

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 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 integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment. You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.

Solution: You create a service hook subscription that uses the code pushed event. Does this meet the goal?

- A. Yes
- B. NO

Answer: A

Explanation:

You can create a service hook for Azure DevOps Services and TFS with Jenkins. References:

<https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins>

NEW QUESTION 2

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.

Your company has a pipeline in Azure DevOps for a new web application. You need to ensure that when code is checked in, a build runs automatically.

Solution: From the Triggers tab of the build pipeline, you selected Batch changes while a build is in progress.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 3

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

• Minimizes image sizes.

• Minimizes the security surface area of the final image. What should you include in 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 4

HOTSPOT

You have a project in Azure DevOps.

You plan to create a build pipeline that will deploy resources by using Azure Resource Manager templates. The templates will reference secrets stored in Azure Key Vault.

You need to ensure that you can dynamically generate the resource ID of the key vault during template deployment.

What should you include in the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```

"resources": [
  {
    "apiversion": "2018-05-01",
    "name" : "secrets",
    "type": 
    "properties": {
      "mode" : "Incremental",
       : {
        "deployment"
        "template"
        "templateLink"
      }
    }
  },
  {
    "contentVersion" : "1.0.0.0",
    "uri" : "[uri(parameters('_artifactsLocation'),
concat('./nested/sqlserver.json',
parameters('_artifactsLocationSasToken')))]"
  }
],
"parameters": {
  "secret": {
    "reference": {
      "keyVault": {
        "id": "[resourceId(parameters('vaultSubscription'),
parameters('vaultResourceGroupName'),
'Microsoft.KeyVault/vaults',
parameters('vaultName'))]"
      },
      "secretName": "[parameters('secretName')]"
    }
  }
}
}
]

```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

"resources": [
  {
    "apiversion": "2018-05-01",
    "name" : "secrets",
    "type": 
    "properties": {
      "mode" : "Incremental",
       : {
        "deployment"
        "template"
        "templateLink"
      }
    }
  },
  {
    "contentVersion" : "1.0.0.0",
    "uri" : "[uri(parameters('_artifactsLocation'),
concat('./nested/sqlserver.json',
parameters('_artifactsLocationSasToken')))]"
  }
],
"parameters": {
  "secret": {
    "reference": {
      "keyVault": {
        "id": "[resourceId(parameters('vaultSubscription'),
parameters('vaultResourceGroupName'),
'Microsoft.KeyVault/vaults',
parameters('vaultName'))]"
      },
      "secretName": "[parameters('secretName')]"
    }
  }
}
}
]

```

```

},
"parameters":{
  "secret":{
    "reference":{
      "keyVault":{
        "id": "[resourceId(parameters('vaultSubscription'),
          parameters('vaultResourceGroupName'),
          'Microsoft.KeyVault/vaults',
          parameters('vaultName'))]"
      },
      "secretName": "[parameters('secretName')]"
    }
  }
}
],

```

NEW QUESTION 5

DRAG DROP

Your company has a project in Azure DevOps.

You plan to create a release pipeline that will deploy resources by using Azure Resource Manager templates. The templates will reference secrets stored in Azure Key Vault.

You need to recommend a solution for accessing the secrets stored in the key vault during deployments. The solution must use the principle of least privilege.

What should you include in the recommendation? To answer, drag the appropriate configurations to the correct targets. Each configuration 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.

