? To answer, drag the appropriate version control systems to the correct projects. Each version control system 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.

Version Control Systems	Answer Area
Git	Project 1: <input type="text"/>
Perforce	Project 2: <input type="text"/>
Subversion	Project 3: <input type="text"/>
Team Foundation Version Control	Project 4: <input type="text"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Team Foundation Version Control

TFVC lets you apply granular permissions and restrict access down to a file level. Box 2: Git

Git is the default version control provider for new projects. You should use Git for version control in your projects unless you have a specific need for centralized version control features in TFVC.

Box 3: Subversion

Note: Xcode is an integrated development environment (IDE) for macOS containing a suite of software development tools developed by Apple

Box 4: Git

Note: Perforce: Due to its multitenant nature, many groups can work on versioned files. The server tracks changes in a central database of MD5 hashes of file content, along with descriptive meta data and separately retains a master repository of file versions that can be verified through the hashes.

References: <https://searchitoperations.techtarget.com/definition/Perforce-Software>

<https://docs.microsoft.com/en-us/azure/devops/repos/git/share-your-code-in-gitxcode> <https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/overview>

NEW QUESTION 10

You have a brand policy in a project in Azure DevOps. The policy requires that code always builds successfully.

You need to ensure that a specific user can always merge change to the master branch, even if the code fails to compile. The solution must use the principle of least privilege.

What should you do?

- A. From the Security setting of the repository, modify the access control for the user.
- B. From the Security settings of the branch, modify the access control for the user.
- C. Add the user to the Build Administrators group.
- D. Add the user to the Project Administrators group

Answer: B

Explanation:

In some cases, you need to bypass policy requirements so you can push changes to the branch directly or complete a pull request even if branch policies are not satisfied. For these situations, grant the desired permission from the previous list to a user or group. You can scope this permission to an entire project, a repo, or a single branch. Manage this permission along with other Git permissions. References: <https://docs.microsoft.com/en-us/azure/devops/repos/git/branchpolicies>

NEW QUESTION 10

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 tie changes into a single commit

Which 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-withQuestions>
& Answers PDF P-43 squash

NEW QUESTION 15

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:

References:

<https://blogs.msdn.microsoft.com/devops/2017/04/25/vsts-visual-studio-teamservices-integration-with-jenkins/>

<http://www.aisoftwarellc.com/blog/post/how-to-setup-automated-builds-using-jenkins-and-visual-studio-team-foundation-server/2044>

NEW QUESTION 19

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:

„hSimplicity: your NuGet.config, .npmrc, or settings.xml contains exactly one feed (your feed).

„hDeterminism: your feed resolves package requests in order, so rebuilding the same codebase at the same commit or changeset uses the same set of packages

„hProvenance: 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

„hPeace 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 build

References: <https://docs.microsoft.com/enus/azure/devops/artifacts/concepts/upstream-sources?view=vsts>

NEW QUESTION 24

Your 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 Style
- B. Microsoft Visual SourceSafe
- C. Black Duck
- D. Jenkins

Answer: C

Explanation:

Secure and Manage Open Source Software

Black 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>

NEW QUESTION 25

You have multi-tier application that h. an Azure Web Apps front end and art Azure SQL Databale back end.
You need to recommend a solution to capture and store telemetry dat

- A. The solution must meet the following requirements:ïE Support using ad-hoc queries to identify baselines.ïE Trigger alerts when metrics in the baseline are exceeded.ïE Store application and database metrics in a central locatio
- B. What should you include in the recommendation?
- C. Azure Application Insights
- D. Azure SQL Database Intelligent Insights
- E. Azure Event Hubs
- F. Azure Log Analytics

Answer: D

Explanation:

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/collectazurepass-posh>

NEW QUESTION 27

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains 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 have an approval process that contains a condition. The condition requires that releases be approved by a team leader before they are deployed.

You have a policy stating that approvals must occur within eight hours.

You discover that deployment fail if the approvals take longer than two hours. You need to ensure that the deployments only fail if the approvals take longer than eight hours.

Solution: From Pre-deployment conditions, you modify the Time between reevaluation of gates option.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Gates allow automatic collection of health signals from external services, and then promote the release when all the signals are successful at the same time or stop the deployment on timeout. Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.