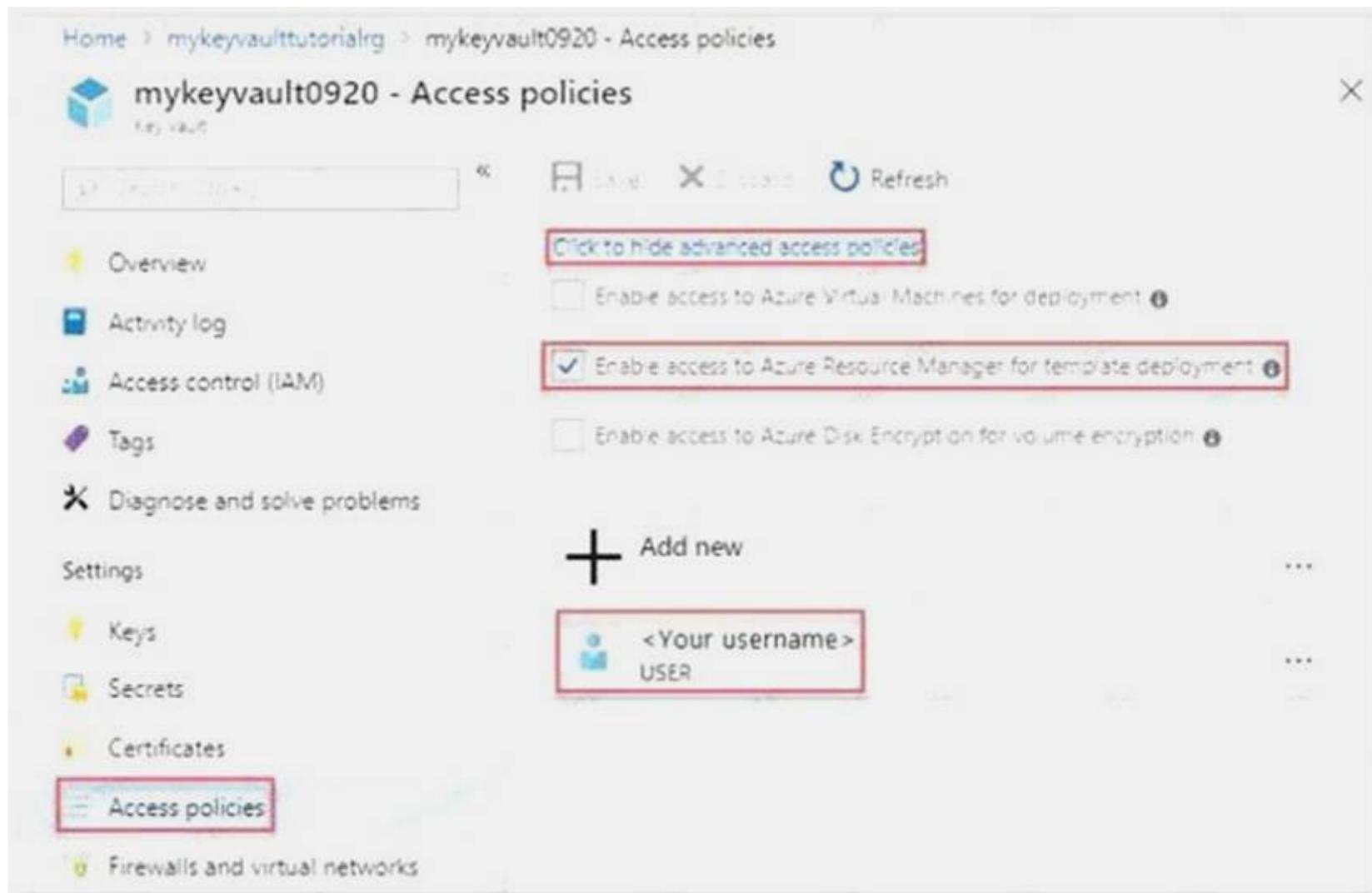
Configurations	Answer Area
A Key Vault access policy	Enable key vaults for template deployment by using: <input type="text"/>
A Key Vault advanced access policy	Restrict access to the secrets in Key Vault by using: <input type="text"/>
RBAC	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: A key Vault advanced access policy



Box 2: RBAC

Management plane access control uses RBAC.

The management plane consists of operations that affect the key vault itself, such as:

- „hCreating or deleting a key vault.
- „hGetting a list of vaults in a subscription.
- „hRetrieving Key Vault properties (such as SKU and tags).
- „hSetting Key Vault access policies that control user and application access to keys and secrets.

References: <https://docs.microsoft.com/en-us/azure/azure-resourcemanager/resource-manager-tutorial-use-key-vault>

NEW QUESTION 6

DRAG DROP

You need to recommend a solution for deploying charts by using Helm and Tiller to Azure Kubemets Service (AKS) in an RBAC-enabled cluster.

Which three commands should you recommend be run in sequence? To answer, move the appropriate commands from the list of commands to the answer area and arrange them in the correct order.

Commands	Answer Area
helm install	
kubectl create	
helm completion	⤴
helm init	⤵
helm serve	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Kubectl create

You can add a service account to Tiller using the --service-account <NAME> flag while you're configuring Helm (step 2 below). As a prerequisite, you'll have to create a role binding which specifies a role and a service account name that have been set up in advance.

Example: Service account with cluster-admin role

```
$ kubectl create -f rbac-config.yaml serviceaccount "tiller" created clusterrolebinding "tiller" created
```

```
$ helm init --service-account tiller
```

Step 2: helm init

To deploy a basic Tiller into an AKS cluster, use the helm init command. Step 3: helm install
 To install charts with Helm, use the helm install command and specify the name of the chart to install.
 References:
<https://docs.microsoft.com/en-us/azure/aks/kubernetes-helm> https://docs.helm.sh/using_helm/#tiller-namespaces-and-rbac

NEW QUESTION 7

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 8

You are developing a multi-tier application. The application will use Azure App Service web apps as the front end and an Azure SQL database as the back end. The application will use Azure functions to write some data to Azure Storage. You need to send the Azure DevOps team an email message when the front end fails to return a status code of 200. Which feature should you use?

- A. Service Map in Azure Log Analytics
- B. Profiler in Azure Application Insights
- C. availability tests in Azure Application Insights
- D. Application Map in Azure Application Insights

Answer: D

Explanation:

Application Map helps you spot performance bottlenecks or failure hotspots across all components of your distributed application. Each node on the map represents an application component or its dependencies; and has health KPI and alerts status. References: <https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-map>

NEW QUESTION 9

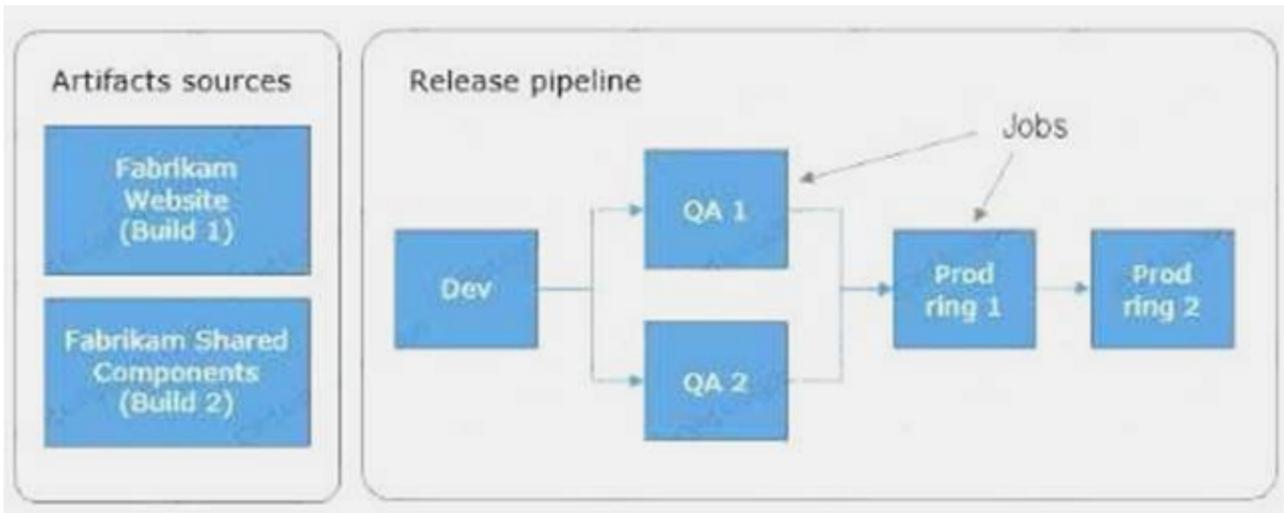
Your company has a project in Azure DevOps for a new web application. The company uses Service Now for change management. You need to ensure that a change request is processed before any components can be deployed to the production environment. What are two ways to integrate into the Azure DevOps release pipeline? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Define a deployment control that invokes the Service Now SOAP API.
- B. Define a post deployment gate after the deployment to the QA stage.
- C. Define a deployment control that invokes the ServiceNow REST API.
- D. Define a pre deployment gate before the deployment to the Prod stag

Answer: BD

Explanation:

An example of a release pipeline that can be modeled through a release pipeline in shown below:



In this example, a release of a website is created by collecting specific versions of two builds (artifacts), each from a different build pipeline. The release is first deployed to a Dev stage and then forked to two QA stages in parallel. If the deployment succeeds in both the QA stages, the release is deployed to Prod ring 1 and then to Prod ring 2. Each production ring represents multiple instances of the same website deployed at various locations around the globe.
 References: <https://docs.microsoft.com/en-us/azure/devops/pipelines/release>

NEW QUESTION 10

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 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>

NEW QUESTION 12

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/>

NEW QUESTION 14

You 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 package
- B. 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: A

Explanation:

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/feedpermissions?view=vsts&tabs=new-nav>

NEW QUESTION 18

You 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/pgSQL
- B. Transact-SQL
- C. Azure Log Analytics
- D. PL/SQL

Answer: C

Explanation:

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>

NEW QUESTION 23

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 plan to create a release pipeline that will deploy Azure resources by using Azure Resource Manager templates. The release pipeline will create the following resources:

- „hTwo resource groups
- „hFour Azure virtual machines in one resource group
- „hTwo Azure SQL databases in other resource group

You need to recommend a solution to deploy the resources.