References: <https://docs.microsoft.com/enus/azure/devops/pipelines/release/approvals/gates>

Approvals and gates give you additional control over the start and completion of the deployment pipeline. Each stage in a release pipeline can be configured with predeployment and post-deployment conditions that can include waiting for users to manually approve or reject deployments, and checking with other automated systems until specific conditions are verified.

NEW QUESTION 28

Your company hosts a web application in Azure. The company uses Azure Pipelines for the build and release management of the application.

Stakeholders report that the past few releases have negatively affected system performance.

You configure alerts in Azure Monitor.

You need to ensure that new releases are only deployed to production if the releases meet defined performance baseline criteria in the staging environment first

What should you use to prevent the deployment of releases that fail to meet the performance baseline?

- A. a trigger
- B. an Azure function
- C. a gate
- D. an Azure Scheduler job

Answer: C

NEW QUESTION 29

Your 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. PDM
- B. OWASPZAP
- C. WhiteSource
- D. Jenkins

Answer: C

NEW QUESTION 33

To resolve the current technical issue, what should you do to the Register- AzureRmAutomationDscNode command?

- A. Change the value of the ConfigurationMode parameter.

- B. Replace the Register-AzureRmAutomationDscNode cmdlet with Register-AzureRmAutomationScheduledRunbook
- C. Add the AllowModuleOverwrite parameter.
- D. Add the DefaultProfile parameter.

Answer: A

Explanation:

Change the ConfigurationMode parameter from ApplyOnly to ApplyAndAutocorrect. The Register-AzureRmAutomationDscNode cmdlet registers an Azure virtual machine as an APS Desired State Configuration (DSC) node in an Azure Automation account.

Scenario: Current Technical Issue

The test servers are configured correctly when first deployed, but they experience configuration drift over time. Azure Automation State Configuration fails to correct the configurations.

Azure Automation State Configuration nodes are registered by using the following command.

```
Register-AzureRmAutomationDscNode
-ResourceGroupName 'TestResourceGroup'
-AutomationAccountName 'LitwareAutomationAccount'
-AzureVMName $vmname
-ConfigurationMode 'ApplyOnly'
```

References: <https://docs.microsoft.com/enus/powershell/module/azurerm.automation/registerazurermautomationdscnode?view=azurerm-6.13.0>

NEW QUESTION 37

HOTSPOT

How should you configure the release retention policy for the investment planning applications suite? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Global release:

Production stage:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Scenario: By default, all releases must remain available for 30 days, except for production releases, which must be kept for 60 days.

Box 1: Set the default retention policy to 30 days

The Global default retention policy sets the default retention values for all the build pipelines. Authors of build pipelines can override these values.

Box 2: Set the stage retention policy to 60 days

You may want to retain more releases that have been deployed to specific stages. References: <https://docs.microsoft.com/enus/azure/devops/pipelines/policies/retention>

NEW QUESTION 42

DRAG DROP

You need to configure Azure Automation for the computers in Pool7.

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.

Actions

Run the New-AzureRmResourceGroupDeployment Azure PowerShell cmdlet.

Create an Azure Resource Manager template file that has an extension of .json.

Run the Import-AzureRmAutomationDscConfiguration Azure PowerShell cmdlet.

Run the start-AzureRmAutomationDscCompilationJob Azure PowerShell cmdlet.

Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.

Answer Area

1

2

3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Run the New-AzureRmResourceGroupDeployment Azure PowerShell cmdlet.

Create an Azure Resource Manager template file that has an extension of .json.

Answer Area

1

2

3

Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.

Run the Import-AzureRmAutomationDscConfiguration Azure PowerShell cmdlet.

Run the start-AzureRmAutomationDscCompilationJob Azure PowerShell cmdlet.

NEW QUESTION 45

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AZ-400 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AZ-400 Product From:

<https://www.2passeasy.com/dumps/AZ-400/>

Money Back Guarantee

AZ-400 Practice Exam Features:

- * AZ-400 Questions and Answers Updated Frequently
- * AZ-400 Practice Questions Verified by Expert Senior Certified Staff
- * AZ-400 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * AZ-400 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year