Solution: Create a main template that will deploy the resources in one resource group and a nested template that will deploy the resources in the other resource

group.
 Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Use two linked templates, instead of the nested template.
 References: <https://docs.microsoft.com/en-us/azure/azure-resourcemanager/resource-group-linked-templates>

NEW QUESTION 26

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. Microsoft Visual SourceSafe
- B. PDM
- C. WhiteSource
- D. OWASP ZAP

Answer: C

Explanation:

WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories. Azure DevOps integration with WhiteSource Bolt will enable you to:

- „hDetect and remedy vulnerable open source components.
- „hGenerate comprehensive open source inventory reports per project or build.
- „hEnforce open source license compliance, including dependencies; licenses.
- „hIdentify outdated open source libraries with recommendations to update. References: <https://www.azuredevopslabs.com/labs/vstsextend/WhiteSource/>

NEW QUESTION 27

Your company develops an app for OS. All users of the app have devices that are members of a private distribution group in Microsoft Visual Studio App Center. You plan to distribute a new release of the app. You need to identify which certificate file you require to distribute the new release from App Center. Which file type should you upload to App Center?

- A. .cer
- B. .pvk
- C. .pfx
- D. .p12

Answer: D

NEW QUESTION 28

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:

- Set the default retention policy to 30 days.
- Set the maximum retention policy to 30 days.
- Set the stage retention policy to 30 days.
- Set the stage retention policy to 60 days.

Production stage:

- Set the default retention policy to 30 days.
- Set the maximum retention policy to 60 days.
- Set the stage retention policy to 30 days.
- Set the stage retention policy to 60 days.

- 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 32

You add the virtual machines as managed nodes in Azure Automation State Configuration. You need to configure the computer in Group7. What should you do?

- A. Run the Register-AzureRmAutomationDscNode Azure Powershell cmdlet.
- B. Modify the ConfigurationMode property of the Local Configuration Manager (LCM).
- C. Install PowerShell Core.
- D. Modify the RefreshMode property of the Local Configuration Manager (LCM).

Answer: A

Explanation:

The Register-AzureRmAutomationDscNode cmdlet registers an Azure virtual machine as an APS Desired State Configuration (DSC) node in an Azure Automation account.

Scenario: The Azure DevOps organization includes: The Docker extension

A deployment pool named Pool7 that contains 10 Azure virtual machines that run Windows Server 2016

Project 7 will contain a target deployment group named Group7 that maps to Pool7. Project7 will use Azure Automation State Configuration to maintain the desired state of the computers in Group7.

References: <https://docs.microsoft.com/enus/powershell/module/azurermsautomation/register-azurermsautomationdscnode>

NEW QUESTION 34

DRAG DROP

You need to implement the code flow strategy for Project2 in Azure DevOps. 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 in the correct order.

Actions	Answer Area
Create a fork	
Create a branch	
Add a build validation policy	⬅
Add a build policy	➡
Create a repository	⬆
Add an application access policy	⬇

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Create a repository

A Git repository, or repo, is a folder that you've told Git to help you track file changes in. You can have any number of repos on your computer, each stored in their own folder.

Step 2: Create a branch

Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards. Step

3: Add a build validation policy

When a build validation policy is enabled, a new build is queued when a new pull request is created or when changes are pushed to an existing pull request targeting this branch. The build policy then evaluates the results of the build to determine whether the pull request can be completed.

Scenario:

Implement a code flow strategy for Project2 that will: Enable Team2 to submit pull requests for Project2.

Enable Team2 to work independently on changes to a copy of Project2.

Ensure that any intermediary changes performed by Team2 on a copy of Project2

will be subject to the same restrictions as the ones defined in the build policy of Project2.

Project2 will use an automatic build policy. A small team of developers named Team2 will work independently on changes to the project. The Team2 members will not have permissions to Project2.

References: <https://docs.microsoft.com/en-us/azure/devops/repos/git/manage-yourbranches>

NEW QUESTION 37

DRAG DROP

You need to implement Project6.

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

- Open the release pipeline editor.
- Open the **Triggers** tab.
- Disable the continuous integration trigger.
- Enable Gates.
- Add a manual intervention task.
- Add Query Work Items.

Answer Area

-
-
-

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- Open the release pipeline editor.
- Open the **Triggers** tab.
- Disable the continuous integration trigger.

Answer Area

- Add a manual intervention task.
- Add Query Work Items.
- Enable Gates.

NEW QUESTION 40

.....

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